GENERAL GOVERNMENT AND HEALTH AND HUMAN SERVICES COMMITTEE AGENDA

January 5, 2021
5:30 PM
Virtual Meeting Held in Accordance with Public Act 254 of 2020
Zoom Virtual Meeting
Meeting ID: 399-700-0062 / Password: LCBOC
https://zoom.us/j/3997000062?pwd=SUdLYVFFcmozWnFxbm0vcHRjWkVIZz09

Pages

1. **CALL TO ORDER**

2. **ROLL CALL**

3. **APPROVAL OF MINUTES** 3

   Minutes of Meeting Dated: December 7, 2020

4. **APPROVAL OF AGENDA**

5. **REPORTS**

6. **CALL TO THE PUBLIC**

7. **RESOLUTIONS FOR CONSIDERATION**

   7.1. **Emergency Medical Services** 10

   Resolution Authorizing the Approval of an EMS Collections Charge

   7.2. **Emergency Medical Services** 12

   Resolution Authorizing a Clinical Training Affiliation Agreement with Pittsfield Twp Fire Department to Provide Clinical Internship Services

   7.3. **Information Technology** 17

   Resolution Authorizing the Purchase of a Five-Year CISCO Flex Subscription for the County's Phone System from Logicalis Inc.

7.4. Information Technology

24

Resolution Authorizing the Purchase of Cyber Security Enhancements and Replacements from Palo Alto Networks

8. CALL TO THE PUBLIC

9. ADJOURNMENT

GENERAL GOVERNMENT & HEALTH AND HUMAN SERVICES COMMITTEE

MEETING MINUTES

December 7, 2020, 4:30 p.m.
Virtual Meeting Held in Accordance with Public Act 228 of 2020
Zoom Virtual Meeting
Meeting ID: 399-700-0062 / Password: LCBOC
https://zoom.us/j/3997000062?pwd=SUdLYVFFcmozWnFxbm0vcHRjWkVIZz09

Members Present: Wes Nakagiri, William Green, Kate Lawrence, and Jay Gross

1. CALL TO ORDER

The meeting was called to order by Commissioner Nakagiri at 4:30 p.m. and thanked all members of the US Armed Forces on its 79th anniversary.

2. ROLL CALL

Indicated the presence of a quorum.

The following Board Members attended remotely from:
Wes Nakagiri, Hartland Township, Michigan
William Green, Deerfield Township, Michigan
Kate Lawrence, City of Brighton, Michigan
Jay Gross, Green Oak Township, Michigan

3. APPROVAL OF MINUTES

Minutes of Meeting Dated: November 2, 2020

Motion to approve the minutes as presented.

Moved by: J. Gross
Seconded by: K. Lawrence

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

4. APPROVAL OF AGENDA

Motion to approve the Agenda as presented.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

5. REPORTS

Commissioner Gross reported the Hamburg Township Board rejected the County's Agreement for a Designated Assessor. Commissioner Gross discussed this with Sue Bostwick, Equalization Director, and anticipates other townships will accept.

6. CALL TO THE PUBLIC

None.

7. RESOLUTIONS FOR CONSIDERATION

7.1 Car Pool

Resolution Authorizing an Increase in Total Authorized Vehicles in the Facilities Services Fleet

Greg Kellogg, Car Pool Director, presented the resolution and answered questions from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: J. Gross

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.2 Equalization Department

Resolution Authorizing the Reorganization of the Equalization Department

Sue Bostwick, Equalization Department Director, presented the resolution and answered questions from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: W. Green
Seconded by: K. Lawrence

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.3 Information Technology

Resolution Authorizing 2021 Renewal Software Maintenance and Services

Kris Tobbe, IT Department Director, presented the resolution and answered questions from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: J. Gross
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.4 MSU Extension

Resolution to Approve the 2021 Memorandum of Agreement (MOA) with MSU Extension as Determined by the 2021 MSUE Budget

Matt Shane, MSU-E District 12 Director, presented the resolution and answered question from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.5 Administration

Resolution Authorizing 2021 Non-Profit Contracts

Nathan Burd, County Administrator, presented the resolution and answered questions from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: J. Gross

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.6 Administration

Resolution to Authorize a Contract with Plante Moran to Provide Professional Auditing Services

Nathan Burd, County Administrator, presented the resolution. Cindy Catanach, Financial Officer, and Jennifer Nash, Treasurer, were present to answer questions as well.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.7 Fiscal Services

Resolution to Amend the Livingston County Procurement Card Policy

Cindy Catanach, Financial Officer, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: J. Gross
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.8 Fiscal Services

Resolution to Amend the Livingston County Procurement Policy

Cindy Catanach, Financial Officer, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.9 Health Department

Resolution Accepting 2021 Grant Funding from the Department of Licensing and Regulatory Affairs, Bureau of Medical Marihuana Regulation

Dianne McCormick, Public Health Officer/Health Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: J. Gross

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.10 Health Department

Resolution Authorizing an Agreement with the Michigan Department of Environment, Great Lakes, and Energy to Conduct Environmental Health Services

Matt Boland, Director of Environmental Health, presented the resolution and answered questions from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: W. Green
Seconded by: J. Gross

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.11 Health Department

COVID-19 Related Resolution Approving Temporarily Authorizing a Livingston County Health Department FLSA Exempt Employee to Accrue Temporary Special Flex Time and Additional Compensation for Hours Worked

Dianne McCormick, Public Health Officer/Health Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.12 Health Department

Resolution Extending Authorization of Resolution 2020-03-079

Dianne McCormick, Public Health Officer/Health Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.13 LETS

Resolution Amending Resolution 2019-02-017 Authorizing Third-Party Contracts between Livingston County and Specialized Services Transportation Providers

Recommend Motion to the Finance Committee.

Moved by: J. Gross
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.14 LETS

Resolution Authorizing Sub-recipient Agreement for Transportation Services between Livingston County (LETS) and People's Express of Whitmore Lake for FY 2021 and Amendment to FY 2020 Agreement

Greg Kellogg, LETS Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.15 LETS

Resolution Authorizing the Reorganization of LETS to Fill the Full-Time Mobility Manager Position and Eliminate One Full-Time Driver Position

Greg Kellogg, LETS Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.16 LETS

Resolution Approving the LETS Public Transportation Agency Safety Plan (PTASP)

Greg Kellogg, LETS Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: W. Green
Seconded by: K. Lawrence

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.17 Emergency Medical Services

Resolution Authorizing the Approval of the EMS Charges for 2021

David Feldpausch, EMS Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: W. Green
Seconded by: K. Lawrence

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.18 Emergency Medical Services

Resolution Authorizing the Clinical/Internship contract with Lake Superior State University

7.19 Emergency Medical Service

Resolution Authorizing a Clinical Training Affiliation Agreement with Oakland Community College to Provide Clinical Internship Services

7.20 Emergency Medical Service

Resolution Authorizing a Clinical Training Affiliation Agreement with Dorsey Emergency Medical Academy to Provide Clinical Internship Services

David Feldpausch, EMS Department Director, presented items 7.18, 7.19, and 7.20 as they are all similar items, and answered from Commissioners.

Recommend Motion of Agenda Items 7.18, 7.19, and 7.20 to the Finance Committee.

Moved by: J. Gross
Seconded by: K. Lawrence

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.21 Emergency Medical Services

Resolution Authorizing Holiday Pay for Regular Part-Time Livingston County Medical Examiner Investigators

David Feldpausch, EMS Department Director, presented the resolution. Ed Moore, MEI, was also present to answer from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

7.22 Emergency Medical Services

Resolution Approving the Reorganization of the Emergency Medical Services Department

David Feldpausch, EMS Department Director, presented the resolution and answered from Commissioners.

Recommend Motion to the Finance Committee.

Moved by: K. Lawrence
Seconded by: W. Green

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

8. CALL TO THE PUBLIC

None.

9. ADJOURNMENT

Motion to adjourn the meeting at 6:37 p.m.

Moved by: K. Lawrence
Seconded by: J. Gross

Yes (4): W. Nakagiri, W. Green , K. Lawrence , and J. Gross

Motion Carried (4 to 0)

Natalie Hunt

Natalie Hunt, Recording Secretary

RESOLUTION **NO:** [Title]

LIVINGSTON COUNTY **DATE:** Click or tap to enter a date.

Resolution Authorizing the Approval of an EMS collections charge.

WHEREAS, Livingston County EMS has a need for collections services provided under a previously approved contract; and

WHEREAS, Livingston County EMS has historically absorbed the fees associated with collection activity; and

WHEREAS, Livingston County EMS would like to add an additional charge to all accounts sent to collections to help reduce the losses associated with collections activity: and

WHEREAS, The contracted collection agency has assisted in the process ensuring that proper notice is provided to all clients allowing for the adition of collection charges.

THEREFORE BE IT RESOLVED that the Livingston County Board of Commissioners hereby authorize Livingston County EMS to add a collection fee of 25% to all account prior to sending them to collection.

# \# \#

MOVED:
SECONDED:
CARRIED:

David Feldpausch
Director

Amy Chapman
Deputy Director

1911 Tooley Rd * Howell, MI 48855
Business (517) 546-6220 * Fax (517) 546-6788 * Emergency 911
www.livgov.com

Memorandum

To: Livingston County Board of Commissioners
Fr: David Feldpausch, EMS Director
Date: 12/22/2020
Re: Resolution authorizing an additional charge on collection accounts

---

We are very excited to begin working without newly approved collection agency (Merchants & Medical) that you approved last month. In conversation during our kick off process they had mentioned that we can legally add an additional charge to all accounts that get sent to them for collections. It does come with some requirements on our end to ensure that all of our clients are aware of the additional charge.

Merchants & Medical provided us with the draft language and we have applied it to our patient signature section, all of our billing letters & statements, and will get it added to our website very soon. With all of these notices in place we can begin to add an additional charge to accounts when they are sent to collections which will reduce our cost for the collection services when a recovery is made.

Our current agreement has the collection agency fee set a 25% and that is the amount that I would like to apply to accounts before sending them to collections. This fee will not make us whole as the collection agency fee will be applied to the entire balance that we send including the additional 25% so we will still lose a small amount on each recovery and if an account proceeds to legal our fee increases to 50% and we are not allowed to increase our fee after it has been sent to collections.

Approving this additional charge will go a long way in reducing our costs in the collection process and passes those fees along to the patient who did not respond to our invoicing process prior to being sent to collections.

If you have any questions or concerns, please do not hesitate to reach out to me any time. 517/294-1853 or dfeldpausch@livgov.com.

RESOLUTION **NO:** [Title]

LIVINGSTON COUNTY **DATE:** Click or tap to enter a date.

Resolution Authorizing a Clinical Training Affiliation Agreement with Pittsfield Twp Fire Department to Provide Clinical Internship Services - Emergency Medical Service

WHEREAS, Pittsfield Twp Fire Department has approached Livingston County EMS wishing to enter into an agreement to allow EMS students to complete their clinical rotations and field internships with LCEMS: and

WHEREAS, the clinical rotations and field internships allow EMS students an opportunity to complete their education requirements while developing the skills necessary to become outstanding practitioners in the field of emergency medical services; and

WHEREAS, the EMS students will ride along with the ALS crews for their clinical rotation and field Internship experience; and

WHEREAS, allows Livingston County EMS to evaluate and recruit future employees from the best students from each class, and

WHEREAS, there is no cost for this program.

THEREFORE BE IT RESOLVED that the Livingston County Board of Commissioners hereby authorize Livingston County EMS entering into a Training Affiliation Agreement with Pittsfield Twp Fire Department after review by leagal counsle.

BE IT FURTHER RESOLVED that the County Administrator is authorized to sign all forms, assurances, contracts/agreements, renewals and future amendments for monetary and contract language adjustments related to the above upon review and/or preparation of Civil Counsel.

# # #

MOVED:
SECONDED:
CARRIED:

Pittsfield Township Fire Department
Emergency Medical Technician Basic
Clinical Contract

Agreement between Pittsfield Township Fire Department and Livingston County EMS.
This Agreement is entered into between Pittsfield Township Fire Department, henceforth known as the *Pittsfield Township Fire Department,* and Livingston County EMS henceforth known as the*, Livingston County EMS* on date, known as the effective date.
The purpose of this Agreement is to set forth the terms and conditions under which the *Pittsfield Township Fire Department* and the *Livingston County EMS* (collectively, the "Parties") will engage in a program for the clinical education of *Pittsfield Township Fire Department* EMS students enrolled in the *Pittsfield Township Fire Department* EMS education programs.
Responsibilities/Rights of the *Livingston County EMS:*
1. To provide clinical experiences for the students of the *Pittsfield Township Fire Department* in specific areas identified at the time of student placement. For the purpose of this Agreement, the placement is defined as *Livingston County EMS.*
2. To provide the clinical experience and assume the following responsibilities:
a. To assist the *Pittsfield Township Fire Department* in supervising the students while on site at the *Livingston County EMS*
(NOTE: Ultimate supervision of the students is the responsibility of the *Pittsfield Township Fire Department).*
b. To cooperate with *the Pittsfield Township Fire Department* in the planning of the student's education experience so that the experience may be appropriate in light of *the Pittsfield Township Fire Department's* education plan.
c. To make available information for educational purposes, such as policies, procedures and clinical reference material available at the *Livingston County EMS.*
d. Be aware that each student is responsible for the costs of any medical care for any illness or injury that might be sustained while the student is participating in this experience at the *clinical facility.*
3. To terminate a student from continuing his/her clinical experience at the *Livingston County EMS* at their discretion at any time.
Responsibilities/Rights of *the Pittsfield Township Fire Department:*
1. To advise students and instructors, and enforce compliance with, all existing policies, rules and regulations the *Livingston County EMS* including, but not limited to the confidentiality of patient and *clinical facility* records and information.
2. To assign students with preparation in the foundation of the Emergency Medical Services Program and to provide evidence of competency in the skills of this program.
3. Appoint a representative for clinical coordination ("Clinical Coordinator") who shall coordinate all aspects of the Agreement with the designated *Livingston County EMS* representative.
4. To provide evidence of an annual chest x-ray or negative tuberculosis skin test, and rubella vaccination or evidence of rubella titer 1:8 or above, from each student and instructor.
5. To provide the *Livingston County EMS* documentation that each student and instructor has been offered, and have either received or declined, hepatitis B vaccine before participating in this Program.
6. To provide pre-clinical instruction to each student in accordance with standards mutually agreeable to both parties, including all MIOSHA required training, which includes but is not limited to blood borne pathogens, prior to the educational experience and to present for clinical experience at the *clinical facility* only those students who have satisfactorily completed the pre-clinical instructional program.

7. To have full responsibility for the conduct of any student, instructor disciplinary proceedings and conduct the same in accordance with all applicable statutes, rules, regulations and case law.
8. To maintain general public liability and professional liability coverage for its instructors and students with minimum limits of liability of One Million Dollars ($1,000,000) per incident and shall furnish the *Livingston County EMS* appropriate certificates of insurance evidencing such continuous current coverage before the beginning of the clinical experience.
9. To indemnify and hold harmless the *Ypsilanti City Fire Department,* its employees, and agents, from all claims, liability or damages, including reasonable attorney's fees, which the *Livingston County EMS* or its employees or agents may incur as a result of claims or costs of judgments against any of them arising out of acts or omissions of the *Pittsfield Township Fire Department* instructors, staff or students while in the performance of their responsibilities under their Agreement.
10. To indemnify and hold harmless the *Livingston County EMS,* its employees and agents from all claims, liability or damages, including reasonable attorney's fees, which the *Livingston County EMS* or its employees or agents may incur as a result of claims or costs of judgments against any of them regarding injuries to the *Pittsfield Township Fire Department* students arising out of their participation in the classes described under this Agreement.
11. The *Pittsfield Township Fire Department* shall maintain all educational records and reports relating to the educational experience completed by individual students at the *Livingston County EMS,* and the *Livingston County EMS* shall have no responsibility regarding the same. The *Livingston County EMS* shall refer all requests for information of such records to the *Pittsfield Township Fire Department.* The *Pittsfield Township Fire Department* agrees to comply with all applicable statutes and regulatory requirements respecting the maintenance of and release of information from such records.
12. The *Pittsfield Township Fire Department* shall certify that each student has provided it with evidence that the student has passed a physical examination prior to beginning education experience and shall certify that such evidence indicated at the time of the physical examination the student was free from contagious diseases as could be ascertained by such examination.
13. The *Pittsfield Township Fire Department* shall have full responsibility for the conduct of any disciplinary proceedings concerning any student, however, the *Livingston County EMS,* at its sole discretion, may deny the educational experience to any individual.
14. The *Pittsfield Township Fire Department* agrees, and shall obtain from each student and furnish to the *Livingston County EMS* a written agreement of each student acknowledging, as a condition of being able to participate in the educational experience, that the Student:
a. shall comply with all the *Livingston County EMS* rules, regulations, policies and procedures;
b. shall comply with all directives of the *Livingston County EMS* regarding conduct;
c. shall refrain from touching in any way any patient except at the patient's consent and with the *Livingston County EMS* personnel's authorization;
d. shall not be considered an employee of the *Livingston County EMS* for the purpose of this agreement;
e. shall not disclose information without written authorization by the *Livingston County EMS* regarding any patient's care, including the identity of the patient or the services performed for that patient;
and
f. shall upon request leave an area of the *Livingston County EMS.*
Major Responsibilities of the *Pittsfield Township Fire Department* students, under the direction of the *Pittsfield Township Fire Department:*
1. To adhere to existing policies and procedures of the *Livingston County EMS.*
2. To report for clinical experiences as assigned or call to report absences.
3. To respect the patients right to confidentiality.
4. The *Pittsfield Township Fire Department* will notify students of 1-3 above.
21
GENERAL PROVISIONS:
The parties mutually acknowledge and agree as follows:

A. Students of the *Pittsfield Township Fire Department* shall not be deemed to be employees of the *Livingston County EMS* for purposes of compensation, fringe benefits, workers' compensation, unemployment compensation, minimum wage laws, income tax withholding, social security, or any other purpose, because of their participation in the EMS program. Each student shall be placed with the *Livingston County EMS* to receive clinical experience as a part of his/her academic curriculum. The duties performed by a student shall not be performed as an employee, but in fulfillment of the student's academic requirements. At no time shall students replace or substitute for any employee of the *Livingston County EMS*. The provisions of this section shall not be deemed to prohibit the employment of any such student by the *Livingston County EMS* under a separate employment agreement. The *Pittsfield Township Fire Department* shall notify each student of the requirements of this paragraph.

B. In the performance of their respective duties and obligations under this Agreement, each party shall be an independent contractor and neither shall be the employee or servant of the other, and each party shall be responsible for their own conduct.

C. Each party shall be responsible for compliance with all laws, including anti-discrimination laws, which may be applicable to their respective activities under the EMS program.

D. No provision of the Agreement shall prevent any patient from requesting not to be a teaching patient or prevent any member of the *Livingston County EMS* professional staff from designating any patient as a nonteaching patient.

E. Neither this Agreement nor any part of it shall be assigned by either Party without prior written consent of the other Party.

F. This Agreement constitutes the entire agreement between the parties, and all prior discussion, agreements and understandings, whether verbal or in writing, are merged in to this agreement. There may be no amendment of the Agreement, unless the same is in writing and signed to the party to be charged.

G. This Agreement shall be effective as the Effective Date and shall continue thereafter until terminated by either party upon 30 days advance written notice of termination, with or without cause.

H. Students will be placed at the *Livingston County EMS* without cost to the *Livingston County EMS.*

This Agreement shall be in effect for one year as of December 19, 2020, and may be renewed annually.

The Livingston County EMS,

______________________________ Date__________ ___________________________ Date___________
Signature Signature

Pittsfield Township Fire Department

______________________________ Date__________ ___________________________ Date___________
Signature Signature

David Feldpausch
Director

Amy Chapman
Deputy Director

1911 Tooley Rd * Howell, MI 48855
Business (517) 546-6220 * Fax (517) 546-6788 * Emergency 911
www.livgov.com

Memorandum

To: Livingston County Board of Commissioners
Fr: David Feldpausch, EMS Director
Date: 11/27/2020
Re: Resolution Authorizing the contract with Pittsfield Twp Fire Department

---

Pittsfield Twp Fire Department has reached out to Livingston County EMS with a proposed contract to allow their EMS students to complete their clinical rotations and field internships with us. These are required practical components of the educational process to become licensed in the EMS filed in the state of Michigan.

These agreements give students the opportunity to complete this portion of their education while also gaining valuable operational knowledge in the application of their education in real life situations under the guidance of one of our senior paramedics.

It also gives us the opportunity to interact with students first hand and evaluate them as potential future employees. Recruitment and retention are both reaching critical points in the EMS field. It is through great opportunities like this that we hope to gain an advantage over other EMS services wishing to recruit the same students upon the completion of their education.

It also provides us valuable insight as to what kind of future employee students might be prior to them even applying for a position. We get to see firsthand not only the student’s skill and knowledge but their interpersonal communication skills and general work ethic these are things that can be challenging to evaluate in a standard interview process.

There is no direct cost to the department under this contract. They will be placed with our employees who are already scheduled to work and no additional compensation will be paid.

If you have any questions or concerns, please do not hesitate to reach out to me any time. 517/294-1853 or dfeldpausch@livgov.com.

RESOLUTION **NO:** [Title]

LIVINGSTON COUNTY **DATE:** Click or tap to enter a date.

Resolution Authorizing the Purchase of a Five-Year CISCO Flex Subscription for the County's Phone System from Logicalis Inc. - Information Technology

WHEREAS, CISCO's Flex Subscription will replace the previously used CISCO SmartNet licensing for the County's phone system; and

WHEREAS, CISCO's Flex Subscription will allow the County's employees to use soft phones, desk phones, and mobile phones all using County numbers and extensions; and

WHEREAS, this project is a five-year deal with Logicalis for a total cost of $186,030; and

WHEREAS, funding is available through the Information Technology Department 2021 budget and will be projected in to the future 2022, 2023, 2024, and 2025 budgets for approval.

THEREFORE BE IT RESOLVED that the Livingston County Board of Commissioners hereby authorizes the purchase of CISCO Flex Subscription from Logicalis for an updated phone system for an amount not to exceed $186,030 for a five-year period, with $37,206 due annually.

BE IT FURTHER RESOLVED that the Livingston County Board of Commissioners is authorized to sign all forms, assurances, contracts/agreements, renewals and future amendments for monetary and contract language adjustments related to the above upon review and/or preparation of Civil Counsel.

# # #

MOVED:
SECONDED:
CARRIED:

LOGICALIS
Architects of Change

Livingston County - Cisco Flex 3.0 Subscription for Callilng - 5-Year Option, Annual Billing
Quotation # 2020-103777v1

Prepared By Logicalis for:
Livingston County

To the attention of :
Kris Tobbe
Livingston County
304 E Grand River Ave
Howell, MI 48843-2488
Tel: 517-540-8803
Email: ktobbe@livgov.com

December 30, 2020

Livingston County - Cisco Flex 3.0 Subscription for Callilng - 5-Year Option, Annual Billing
Quotation # 2020-103777v1

Customer Name & Address	Logicalis Account Executive
Kris Tobbe Livingston County 304 E Grand River Ave Howell, MI 48843-2488 517-540-8803 ktobbe@livgov.com	Lisa Nowak Logicalis Inc. 120 N Washington Square Suite 600 Lansing, MI 48933 +1 5173361052 lisa.nowak@us.logicalis.com
Bill To Address	**Ship to Address**
Livingston County 304 E Grand River Ave Howell, MI 48843-2488	Livingston County 304 E Grand River Ave Howell, MI 48843-2488 ATTN: Kris Tobbe 517-540-8803 ktobbe@livgov.com

Quotation expiration date: January 30, 2021
This Quotation adheres to the pricing requirements of the NASPO ValuePoint Master Agreement #AR233 (14-19), Cisco Participating Addendum MI #071B4300124 contract.

Item	Qty	Part Number	Description	Term (Months)	Invoicing Frequency	Recurring Charge	Extended Price
Annuity							
1	1	A-FLEX-3	Collaboration Flex Plan 3.0 Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
2	1	SVS-FLEX-SUPT-BAS	Basic Support for Flex Plan Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
3	636	A-FLEX-EAPL	EntW On-Premises Calling Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$37,206.00	$186,030.00
4	764	A-FLEX-SRST-E	SRST Endpoints (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
5	1	A-FLEX-EXP-PAK	Expressway Product Authorization Key (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00

6	764	A-FLEX-C-DEV-ENT	Cloud Device Registration Entitlement Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
7	764	A-FLEX-MSG-ENT	Messaging Entitlement Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
8	15264	A-FLEX-FILESTG-ENT	File Storage Entitlement Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
9	764	A-FLEX-PROPACK-ENT	Pro Pack for Cisco Control Hub Entitlement Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
10	32	A-FLEX-EXP-RMS	Expressway Rich Media Session (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
11	1	A-FLEX-SME-S	Session Manager (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
12	764	A-FLEX-P-EA	On-Premises Smart License - EA (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
13	128	A-FLEX-P-ACC	Access Smart License (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
14	318	A-FLEX-P-CA	Common Area Smart License (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
15	764	A-FLEX-P-UCXN	Unity Connection Smart License (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
16	1908	A-FLEX-P-ER	Emergency Responder Smart License (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00

17	1	A-FLEX-SW-12.5-K9	On-Premises & Partner Hosted Calling SW Bundle v12.5 (1) Est. Start Date: 01-01-2021 Est. End Date: 12-31-2025	60	Annual	$0.00	$0.00
					Annuity Total:	$37,206.00	$186,030.00

Grand Total	
Products Subtotal:	$186,030.00
Grand Total:	**$186,030.00**

Terms and Conditions

Terms Applicable to All Sales

1. In the event Customer chooses to lease the Products and/or Services from a third party leasing company, Customer remains liable for payment to Logicalis for all Products and/or Services purchased until Logicalis receives payment from such leasing company.
2. All items not specifically included in this document are out of scope.
3. Prices are valid for 30 days from date of the document unless otherwise stated.
4. The information in this document is considered proprietary and confidential to Logicalis. By acceptance of this Quotation, Customer agrees to maintain this confidentiality and use such information for internal purposes only.

Terms Applicable for Product Sales

1. To the extent applicable, the terms of the NASPO ValuePoint Master Agreement #AR233 (14-19), Cisco Participating Addendum MI #071B4300124 are incorporated herein by reference. For all other terms not addressed in the previously stated contract, Logicalis Terms of Sale, found on our website at www.us.logicalis.com/tcsales apply and are incorporated herein by reference.
2. Any variation in quantity or requested delivery may result in price changes.
3. Prices are subject to change without notice in the event the Product's manufacturer/distributor changes the price to Logicalis.
4. Shipping and taxes are added at time of invoice. Shipping charges are subject to handling fees for specifying carriers and same day shipments.
5. Logicalis collaborates with the OEM/distributor to schedule delivery to Customer’s loading dock; inside delivery is available upon request and may increase the cost of delivery.
6. To the extent this Quotation includes Cisco Cloud Services, the following link shall apply: www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html. “Cisco Cloud Services” shall mean any of the offerings described on the aforementioned link. If Customer does not issue a purchase order to Logicalis or otherwise accept a Logicalis quotation to renew such Cisco Cloud Services, or does not otherwise provide written notice of non-renewal, at least forty-five (45) days prior to the end of the then-current subscription term thereof, then the Cisco Cloud Services shall automatically renew and Customer agrees to pay Logicalis for such renewed subscription term at the rates charged by Logicalis therefor.

Quotation Acceptance

By signing below, the undersigned accepts this offer and confirms that he/she is authorized to purchase these items on behalf of Customer. This offer may be accepted by purchase order or other acknowledgement of acceptance, including, without limitation, by signing this document. Any reference to a Customer's Purchase Order or P.O. number does not indicate Logicalis' acceptance of terms and conditions referenced on/attached to any such P.O.

Accepted By: Livingston County	Accepted By: Logicalis, Inc.
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date

RESOLUTION		**NO:**	[Title]
LIVINGSTON COUNTY		**DATE:**	Click or tap to enter a date.

Resolution Authorizing the Purchase of Cyber Security Enhancements and Replacements from Palo Alto Networks - Information Technology

WHEREAS, cyber security is ground zero for the defense and protection of today's modern corporate network. Cyber security is always on the mind of the County's Information Technology professionals. Ensuring the County's cyber defense and protections are updated with the latest technologies and methodologies is mission critical to make sure organizational data and operations can continue to move forward; and

WHEREAS, the County's current cyber defenses are aged, undersized, disjointed, and do not protect all computers with a single solution. Our current firewall was undersized for our needs at the time of purchase, and is no longer supported by the manufacturer; and

WHEREAS, there is a strong need to enhance and secure the County's computers and unify our systems on a single platform that dovetails and integrates with our firewall systems. The County currently has two separate computer systems in place, and the contract for the current systems ends in 2020; and

WHEREAS, with this purchase, the County will be unifying and strengthening our cyber firewall and endpoint operations under Palo Alto Networks, a world class leader in cyber security technologies, all while taking advantage of specialized pricing that maximizes savings to our taxpayers; and

WHEREAS, this project will deploy a high availability pair of firewalls, 1,000 licenses of Palo Alto Networks' Cortex XDR endpoint protection that will cover all of the County's desktop computers, laptops, and servers, as well as the highly effective Palo Alto Networks' Data Lake defense aggregation platform; and

WHEREAS, with the issuance of a Participating Addendum, the County is able to use the NASPO ValuePoint Cooperative Purchasing Program which provides Amerinet the ability to provide enhanced cyber security platforms at a significant cost savings of 47% or $400,000 in up-front savings; and

WHEREAS, this project is a three (3) year deal with Palo Alto and offers 0% financing; and

WHEREAS, funding is available from the 2021, 2022 projected, and 2023 projected fiscal years Capital Improvement Plan funding.

THEREFORE BE IT RESOLVED that the Livingston County Board of Commissioners hereby authorizes the purchase of Plato Alto Networks enhanced Cyber Security Platform through Amerinet in an amount not to exceed $442,800 split into three payments over the years 2021, 2022, 2023 at $147,600.00 per year.

BE IT FURTHER RESOLVED that the Livingston County Board of Commissioners hereby authorizes the Treasurer to transfer funds from Capital Replacement F403 to IT Fund 636 in an amount not to exceed $147,600 each year over the years 2021, 2022, and 2023 until the completion of the project.

BE IT FURTHER RESOLVED that the Livingston County Board of Commissioners is authorized to sign all forms, assurances, contracts/agreements, renewals and future amendments for monetary and contract language adjustments related to the above upon review and/or preparation of Civil Counsel.

# # #

MOVED:
SECONDED:
CARRIED:

Livingston County
Information Technology
Department

Report

To: Livingston County Board of Commissioners, Livingston County Administrator - Nathan Burd, Livingston County Chief Financial Officer - Cindy Catanach

From: Kristoffer Tobbe Livingston County Chief Information Officer

Date: December 30, 2020

Re: Livingston County Information Technology Department: Cyber Security Enhancements and Replacement

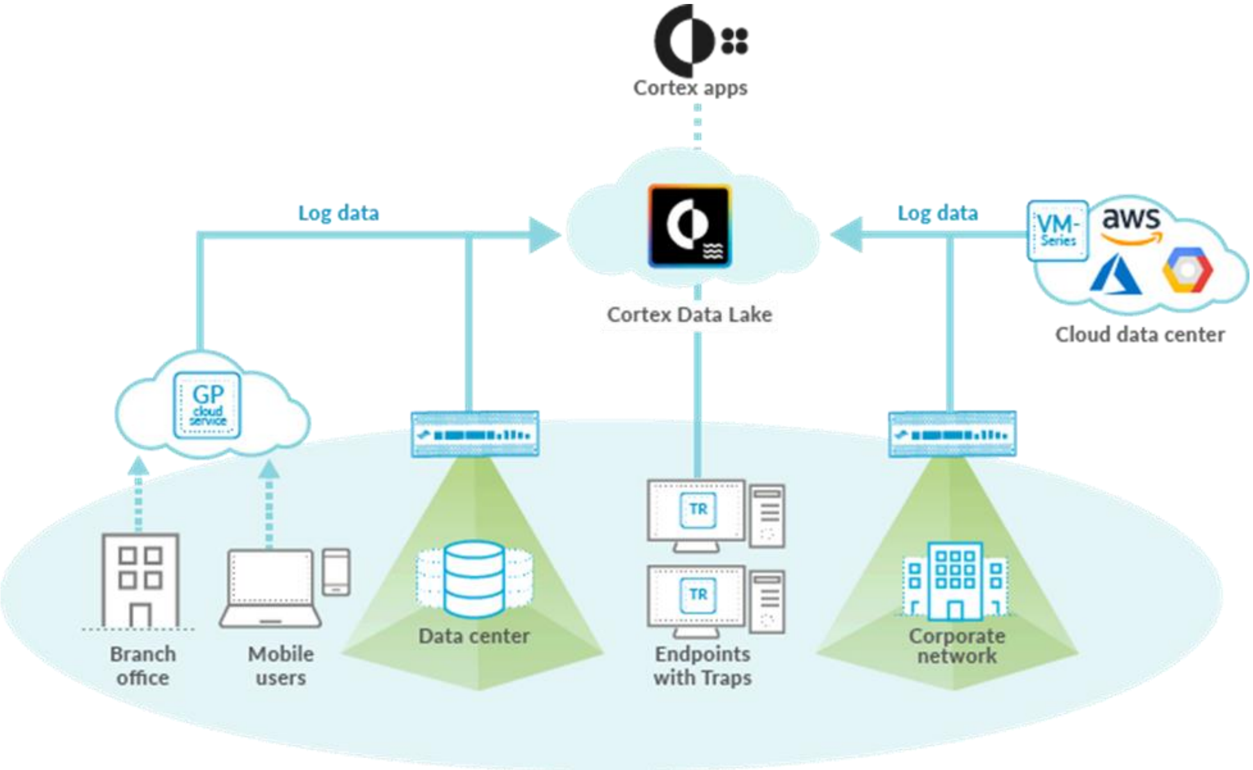
---

Request for Approval

Cyber security is ground zero for the defense and protection of today's modern corporate network. Ensuring cyber defense and protections are updated with the latest technologies and methodologies is mission critical to make sure organization data and operations can continue to move forward.

The projects before you were not hastily put together based on the headlines over the past month. Cyber security is always on the mind of the Information Technology professionals employed by Livingston County. These cyber security projects have been priorities for the Livingston County Information Technology Department for the past four Capital Improvement Plans, CIP 2018, 2019, 2020, & CIP 2021. We have chosen to submit these projects for Board approval because we believe that now is the time to not only significantly enhance our cyber operations, but to also take advantage of specialized pricing that maximizes savings to tax payers.

With this proposal, we will also be unifying and strengthening our cyber defense operations significantly with Palo Alto Networks, a world class leader in cyber security technologies. This project will deploy a high availability pair of next generation firewalls, 1000 licenses of Palo Alto Networks' Cortex XDR endpoint protection that will cover all the County's desktop computers, laptops, and servers, as well as the highly effective Palo Alto Networks' Data Lake defense aggregation platform.



These platforms are all supported by Palo Alto Networks' Engineering, Critical Response, Crypsis and Unit 42 cyber defense and threat hunting teams, offering years of experience detecting and preventing attacks. The Unit 42 and Crypsis teams are one of the best threat intelligence teams in the world. These team follow advanced threat intelligence cycles. Then analysts determine what data is necessary to answer specific questions about threats to Palo Alto Networks and its customers. These teams collect that data from internal and external sources and runs it through a detailed threat analysis process that includes not only automated systems to correlate incoming data, but also expert human analysis to interpret the data, identify patterns, formulate hypotheses, and evaluate them against our entire data set. By doing this, the Palo Alto teams can put threats into context and help others determine how to best defend against future attacks and push those highly defined profiles directly to the Palo Alto firewalls and endpoint protection platforms through their Wildfire update technologies helping to protect against zero-day threats.

- What are next generation Firewalls?
    - https://youtu.be/a_6YbFLTt7s
    - https://www.youtube.com/watch?v=W_rOYetDQUQ
- Endpoint protection explained
    - https://youtu.be/51qpRPyvbWM
    - https://youtu.be/D_q-MzhMENw
    - https://enterprise.comodo.com/blog/what-is-endpoint-security/

Livingston County’s current cyber defenses are aged, undersized, disjointed, and do not protect all the endpoints (computers) with a best in class single solution.

- Livingston County’s current firewall was purchased in 2014. At that time, the firewall was undersized for the County’s needs.
- Since original purchase, the County has expanded 6-fold and our current firewalls are vastly undersized.
- The system was end of life in 2019 and is no longer supported by the manufacture.
- Replacing the County’s firewall system is a necessary project as our current system is an outdated and massively undersized platform.

There is a strong need to enhance and secure the County’ endpoints and unify our systems on a single platform that dovetails and integrates with our firewalling systems.

- The County currently has 2 separate endpoint systems in place, but they are not unified and the system is not an integrated security platform.
- The contract for the current endpoint system ends in 2020.
- This project aligns with best practices and is important part of upgrading, protecting, and securing the County’s technology systems and data.
- This project has specific importance due to our end points (user’s computers) being one of the weakest links within our County’s technology environment.
- End point protection will help the Information Technology Department detect, isolate, and secure problem machines regardless of being directly or indirectly (remotely) connected to the County’s system.
- Only 300 of over 1,000 computers are fully protected with advanced endpoint protection.

This project will unify firewall and endpoint protection and enhance Livingston County’ cyber defenses. The comprehensive plan includes:

- 2 High availability pair Palo Alto Next generation firewalls
- 1000 seats of Palo Alto Cortex XDR Endpoint Protection to protect all of the computers in our network, including our mobile in-car terminals used for public safety
- Five Tera Bytes of Cortex Data Lake Data Aggregation storage
- Installation Services for Cortex XDR at no cost
- Quick Start Services for Next Generation Firewalls at no cost
- Palo Alto Firewall Essentials training courses for two Livingston County Information Technology Cyber Professionals at no cost
- 3 years of Support and Maintenance for all products

Useful links

- Why Palo Alto Networks?

  - General Info
    - https://youtu.be/Un6MIBVr-JA
  - Ada County
    - https://www.youtube.com/watch?v=m-n2DZUfLjk
  - Temple University
    - https://www.youtube.com/watch?v=8Hw-nUUtQTk

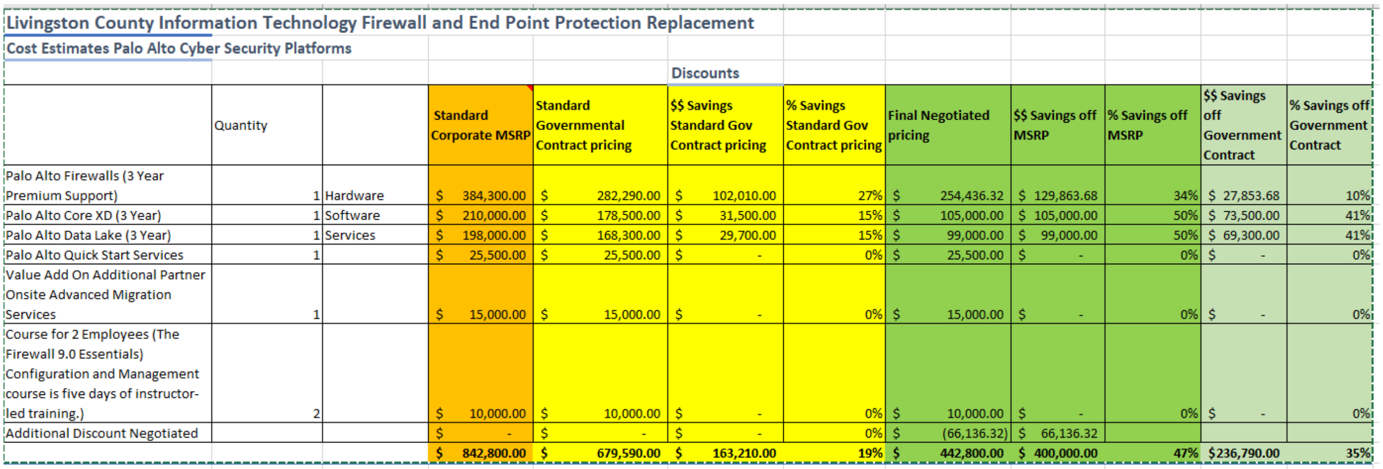
- Cortex platform
  - https://www.youtube.com/watch?v=&feature=emb_logo
  - https://www.youtube.com/watch?v=8zy3NY3S9kA
- Unit 42
  - https://unit42.paloaltonetworks.com/about-unit-42/

Current purchase pricing

The Livingston County Information Technology Department has successfully worked with our technology partners AmeriNet and Palo Alto Networks to put together this comprehensive proposal for the replacement and enhancement cyber security. The proposal utilizes the Livingston County approved NASPO contract to obtain and streamline the procurement process. This standardized governmental contract standardizes negotiated governmental pricing, however we have successfully partnered with Amerinet and Palo Alto to achieve significant discounts for the County tax payers that are much greater than standard pricing, and NASPO government pricing contract pricing (as exhibited in the data table below and attached).

The discount negotiated for Livingston County is 47% off of the standard corporate rate and an 35% off of the governmental contract pricing. These discounts are in the upper echelon of discounts offered by Palo Alto as described by GARTNER.

The final pricing is $442,800. This lowered price will save our Livingston County Tax Payers $400,000 off of the standard pricing, and will achieve $236,790 in savings from the standard government pricing.



Livingston County Information Technology Firewall and End Point Protection Replacement

Cost Estimates Palo Alto Cyber Security Platforms

					Discounts						
	Quantity		Standard Corporate MSRP	Standard Governmental Contract pricing	$$ Savings Standard Gov Contract pricing	% Savings Standard Gov Contract pricing	Final Negotiated pricing	$$ Savings off MSRP	% Savings off MSRP	$$ Savings off Government Contract	% Savings off Government Contract
Palo Alto Firewalls (3 Year Premium Support)	1	Hardware	$ 384,300.00	$ 282,290.00	$ 102,010.00	27%	$ 254,436.32	$ 129,863.68	34%	$ 27,853.68	10%
Palo Alto Core XD (3 Year)	1	Software	$ 210,000.00	$ 178,500.00	$ 31,500.00	15%	$ 105,000.00	$ 105,000.00	50%	$ 73,500.00	41%
Palo Alto Data Lake (3 Year)	1	Services	$ 198,000.00	$ 168,300.00	$ 29,700.00	15%	$ 99,000.00	$ 99,000.00	50%	$ 69,300.00	41%
Palo Alto Quick Start Services	1		$ 25,500.00	$ 25,500.00	$ -	0%	$ 25,500.00	$ -	0%	$ -	0%
Value Add On Additional Partner Onsite Advanced Migration Services	1		$ 15,000.00	$ 15,000.00	$ -	0%	$ 15,000.00	$ -	0%	$ -	0%
Course for 2 Employees (The Firewall 9.0 Essentials) Configuration and Management course is five days of instructor-led training.)	2		$ 10,000.00	$ 10,000.00	$ -	0%	$ 10,000.00	$ -	0%	$ -	0%
Additional Discount Negotiated			$ -	$ -	$ -	0%	$ (66,136.32)	$ 66,136.32			
			$ 842,800.00	**$ 679,590.00**	**$ 163,210.00**	**19%**	**$ 442,800.00**	**$ 400,000.00**	**47%**	**$236,790.00**	**35%**

Recommendation

At this time, we are recommending moving forward to take advantage of the aggressive pricing negotiated by the Livingston County Information Technology team, Amerinet, and Palo Alto Networks and the purchase of the new next generation firewalls and endpoint protection platform that includes the components as well as 3 years of support and maintenance contained in the Amerinet Proposal “QUO-19878-M5R8”” Dated December 29, 2020

Funding recommendation:

We are recommending that:

Capital Improvement funds be utilized to make 3 payment be made over the next three years in the amount of $147,600

CIP Funding available	2021	2022 (Projected)	2023 (Projected)	Total CIP Funding
Network Security Upgrade	$51,000.00	$51,000.00	$51,000.00	$153,000.00
Network Firewall Upgrade	$96,600.00	$96,600.00	$96,600.00	$289,800.00
Total	$147,600.00	$147,600.00	$147,600.00	$442,800.00

Finance options

Though our conversations with Amerinet and Palo Alto Networks we inquired as to finance options, Amerinet has put forth a generous 3-year 0% financing option based on Livingston County’s Aaa bond rating. See below for specifics.

$442,800 / 3 years = $147,600 each year

Year 2021 Payment: $147,600

Year 2022 Payment: $147,600

Year2023 Payment: $147,600

	Purchase options	
1	**0% 3-year option (Palo Alto Finance)**	$ 147,600.00
2	**Purchase outright**	$ 442,800.00

Livingston County Information Technology Firewall and End Point Protection Replacement

Cost Estimates Palo Alto Cyber Security Platforms

					Discounts						
	Quantity		Standard Corporate MSRP	Standard Governmental Contract pricing	$$ Savings Standard Gov Contract pricing	% Savings Standard Gov Contract pricing	Final Negotiated pricing	$$ Savings off MSRP	% Savings off MSRP	$$ Savings off Government Contract	% Savings off Government Contract
Palo Alto Firewalls (3 Year Premium Support)	1	Hardware	$ 384,300.00	$ 282,290.00	$ 102,010.00	27%	$ 254,436.32	$ 129,863.68	34%	$ 27,853.68	10%
Palo Alto Core XD (3 Year)	1	Software	$ 210,000.00	$ 178,500.00	$ 31,500.00	15%	$ 105,000.00	$ 105,000.00	50%	$ 73,500.00	41%
Palo Alto Data Lake (3 Year)	1	Services	$ 198,000.00	$ 168,300.00	$ 29,700.00	15%	$ 99,000.00	$ 99,000.00	50%	$ 69,300.00	41%
Palo Alto Quick Start Services	1		$ 25,500.00	$ 25,500.00	$ -	0%	$ 25,500.00	$ -	0%	$ -	0%
Value Add On Additional Partner Onsite Advanced Migration Services	1		$ 15,000.00	$ 15,000.00	$ -	0%	$ 15,000.00	$ -	0%	$ -	0%
Course for 2 Employees (The Firewall 9.0 Essentials) Configuration and Management course is five days of instructor-led training.)	2		$ 10,000.00	$ 10,000.00	$ -	0%	$ 10,000.00	$ -	0%	$ -	0%
Additional Discount Negotiated			$ -	$ -	$ -	0%	$ (66,136.32)	$ 66,136.32			
			$ 842,800.00	**$ 679,590.00**	**$ 163,210.00**	**19%**	**$ 442,800.00**	**$ 400,000.00**	**47%**	**$ 236,790.00**	**35%**

Livingston County | Palo Alto | PA-5220

To:	From:
Kris Tobbe	Paul Laurio
Livingston County	AmeriNet
304 E. Grand River Ave.	1241 S. Maple Rd.
Howell, MI 48843	Ann Arbor, MI 48103
517.548.3230	Phone: 734-995-1233
ktobbe@livgov.com	plaurio@amerinet.com

Summary

Total Amount:	**$442,800.00**	Quote ID:	QUO-19878-M5R8
Shipping Method:		Date:	12/29/2020
Payment Terms:	Net 30		

Details

Product ID	Product	Quantity	Price	Sub Total
PA-5220	Palo Alto Networks PA-5220 with redundant AC power supplies	2.00	$31,500.00	$63,000.00
GlobalProtect subscription	GlobalProtect subscription 3 year prepaid for device in an HA pair, PA-5220	2.00	$14,800.00	$29,600.00
Threat prevention	Threat prevention subscription 3 year prepaid for device in an HA pair, PA-5220	2.00	$14,800.00	$29,600.00
PANDB URL filtering	PANDB URL filtering subscription 3 year prepaid for device in an HA pair, PA-5220	2.00	$14,800.00	$29,600.00
WildFire subscription	WildFire subscription 3 year prepaid for device in an HA pair, PA-5220	2.00	$14,800.00	$29,600.00
DNS Security subscription	DNS Security subscription 3 year prepaid for device in an HA pair, PA-5220	2.00	$14,800.00	$29,600.00
Premium support	Premium support 3-year prepaid, PA-5220	2.00	$21,660.00	$43,320.00
AmeriNet Professional Services	AmeriNet Professional Services block hours are used to cover any consulting time that has been scheduled with an APS engineer that is M-F 8-5. Hours quoted is an estimate. After hours and weekend work will be charged at the appropriate rates.	75.00	$200.00	$15,000.00
Cortex XDR Pro	Cortex XDR Pro for 1 TB, includes 1TB of Cortex Data Lake	6.00	$16,500.00	$99,000.00
Cortex XDR Pro	Cortex XDR Pro for 1 endpoint, includes 30 days of data retention	1,000.00	$105.00	$105,000.00
QuickStart Service	QuickStart Service for Cortex XDR Pro Per Endpoint or Cortex XDR Prevent - Up to 2,500 XDR agents	1.00	$10,000.00	$10,000.00
QuickStart Service	QuickStart Service for Cortex XDR Pro per TB - Up to 5 Network Firewall Devices	1.00	$15,500.00	$15,500.00
PAN-EDU-210	PAN-EDU-210: Firewall 10.0 Essentials - Configuration and Management - 1 Student | The Firewall 10.0 Essentials: Configuration and Management course is five days of instructor-led training that will help you to: Configure and manage the essential features of Palo Alto Networks next-generation firewalls. Configure and manage GlobalProtect to protect systems that are located outside of the data-center perimeter. Configure and manage firewall high availability.	2.00	$5,000.00	$10,000.00
4 post rack mount kit.	Palo Alto Networks PA-5200 4 post rack mount kit.	2.00	$58.16	$116.32

Thank you for the opportunity to quote these products. Please note: Prices quoted are valid for 30 days. Applicable taxes and shipping charges are additional. Returns or cancellation of order(s) may be subject to a fee. We look forward to helping you in the future.

January promotion	January promotion - Based on purchasing the full bill of material on this quote by January 25, 2021	1.00	($66,136.32)	($66,136.32)
Finance option	This quote includes the option to make 3 annual payments of $147,600.00. This option is provided by Arrow Capital Solutions.	1.00	$0.00	$0.00

Total	**$442,800.00**

NASPO Contract (AR3229)

Cyber Security Proposal

Prepared for: Livingston County, Michigan

Brian Nufer
Territory Account Manager
Palo Alto Networks

Andy Nyquist
Systems Engineer
Palo Alto Networks

Paul Laurio
Account Manager
AmeriNet

Patrick Donlin
Systems Engineer
AmeriNet

Executive Summary -

The Problem:

- Livingston County (LC) currently utilizes several unique security solutions for firewall, endpoint protection, secure remote access (SSLVPN), and network-based forensics and end-user behavioral analytics.
- The current Sonicwall firewall solution is 5+ years old, limited in capability, and undersized for the current environment.
- The existing solutions are not tightly integrated and as a result, the IT Network/Security team spends a significant amount of time dealing with alerts and collecting information from several unique consoles and logs when responding to security threats and incidents.

The Proposed Solution:

- Palo Alto proposes to meet those challenges by delivering a single, comprehensive cyber-security platform that tightly integrates firewall, cloud-delivered malware analysis and protections, secure remote access/SSLVPN, next generation endpoint security, host and network-based behavioral analytics.
  - The proposed PA-5220 Next Generation Firewall (NGFW) with its unique Single-Pass Architecture, provides up to 9 GB of throughput while continuously supporting Threat Prevention (TP), URL Filtering, Wildfire (WF) cloud-delivered Malware Analysis and Protection of unknown threats, DNS Security, and Global Protect (GP) Secure Remote Access.
  - The Proposed Cortex XDRPro Endpoint Security solution provides host-based protections and blocking of known and unknown malware and is integrated with the NGFWs through the cloud-delivered Cortex Data Lake.

Executive Summary - continued

The Benefits:

- Through consolidation of multiple disparate solutions into a single integrated platform, the County can improve its overall security posture, reduce the administrative effort and burden on the IT staff, and potentially reduce overall cost of ownership of the cyber security environment.

- The proposed solution will collect, integrate, and normalize your enterprise's security data across Firewall and Endpoints without a dedicated SIEM or SOC. In addition, the solution provides:
  - The unique ability to stitch together events from Cortex XDR Endpoints and the Next Generation Firewall in the purpose built Cortex Data Lake
  - Benefits of public cloud scalability and agility that grows on demand with your organization.
  - The automatic normalization of data in a consistent format, ensuring the effectiveness of large-scale analytics.

- Advanced AI/ML with cloud scale data storage and compute.

- Leverage Industry leading Global Threat Intelligence
  - Palo Alto's Global Threat Intelligence team, Unit 42, a team of industry experts whose mission is to research and document the details of adversaries' playbooks and quickly share them with the systems, people, and organizations that can use them to prevent successful cyber attacks.
  - WildFire is a malware prevention service that collects trillions of constantly growing threat artifacts from tens of thousands of independent organizations.
  - Stop known, unknown, and behavioral based threats.

Current Environment Challenges

Current Solution

Livingston County IT is currently utilizing the following security solutions to protect the environment.

- Sonicwall firewalls (HA Pair)
- Cisco Firewalls centrally located to protect substations
- Stand-alone VPN Appliance for secure remote access
- FireEye NX and HX network and host-based intrusion prevention
- DarkTrace/Antigena for network-based visibility and AI-driven detection/response to cyber threats

Challenges

- The Sonicwall Firewalls are undersized for the current environment and are reaching end of life.
- The multi-vendor security solutions currently deployed require the IT staff to correlate security incidents across multiple information sources and consoles. This leads to extended effort and time required to investigate and resolve security incidents.
- The Sonicwall Firewalls, SSLVPN appliance, FireEye solutions, Darktrace solution, and the additional Cisco Firewalls each have a unique user interface which adds complexity to the environment.

Required Outcomes

- Optimal Security posture for the County.
- Reduced administrative overhead/burden on the IT staff
- A single (or minimal) console(s) from which to configure and monitor the cybersecurity infrastructure and to troubleshoot/investigate/automate security detection & response
- Deep visibility into applications, users, context, and devices so that granular security policies can be applied across any environment
- AI driven and automated correlation of multiple events/alerts from Firewalls, servers and endpoints to reduce false positive alerts and reduce time to detect, block, and respond to attacks or incidents of compromise.

Proposed Solution

Required Capabilities

- Deep visibility into Applications, users, devices, and context to put in place granular protections and provide a simplified and optimal security posture.
- Host and network-based protection against known and unknown threats with the ability to automaticaly block or shutdown malicious activity
- AI/ML-driven security that is also based on behavioral analytics
- Cloud-delivered and scalable malware protection that continually provides updated protections to the firewalls and host-based agents - in 5 minutes or less
- Centralized management of physical and virtual or cloud-based firewalls

Proposed Solution

- **PA-5220 Firewalls** (HA Pair) to replace existing Sonicwall Firewalls that include the following security subscriptions:
  - Threat Prevention, URL Filtering, DNS Security, Global Protect Secure Remote Access, Wildfire - cloud integrated and delivered malware protection
- **Cortex XDR Pro with Data Lake** - extended detection and response platform that runs on integrated endpoint, network and cloud data to reduce noise and focus on real threats.

- Optional PA-220 Firewalls to replace Cisco substation firewalls
- Optional Panorama Centralized Firewall Management Solution

Customer Impact

- Improved overall security posture due to integration of NGFW, End-point Protection, and Cloud-delivered protections and analytics
- Reduced administrative effort for configuration and management
- Fewer solutions (5 -> 2) and Vendors (5 -> 1) to manage
- Reduced time spent on event correlation and response
- Greatly increased FW throughput and scalability
- Additional protections such as DNS Security, Anti-Phishing/Ransomware protections that may not be currently provided with existing solutions

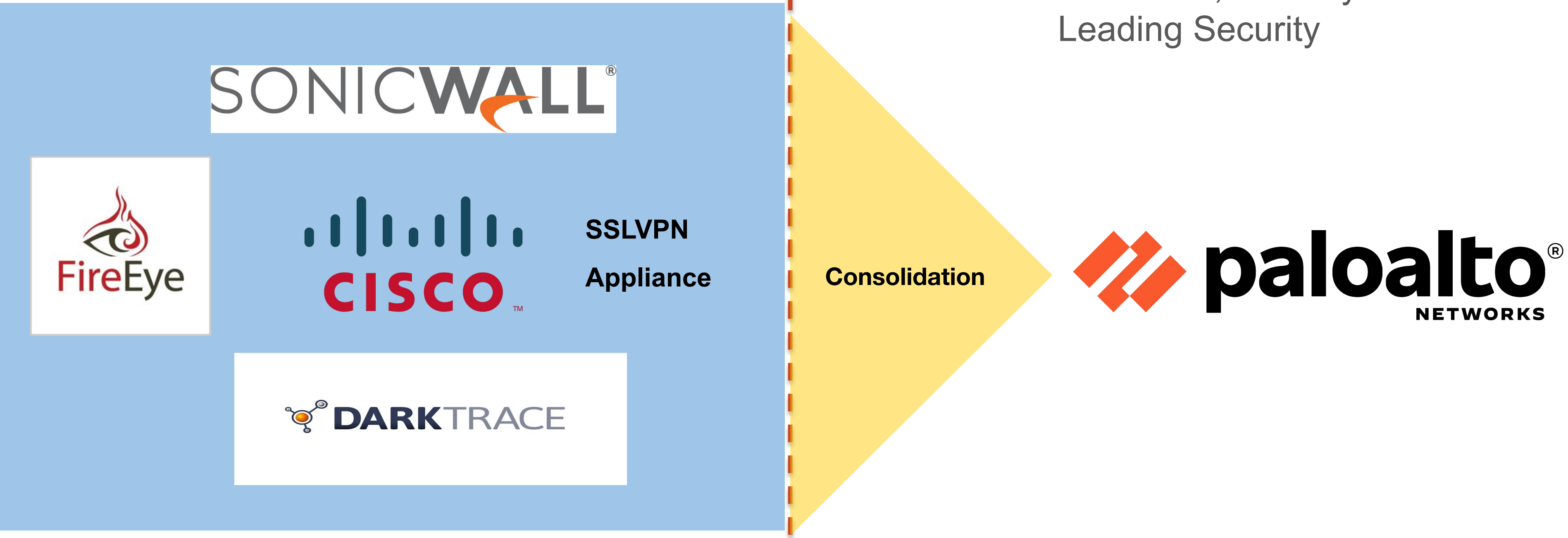
Impact - 5 Point Solutions Consolidated

Livingston County Government Current State

Multi-Point Solutions

Proposed Future State

Consolidated, Industry-Leading Security



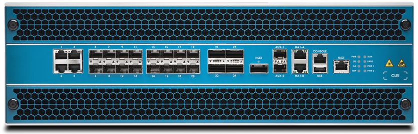
SSLVPN

Appliance

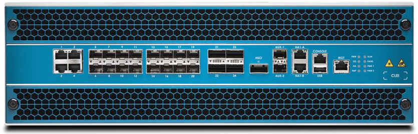
Consolidation

Introducing the PA-5200 Series

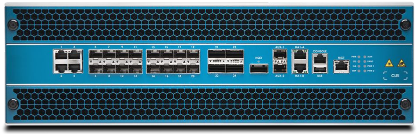
PA-5200 Series



PA-5260
63 Gbps App-ID
32 Gbps Threat



PA-5250
40 Gbps App-ID
21 Gbps Threat



PA-5220
20 Gbps App-ID
9 Gbps Threat

- Up to 5x performance increase
- Up to 20x decryption session capacity increase
- Dedicated HA and management interfaces
- Up to 7x decryption performance increase
- Dual SSD system drives (240 GB) and dual HDD logging drives (2 TB)
- Max Tunnels 15,000 (SSL, IPSec, and IKE with XAuth)

Performance and Summary

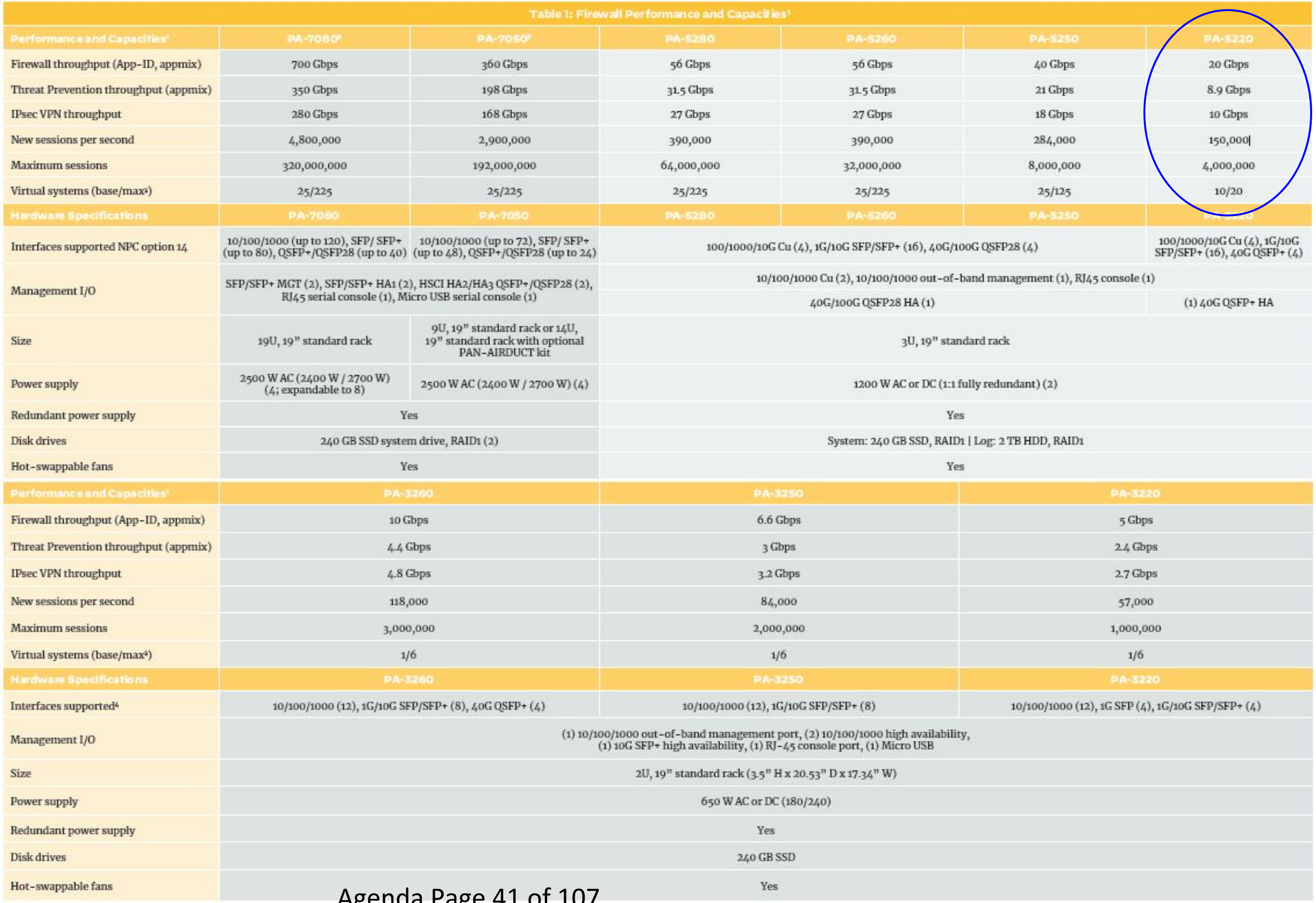
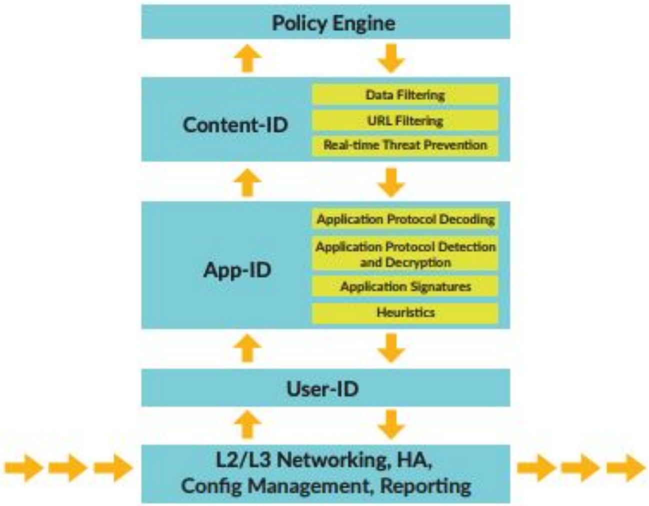


Table 1: Firewall Performance and Capacities[1]

Performance and Capacities[1]	PA-7080[2]	PA-7050[2]	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID, appmix)	700 Gbps	360 Gbps	56 Gbps	56 Gbps	40 Gbps	20 Gbps
Threat Prevention throughput (appmix)	350 Gbps	198 Gbps	31.5 Gbps	31.5 Gbps	21 Gbps	8.9 Gbps
IPsec VPN throughput	280 Gbps	168 Gbps	27 Gbps	27 Gbps	18 Gbps	10 Gbps
New sessions per second	4,800,000	2,900,000	390,000	390,000	284,000	150,000
Maximum sessions	320,000,000	192,000,000	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[3])	25/225	25/225	25/225	25/225	25/125	10/20
Hardware Specifications	**PA-7080**	**PA-7050**	**PA-5280**	**PA-5260**	**PA-5250**	**PA-5220**
Interfaces supported NPC option 14	10/100/1000 (up to 120), SFP/ SFP+ (up to 80), QSFP+/QSFP28 (up to 40)	10/100/1000 (up to 72), SFP/ SFP+ (up to 48), QSFP+/QSFP28 (up to 24)	100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)			100/1000/10G Cu (4), 1G/10G SFP/SFP+ (16), 40G QSFP+ (4)
Management I/O	SFP/SFP+ MGT (2), SFP/SFP+ HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)		10/100/1000 Cu (2), 10/100/1000 out-of-band management (1), RJ45 console (1)			
			40G/100G QSFP28 HA (1)			(1) 40G QSFP+ HA
Size	19U, 19" standard rack	9U, 19" standard rack or 14U, 19" standard rack with optional PAN-AIRDUCT kit	3U, 19" standard rack			
Power supply	2500 W AC (2400 W / 2700 W) (4; expandable to 8)	2500 W AC (2400 W / 2700 W) (4)	1200 W AC or DC (1:1 fully redundant) (2)			
Redundant power supply	Yes		Yes			
Disk drives	240 GB SSD system drive, RAID1 (2)		System: 240 GB SSD, RAID1 | Log: 2 TB HDD, RAID1			
Hot-swappable fans	Yes		Yes			

Performance and Capacities[1]	PA-3260	PA-3250	PA-3220
Firewall throughput (App-ID, appmix)	10 Gbps	6.6 Gbps	5 Gbps
Threat Prevention throughput (appmix)	4.4 Gbps	3 Gbps	2.4 Gbps
IPsec VPN throughput	4.8 Gbps	3.2 Gbps	2.7 Gbps
New sessions per second	118,000	84,000	57,000
Maximum sessions	3,000,000	2,000,000	1,000,000
Virtual systems (base/max[3])	1/6	1/6	1/6
Hardware Specifications	**PA-3260**	**PA-3250**	**PA-3220**
Interfaces supported[4]	10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)	10/100/1000 (12), 1G/10G SFP/SFP+ (8)	10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
Management I/O	(1) 10/100/1000 out-of-band management port, (2) 10/100/1000 high availability, (1) 10G SFP+ high availability, (1) RJ-45 console port, (1) Micro USB		
Size	2U, 19" standard rack (3.5" H x 20.53" D x 17.34" W)		
Power supply	650 W AC or DC (180/240)		
Redundant power supply	Yes		
Disk drives	240 GB SSD		
Hot-swappable fans	Yes		

Key Differentiators:
Predictable and Programmable Hardware for Firewall Longevity



Policy Engine

Content-ID
- Data Filtering
- URL Filtering
- Real-time Threat Prevention

App-ID
- Application Protocol Decoding
- Application Protocol Detection and Decryption
- Application Signatures
- Heuristics

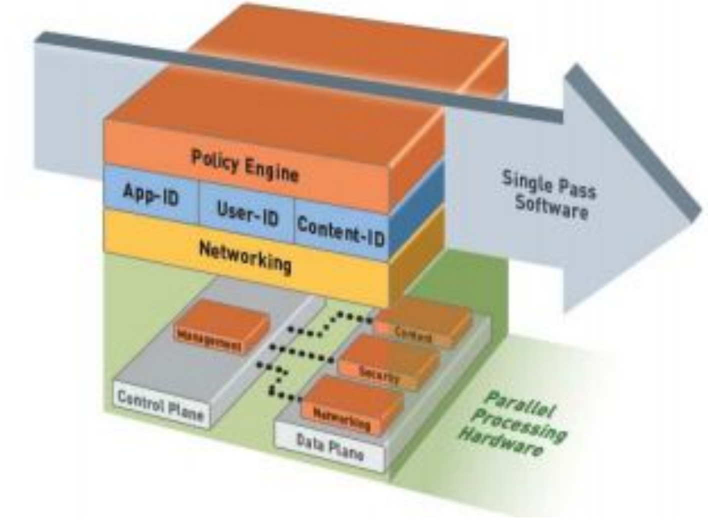
User-ID

L2/L3 Networking, HA,
Config Management, Reporting

Figure 1: Single-Pass Architecture Traffic Flow

A single pass: With only one stack to go through, speed is easy to achieve.

Palo Alto Networks SP3 Architecture and Processing



Parallel processing: Hardware and cloud checks all run in parallel, not waiting on each other to finish.

Our Commitment to Cyber Hygiene and Best Practices

Expedition

Reduce rule set by 10X

Datasheet ▶

IronSkillet

Start with default best practice config

Getting started ▶

Best Practice Assessment

Assess your prevention level

Learn more ▶

Policy Optimizer

Replace legacy rules with app-based rules

Watch the video

▶

Rewiring SecOps with Cortex

Prevent everything you can

CORTEX XDR
BY PALO ALTO NETWORKS

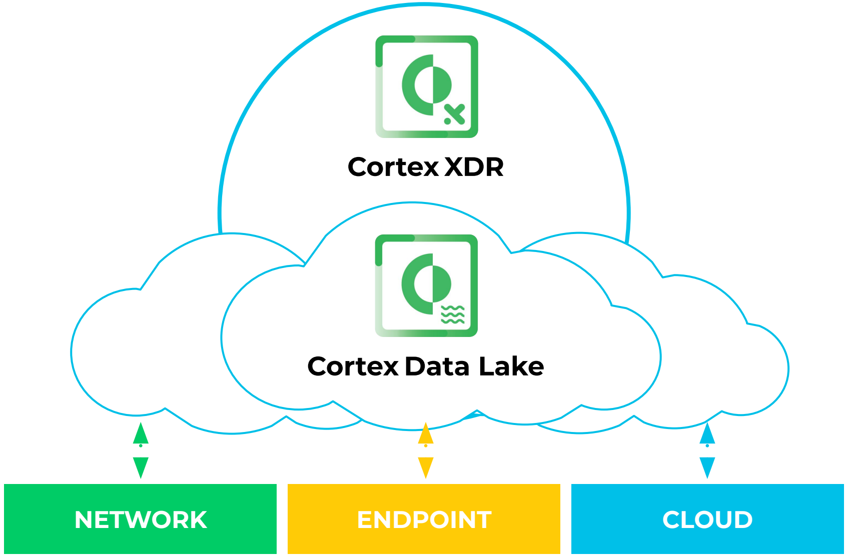
Everything you can't prevent, detect and investigate fast

CORTEX XDR
BY PALO ALTO NETWORKS

Automate response and get smarter with each incident

CORTEX XSOAR
BY PALO ALTO NETWORKS

Cortex XDR Detects and Investigates Sophisticated Attacks



Automatically detect attacks using rich data and cloud-based behavioral analytics

Accelerate investigations by stitching data together to reveal root cause

Tightly integrate with enforcement points to stop threats and adapt defenses

|

Summary: Cortex XDR value

Reduce risk of a breach

Cut detection & response times 8x

Increase SecOps efficiency

Reduce alerts 50x with alert grouping

Maximize investments

Lower TCO by 44%

Established 1864

“I would get 400 or 500 alerts a day. Now I'm down to maybe seven or eight…We're not spending six hours on incident response, we're spending 10 minutes”

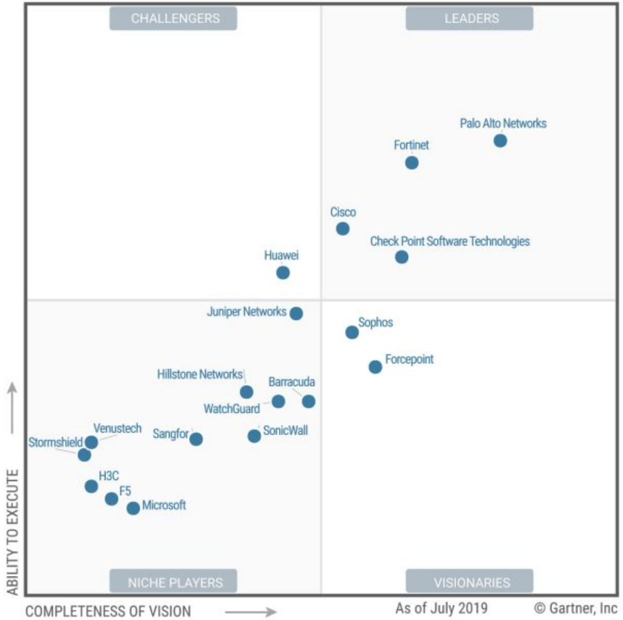
Challenge

- Protecting infrastructure and data
- Limited network to endpoint activity
- 500 alerts per day with long MTTR

Impact

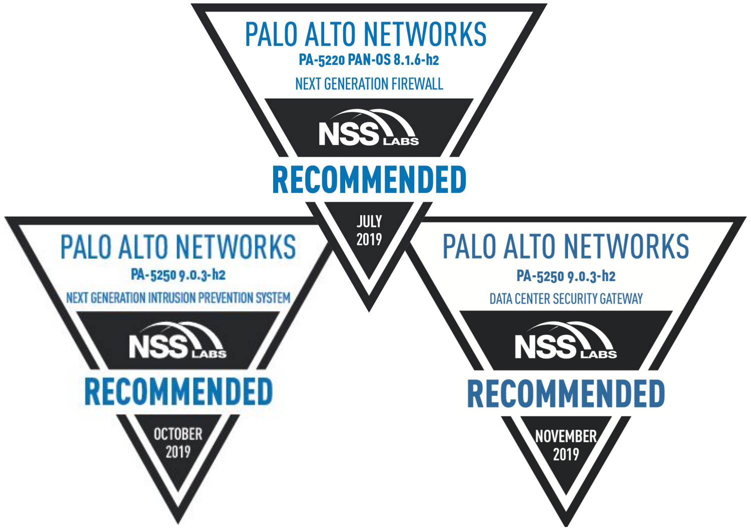
- Deep insight into network and endpoints
- Alert reduction from 500 to 7
- MTTR reduced from 6 hours to 10min

8-time Leader in the Gartner Firewall MQ, NSS Labs Recommended



Source: Gartner (September 2019)

2019 Gartner Magic Quadrant for Network Firewalls



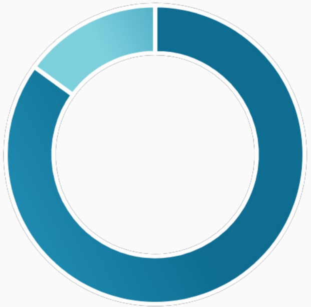
NSS Labs Recommended

The World’s Leading Cybersecurity Company

95

of Fortune 100

Rely on Palo Alto Networks



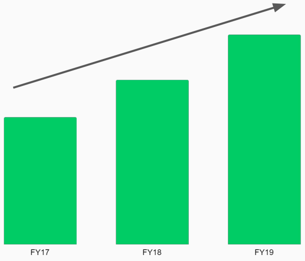
71% of the Global 2K

Are Palo Alto Networks Customers

#1

in Enterprise Security

Revenue trend 27% CAGR
CY17 – CY19



15% Year-Over-Year

Revenue Growth

70,000

Customers

In 150+ Countries

5
YEARS
IN A ROW
J.D. POWER
2019
CERTIFIED ASSISTED
TECHNICAL SUPPORT
2019
tsia
RATED
OUTSTANDING
PALO ALTO NETWORKS | GLOBAL
ASSISTED SUPPORT
2015 • 2016 • 2017 • 2018 • 2019

9/10

Average CSAT Score

FY19 Revenue for all periods reflect adoption of ASC 606
Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19, 20 March 2020

CUSTOMER SUCCESS MISSION

We Focus on **Three Key Pillars** to Help You Succeed

1 Achieve desired customer business outcomes

2 Ensure customers are gaining value from investment

3 Continuous commitment to preventing successful cyberattacks

paloalto NETWORKS

Thank you

paloaltonetworks.com

Magic Quadrant for Network Firewalls

Published 9 November 2020 - ID G00456338 - 55 min read

By Analysts Rajpreet Kaur, Adam Hils, Jeremy D'Hoinne

Initiatives: Infrastructure Security

Network firewalls are evolving to secure newer use cases, including cloud and sudden shift to growing remote workforce. Firewall vendors have been slow in responding to growing hybrid networks with a lack of appropriate product offerings and related support.

This Magic Quadrant is related to other research:

Critical Capabilities for Network Firewalls

View All Magic Quadrants and Critical Capabilities

Strategic Planning Assumptions

By 2025, 30% of new distributed branch office firewall deployments will switch to firewall as a service, up from less than 5% in 2020.

By year-end 2024, 25% of firewall end-user spend will be contained within larger security “platform” deals delivered by enterprise license agreements (ELAs), up from less than 5% today.

Market Definition/Description

Gartner defines the network firewall market as composed primarily of firewalls offering bidirectional controls (both egress and ingress) for securing networks. These networks can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud. The product has the capability to support one or more firewall deployment use cases, such as perimeter, small and midsize businesses (SMBs), data center, cloud, and distributed offices.

This market is no longer restricted to appliance-only vendors. and extends to vendors offering virtual versions and firewall as a service (FWaaS), offered as native firewall controls or dedicated offerings by public and private cloud vendors.

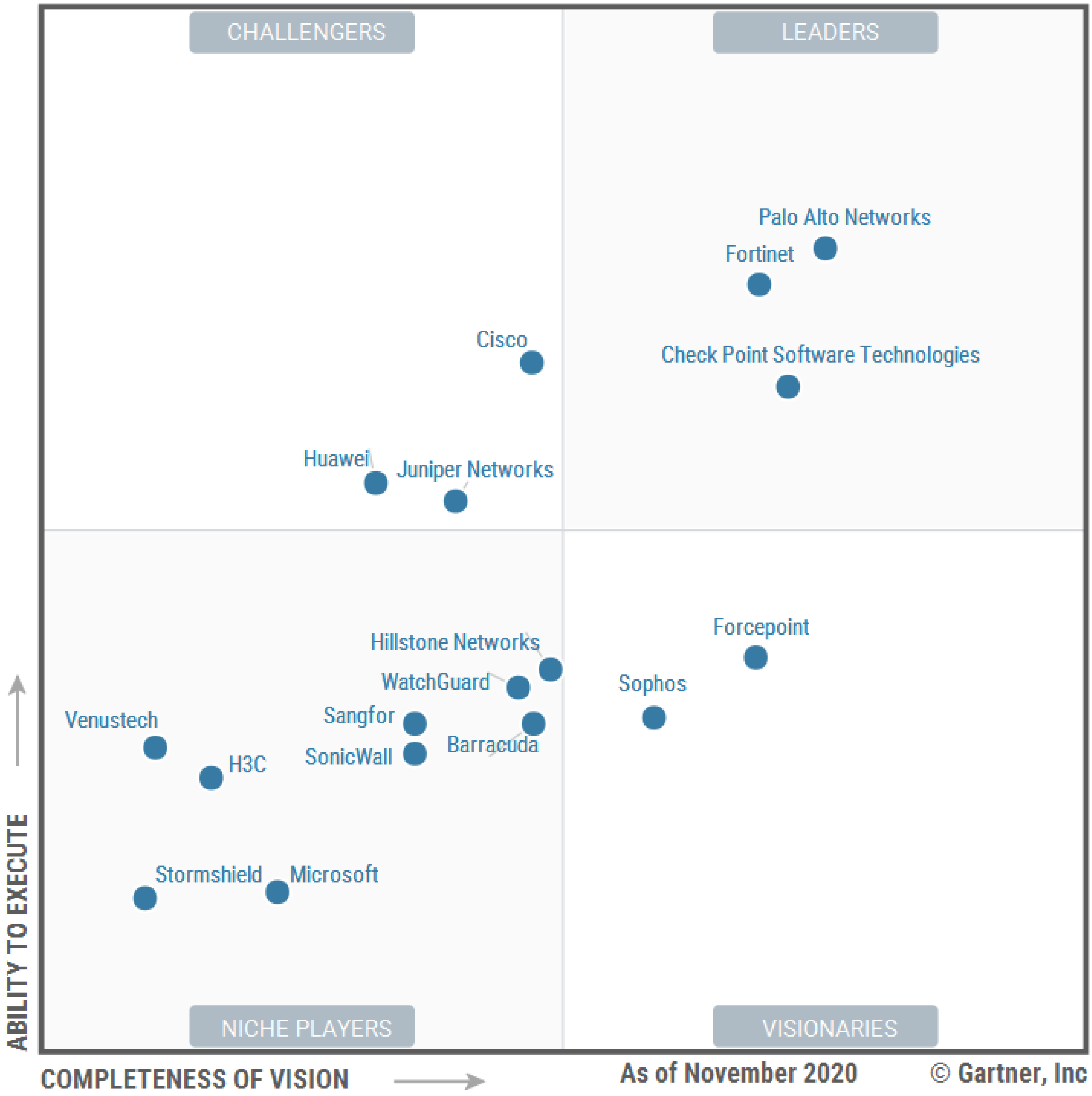
Network firewalls can also offer additional capabilities, such as application awareness and control, intrusion detection and prevention, advanced malware detection, and logging and reporting.

This Magic Quadrant includes the following types of network firewalls:

- Purpose-built physical appliances
- Virtual appliances
- Embedded firewall modules
- Firewall controls delivered from infrastructure as a service (IaaS) platform providers
- Dedicated FWaaS (Note: FWaaS is a service directly hosted and sold by the vendor, and is not a hosted firewall service offered by managed security service providers [MSSPs], telcos or any other partner).

Magic Quadrant

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

Vendor Strengths and Cautions

Barracuda

Barracuda is a Niche Player in this Magic Quadrant. Its firewall product line is called Barracuda CloudGen Firewalls. It has dedicated firewalls for operational technology (OT) and industrial control system (ICS) use cases.

This year, Barracuda has introduced Barracuda CloudGen WAN, hosted on Microsoft Azure as a secure SD-WAN offering. Other updates include Firewall Insights, which is Barracuda's analytics and reporting product offering, and enhancements to cloud IaaS support and Internet of Things (IoT) security.

Barracuda focuses on public cloud IaaS and distributed office use cases for its firewalls. Hence, Barracuda CloudGen Firewalls are a good candidate for enterprises looking for mature public IaaS firewall features and integrated native SD-WAN and VPN features.

Strengths

- **Market execution:** Barracuda CloudGen Firewalls offer better support features for Amazon Web Services (AWS) and Microsoft Azure platforms as compared to other firewalls. These capabilities include support for Azure Operations Management Suite (OMS), Azure Security Center (ASC), Azure Sentinel and AWS Amazon CloudWatch, which most other firewall vendors fail to offer.

- **Product strategy:** Barracuda is a good shortlist candidate for the distributed office use case, with integrated SD-WAN and mature VPN capabilities. The vendor regularly introduces enhancements to these features. Recently, it introduced Barracuda CloudGen WAN, hosted on Microsoft Azure as a secure SD-WAN offering.

- **Pricing:** Barracuda CloudGen Firewalls win on pricing versus features. Their subscriptions are bundled and come with inclusive basic technical support. This makes them desirable firewalls for SMBs, for which pricing is one of the key shortlisting criteria.

- **Product strategy:** Apart from dedicated firewalls for OT and ICS use cases, Barracuda also offers secure connector products for IoT device connectivity. These connectors provide centralized management and access through Barracuda's firewall centralized manager — Firewall Control Center — of various IoT devices. CloudGen Firewall products offer support for OT protocols such as S7+, IEC 61850, IEC 60870-5-105, Modbus and DNP3.

Cautions

- **Product strategy:** Despite Barracuda offering multiple security product lines, it offers no integration with CloudGen Firewalls, hence not offering operational simplicity to clients consolidating toward a single vendor.

- **Sales execution:** Gartner doesn't see ELA deals promoted by the vendor for clients that want to consolidate toward Barracuda for their multiple security solutions. All the firewall deals are generally stand-alone ones, while other vendors that offer multiple security product lines are promoting ELAs for pricing simplicity for their clients.

- **Market responsiveness:** Despite a strong focus on the distributed office use case, the vendor doesn't offer a cloud-based firewall manager. Barracuda has recently launched a secure SD-WAN service hosted in Microsoft Azure that includes cloud-based management not currently available with its CloudGen Firewall.

- **Customer feedback:** Gartner clients have reported below-satisfactory technical support feedback, contradictory to excellent support feedback that clients used to cite a few years ago.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. Its firewall product is its main security product line; its new Quantum Security Gateways series offers firewalls for all use cases, including containers. CloudGuard Connect is the FWaaS offering. Major updates include extending support for cloud security and enhancements around threat prevention, performance and support for IoT security. The vendor has also introduced the centralized cloud-based management portal Smart-1 Cloud, Infinity portal and FWaaS.

Check Point firewalls are good shortlist candidates for enterprises with a cloud security focus. The vendor also offers high-performing firewalls for the data center use case. Check Point leads in centralized management capabilities and integration with its endpoint security and mobile security product lines.

Strengths

- **Centralized management:** Launched in April 2020, and still too recent to have received customer feedback, Smart-1 Cloud offers feature parity with the Smart-1 on-premises console. Check Point Smart-1's console appeals especially to managed security service provider customers and prospects, and distributed enterprises.

- **Policy management:** In the hybrid world, where firewall vendors face stronger competition from network security policy management tools for their ability to manage IaaS native controls and multiple brands, Check Point has a strong base of faithful and satisfied users, praising the policy editors and the recent improvement in the R80.x versions.

- **Product strategy:** Check Point has accelerated the pace of its cloud security execution, including the integration of CloudGuardDome9, a cloud security posture management solution, and CloudGuard Workload serverless security.

- **Threat prevention:** Check Point continues to improve its threat detection capabilities. Customers using Threat Extraction, the content disarm and reconstruction feature that is part of the SandBlast bundle, welcome the addition of web downloads as a new layer of protection for employees.

Cautions

- **Pricing strategy:** Although Check Point has succeeded in simplifying its pricing strategy, it lags behind its leading competitors in its ability to sell enterprise-level agreements to the largest customers.

- **Pricing execution:** In the past few years, Gartner analysts continued to receive a sizable amount of reports regarding dissatisfaction with pricing, which have slowly shifted from a focus on total cost of ownership (TCO) to more on the high cost of renewing Check Point subscriptions.

- **Product strategy:** Check Point's strategy to integrate its security virtual machine (VM) with leading SD-WAN providers, rather than add native SD-WAN capabilities, creates a disadvantage against its leading competitors when competing for the branch perimeter appliance use case.

- **Support:** For providers with a long history and large market share, Gartner expects to receive more feedback on occasional support issues. While it improved last year, feedback on Check Point support, especially outside of North America, continues to be slightly worse than its competitors.

Cisco

Cisco is a Challenger in this Magic Quadrant. Cisco offers multiple firewall product lines, the primary ones being Cisco Firepower Threat Defense (FTD) Next-Generation Firewall (NGFW) Series and the Meraki MX series. Cisco also offers FWaaS as a part of its Umbrella secure internet gateway, and industrial firewalls (the ISA series).

Major updates include those around its Firepower Management Center user interface. It also introduced SecureX, an integrated management platform that enables visibility and control across network, endpoint, cloud and application security.

Cisco's firewall is a good fit for organizations that have experience with Cisco products and want to consolidate with the same vendor for their security and network products.

Strengths

- **Sales strategy:** Cisco has a broad product portfolio, and drives customers effectively toward enterprise ELAs, which often include firewall subscriptions and support. It is also an attractive proposition for clients that want to consolidate with a single vendor.

- **Capability:** Customers value the Talos threat research and advanced malware protection (AMP) features available on Firepower. Existing Sourcefire customers also like the IPS integration on Firepower. SecureX is the vendor's extended detection and response (XDR) platform that enables visibility and control across Cisco's network, endpoint, cloud and application security products.

- **Market execution:** Cisco Meraki MX provides a simplified security and networking experience to customers with distributed small offices that need easy-to-configure, deploy and manage networking and firewall solutions.

- **Feature:** Gartner clients remark on the high quality of Cisco's VPN, and report that the site-to-site VPN is stable and easy to configure. Many Gartner clients that replace their Cisco Adaptive Security Appliances (ASAs) with a firewall from a different vendor continue to use ASAs for VPN only.

Cautions

- **Product strategy:** Cisco offers multiple different security management portals, causing a lot of overlap and confusion within the end-user community. The vendor offers Cisco Defense Orchestrator as a cloud-based centralized manager, Cisco Threat Response (CTR) cloud-based threat correlation, Security Analytics and Logging (SAL) cloud-based reporting portal, and the latest addition, the SecureX extended detection and response platform.

- **Product strategy:** Despite having multiple cloud security products, the vendor only offers support for AWS and Azure through Cisco NGFWv, and ASAv and ASA for Cisco Meraki vMX. These lack any integration with Cisco's Tetration, its cloud workload protection platform (CWPP) offering. As a result, Gartner seldom sees Cisco firewall deployments in public cloud IaaS scenarios.

- **Product strategy:** Cisco has different firewall product lines for different deployment use cases. The Meraki and FTD product lines are led by different product teams and have distinct capabilities and operating systems, leading to operational complexities despite consolidating toward a single vendor.

- **Sales execution:** Cisco continues to struggle to win firewall evaluations against competitors in pure firewall deals based on technical evaluation alone. "Cisco shops" are the predominant base of Cisco firewall customers.

Forcepoint

Forcepoint is a Visionary in this Magic Quadrant. During the evaluation period, it introduced several new firewall models. It also brought a new secure access service edge (SASE) offering to market. Other updates include enhancements to AWS and Azure integrations, and a browser-based interface for its Security Management Center (SMC) central management system, for easier administration.

Forcepoint firewalls are good shortlist candidates for distributed office use cases where clients are looking for mature SD-WAN, VPN and centralized management capabilities, and FWaaS. They have advanced clustering/high availability, and are also good candidates for midsize enterprises looking for mature advanced threat detection features.

Strengths

- **Product execution:** Forcepoint has strong SD-WAN and VPN capabilities. It plays to these strengths by releasing enhancements regularly. It maintains a single endpoint client approach for all its end-user connectivity, irrespective of the service. Forcepoint offers Wi-Fi on the smaller modules through additional modules.

- **Offering:** Forcepoint firewalls offer some unique capabilities such as built-in user and entity behavior analytics (UEBA) capability, and integration with AWS Sentinel and Azure Security Center as public IaaS support. There is seamless service-chaining between Forcepoint's firewalls and its web security and data loss prevention (DLP) products.

- **Product strategy:** This year, Forcepoint introduced its FWaaS. Other than that, it offers a compelling list of cloud security services: Forcepoint Web Security, Forcepoint CASB, Forcepoint Email Security, Forcepoint Dynamic User Protection and Forcepoint Dynamic Data Protection. This shows its strong product strategy toward offering a cloud security service model.

- **Centralized manager:** Forcepoint's centralized firewall manager, SMC, is a very intuitive and easy-to-use interface, and customer feedback is positive. Administrator roles can be defined, and mapped with select NGFWs, access control lists and domains. There is also an administrator privilege for approving pending changes with features such as drag-and-drop.

Cautions

- **Market execution:** Forcepoint focuses too heavily on the distributed office use case and support of the emerging SASE trend. While its firewalls have the potential to serve other use cases, the vendor's roadmap sacrifices data center features, potentially falling behind other vendors in the market.
- **Marketing:** Forcepoint does not have much market awareness, and is rarely mentioned as a shortlist candidate by Gartner clients. While it has some presence within the U.S. federal government sector, it lacks traction in other markets.
- **XDR:** The vendor lacks native endpoint detection and response (EDR) client integration capabilities. It also lacks firewall integration with third-party EDR clients.
- **Customer feedback:** Customers remark that Forcepoint's feature releases occur behind those of the leading vendors. This holds the vendor back from leading the market.

Fortinet

Fortinet is a Leader in this Magic Quadrant. The vendor offers multiple firewall virtual and hardware models to meet different firewall deployment use cases.

The major update this year has been the acquisition of OPAQ, a SASE cloud provider. New feature updates include multiple enhancements to the latest version of FortiOS, including integration support with Kubernetes through FortiOS 6.2 and release of the NP7 network processor.

Fortinet firewalls are leaders in integrated SD-WAN capabilities with advanced networking, making them top candidates for firewall-appliance-based distributed office use cases. They also lead in price versus performance, and are desirable candidates in price-conscious enterprises.

Strengths

- **Advanced networking:** Fortinet offers fully integrated SD-WAN capabilities in its firewalls. Fortinet Fabric Management Center (FMC) offers strong automation and orchestration capabilities for full mesh overlay links for secure connectivity capabilities between sites.
- **Product:** Fortinet's security fabric offers open API capabilities to integrate with third-party products in the client's ecosystem. It also offers GUI plug-ins to its API interface for several third-party products/partners such as AWS, Azure. VMware vCenter and others.
- **Product strategy:** FortiManager provides central management with additional Fortinet Fabric plug-ins, which offer management of FortiSwitch, FortiAP, FortiWifi, FortiWLM, FortiExtender and FortiAnalyzer.
- **Price execution:** One of the primary reasons Gartner has seen data center and large enterprises shortlisting Fortinet firewalls is their competitive price/performance ratio and bundled pricing models, which makes product licenses easy to consume and allows for a realistic estimation of TCO.

Cautions

- **Market execution:** Despite having a large product portfolio, Gartner does not see Fortinet clients tempted to consolidate toward its multiple product lines other than firewalls and web application firewalls (WAFs). Gartner finds a less aggressive vendor focus on developing and upgrading other security products to compete with the best of breed in the market, such as FortiNAC, FortiClient and FortiCASB. Also, the vendor lacks the automation capabilities of different security product lines with FortiGate firewalls.
- **Market responsiveness:** During the evaluation period of this research, Fortinet announced the acquisition of OPAQ, a SASE cloud provider, but still lacks an FWaaS offering. The vendor might start offering it as an independent solution immediately, considering the demand in the market. It is recommended that Gartner clients consider it as an independent offering, and evaluate the integration capabilities.
- **Market execution:** Despite Fortinet supporting multiple cloud platforms, Gartner generally does not see the vendor's firewalls shortlisted for the cloud deployment use case, as compared to other direct competitors. Gartner also finds that Fortinet lacks marketing and promotion related to the cloud deployment use case, making it seem like the vendor is more hardware-focused.
- **Customer feedback:** Fortinet continuously releases multiple different new feature enhancements for its firewall product, which often leads to new management changes in the UI. Clients have citied this as making firewall management more complex for day-to-day administration after the new update is applied.

H3C

H3C is a Niche Player in this Magic Quadrant. It is an infrastructure vendor. SecPath is its firewall product line. H3C also offers a dedicated industrial firewall product line, Industrial Control Security.

Major updates this year include multiple feature enhancements in advanced routing, firewalling capabilities and cloud support.

H3C is a good candidate for enterprises in China that want to consolidate toward a single vendor for their infrastructure requirements to reduce licensing complexities. It offers different firewall models to meet different firewall deployment use cases, with high-end data center models.

Strengths

- **Product portfolio:** Like many large Chinese security vendors, H3C also offers a broad range of network products in its portfolio that are ideal for network teams looking for vendor consolidation. Its firewalls offer built-in WAF and vulnerability scanning. H3C also offers a dedicated product line for industrial/OT security.
- **Scalability:** The vendor offers high-throughput firewalls for the data center use case. Its VSYS feature for firewall model M9000, can support more than 4,000 virtual firewall instances.

- **Market execution:** The H3C firewalls have a prominent presence in the telco vertical. The vendor offers strong support for OpenStack, especially for telcos that want to offer hosted security services to their clients. H3C SecCloud Operation Management Platform (OMP) is a centralized management platform for large-scale deployments and cloud deployments.
- **EDR:** H3C offers Terminal Safety Protection System (TSPS), an endpoint protection client. This client software provides EDR and antivirus functions. The TSPS management platform and firewall utilize Cybersecurity Situation Awareness Platform (CSAP) to analyze the information and trigger actions, notifying the TSPS platform to restrict the infected host's network access and infected file transmission, etc.

Cautions

- **Market execution:** H3C is more focused toward hardware and OpenStack product lines to support its native private cloud and telco-hosted platforms, only available on Alibaba Cloud. The vendor lacks direct security services offered to clients as SaaS. It also lacks a direct FWaaS offering.
- **Sales execution:** Despite a broad product line, the vendor lacks Enterprise Support Agreements (ESAs) to benefit H3C clients and reduce multiyear licensing complexities.
- **Geographic strategy:** The vendor has a presence primarily in China and lacks a presence in other parts of the Asia/Pacific region. Gartner does not see H3C being shortlisted by clients outside of China.

Hillstone Networks

Hillstone Networks is a Niche Player in this Magic Quadrant. It sells firewalls for different use cases under different product lines: E-Series NGFW, T-Series iNGFW, X-Series Data Center Firewall, CloudEdge (virtual NGFW), CloudHive (microsegmentation) and CloudPano (FWaaS in the China market only). Other than firewalls, Hillstone sells WAF, application delivery controller (ADC), network traffic analytics (NTA) and intrusion detection and prevention system (IDPS) products.

Product updates this year include IoT security (IP camera network protection) and enhancements related to policy optimization, reporting and SD-WAN.

Hillstone has a strong focus on supporting China's regional cloud. It offers firewall models for different firewall deployment use cases. It is a good shortlist candidate for enterprises looking for virtual firewalls for cloud in China.

Strengths

- **Product portfolio:** Hillstone offers a broad network security portfolio, ideal for enterprises seeking consolidation toward a single vendor. Besides firewalls, the vendor offers FWaaS in China via CloudPano, WAF, ADC, NTA and IPS products.

- **Microsegmentation:** Hillstone offers a dedicated firewall offering for the microsegmentation use case, called CloudHive. It continues to enhance CloudHive by adding advanced features. CloudHive offers policy assistant features and a policy duplication detection engine, which uses prelearning network traffic to help in policy optimization of east-west traffic. CloudHive also offers traffic visualization capabilities, automatic discovery of service chains and the ability to detect service down gradation.

- **Product strategy:** Hillstone was one of the first Chinese security vendors with a strong cloud security strategy. The vendor offers CloudPano in China. The Hillstone firewalls offer support for AWS, Azure, Alibaba Cloud, Tencent Cloud and Huawei Cloud as bring your own license (BYOL). They are also available as pay as you go (PAYG) on AWS and Alibaba Cloud.

- **Product portfolio:** The vendor offers Hillstone sBDS, its NDR platform, available globally, and a SIEM solution called iSource, currently sold only in China. This offers multiple product consolidation options for Hillstone firewall clients.

Cautions

- **Cloud portal:** Hillstone's CloudView, a cloud-based security management system, offers monitoring-only capabilities, confining the centralized product changes and upgrade management to an on-premises centralized manager only.

- **Feature:** Hillstone firewalls lack support for TLS 1.3, and do not support the selective SSL decryption feature based on selective categories.

- **Feature:** Hillstone firewalls offer basic firewall optimization features, limited only to duplicate objects and rule hits, whereas other vendors are enhancing this feature to offer more recommendations to administrators to fine-tune and optimize the configurations.

- **XDR:** Although Hillstone offers partnerships with global and regional EDR vendors, it offers basic integration. The vendor lacks a native EDR client and does not offer XDR capabilities.

Huawei

Huawei is a Challenger in this Magic Quadrant. It sells two separate firewall product lines: the USG and the Eudemon series.

Major features introduced this year are enhancements to threat detection, and SD-WAN and access management capabilities based on integrated risk assessment.

Huawei firewalls are a good shortlist candidate for clients looking for a complete firewall solution at competitive pricing primarily in Southeast Asia, Europe and Latin America. Also, Huawei firewalls are a good candidate as a part of large Huawei infrastructure deals, from a consolidation point of view.

Strengths

- **Product:** Huawei firewalls offer a CASB-like feature called cloud access security awareness, which enables administrators to manage access to cloud-based SaaS applications. This makes management of SaaS applications easier for administrators.

- **Price:** One of the primary selection criteria many Gartner clients cite for Huawei firewalls is its competitive price versus performance ratio. The vendor offers simple bundle-based subscriptions that are cost-effective and bring down the TCO as compared to many other competitors in the space.

- **Product strategy:** The vendor offers identity access management through a risk assessment model that uses its security orchestration, analytics and reporting (SOAR) and firewall. This involves third-party identity and access management (IAM) that can be integrated with the SOAR, enabling risk assessment for users. Access control is defined on the firewalls.

- **Market execution:** Huawei introduced its direct MSS services, especially targeted toward SMB clients, with managed detection and response (MDR) capabilities. This service is offered by the vendor using its native suite of security products and firewall. It will be useful for clients seeking managed firewall service directly from the vendor.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering. The cloud-based management offered for its firewalls provides basic administration features.

- **Market understanding:** The vendor lacks a strong product strategy around cloud security. It does not offer any cloud-based security services to clients. Huawei firewalls are also not available as PAYG on any public cloud platform. This makes the vendor a less desirable shortlist candidate for enterprises with hybrid environments.

- **Product strategy:** The vendor does not have a big partner ecosystem; as a result, the firewall does not offer integration with common security vendors, other than limited regional vendor partnerships such as with Jiangmin, Tencent and Bamboo.

- **Market execution:** The vendor does not offer a native EDR client; hence, it lacks XDR capabilities. Huawei firewalls do not offer direct integration with third-party EDR vendors, and the vendor has partnerships with only two regional EDR vendors, Jiangmin and Tencent, through its CIS platform.

Juniper Networks

Juniper Networks is a Challenger in this Magic Quadrant. Its firewall product line is SRX. It also offers Contrail Security Orchestration (CSO) as a service, which is sold as part of the vendor's FWaaS offering.

Major features introduced recently are SecIntel, Juniper's distributed threat intelligence (TI) shared between SRX firewalls, switches, routers and access points (APs) enhancements around IoT security; enhanced support for public cloud; support for 5G; and network security enhancements.

Juniper firewalls meet all the firewall deployment use cases, including containers. Juniper firewalls are a good shortlist candidate for network teams looking to consolidate network and firewall components with a single vendor.

Strengths

- **Product strategy:** Juniper Connected Security is the vendor's product strategy that focuses on integration of its network product lines with its firewalls. In addition to centralized management and reporting, Juniper introduced a shared TI offering called SecIntel, which is integrated with Juniper's SRX, MX, EX/QFX and Mist AP product lines.
- **Market execution:** Juniper firewalls are available as PAYG on multiple public IaaS platforms such as AWS, Microsoft Azure, IBM Cloud and Google Cloud Platform, making it one of the few firewall vendors supporting maximum public IaaS platforms as PAYG. Its container-based firewall, cSRX, is available on the AWS container marketplace.
- **Offering:** Juniper's Junos Space Security Director offers mature firewall policy orchestration and reporting capabilities. It has multiple different policy filters to provide search based on different objects, including metadata/security tags. It also offers an intuitive reporting dashboard where the highest-consuming applications can be directly blocked through the monitoring dashboard display.
- **Scalability:** While Juniper offers high-throughput firewalls, its Junos Space Security Director centralized manager can scale to manage a large number of different Juniper devices, including switches and routers.

Cautions

- **Market execution:** While other network security vendors in the market are expanding their security product portfolios through acquisitions, Juniper is not. It primarily works through vendor partnerships for offerings like network access control (NAC), EDR, NTA, etc., instead of expanding outside SRX firewalls.
- **Product strategy:** Juniper continues to promote itself as a network-centric vendor. It has a continuous product strategy that works toward integration of SRX firewalls with its other Juniper network products. This makes it a desirable candidate for network teams as opposed to security teams.
- **Feature:** The vendor's application control feature is still not rated high compared to its competitors. It lacks granularity and offers limited subcontrols for many applications. It is recommended that clients evaluate the level of controls to make sure it meets their requirements.
- **Offering:** Juniper continues to offer multiple different centralized managers with distinct features, including Junos Space Security Director, Juniper Sky Enterprise and Juniper Contrail Service Orchestration. This requires clients to use multiple management tools based on their use cases.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. It offers a firewall as part of its Azure networking services. Azure Firewall can be managed and monitored by the vendor's built-in tools or by third-party network security policy management solutions.

In the last year, Microsoft released Azure Firewall Manager, its centralized firewall policy management solution. Microsoft Azure Firewalls have attained the ICSA Labs Corporate Firewall Certification. The vendor also added support for multiple public IPs and availability zones, including the "four nines" SLA. The firewall also supports more NAT configurations, and Azure IP groups can be included in the firewall rules and multiple other network related features.

Azure Firewall remains a good shortlist candidate for enterprises automating their Azure infrastructure.

Strengths

- **PaaS:** Azure Firewall is fully integrated with the Azure platform, starting with the on-demand pricing. The product includes built-in high availability, auto-scaling and availability zone support. Azure Firewall leverages Microsoft Threat Intelligence Cloud.

- **Roadmap execution:** The vendor has shown that it delivers new features as planned, but takes the time for a long beta before making a feature generally available.

- **Centralized management:** Azure Firewall Manager, the centralized policy portal, allows rules to be deployed across multiple Azure Firewall instances, with support for global and local policies. The firewall can forward the web traffic to third-party secure web gateway (SWG) products. Migration of such rules is facilitated by importing policies from individual Azure Firewall configurations.

- **Geographic presence:** Microsoft Azure is a global IaaS infrastructure with strong resiliency and stringent SLAs, making it easier for distributed organizations to deploy firewalls close to all their local points of presence.

Cautions

- **Product strategy:** Azure Firewall is a recent purpose-built product intended to meet Azure's IaaS client needs. It lacks many features that stand-alone firewall providers have included for years, such as URL filtering or IDPS. The vendor does not rush to achieve a comprehensive feature set, but releases improvements regularly.

- **Ease of use:** Security teams lacking Azure operation skills report that configuring the firewall using the standard UI looks more difficult than with the vendor's appliance-based competitors. They specifically mention that the firewall policy lags behind the competition.

- **Feature:** Azure Firewall does not decrypt TLS traffic and lacks cloud-delivered sandboxing for file inspection. It only supports IPv4.

- **Customer feedback:** Clients adopting multicloud find that adopting a third-party firewall vendor common across public cloud vendors is operationally easier than developing expertise in native public cloud firewall skills.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Along with selling firewalls as hardware and virtual appliances, the vendor also offers FWaaS, via Prisma Access.

This year, Palo Alto Networks announced the acquisition of CloudGenix, a cloud-based SD-WAN vendor. The vendor also introduced SD-WAN, support for TLS 1.3, and other feature- and product-related updates.

Palo Alto Networks' firewall is a good shortlist candidate for clients looking for a firewall with premium subscriptions at a premium price. With a broad product portfolio, the vendor also can be a good candidate for clients looking to consolidate with a single vendor for their various security requirements.

Strengths

- **Market execution:** Palo Alto Networks was an early hardware firewall vendor introducing FWaaS in the market. Recently, it introduced DLP to Prisma Access. The vendor's hybrid network firewall clients use Prisma Access for their remote users and branch office setups.
- **Sales strategy:** Palo Alto Networks offers flexible ELA and ESA deals. These are becoming popular with clients interested in procuring different product lines with multiyear deals, leading to easy-to-consume licensing models for clients making large deals with the vendor.
- **Product:** Palo Alto Networks firewalls offer strong granular application controls for social media applications and an application-usage-based policy optimization feature. Gartner clients often highlight granular application control as one of the primary reasons for shortlisting the firewall. The firewall offers TLS usage monitoring for traffic across different versions of TLS.
- **Market responsiveness:** The vendor shows a strong focus on cloud security — the Prisma product line is focused on it. The offering includes different security products, including microsegmentation, FWaaS and CWPP.

Cautions

- **Pricing:** Palo Alto Networks continues to be one of the most expensive vendors in the firewall market. Gartner clients are often dissatisfied with the renewal cost, which does not come with similar discounts received on support and services when buying the firewall for the first time. This makes the TCO higher and, in a few cases, clients are switching to a less expensive vendor.
- **Offering:** The vendor lacks a direct cloud-based centralized manager offering for its firewall appliances. It offers an on-premises centralized manager, Panorama, which can also be deployed in the cloud by the client.

- **Offering:** Despite the vendor offering multiple security product lines, most of them have a dedicated management interface for administration, thus they work as stand-alone products. Gartner clients using multiple Palo Alto Networks' product lines beyond firewalls often highlight the lack of a centralized management interface as a drawback.
- **Customer feedback:** Clients have reported scalability issues with large Prisma Access deployments beyond 60,000 users. Also, clients report connectivity issues with Prisma Access in a few places, such as the Asia/Pacific region and Latin America.

Sangfor

Sangfor is a Niche Player in this Magic Quadrant. Its firewall product line is called Sangfor Next Generation Application Firewall (NGAF), available in the form of physical and virtual appliances.

Major features rolled out this year include the introduction of XDR, NTA and UEBA in Cyber Command with endpoint automation; Platform-X, a cloud-based centralized manager; and a network policy configuration optimization feature.

Sangfor shows a strong cloud security vision and product strategy with multiple SaaS-based security services. It is an ideal shortlist candidate for enterprises that want to consolidate with a single vendor for multiple security needs.

Strengths

- **Product portfolio:** Sangfor offers a large security product portfolio. FWaaS is offered via Sangfor Cloud Shield. Other than firewalls, the vendor offers an SSL VPN appliance, IAM, endpoint security, mobile device management, advanced treat detection and a security management solution. Consulting and MDR services are also offered. All this makes it a good shortlist candidate for enterprises looking to consolidate with a single vendor.
- **Market responsiveness:** Sangfor is one of the few Chinese firewall vendors showing a strong cloud security vision. Sangfor firewalls support AWS Global, AWS in China, Azure, Alibaba Cloud, Tencent Cloud, Huawei Cloud and Sangfor HCI/XY clouds. The vendor offers different SaaS-based security services, cloud-based vulnerability assessment (cloud VA), cloud-based WAF (cloud WAF), cloud-based anti-DDoS (in cooperation with Tencent) and a cloud-based SWG (ISSP), which are more globally adopted as opposed to hardware appliances.
- **XDR:** Sangfor introduced XDR capabilities this year. Sangfor XDR (Cyber Command) integrated NTA and UEBA capabilities with Sangfor NGAF. The vendor offers a centralized log and event management center for firewalls, endpoints and SWGs. The XDR also provides an endpoint host block and quarantine through firewall. Sangfor also offers Platform-X, its cloud-based threat correlation platform.
- **Market execution:** The vendor offers MDR directly to end users as a part of its MSS offering. It also offers the Cloud Eye service, which can actively and continuously detect assets of users and provide

continuous risk assessment, real-time monitoring, tampering disposal and emergency confrontation services for internet service.

Cautions

- **Offering:** The vendor does not have a PAYG firewall offering on Alibaba Cloud, which is one of the largest public IaaS providers in the region. In fact, Sangfor firewalls are only available as PAYG on the Sangfor HCI cloud.
- **Geographic presence:** The vendor continues to have a major presence in China, and a very limited presence in other parts of Southeast Asia.
- **Sales execution:** Despite having higher-end firewall models, Gartner finds Sangfor to be more prominent in the midsize use case as opposed to other firewall use cases.
- **Sales execution:** Despite a broad product portfolio, Gartner does not find vendor sales teams promoting ELA deals to customers that encourage end users to consolidate for multiple security products with Sangfor. Gartner has found more a la carte contracts and quotations from the vendor, and Sangfor offering bundled pricing models.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. The vendor offers multiple firewall product lines, branded as TZ Series, NSA Series, SuperMassive Series, NSsp Series and NSv Series.

Recent company news includes the introduction of new models in the TZ Series and a new operating system featuring multi-instance multitenancy and on-premises ATP appliances. In addition, SonicWall launched NSv for KVM, expanded PAYG models, and introduced low-cost virtual firewall models for public cloud. Other updates include product- and feature-related enhancements.

SonicWall is a suitable shortlist candidate for midsize enterprises that seek an easy-to-install firewall with a wide range of security features at a good value. Customers with public cloud use cases should evaluate whether support for Azure and AWS only is enough.

Strengths

- **Offering:** Capture Security Center (CSC), the vendor’s cloud-based manager, offers a complete set of centralized management for all its products, and offers features such as a bulk firmware upgrade and a pushing of rules. Customers often mention ease of deployment and configuration using the zero-touch deployment feature integrated within CSC.
- **Product:** SonicWall’s on-premises centralized manager, Global Management System (GMS) and cloud-native Network Security Manager (NSM), offers mature management and multitenancy features desired by MSSPs. Like CSC, in addition to managing firewalls, GMS can also manage and report on SonicWall’s Secure Mobile Access and email security, integrated SonicWall wireless access points,

switches, and WAN acceleration solutions, offering centralized management capabilities for multiple product lines.

- **Feature:** Customers value the wireless features embedded in the firewall and available separately, They comment on the value of all products — specifically wireless — being managed in one console.
- **CASB:** SonicWall offers CASB capabilities in SonicWall Cloud App Security (CAS). It offers security for SaaS applications such as Office 365 and G Suite by offering cloud-based email scanning and access controls, and preventing the upload of sensitive or confidential files and data.

Cautions

- **Sales execution:** While SonicWall's product portfolio has added much more offering breadth and feature depth, its firewalls are not particularly visible on Gartner client shortlists.
- **Market execution:** The vendor lacks an FWaaS offering, making it a less-desirable shortlist candidate for the distributed enterprise use case, and those that want to move away from appliance-based firewalls and remote working use cases seeking FWaaS capabilities.
- **Cloud security:** Despite introducing multiple virtual appliances, the vendor's firewalls still lack support for Cisco ACI, something that is offered by most of its competitors in the market. SonicWall also offers limited support for public IaaS platforms, with support only for AWS as PAYG.
- **Customer feedback:** During the evaluation period, customers mention some difficulty and delay in getting Level 1 support calls answered, although they are more satisfied with the quality of premier support.

Sophos

Sophos is a Visionary in this Magic Quadrant. Its firewall product line is XG.

During this evaluation period, Sophos introduced the Xstream architecture (Xstream SSL Inspection, Xstream DPI Engine and Xstream Network Flow FastPath). Other new features include enhancements to improve SD-WAN capabilities, advanced threat detection and central management.

Sophos continues to lead the market with its XDR capabilities between firewall and endpoint security products. It is prominent in midsize use cases. The vendor wins deals primarily because of its XDR capabilities, cost savings and ease-of-use capabilities.

Strengths

- **Offering:** Sophos continues to enhance its TLS 1.3 decryption performance and threat detection lead among its midsize-enterprise-competitive cohorts. It supports software-based TLS decryption with end-to-end TLS 1.3 decryption, without downgrade, and includes a comprehensive exception list in its default configuration.

- **Market execution:** Sophos offers cloud-native policy control with Cloud Optix through a separate offering. It also offers the Managed Threat Response service directly to end users.
- **Sales execution:** Sophos highly promotes its mature XDR capabilities and wins deals by offering easy pricing models and huge cost savings on the TCO of both firewalls and endpoint security, and a bundled deal. These days, it is also packaging its MDR services, making Sophos an ideal security vendor for midsize organizations.
- **Product:** Sophos continues to lead in the XDR use case as compared to other firewall vendors with similar offerings, but lacks advanced integration and automation. It shares threat- and health-related intelligence between endpoints and firewalls using the Synchronized Security feature to correlate and identify compromised systems, enabling firewalls to automatically isolate the infected endpoints.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering, making it a less favorable shortlist candidate for remote working and for enterprises that want to switch to FWaaS for their branch offices.
- **Visibility:** Sophos firewalls are not frequently seen on Gartner SMB clients' shortlists and have reduced visibility as compared to other direct competitors in the market.
- **Product strategy:** The vendor continues to focus on midsize enterprise use cases and has no visibility in enterprise edge use cases, despite offering high-throughput models. Sophos also offers limited firewall support for public IaaS and does not seem to have a strong product strategy around it.
- **Sales execution:** Sophos firewalls are more often being shortlisted when bundled with the vendor's endpoint security, rather than for firewall-only deals. With other vendors also offering endpoint security products, gradually Sophos will have to be more innovative and explore other firewall use cases beyond XDR.

Stormshield

Stormshield is a Niche Player in this Magic Quadrant. Other than firewalls, the vendor offers Stormshield Endpoint Security and Stormshield Data Security products. It also offers dedicated industrial firewalls, SNi40 and SNi20.

Major updates to Stormshield's firewalls are firmware performance improvements and other enhancements related to firewall security features.

Stormshield firewalls are good shortlist candidates for SMBs, especially government clients in Europe due to their European certifications and OT security use case. Being local to the European region, the vendor offers strong regional support.

Strengths

- **Product offering:** Stormshield offers vulnerability assessment as a firewall feature. It provides a view of assets in the networks, operating systems and applications run with its version, and provides a warning when a known vulnerability affects the installed OS/application version.
- **Product strategy:** The vendor offers a strong product strategy toward OT security. While Stormshield offers dedicated industrial firewalls in SNi40 and SNi20 (introduced in 2020), its IPS firewall feature covers a wide range of SCADA/ICS/IoT infrastructure protocols, such as BACnet/IP, CIP, Ethernet/IP and IEC 60870-5-104.
- **Product:** Stormshield offers an easy-to-use network firewall with a complete offering at competitive pricing. It offers multiple integrated features in its firewalls, making it a suitable shortlist candidate for SMBs. The vendor offers built-in DLP features for web and email files, with end-to-end encryption. Broad coverage of OT protocols and an integrated vulnerability management feature make this offer unique compared to many other direct competitors in the market.
- **Feature:** Stormshield firewalls utilize external reputable third-party indicators of compromise for their cloud-based sandboxing service as a third-party source, instead of relying solely on their native TI.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering for remote users and distributed offices that want to use cloud-based services instead of firewall appliances.
- **Product strategy:** Stormshield firewalls lack a strong focus on cloud security. They are not available as PAYG on any public cloud platforms. The vendor also lacks a cloud-based management portal for its firewalls.
- **Offering:** The centralized firewall manager lacks multitenancy features desirable for MSSs. Features such as policy optimization are not offered. Stormshield firewalls do not support TLS 1.3 decryption.
- **Market execution:** Despite being an Airbus subsidiary, Stormshield is relatively slower in introducing new product updates and enhancements as compared to other competitors, as more international firewall vendors are competing with regional players. The vendor has a European presence that is more concentrated toward certain regions with limited use cases.

Venustech

Venustech is a Niche Player in this Magic Quadrant. It sells multiple firewall product lines, including Venusense Unified Threat Management, Venusense WAF and Venusense NGFW. It also sells a dedicated industrial firewall product line, Venusense IFW.

This year, Venustech introduced SD-WAN capabilities, an NGFW based on ARM and VCloud SaaS. It also developed enhancements to its industrial security offering.

Venustech is a good shortlist candidate for enterprises in China that want to consolidate with a single vendor for their different security products. It offers high-throughput firewalls at competitive pricing ideal for enterprise edge and data center use cases.

Strengths

- **Feature:** Venustech offers granular DLP feature support for endpoints, web and email traffic; it comes as a separate subscription. Detection methods include keywords, regular expressions, file attributes, file fingerprints, classification fingerprints and mail recipients.
- **Market execution:** Venustech continues to focus on industrial security use case. The vendor offers a dedicated IFW product line with different models. IFW offers support for in-depth filtering based on Modbus/TCP, Modbus/RTU, nIEC104, OPC and Ethernet/IP, and provides enhanced feature support beyond basic firewall features.
- **Centralized firewall policy management:** Venustech's Venusense FlowEye is the vendor's firewall policy management and NTA solution. The product can perform centralized firewall policy management beyond Venustech firewalls, extending support to all leading global and regional firewall players such as Fortinet, Check Point Software Technologies, Palo Alto Networks, Juniper Networks, Cisco and H3C.
- **Product strategy:** The vendor has a TI correlation platform that is a separate product, called VenusEye Threat Intelligence Center. This platform correlates TI from different VenusEye resources and products, and offers centralized correlation and threat scoring based on built-in templates. This product has a direct integration with the Venustech firewall from within the administration UI, which makes it easy to use for firewall users that require additional TI.

Cautions

- **Public cloud:** Venustech firewalls lack support for public IaaS platforms, while most firewall vendors offer it. The vendor also does not offer a direct FWaaS offering.
- **Offering:** The vendor only offers an on-premises sandboxing appliance and lacks cloud-based sandboxing services, which most competitors offer as an add-on subscription.
- **TLS decryption:** Venustech firewalls do not offer TLS traffic decryption. It claims to use TI and certificate-based inspection.
- **Geographic presence:** Venustech primarily sells its products in China and has a limited presence in Japan; however, the vendor is trying to expand in Southeast Asia.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. Its portfolio of security products and services includes the following firewalls: Firebox; Firebox T35-R, the industrial firewall model; FireboxV and Firebox Cloud. Additional offerings include multifactor authentication, endpoint and wireless product lines.

Major updates include the addition of Access Portal (reverse proxy), Firebox system management from WatchGuard Cloud, support for TLS 1.3 inspection and DNSWatchGO.

WatchGuard is a good shortlist candidate for SMBs looking for a complete firewall solution that is easy to use and has simplified pricing.

Strengths

- **Market execution:** As WatchGuard recently completed the acquisition of Panda Security (and its server and endpoint security), this broadens its portfolio toward mature endpoint security, as opposed to the basic endpoint security client it currently has. Clients must check the integration timelines of this newly acquired vendor with WatchGuard firewalls and Panda's security. As of now, Panda products are being sold as stand-alone offerings by WatchGuard.

- **Offering:** The vendor offers the Threat Detection and Response cloud-based threat correlation portal. This portal offers combined TI-based analytics through WatchGuard's current endpoint agent, host sensor and firewall, combining network and endpoint-based events. This feature also offers automation through which infected hosts isolate themselves from the network.

- **Customer feedback:** Clients often cite pricing with simplified bundled licensing and ease of use as the primary reasons to shortlist the vendor's firewalls. Firebox is bundled with one of two security service packages: Total Security Suite or Basic Security Suite.

- **Offering:** The vendor offers DNSWatchGO as a stand-alone cloud-based service. The addition of DNSWatchGO allows companies to add recursive DNS-level protection from a single vendor without having to deploy additional hardware or services.

Cautions

- **Offering:** The vendor lacks an FWaaS offering. This makes it a less desirable shortlist candidate for enterprises looking to move toward FWaaS for remote work and branch office use cases, as opposed to an appliance-based approach.

- **Product:** The vendor lacks a mature cloud-based management portal. The current offering is WatchGuard Cloud, which is primarily focused on monitoring and reporting.

- **Market execution:** While the direct competitors of WatchGuard have been moving beyond firewalling capabilities to lead in overlapping use cases like public IaaS and mature distributed offices, WatchGuard has been primarily focusing on providing firewalls for SMB use cases only. However, the recent Panda Security acquisition can help WatchGuard expand beyond firewall use cases and offer overlapping capabilities based on an integration product strategy and timelines.

- **Sales execution:** Despite being a global vendor, WatchGuard firewalls are not frequently seen shortlisted by Gartner clients as compared to direct competitors. It has more end-user visibility in the North American region, and is rarely seen in Asia/Pacific region firewall deals for SMBs.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No vendors were added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

Vendors that provide network firewall functions that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have assessed that the vendor can effectively compete in the network firewall market.
- Gartner has determined that the vendor is a significant player in the market, due to market presence, competitive visibility and/or technology innovation.
- The vendor demonstrates a competitive presence in enterprises and sales for enterprise and/or cloud networks.
- The vendor must meet the firewall revenue criteria of $30 million in 2019, as applicable to vendors selling firewall hardware appliances/virtual firewalls/FWaaS. In the case of IaaS vendors, at least 50% of the installed base should be using the native firewall controls offered by them.
- The vendor must demonstrate minimum signs of a global presence, including:
  - Gartner received strong evidence that more than 10% of its customer base is outside its home region.
  - It offers 24/7 direct support, including phone support (in some cases, this is an add-on, rather than being included in the base service).
  - The vendor appearing in Gartner client inquiries, its competitive visibility, its client references and its local brand visibility are considered to determine inclusion.

Vendors must provide evidence to support meeting the above inclusion requirements.

Evaluation Criteria

Ability to Execute

Product or Service: This includes service and customer satisfaction in network firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a vendor has demonstrated to Gartner analysts that its products are successfully and continually deployed in enterprises and/or cloud environments, and that the vendor wins a large percentage in competition with other vendors.

Vendors that execute strongly generate pervasive awareness and loyalty among Gartner clients, and also generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a vendor's Ability to Execute. While sales are a factor, winning in competitive environments through innovation and quality of product and service are more important than revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency and secondary product capabilities (logging, event management, compliance, rule optimization and workflow). Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery or enabling firewall functions for additional workloads in cloud environments, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise/cloud needs.

Overall Viability: This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (which are compared with Gartner data on such competitions held by our clients), and devices or instances in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Rather, we consider the use of these firewalls to protect the key business systems of enterprise clients and those being considered on competitive shortlists.

Sales Execution/Pricing: We evaluate the vendor's pricing, deal size, installed base and, in the case of cloud vendors, the number of customers using native firewall controls. This includes the strength of the vendor's sales and distribution operations. Presales and postsales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, and includes the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains, and think in terms of value over sheer low cost.

Market Responsiveness/Record: This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in demand for new features and form factors in the firewall market, and how enterprises deploy network security. The criterion will also cover the capability of the vendor in securing hybrid networks and/or cloud networks because of rapid adoption of these networks.

Marketing Execution: Competitive visibility is a key factor; it includes which vendors are most commonly considered to have top competitive solutions during the RFP and selection process. In addition to buyer and analyst feedback, this criterion looks at which vendors consider the others to be direct competitive threats, such as by driving the market on innovative features co-packaged within the firewall, or by offering innovative pricing or support offerings. Unacceptable device or software failure rates, vulnerabilities, poor performance and a product's inability to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

Customer Experience: This criterion evaluates products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions technical support or account support. Quality and responsiveness of the escalation process and transparency are important. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet goals and commitments. Factors include: quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. These also include management experience and track record, and the depth of staff experience — specifically in the security marketplace. Gartner analysts also monitor repeated release delays, frequent changes in strategic directions and how recent organizational changes might influence the effectiveness of the organization.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (November 2020)

Completeness of Vision

Market Understanding: This criterion looks at the ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market listen, understand customer demands, and can shape or enhance market changes with their added vision.

This includes providing a track record of delivering on innovation that precedes customer demand, rather than an “us too” roadmap. We also evaluate the vendor’s overall understanding of and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research.

Vendors cannot merely state aggressive future goals; they must also put plans in place, show that they are following their plans and modify those plans as they forecast how market directions will change. Understanding and delivering on network firewall realities and needs are important, and having a viable and progressive roadmap and continuing delivery of innovative new features are weighted very highly. The new capabilities are expected to be integrated to achieve correlation improvement and functional improvement.

Marketing Strategy: This criterion evaluates whether the vendor has clear, differentiated messaging consistently communicated internally, and externalized through social media, advertising, customer programs and positioning statements.

Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detecting events, including zero-day events and other advanced threats. Building loyalty through credibility with a full-time network firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security and/or cloud workload buying center correctly, and they must do so in a technically direct manner, rather than just selling fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on network security.

Offering (Product) Strategy: This criterion focuses on a vendor's product roadmap and current features, such as network firewall feature integration and enhancement, virtualization, cloud security services, support for "work from home" environments, and performance. Integration with other security components is also weighted, as well as product integration with other IT systems. Innovation, such as introducing practical new forms of intelligence to which the firewall can apply policy, is highly rated. An articulated, viable strategy for addressing the challenges in software-defined network (SDN) deployments and microsegmentation across hybrid environments is important, as it is evidence of execution within cloud and virtualized environments.

Business Model: This includes the process and success rate for developing new features and innovation. It also includes R&D spending.

Innovation: This includes R&D and quality differentiators, such as:

- Performance, which includes low latency, new firewall mechanisms, and achieving high throughput and low appliance latency.
- Firewall virtualization and securing virtualized environments. This includes public and private cloud environments, and support for work-from-home environments.
- Integration with other security products (native and third party) and microsegmentation capabilities. This also includes features and a roadmap showing strong integration capabilities to offer XDR across hybrid environments.
- Management interface, cloud-based management portal and clarity of reporting — that is, the more a product mirrors the workflow of the enterprise/cloud operation scenario, the better the vision.
- "Giving back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity.
- Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this criterion.

Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Geographic Strategy: This criterion evaluates the vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (November 2020)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that build products that fulfill enterprise requirements around firewalls. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rule/policy minimization. These vendors have led the market with innovation. They are quicker to respond to the end-user market. They meet all the firewall deployment use cases. They have a large market share. Vendors in this quadrant lead the market in offering new features that protect customers from emerging threats; meet the requirement of evolving hybrid networks, including public and private cloud; provide expert capability rather than treat the firewall as a commodity and have a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss, offering options for hardware acceleration, support for private and public cloud platforms, and offering form factors that protect enterprises as they move to new infrastructure form factors.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not consistently leading with differentiated next-generation capabilities. Many Challengers have not fully matured their firewall capability — or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challengers' products are often well-priced and, because of their strength in execution, these vendors can offer economical security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they choose to place security or firewall products at a lower priority in their overall product sets. Firewall market Challengers will often have significant market share, but trail smaller market share leaders in the release of features.

Visionaries

Visionaries lead in innovation, but are limited to one or two firewall deployment use cases. They have the right designs and features, but lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Sometimes, it is a conscious decision of the vendor to only focus on limited firewall use cases rather than all of them. Most Visionaries' products have good NGFW capabilities, but lack in performance capabilities and support networks. The vendors in this quadrant show strong vision and market-leading innovation in use cases such as automated east-west microsegmentation in public cloud and SDN environments, and innovative threat detection automation capabilities.

Niche Players

Most vendors in the Niche Players quadrant have a prime installed base or are prominent in a particular use case, such as data centers or telcos, distributed enterprises, SMBs, and public IaaS. Some of these vendors that offer a firewall as a module with their other services/components consciously focus on a particular use case. Vendors in this quadrant lack in execution because of a limited client base and do not show innovation. Some Niche Players are confined to particular regions and are not present in other regions.

Context

The firewall vendors are expanding their product portfolios to other security product lines, offering an attractive consolidation proposition to enterprises. While consolidation offers pricing simplicity, end users have to be mindful of the feature limitations, integration and centralized management limitations that come with such a consolidation. Firewall vendors are racing to broaden their portfolios. introducing products that are not mature enough to compete with stand-alone products that are also lacking integration and centralized management in their product lines.

Market Overview

In 2019, worldwide market network firewall revenue grew by 11.1%, compared to 15.9% in 2018. As the COVID-19 pandemic has impacted the world and businesses, enterprises faced a major challenge to support work from home for all their full-time office employees, which required some immediate upgrades to infrastructure, which also impacted the firewall market positively. The impact of the shift to work from home on the firewall market, as observed by Gartner based on end-user inquiries from Gartner clients, includes:

- Hardware upgrades: The immediate impact on firewalls of employees working from home was the need for hardware upgrades of the existing data center firewalls to meet the sudden spike in inbound traffic through the VPN. This required the firewall vendors to offer high-performing hardware firewalls.
- Adoption of FWaaS: There was a growth in adoption of FWaaS, for faster onboarding and setup of work-from-home employees' access. Clients that were in the process of evaluating FWaaS adopted it smoothly. Enterprises that already had a security vendor offering FWaaS in their infrastructure adopted FWaaS or continue to evaluate it.
- Cloud adoption: This situation has accelerated adoption of cloud and, as a result, enterprises are seeking cloud security solutions and shortlisting firewall vendors with a strong cloud security focus and that offer cloud security solutions in their portfolio.
- Move toward zero trust network access (ZTNA): With remote working and adoption of cloud, enterprises are looking to enable ZTNA for a modern style of remote access. As a result, this consolidation also moves organizations toward network security vendors offering microsegmentation and FWaaS offerings as well.
- Cost optimization: As a result of the economic recession, businesses are demanding cost optimization outcomes while still securing their infrastructure, which included them consolidating their branch offices and migration toward cloud for their shared resources. This change in infrastructure requires enterprises to adopt different security architectures and the products that enable them. As a result, vendor consolidation and ELA cost-saving contracts are attractive value propositions for businesses today.

Due to all the above factors, the following firewall vendor characteristics (in no particular order) are desirable for shortlists:

- Vendors having a strong cloud security product strategy
- Vendors offering strong integration and centralized visibility and management between their security product lines for ease of operation across hybrid environments, especially vendors offering mature XDR and integration cloud security management.
- Vendors offering FWaaS

- Vendors leading in price versus performance ratio of hardware firewalls
- Vendors offering cost-effective bundled licensing and technical support to reduce firewall TCO
- Vendors offering cost-effective ELA contracts for enterprises trying to consolidate toward a single vendor for their multiple security products/services
- Vendors offering mature threat correlation and automation actions with actionable recommendations

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Document Revision History

Magic Quadrant for Network Firewalls - 17 September 2019

Magic Quadrant for Enterprise Network Firewalls - 4 October 2018

Magic Quadrant for Enterprise Network Firewalls - 10 July 2017

Magic Quadrant for Enterprise Network Firewalls - 25 May 2016

Magic Quadrant for Enterprise Network Firewalls - 22 April 2015

Magic Quadrant for Enterprise Network Firewalls - 15 April 2014

Magic Quadrant for Enterprise Network Firewalls - 7 February 2013

Magic Quadrant for Enterprise Network Firewalls - 14 December 2011

Magic Quadrant for Enterprise Network Firewalls - 15 March 2010

Magic Quadrant for Enterprise Network Firewalls - 21 November 2008

Magic Quadrant for Enterprise Network Firewalls, 2H07 - 13 September 2007

Magic Quadrant for Enterprise Network Firewalls, 1H06 - 5 June 2006

Recommended by the Authors

How Markets and Vendors Are Evaluated in Gartner Magic Quadrants

ENDPOINT SECURITY (HTTPS://ENTERPRISE.COMODO.COM/BLOG/CATEGORY/ENDPOINT-SECURITY/?AF=7639)

ENDPOINT PROTECTION (HTTPS://ENTERPRISE.COMODO.COM/BLOG/CATEGORY/ENDPOINT-PROTECTION/?AF=7639)

What Is Endpoint Security? and Why Is It Crucial Today?

May 3, 2019 | By Comodo (https://enterprise.comodo.com/blog/?author=1&af=7639)
★★★★★ *(**721** votes, average: **4.97** out of 5)*

Endpoint security refers to the approach of protecting an endpoint business network when accessed by remote devices like smartphones, laptops, tablets or other wireless devices. It includes monitoring status, software, and activities.

The **endpoint protection software** is installed on all network servers and on all endpoint devices.

With the proliferation of mobile devices like laptops, smartphones, tablets, notebooks etc., there has been a sharp increase in the number of devices being lost or stolen as well. These incidents potentially translate as huge loss of sensitive data for enterprises which allow their employees to bring in these mobile devices (enterprise-provided or otherwise) into their enterprise.

To solve this problem, enterprises have to secure the enterprise data available on these mobile devices of their employees in such a way that even if the device falls into the wrong hands, the data should stay protected. This process of securing enterprise endpoints is known as endpoint security.

Apart from this it also helps enterprises successfully prevent any misuse of their data which they've made available on the employee's mobile devices. (Example: a disgruntled employee trying to cause nuisance to the enterprise or someone who may be a friend of the employee trying to misuse the enterprise data available on the device).

Endpoint Security Definition

Endpoint Security is often confused with a number of other **network security** tools like antivirus, firewall, and even network security. In this page, we list some of the differences between **endpoint security (or) endpoint protection** and the network against various evolving security threats of today.

Why Is It Called 'Endpoint' Security?

As you can realize, every device which can connect to a network poses a considerable danger. And as these devices are placed outside of the corporate firewall on the edge of the network using which individuals have to connect to the central network, they are called as endpoints. Meaning endpoints of that network.

As already stated endpoint can be any mobile device ranging from laptops to the notebooks of today, which can be connected to a network. And the strategy you employ in security these endpoints is known as ‘endpoint security’.

Endpoint Security Is Not The Same As Antivirus

Although the objective of endpoint security solutions (https://www.comodo.com/endpoint-protection/endpoint-security.php?af=7639) is the same – secure devices – there is a considerable difference between endpoint security and antivirus. Antivirus is about protecting PC(s), – single or many depending upon the type of antivirus being deployed – whereas endpoint security covers the entire picture. It’s about securing every aspect of the network.

Endpoint security usually includes ‘provisions for application whitelisting, network access control, endpoint detection and response’, things which are usually not available in antivirus packages. It can also be said that antivirus packages are simpler forms of endpoint security.

Endpoint Security Is Different For Consumers and Enterprises

Endpoint security solutions can be broadly classified into 2 different types. One for the consumers and the other for enterprises. The major difference between the two is that there’s no centralized management and administration for consumers, whereas, for enterprises, centralized management is necessary. This central administration (or server) streamlines the configuration or installation of endpoint security software on individual **endpoint devices** and performance logs and other alerts are sent to the central administration server for evaluation and analysis.

What Do These Endpoint Security Solutions Typically Contain?

While there’s certainly no limit to what endpoint security can contain – and this list is only going to expand in the future – there are some applications which are core to any endpoint security solution. (Because, well, securing a network is altogether a different ball game from securing a computer).

Some of these applications are firewalls, antivirus tools, internet security tools, mobile device management tools, encryption, intrusion detection tools, mobile security solutions etc, to name a few.

Traditional Vs Modern Endpoint Security

This is a no-brainer. Yet something which needs to be pointed out. Because enterprises are often reluctant to changes. Even if it is for their own good. But endpoint security is one area where enterprises have no choice but to adopt the modern endpoint security. Because they are much more than just an **anti-malware tool** which can go a long way in securing your network against various evolving security threats of today.

Difference between Endpoint Security and Antivirus

Antivirus is one of the components of **endpoint security**. Whereas endpoint security is a much broader concept including not just antivirus but many security tools (like Firewall, HIPS system, White Listing tools, Patching and Logging/Monitoring tools etc.,) for safeguarding the various endpoints of the enterprise (and the enterprise itself against these endpoints) and from different types of security threats.

More precisely, endpoints security employs a server/client model for protecting the various endpoints of the enterprise. The server would have a master instant of the security program and the clients (endpoints) would have agents installed within them. These agents would communicate with the server the respective devices’ activities like the devices’ health, user authentication/authorization etc., and thus keep the endpoints secure.

Whereas antivirus is usually a single program responsible for scanning, detecting and removing viruses, malware, adware, spyware, ransomware and other such malware. Simply put, antivirus is a one-stop shop for securing your home networks, and endpoint security is suitable for securing enterprises, which are larger and much more complex to handle.

Difference between Endpoint Security and Network Security

Endpoint security is about securing your enterprise endpoints (mobile devices like laptops, smartphones and more) – and, of course, the enterprise against the dangers posed by these endpoints as well – whereas network security is about taking security measures for protecting your entire network (the whole IT infrastructure) against various security threats.

The main difference between endpoint security and network security is that in the case of former, the focus in on securing endpoints, and in the case of latter, the focus is on securing the network. Both types of security are important. Ideally, it's best to start from securing the endpoints and building out. You wouldn't leave the doors to your home open, just because there's a security guard out there, would you? In the same sense, both are important and should be given equal importance, starting from the endpoints and slowly building out.

In very simple terms, your network would be secure only if your endpoints are secured first. This you should make note of before starting to look for endpoint security and network security products.

Difference between Endpoint Security and Firewall

Firewalls are responsible for filtering the traffic flowing into and going out of your network based on 'a set of security rules'. Like, for example, restricting traffic flowing into the network from a particular potentially dangerous website. Whereas endpoint security concerns itself not just with network filtering but performs many other tasks like patching, logging, and monitoring etc., for safeguarding the endpoints.

Both antivirus and firewall are crucial elements of endpoint security. Their objective remains the same, though the model adopted (client/server model) and the number of computers they protect differ. And within the endpoint security model, operating with other security tools, they become even more efficient.

Difference between Endpoint Security and Endpoint Protection

Both are pretty much the same. Their primary objective is the same – to safeguard the endpoints as well as the enterprise against the dangers they pose. But there is a subtle difference. Endpoint security usually refers to an on-premise solution. Whereas **Endpoint Protection** refers to a cloud-based solution.

An on-premise solution is a solution which has to be installed on the network for deployment and a cloud-based solution is one which is available in the cloud and enterprises have to subscribe to it.

Windows 10 and Endpoint Security

Windows 10 although proclaimed to be the safest Windows OS is not without its flaws. Security experts have proved that the in-built security features of Windows like Windows Defender, Firewall etc., too are proving ineffective. Therefore enterprises making use of Windows 10 OS need endpoint security for safeguarding the various endpoints which connect to the network and for safeguarding the network itself.

Why Your Windows – Not Just Windows 10 – Needs Endpoint Security?

Inbuilt Windows Security is never going to be sufficient. Because the security attack vectors of today are just too many to be handled. Which means we no longer live in a world where e-mail attachments or web downloads are the only sources of malware infection. Simply put, your windows OS needs additional layers of protection in the form of antivirus for windows or, maybe, much more, depending on your requirements.

With this in mind, let's take a look at how you can protect your Windows OS from various security threats:

1. **Keep Your Windows OS Up-to-Date:** Today it's Windows 10. Tomorrow there'll be another new version. Whatever it may be, ensure your PC is updated to the latest version. This is probably the next best thing you can do apart from providing antivirus for windows. Because the latest update is usually the one which safeguards users against all known security vulnerabilities.
2. **Ensure Other Applications Are Up-to-Date:** What's inside of your Windows OS too matters. We mean other main programs and applications. Ensure all of them are updated and contain the latest security patches. Because it's a well-known fact that hackers try to exploit popular software like Java, Adobe Flash, Adobe Acrobat etc.,
3. **Use Proactive Security Solution:** Unfortunately traditional antivirus alone is not going to be enough. Especially when it comes to combating modern-day malware which employs sophisticated methods. Therefore to tackle the ever-changing cybersecurity threat landscape, users need proactive security solutions like internet security (for home users) and endpoint protection (for enterprises).
4. **Use Local Account Instead Of Microsoft Account:** If you are using Windows 10, it's best to avoid Microsoft account and instead opt for a Local account, as using Microsoft account means saving some of your personal details on the cloud, which is not such a wise thing to do. To opt for a local account, visit: Settings>Accounts>"Your info and select 'Sign in with a local account instead".
5. **Keep User Account Control Always Turned On:** UAC (User Account Control) is a Windows security responsible for preventing unauthorized changes (initiated by applications, users, viruses or other forms of malware) to the operating system. It ensures changes are applied to the operating system only with the approval of the administrator. Therefore keep it turned ON always.
6. **Perform Regular Back-Ups:** Prepare yourself with the 'worst' in mind when it comes to dealing with security threats. Therefore perform regular backups of your system (both online and offline) so that all your data is not lost in case your PC(s) are badly affected by security threats or encounter an irreparable hardware issue.
7. **Keep Your Browser Updated:** Browsers are what we use to access the internet. Therefore security vulnerabilities in them mean entry path for security threats. Therefore, just as with OS and other applications, keep your web browser updated as well. Other security measures you can take: 1) opt for private browsing mode to prevent sensitive details from being stored 2) prevent or block pop-ups 3) configure web browser security settings to improve security etc.,
8. **Turn Off Location Tracking:** If you are using Windows 10 or any other version which contains Location Tracking, it's best to turn it Off or use it only when it is absolutely necessary. For example, if you want to know about the local weather or the various shops nearby etc., To turn off Location Tracking, go to Privacy >> Location >> click Change button and move the slider from On to Off.
9. **Use The Internet Wisely:** All of the security measures listed here would become useless if you don't exercise caution while online. Therefore ensure you don't click on dangerous looking links, download malicious email attachments or other web downloads, avoid visiting suspicious looking websites and any other action which the current security practices deem as unwise.

Windows OS is probably the best and that is why it is hugely popular and has so much following – despite the security threats. And there's nothing wrong with sticking to your favorite OS. Just ensure you beef it up with the right security products like Comodo Endpoint Protection and follow the security best practices. These will ensure your Windows OS stays safe no matter what.

About Comodo Advanced Endpoint Protection (AEP)

Comodo Advanced Endpoint Protection (AEP), which comes equipped with impressive security features, is the best endpoint protection or security tool available in the IT security market. Backed by Containment technology, all the unknown (and therefore suspicious) files are run within virtual containers without affecting the host system's resources or user data.

Security Features:

- **Antivirus Scanning:**Comodo Advanced Endpoint Protection (AEP) has an antivirus scanning (https://www.comodo.com/home/internet-security/antivirus.php?af=7639) feature capable of scanning endpoints against a massive list of known good and bad files compiled from years as the world's largest certificate authority and from the 85 million endpoints deployed worldwide.
- **VirusScope behavioral analysis:** Uses techniques such as API hooking, DLL injection prevention, and more to identify indicators of compromise while keeping the endpoint safe and without affecting usability
- **Valkyrie verdict decision engine:** While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, returning a verdict within 45 seconds for 95% of the files submitted.
- **Human analysis:** In the 5% of cases where VirusScope and Valkyrie are unable to return a verdict, the file can be sent to researchers for human analysis who make a determination within SLA timelines.
- **Host intrusion prevention:** Rules-based HIPS that monitors application activities and system processes, blocking those that are malicious by halting actions that could damage critical system components.
- **Personal packet filtering firewall:** Provides granular management of inbound and outbound network activities, hides system ports from scans, and provides warnings when suspicious activities are detected. Can be administered remotely or by a local administrator

Device Management and Application Security

Device management and application security are central to endpoint security. And both these factors are given equal importance. 'Strong mobile policies, easy-to-implement default profiles, over-the-air enrollment, antitheft provision, remote data wipe and many other features ensure comprehensive device management. Whereas features like 'application inventory, application blacklisting and whitelisting, remote management, patch management ensure comprehensive application management as well.

Minimum System Requirements

Comodo Application Endpoint Protection (AEP) is extremely lightweight and therefore has minimum requirements. They are: 384 MB available RAM, 210 MB hard disk space for both 32-bit and 64-bit versions, CPU with SSE2 support, Internet Explorer version 5.1 or above.

Compatible With All Operating Systems

Comodo AEP is compatible with all versions of Windows. Be it Windows 10, Windows 8, Windows 7, Windows Vista or XP. Compatible with Android, Linux and Windows server editions (like Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2 etc,.) as well.

Comodo Advanced Endpoint Protection (AEP) Related Statistics

Our Comodo AEP performance survey indicates that each year 85 Million endpoints are being protected our security software. Its verdict on analyzing unknown files correctly is an astounding 100% and the time taken to return each individual verdict is only 45 seconds. If these stats fail to impress you, you can try out Comodo AEP for a free 30-day trial period and see for yourself how it performs.

Or if you prefer to set up a demo (https://www.comodo.com/schedule-a-demo.php?af=7639) or proof-of-concept project, contact us (https://www.comodo.com/support.php?af=7639) at EnterpriseSolutions@comodo.com or +1 888-256-2608.

Secure Your Enterprise Endpoints!

Website Backup (https://cwatch.comodo.com/website-backup/?af=7639)

Website Status (https://cwatch.comodo.com/website-status-checker.php?af=7639)

Be Sociable, Share!

(//tw[illegible]Article?
text=[illegible]%20Today%3F&body=htt
Tweet [illegible]ps%3A Like 147 [illegible] Share [illegible] Pin [illegible].com%2Fblog%2Fwhat-
is- endpoint- endpoint-
endp[illegible]
security%2F%20 Is Is is-
) Endpoint Endpoint-
Security? security%2F&srcTitle=Comodo+News+For+Enterprise+Security+)
and and
Why Why
Is It Is It
Crucial Crucial
Today? Today?
&af=7639) &notes=Endpoint
security
refers
to

← (/blog/what-to-do-if-your-company-has-been-hacked/?af=7639)
What to do if your company has been hack.. (/blog/what-to-do-if-your-company-has-been-hacked/?af=7639)

What Is Shurlockr Ransomware?.. (/blog/what-is-shurlockr-ransomware/?af=7639) → (/blog/what-is-shurlockr-ransomware/?af=7639)

Be part of an IT community with thousands of subscribers. Get the latest news, blogs, and thought leadership articles. Subscribe now

Email*

Subscribe

of

other
wireless
devices.
It
includes
monitoring
status,
software,
and
activities.
The
endpoint
p&af=7639)

Learn About Endpoint Protection (http://explore.comodo.com/endpoint-protection?af=7639)

Start Protecting Your Endpoints With 30-Day FREE Trial

Name *

Email *

Telephone Number *

Company Name *

START MY FREE TRIAL

Popular Posts

- What Is Endpoint Security? and Why Is It Crucial Today? (https://enterprise.comodo.com/blog/what-is-endpoint-security/?af=7639)
- What Is Network Security? (https://enterprise.comodo.com/blog/what-is-network-security/?af=7639)
- What is Malicious Software? (https://enterprise.comodo.com/blog/what-is-malicious-software/?af=7639)
- Computer Vulnerability: Definition (https://enterprise.comodo.com/blog/computer-vulnerability-definition/?af=7639)
- Top Five Best Malware Removal Tools 2020 (https://enterprise.comodo.com/blog/top-five-best-malware-removal-tools/?af=7639)

Archives

November 2020 (https://enterprise.comodo.com/blog/2020/11/?af=7639) (1)
October 2020 (https://enterprise.comodo.com/blog/2020/10/?af=7639) (1)
September 2020 (https://enterprise.comodo.com/blog/2020/09/?af=7639) (51)
August 2020 (https://enterprise.comodo.com/blog/2020/08/?af=7639) (48)
May 2020 (https://enterprise.comodo.com/blog/2020/05/?af=7639) (1)
March 2020 (https://enterprise.comodo.com/blog/2020/03/?af=7639) (1)
February 2020 (https://enterprise.comodo.com/blog/2020/02/?af=7639) (1)
July 2019 (https://enterprise.comodo.com/blog/2019/07/?af=7639) (1)
May 2019 (https://enterprise.comodo.com/blog/2019/05/?af=7639) (1)
April 2019 (https://enterprise.comodo.com/blog/2019/04/?af=7639) (1)
March 2019 (https://enterprise.comodo.com/blog/2019/03/?af=7639) (3)
February 2019 (https://enterprise.comodo.com/blog/2019/02/?af=7639) (5)
January 2019 (https://enterprise.comodo.com/blog/2019/01/?af=7639) (3)
December 2018 (https://enterprise.comodo.com/blog/2018/12/?af=7639) (9)
November 2018 (https://enterprise.comodo.com/blog/2018/11/?af=7639) (2)
October 2018 (https://enterprise.comodo.com/blog/2018/10/?af=7639) (5)
September 2018 (https://enterprise.comodo.com/blog/2018/09/?af=7639) (3)
August 2018 (https://enterprise.comodo.com/blog/2018/08/?af=7639) (6)
July 2018 (https://enterprise.comodo.com/blog/2018/07/?af=7639) (7)

- June 2018 (https://enterprise.comodo.com/blog/2018/06/?af=7639) (5)
- May 2018 (https://enterprise.comodo.com/blog/2018/05/?af=7639) (2)
- April 2018 (https://enterprise.comodo.com/blog/2018/04/?af=7639) (6)
- March 2018 (https://enterprise.comodo.com/blog/2018/03/?af=7639) (4)
- February 2018 (https://enterprise.comodo.com/blog/2018/02/?af=7639) (8)
- January 2018 (https://enterprise.comodo.com/blog/2018/01/?af=7639) (12)
- December 2017 (https://enterprise.comodo.com/blog/2017/12/?af=7639) (1)
- November 2017 (https://enterprise.comodo.com/blog/2017/11/?af=7639) (2)
- July 2017 (https://enterprise.comodo.com/blog/2017/07/?af=7639) (1)

Enterprise Support

Vulnerability Assessment Definition (https://enterprise.comodo.com/blog/what-is-vulnerability-assessment/?af=7639)
Zero Trust (https://enterprise.comodo.com/blog/what-is-zero-trust/?af=7639)

Comodo Services

Best Windows 10 Anti Virus Software (https://antivirus.comodo.com/antivirus-for-windows-10/?af=7639)

Best Antivirus Software (https://antivirus.comodo.com/blog/computer-safety/best-antivirus-of-2019/?af=7639)

Antivirus for Android (https://antivirus.comodo.com/antivirus-for-android.php?af=7639)

Antivirus for Windows 8 (https://antivirus.comodo.com/antivirus-for-windows-8/?af=7639)

Antivirus for Windows 7 (https://antivirus.comodo.com/antivirus-for-windows-7/?af=7639)

Malware Removal (https://antivirus.comodo.com/blog/comodo-news/5-best-free-malware-removal-tools-2019/?af=7639)

Spyware Removal (https://antivirus.comodo.com/blog/computer-safety/best-free-spyware-removal-software/?af=7639)

Website Malware Scanner (https://www.webinspector.com/website-malware-scanner/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

MDR Services (https://mdr.comodo.com/?af=7639)

SOC as a Service (https://mdr.comodo.com/soc-as-a-service.php?af=7639)

Incident Handling (https://mdr.comodo.com/incident-handling.php?af=7639)

Threat Detection (https://mdr.comodo.com/threat-detection.php?af=7639)

Alert Monitoring (https://mdr.comodo.com/alert-monitoring.php?af=7639)

Managed Security Information Management (https://mdr.comodo.com/managed-security-information-management.php?af=7639)

Managed SOC (https://mdr.comodo.com/managed-soc.php?af=7639)

Home Automations (https://whichhomeautomation.com/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

EZlo Products

Ezlo Shop (https://ezlo.shop/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Tweets by @comododesktop

Comodo
@comododesktop
Is Your Security Provider Failing to Detect Malware Files? Comodo Threat Research Lab's free tool allows you to select your provider & see what malware it is not detecting. hubs.la/H0CNpnk0

Dec 23, 2020

Comodo
@comododesktop
Comodo Announces BlueGrass Technologies as Partner for Middle East Cybersecurity Marketplace url-shortener.newsdirect.com/IyCv3uGI

Comodo Announces BlueGrass Technologies as Partner f…
Comodo Announces BlueGrass Technologies as Partner for Middle East Cybersecurity Marketplace
newsdirect.com

Dec 23, 2020

Embed View on Twitter

Comodo Enterprise Solutions

Comodo Endpoint Security (https://www.comodo.com/endpoint-protection/endpoint-security.php?af=7639)

Comodo Endpoint Protection (https://enterprise.comodo.com/blog/what-is-endpoint-security/?track=9247&af=7639)

RMM (https://www.itarian.com/rmm.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

POS Security (https://securebox.comodo.com/pos-system/pos-security?af=7639)

Patch Management Software (https://www.itarian.com/patch-management.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Service Desk (https://www.itarian.com/service-desk.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Network Assessment (https://www.itarian.com/itcm-network-assessment.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

What is Endpoint Security? (https://enterprise.comodo.com/blog/what-is-endpoint-security/?af=7639)

Clean WordPress Site Malware (https://cwatch.comodo.com/guides/how-to-clean-a-hacked-wordpress-site.php?af=7639)

Endpoint Detection Response (https://mdr.comodo.com/?af=7639)

Total NOC Support Service (https://totalnocsupport.com/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Website Vulnerability Scanner (https://cwatch.comodo.com/best-website-vulnerability-scanner.php?af=7639)

SIEM (https://www.comodo.com/siem.php?af=7639)

IT Platform

HelpDesk (https://www.itarian.com/helpdesk.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Best Remote Desktop Software (https://www.itarian.com/best-remote-desktop.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Ticketing System (https://www.itarian.com/ticketing-system.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Remote Desktop Connection Manager (https://www.itarian.com/remote-desktop-connection-manager.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

ITSM (https://www.itarian.com/itsm.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Website Security (https://cwatch.comodo.com/?af=7639)

Website Security Check (https://cwatch.comodo.com/features.php?af=7639)

Website Malware Removal (https://www.webinspector.com/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Antispam (https://www.comodo.com/business-security/email-security/antispam-gateway.php?af=7639)

Website Malware Scanner (https://www.webinspector.com/website-malware-scanner/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Scan URL (https://cwatch.comodo.com/free-url-scanner.php?af=7639)

Virus Removal (https://antivirus.comodo.com/free-virus-removal-software.php?af=7639)

Comodo Antivirus (https://antivirus.comodo.com/?af=7639)

Best Virus Removal (https://antivirus.comodo.com/blog/computer-safety/five-best-virus-and-malware-removal-tools/?af=7639)

Antivirus Software (https://www.comodo.com/home/internet-security/antivirus.php?af=7639)

Free CRM Software (https://www.itarian.com/customer-relationship-management.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Antivirus for PC (https://antivirus.comodo.com/blog/comodo-news/best-antivirus-windows-pc-2019/?af=7639)

Antivirus for Mac (https://www.comodo.com/home/internet-security/antivirus-for-mac.php?af=7639)

Antivirus for Linux (https://www.comodo.com/home/internet-security/antivirus-for-linux.php?af=7639)

Antivirus for Android (https://antivirus.comodo.com/antivirus-for-android.php?af=7639)

Cyber Security Solutions (https://www.comodo.com/company-narrative-1.php?af=7639)

Malware Removal (https://antivirus.comodo.com/blog/comodo-news/5-best-free-malware-removal-tools-2019/?af=7639)

Free Antivirus (https://antivirus.comodo.com/free-antivirus.php?af=7639)

Windows Antivirus (https://antivirus.comodo.com/blog/comodo-news/does-windows-10-need-antivirus/?af=7639)

Best Website Security (https://cwatch.comodo.com/best-website-security-for-enterprise.php?af=7639)

Website Backup (https://cwatch.comodo.com/website-backup/?track=17918&af=7639)

Knowledge base

What is CRM? (https://www.itarian.com/what-is-crm.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

What is Ransomware? (https://enterprise.comodo.com/ransomware/?af=7639)

What is RMM? (https://www.itarian.com/rmm.php?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

What is Malware? (https://antivirus.comodo.com/blog/how-to/what-is-malware/?af=7639)

What is Computer Virus? (https://antivirus.comodo.com/blog/computer-safety/what-is-virus-and-its-definition/?af=7639)

What is locky Ransomware? (https://enterprise.comodo.com/blog/what-is-locky-ransomware/?af=7639)

What is Antimalware? (https://enterprise.comodo.com/blog/what-is-antimalware/?af=7639)

What is Network Security? (https://enterprise.comodo.com/blog/what-is-network-security/?af=7639)

What is a Trojan Virus? (https://enterprise.comodo.com/what-is-a-trojan-virus.php?af=7639)

What is Antispam? (https://blog.comodo.com/antispam/what-is-anti-spam/?af=7639)

What is vulnerability assessment? (https://enterprise.comodo.com/blog/what-is-vulnerability-assessment/?af=7639)

What is Cyber Security? (https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php?af=7639)

What is Firewall? (https://personalfirewall.comodo.com/what-is-firewall.html?af=7639)

Best CDN (https://belugacdn.com/best-cdn/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Cheap CDN (https://belugacdn.com/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

CDN for Wordpress (https://www.belugacdn.com/content-delivery-network-in-wordpress/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Student Safety (https://www.nuedusec.com/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Comodo Resources

Terms & Conditions (https://www.comodo.com/repository/terms.php?af=7639)

Privacy Policy (https://www.comodo.com/repository/privacy-policy.php?af=7639)

Legal Repository (https://www.comodo.com/about/comodo-agreements.php?af=7639)

Contact Us (https://enterprise.comodo.com/contact-us.php?track=9249&af=7639)

Support (https://www.comodo.com/support.php?af=7639)

Free Demo (https://www.comodo.com/schedule-a-demo.php?af=7639)

Get Quote (https://www.comodo.com/pricing-product.php?af=7639)

Partners (https://enterprise.comodo.com/partners/contact.php?af=7639)

Ransomware

Recent Ransomware Attacks (https://enterprise.comodo.com/recent-ransomware-attacks.php?af=7639)

Ransomware Examples (https://enterprise.comodo.com/ransomware-examples.php?af=7639)

Ransomware Removal (https://enterprise.comodo.com/forensic-analysis/how-to-remove-ransomware-virus.php?af=7639)

How to Prevent Ransomware (https://enterprise.comodo.com/how-to-prevent-ransomware.php?af=7639)

Ransomware Types (https://enterprise.comodo.com/different-types-of-ransomware.php?af=7639)

Ransomware Protection (https://enterprise.comodo.com/forensic-analysis/ransomware-protection-software.php?af=7639)

Does Paying Ransomware Work (https://enterprise.comodo.com/does-paying-ransomware-work.php?af=7639)

Social

Comodo TV (https://www.comodo.tv/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639)

Comodo Forums (https://forums.comodo.com/?af=7639)

Signup for Newsletter

Email*

Subscribe

Connect with Comodo:

(https://www.facebook.com/ComodoHome/) (https://twitter.com/comododesktop) (https://www.linkedin.com/company/comodocybersecurity/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32) (https://www.instagram.com/comododesktop/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639) (https://www.youtube.com/channel/UCMxfiKdoQhg2KyOcynb1Cuw)

Cortex XDR

Safeguard Your Entire Organization with the Industry's First Extended Detection and Response Platform

Security teams are inundated with inaccurate, incomplete alerts. Today's siloed security tools force analysts to pivot from console to console to piece together investigative clues, resulting in painfully slow investigations and missed attacks. Even though they've deployed countless tools, teams still lack the enterprise-wide visibility and deep analytics needed to find threats. Faced with a shortage of security professionals, teams must simplify operations.

Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom detection rules.
- **Reduce alerts by 98%:** Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts.
- **Investigate eight times faster:** Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- **Stop attacks without degrading performance:** Obtain the most effective endpoint protection available with a lightweight agent.
- **Maximize ROI:** Use existing infrastructure for data collection and control to lower costs by 44%.

Prevent, Detect, Investigate, and Respond to All Threats

Cortex XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. Combined with our Managed Threat Hunting service, Cortex XDR gives you round-the-clock protection and industry-leading coverage of MITRE ATT&CK® techniques.

Block the Most Endpoint Attacks with Best-in-Class Prevention

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response. The agent shares protections across network and cloud security offerings from Palo Alto Networks to provide ironclad, consistent security across the entire enterprise.

Detect Stealthy Threats with Machine Learning and Analytics

Cortex XDR identifies evasive threats with unmatched accuracy by continuously profiling user and endpoint behavior with analytics. Machine learning models analyze data from Palo Alto Networks and third-party sources to uncover stealthy attacks targeting managed and unmanaged devices.

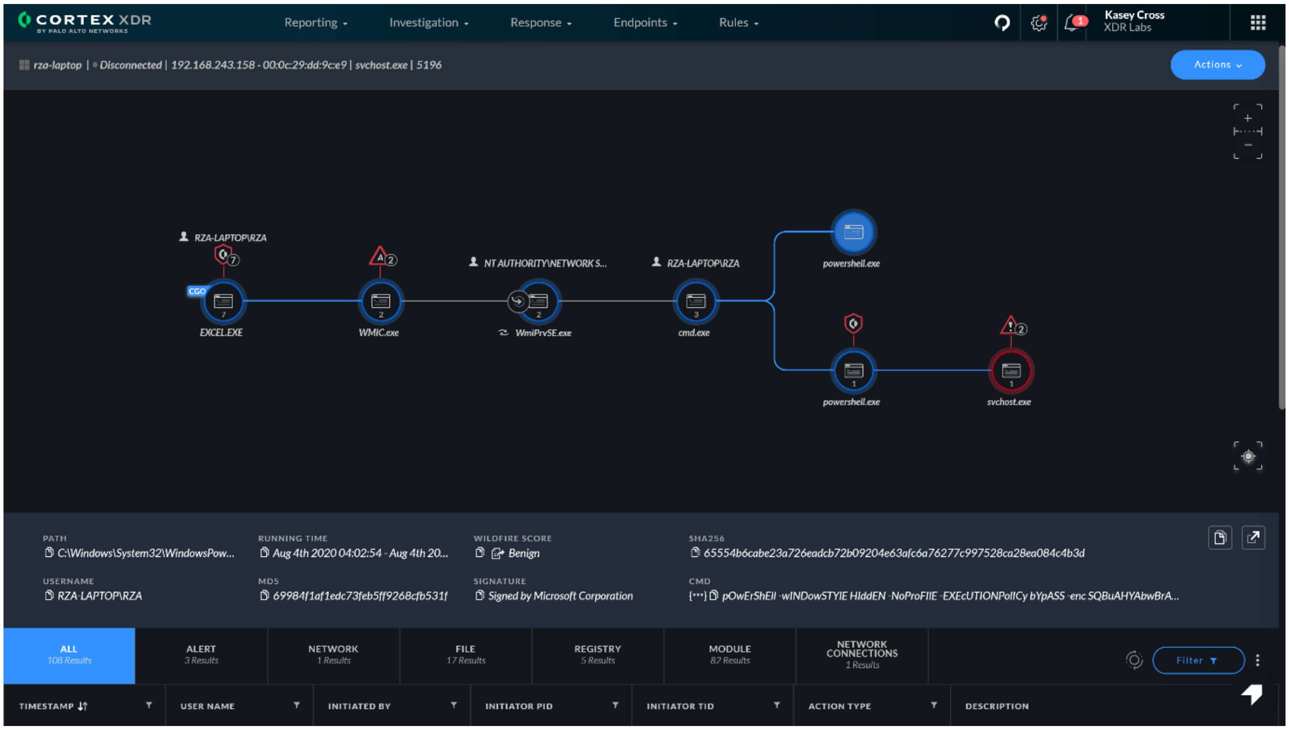
Investigate and Respond at Lightning Speed

Cortex XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

Key Capabilities

Safeguard Your Assets with Industry-Best Endpoint Protection

Prevent threats and collect data for detection and response with a single, cloud native agent. The Cortex XDR agent offers a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptive AI-driven local analysis engine that's always learning to counter new attack techniques. A Behavioral Threat Protection engine examines the behavior of multiple, related processes to uncover attacks as they occur. Integration with the Palo Alto Networks WildFire® malware prevention service boosts security accuracy and coverage. Visit us online to read more about endpoint protection.



rza-laptop | Disconnected | 192.168.243.158 - 00:0c:29:dd:9c:e9 | svchost.exe | 5196

PATH: C:\Windows\System32\WindowsPow...
RUNNING TIME: Aug 4th 2020 04:02:54 - Aug 4th 20...
WILDFIRE SCORE: Benign
SHA256: 65554b6cabe23a726eadcb72b09204e63afc6a76277c997528ca28ea084c4b3d
USERNAME: RZA-LAPTOP\RZA
MD5: 69984f1af1edc73feb5ff9268cfb531f
SIGNATURE: Signed by Microsoft Corporation
CMD: {***} pOwErShEll -wINDowSTYlE HIddEN -NoProFIlE -EXEcUTIONPolICy bYpASS -enc SQBuAHYAbwBrA...

Figure 1: Cortex XDR triage and investigation view

Securely Manage USB Devices

Protect your endpoints from malware and data loss with Device Control. The Cortex XDR agent allows you to monitor and secure USB access without needing to install another agent on your hosts. You can restrict usage by vendor, type, endpoint, and Active Directory® group or user. Granular policies allow you to assign write or read-only permissions per USB device.

Protect Endpoint Data with Host Firewall and Disk Encryption

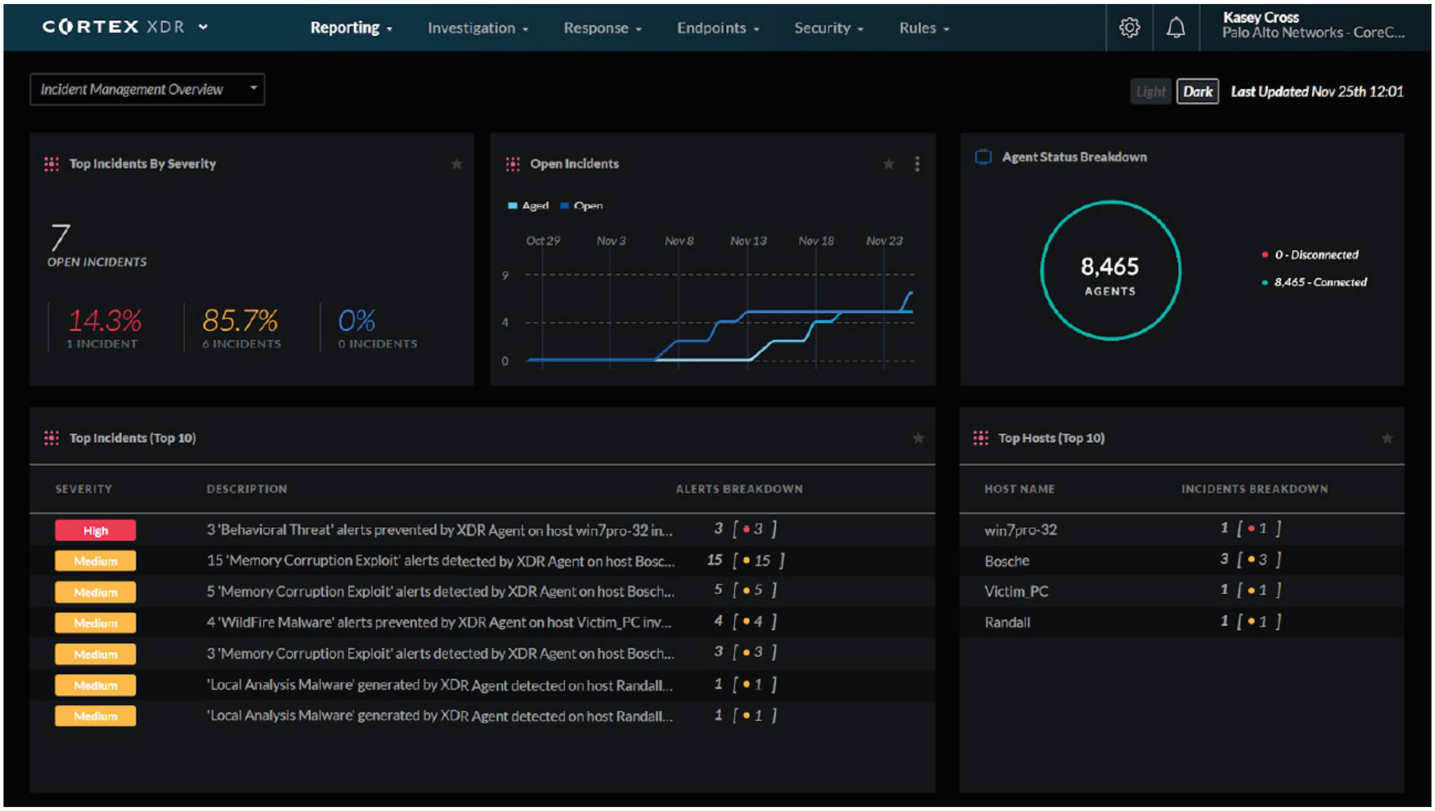
Reduce the attack surface of your endpoints. With host firewall and disk encryption capabilities, you can lower your security risks as well as address regulatory requirements. The Cortex XDR host firewall enables you to control inbound and outbound communications on your Windows® and macOS® endpoints. Additionally, you can apply BitLocker® or FileVault® encryption on your endpoints by creating disk encryption rules and policies. Cortex XDR provides full visibility into endpoints that were encrypted and lists all encrypted drives. Host firewall and disk encryption capabilities let you centrally configure your endpoint security policies from the Cortex XDR management console.

Get Full Visibility with Comprehensive Data

Break security silos by integrating all data. Cortex XDR automatically stitches together endpoint, network, and cloud data to accurately detect attacks and simplify investigations. It collects data from Palo Alto Networks products as well as third-party logs and alerts, enabling you to broaden the scope of intelligent decisions across all network segments. Third-party alerts are dynamically integrated with endpoint data to reveal root cause and save hours of analysts' time. Cortex XDR examines logs collected from third-party firewalls with behavioral analytics, enabling you to find critical threats and eliminate any visibility blind spots.

Discover Threats with Continuous ML-Based Threat Detection

Find stealthy threats with analytics and out-of-the-box rules that deliver unmatched MITRE ATT&CK coverage. Cortex XDR automatically detects active attacks, allowing your team to triage and contain threats before the damage is done. Using machine learning, Cortex XDR continuously profiles user and endpoint behavior to detect anomalous activity indicative of attacks. By applying analytics to an integrated set of data, including security alerts and rich network, endpoint, and cloud logs, Cortex XDR meets and exceeds the detection capabilities of siloed network traffic analysis (NTA), endpoint detection and response (EDR), and user behavior analytics (UBA) tools. Automated detection works all day, every day, providing you peace of mind.



SEVERITY	DESCRIPTION	ALERTS BREAKDOWN
High	3 'Behavioral Threat' alerts prevented by XDR Agent on host win7pro-32 in...	3 [• 3]
Medium	15 'Memory Corruption Exploit' alerts detected by XDR Agent on host Bosc...	15 [• 15]
Medium	5 'Memory Corruption Exploit' alerts detected by XDR Agent on host Bosch...	5 [• 5]
Medium	4 'WildFire Malware' alerts prevented by XDR Agent on host Victim_PC inv...	4 [• 4]
Medium	3 'Memory Corruption Exploit' alerts detected by XDR Agent on host Bosch...	3 [• 3]
Medium	'Local Analysis Malware' generated by XDR Agent detected on host Randall...	1 [• 1]
Medium	'Local Analysis Malware' generated by XDR Agent detected on host Randall...	1 [• 1]

HOST NAME	INCIDENTS BREAKDOWN
win7pro-32	1 [• 1]
Bosche	3 [• 3]
Victim_PC	1 [• 1]
Randall	1 [• 1]

Figure 2: Customizable dashboard

Investigate Eight Times Faster

Automatically reveal the root cause of every alert. With Cortex XDR, your analysts can examine alerts from any source—including third-party tools—with a single click, streamlining investigations. Cortex XDR automatically reveals the root cause, reputation, and sequence of events associated with each alert, lowering the experience level needed to verify an attack. By consolidating alerts into incidents, Cortex XDR slashes the number of individual alerts to review and alleviates alert fatigue. Each incident provides a complete picture of an attack, with key artifacts and integrated threat intelligence details, accelerating investigations.

Hunt for Threats with Powerful Search Tools

Uncover hidden malware, targeted attacks, and insider threats. Your security team can search, schedule, and save queries to identify hard-to-find threats. Flexible searching capabilities let your analysts unearth threats using an intuitive Query Builder as well as construct advanced queries and visualize results with XQL Search. By integrating threat intelligence with an extensive set of security data, your team can catch malware, external threats, and malicious insiders. An Asset Management feature streamlines network management and reveals potential threats by showing you all the devices in your environment, including managed and unmanaged devices.

Coordinate Response Across Endpoint, Network, and Cloud Enforcement Points

Stop threats with fast and accurate remediation. Cortex XDR lets your security team instantly contain endpoint, network, and cloud threats from one console. Your analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update prevention lists like bad domains through tight integration with enforcement points. The powerful Live Terminal feature lets Tier 1 analysts swiftly investigate and shut down attacks without disrupting end users by directly accessing endpoints; running Python®, PowerShell®, or system commands and scripts; and managing files and processes from graphical file and task managers.

Get Unprecedented Visibility and Swift Response with Host Insights

Understand your risks and contain threats quickly before they can spread. Host Insights, an add-on module for Cortex XDR, combines vulnerability management, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Vulnerability Management provides you real-time visibility into vulnerability exposure and current patch levels across your endpoints. Host inventory presents detailed information about your host applications and settings while Search and Destroy lets you swiftly find and eradicate threats across all endpoints. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breaches.

24/7 Threat Hunting Powered by Cortex XDR and Unit 42 Experts

Augment your team with the industry's first threat hunting service operating across endpoint, network, and cloud data. Cortex XDR Managed Threat Hunting offers round-the-clock monitoring from world-class threat hunters to discover attacks anywhere in your environment. Our Unit 42 experts work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware. To detect adversaries hiding in your organization, our hunters comb through comprehensive data from Palo Networks and third-party security solutions. Detailed Threat Reports reveal the tools, steps, and scope of attacks so you can root out adversaries quickly, while Impact Reports help you stay ahead of emerging threats.

Natively Integrate with Cortex XSOAR for Security Orchestration and Automation

Standardize and automate response processes across your security product stack. Cortex XDR integrates with Cortex™ XSOAR, our security orchestration, automation, and response platform, enabling your teams to feed incident data into Cortex XSOAR for automated, playbook-driven response that spans more than 450 product integrations and promotes cross-team collaboration. Cortex XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks.

Unify Management, Reporting, Triage, and Response in One Intuitive Console

Maximize productivity with a seamless platform experience. The management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response. You can quickly assess the security status of your organization's or individual endpoints with customizable dashboards as well as summarize incidents and security trends with graphical reports that can be scheduled or generated on demand. Public APIs extend management to third-party tools, enabling you to retrieve and update incidents, collect agent information, and contain endpoint threats from the management platform of your choice.

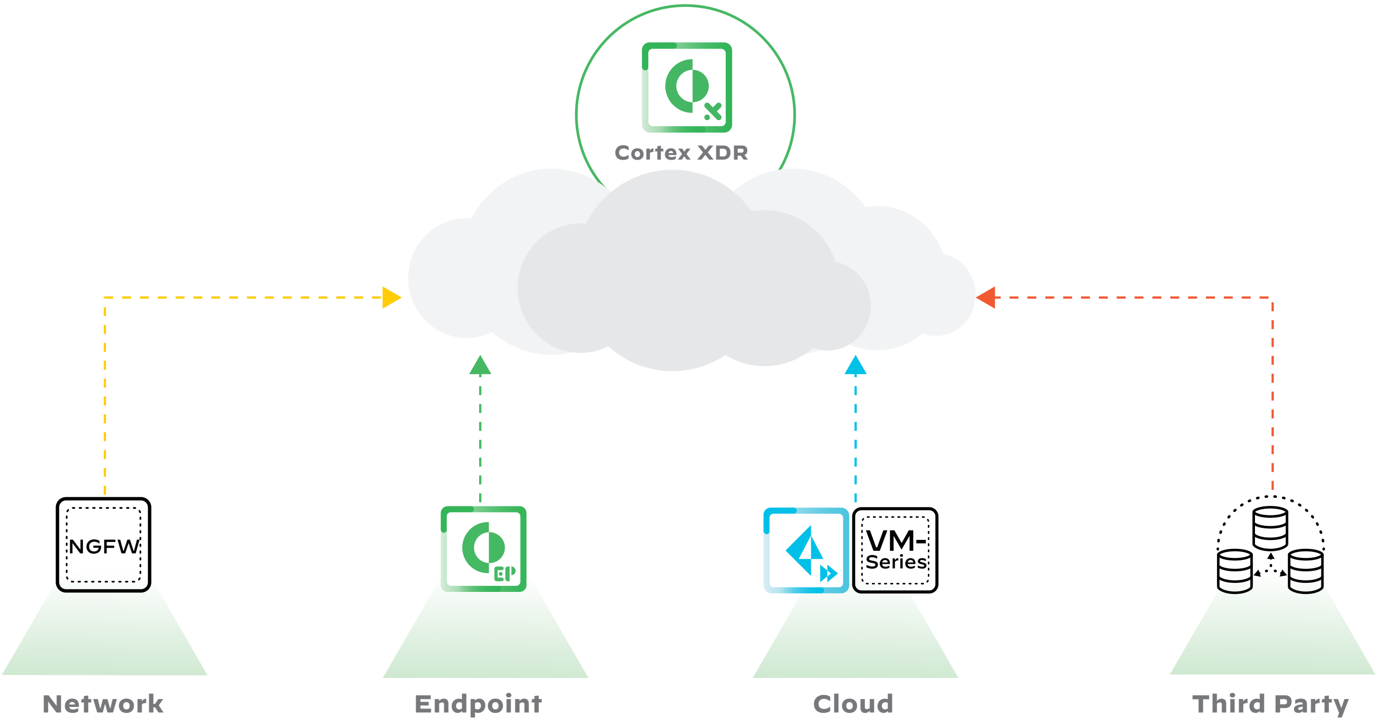


Figure 3: Analysis of data from any source for detection and response

Operational Benefits

Block known and unknown attacks with powerful endpoint protection: Leverage AI-based local analysis and Behavioral Threat Protection to stop the most malware, exploits, and fileless attacks in the industry.

Gain visibility across network, endpoint, and cloud data: Collect and correlate data from Palo Alto Networks and third-party tools to detect, triage, investigate, hunt, and respond to threats.

Automatically detect sophisticated attacks 24/7: Use always-on AI-based analytics and custom rules to detect advanced persistent threats and other covert attacks.

Avoid alert fatigue and personnel turnover: Simplify investigations with automated root cause analysis and a unified incident engine, resulting in a 98% reduction in alerts and lowering the skill required to triage alerts.

Increase SOC productivity: Consolidate endpoint security policy management and monitoring, investigation, and response across your network, endpoint, and cloud environments in one console, increasing SOC efficiency.

Eradicate threats without business disruption: Shut down attacks with surgical precision while avoiding user or system downtime.

Eliminate advanced threats: Protect your network against malicious insiders, policy violations, external threats, ransomware, fileless and memory-only attacks, and advanced zero-day malware.

Supercharge your security team: Disrupt every stage of an attack by detecting indicators of compromise (IOCs), anomalous behavior, and malicious patterns of activity.

Restore hosts to a clean state: Simplify response with recommended next steps for remediation. You can rapidly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys.

Extend detection, investigation, and response to third-party data sources: Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster, more effective investigations.

Ease Deployment with Cloud Delivery

Get started in minutes. The cloud native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy new on-premises network sensors or log collectors. You can use your Palo Alto Networks products or third-party firewalls to collect data, reducing the number of products you need to manage. You only need one source of data, such as Next-Generation Firewalls or Cortex XDR agents, to detect and stop threats, but additional sources can eliminate blind spots. Easily store data in Cortex Data Lake, a scalable and efficient cloud-based data repository. By integrating data from multiple sources together, automating tasks, and simplifying management, Cortex XDR delivers a 44% cost savings compared to siloed security tools.

Table 1: Cortex XDR Features and Specifications

Detection and Investigation Features and Capabilities	
Automated stitching of network, endpoint, and cloud data from Palo Alto Networks and third-party sources	Machine learning-based behavioral analytics
Third-party alert and log ingestion from any source with required network information	Custom rules to detect tactics, techniques, and procedures
Third-party log data from Check Point, Fortinet, Cisco ASA firewalls, Okta, PingOne, Azure Active Directory, Google Cloud, and Windows Event Collector	Root cause analysis of alerts
Host Insights add-on module, providing Vulnerability Management, Search and Destroy, and Host Inventory	Asset management
Cortex XDR Managed Threat Hunting service	Timeline analysis of alerts
Malware and fileless attack detection	Unified incident engine
Detection of targeted attacks, malicious insiders, and risky user behavior	Post-incident impact analysis
Network detection and response (NDR) and user behavior analytics (UBA)	Dashboards and reporting
Endpoint detection and response (EDR)	Threat intelligence integration
Native integration with Cortex XSOAR for orchestration, automation, and response	Threat hunting
Incident management	Incident response and recovery
Endpoint Protection Capabilities	
Malware, ransomware, and fileless attack prevention	Customizable prevention rules (available with Cortex XDR Pro)
Behavioral Threat Protection	Endpoint script execution (available with Cortex XDR Pro)
AI-based local analysis engine	Network isolation, quarantine, process termination, file deletion, file block list
Cloud-based malware prevention with WildFire	Live Terminal for direct endpoint access
Child process protection	Remediation suggestions for host restore (available with Cortex XDR Pro)
Exploit prevention by exploit technique	Public APIs for response and data collection
Device control for USB device management	Credential theft protection
Host firewall	Scheduled and on-demand malware scanning
Disk encryption with BitLocker and FileVault	Optional automatic agent upgrades
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Reduction of MTTD and MTTR
Investigation of every alert and incident generated by Cortex XDR	Custom tuning of Cortex XDR for enhanced prevention, visibility, and detection
Guided or full threat remediation actions	Direct access to partners' analysts and forensic experts

Table 1: Cortex XDR Features and Specifications (continued)

Specification	Cortex XDR
Delivery model	Cloud-delivered application
Data retention	30-day to unlimited data storage
Cortex XDR Prevent subscription	Endpoint protection with Cortex XDR agents
Cortex XDR Pro per endpoint subscription	• Detection, investigation, and response across endpoint data sources • Endpoint protection with Cortex XDR agents
Cortex XDR Pro per TB subscription	Detection, investigation, and response across network and cloud data sources, including third-party data
Cortex XDR Managed Threat Hunting subscription	24/7 threat hunting powered by Cortex XDR and Unit 42 experts
Cortex XDR Pathfinder endpoint analysis service	Collects process information from endpoints that do not have Cortex XDR agents; included with all Cortex XDR subscriptions

Reinvent Security Operations with Cortex

Cortex XDR is part of Cortex™, the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities. The suite is built on the tightly integrated offerings of Cortex XDR and Cortex XSOAR, enabling you to transform your SOC operations from a manual, reactive model that required endless resources to a lean, proactive, and automated team that reduces both MTTD and MTTR for every security use case.

Operating System Support

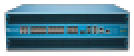
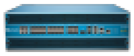
The Cortex XDR agent supports multiple endpoints across Windows, macOS, Linux, Chrome® OS, and Android® operating systems. For a complete list of system requirements and supported operating systems, please visit the Palo Alto Networks Compatibility Matrix. Cortex XDR Pathfinder minimum requirements: 2 CPU cores, 8 GB RAM, 128 GB thin-provisioned storage, VMware ESXi™ V5.1 or higher, or Microsoft Hyper-V® 6.3.96 or higher hypervisor.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Feature	**PA-5250** 	**PA-5220** 
Performance **1. Firewall throughput measured with App-ID and User-ID features enabled utilizing AppMix transactions. 2. Threat prevention throughput measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled utilizing AppMix transactions. 3. New sessions per second measured with 1 byte HTTP transactions. Additionally, for VM models, please refer to hypervisor, cloud specific data sheet for associated performance.*		
App-ID firewall throughput	40 Gbps	20 Gbps
Threat prevention throughput	21 Gbps	8.9 Gbps
IPSec VPN throughput	18 Gbps	10 Gbps
Connections per second	297,000	133,000
Sessions		
Max sessions (IPv4 or IPv6)	8,000,000	4,000,000
Policies		
Security rules	65,000	30,000
Security rule schedules	256	256
NAT rules	8,000	6,000
Decryption rules	5,000	3,500
App override rules	4,000	3,500
Tunnel content inspection rules	8,500	2,500
SD-WAN rules	500	300
Policy based forwarding rules	2,000	2,000
Captive portal rules	8,000	8,000
DoS protection rules	2,000	2,000
Security Zones		
Max security zones	17,000	4,000
Objects (addresses and services)		
Address objects	160,000	80,000
Address groups	80,000	40,000

Members per address group	2,500	2,500
Service objects	12,000	8,000
Service groups	6,000	4,000
Members per service group	2,500	2,500
FQDN address objects	6,144	6,144
Max DAG IP addresses _*System wide capacity_	500,000	500,000
Tags per IP address	32	32

Security Profiles

Security profiles	750	750

App-ID

Custom App-ID signatures	6,000	6,000
Shared custom App-IDs	512	512
Custom App-IDs (virtual system specific)	6,416	6,416

User-ID

User-IP mappings (management plane)	512,000	512,000
User-IP mappings (data plane)	512,000	512,000
Active and unique groups used in policy _*Aggregate of LDAP groups, XML API Groups and Dynamic User Groups_	10,000	10,000
Number of User-ID agents	100	100
Monitored servers for User-ID	100	100
Terminal server agents	2,500	2,500
Tags per User _*Only valid for PAN-OS 9.1 and above_	32	32

SSL Decryption

Max SSL inbound certificates	1,200	600
SSL certificate cache (forward proxy)	24,000	16,000
Max concurrent decryption sessions	800,000	400,000
SSL Port Mirror	Yes	Yes
SSL Decryption Broker	Yes	Yes
HSM Supported	Yes	Yes

URL Filtering

Total entries for allow list, block list and custom categories	100,000	100,000
Max custom categories	2,849	2,849

Max custom categories (virtual system specific)	500	500
Dataplane cache size for URL filtering	250,000	250,000
Management plane dynamic cache size	600,000	600,000

EDL

Max number of custom lists	30	30
Max number of IPs per system	150,000	150,000
Max number of DNS Domains per system	4,000,000	4,000,000
Max number of URL per system	250,000	250,000
Shortest check interval (min)	5	5

Interfaces

Mgmt - out-of-band	10/100/1000, RJ45 console	10/100/1000, RJ45 console
Mgmt - 10/100/1000 high availability	NA	NA
Mgmt - 40Gbps high availability	1	1
Mgmt - 10Gbps high availability	NA	NA
Traffic - 10/100/1000	NA	NA
Traffic - 100/1000/10000	4	4
Traffic - 1Gbps SFP	0/16	0/16
Traffic - 10Gbps SFP+	0/16	0/16
Traffic - 40Gbps QSFP	4x40/100	4X40
802.1q tags per device	4,094	4,094
802.1q tags per physical interface	4,094	4,094
Max interfaces (logical and physical)	4,096	4,096
Maximum aggregate interfaces	8	8
Maximum SD-WAN virtual interfaces	1,500	1,500

Virtual Routers

Virtual routers	125	20

Virtual Wires

Virtual wires	2,048	2,048

Virtual Systems

Base virtual systems	25	10
Max virtual systems _*Additional licenses are required for virtual system capacities above the base virtual systems capacity_	125	20

Routing

IPv4 forwarding table size **Entries shared across virtual routers*	100,000	100,000
IPv6 forwarding table size **Entries shared across virtual routers*	100,000	100,000
System total forwarding table size	200,000	200,000
Max route maps per virtual router	50	50
Max routing peers (protocol dependent)	1,000	1,000
Static entries - DNS proxy	1,024	1,024
Bidirectional Forwarding Detection (BFD) Sessions	1,024	1,024

L2 Forwarding

ARP table size per device	128,000	128,000
IPv6 neighbor table size	128,000	128,000
MAC table size per device	128,000	128,000
Max ARP entries per broadcast domain	128,000	128,000
Max MAC entries per broadcast domain	128,000	128,000

NAT

Total NAT rule capacity	8,000	6,000
Max NAT rules (static) **Configuring static NAT rules to full capacity requires that no other NAT rule types are used.*	8,000	6,000
Max NAT rules (DIP) **Configuring DIP NAT rules to full capacity requires that no other NAT rule types are used.*	8,000	4,000
Max NAT rules (DIPP)	6,000	4,000
Max translated IPs (DIP)	160,000	64,000
Max translated IPs (DIPP) **DIPP translated IP capacity is proportional to the DIPP pool oversubscription value. The capacity shown here is based on an oversubscription value of 1x.*	6,000	4,000
Default DIPP pool oversubscription **Source IP and source port reuse across concurrent sessions*	8	8

Address Assignment

DHCP servers	500	500
DHCP relays **Maximum capacity represents total DHCP servers and DHCP relays combined*	4,096	2,048

Max number of assigned addresses	64,000	64,000
High Availability		
Devices supported	2	2
Max virtual addresses	4,096	4,096
QoS		
Number of QoS policies	4,000	4,000
Physical interfaces supporting QoS	12	12
Clear text nodes per physical interface	63	63
DSCP marking by policy	Yes	Yes
Subinterfaces supported	2,048	2,048
IPSec VPN		
Max IKE Peers	4,000	3,000
Site to site (with proxy id)	12,000	10,000
SD-WAN IPSec tunnels	4,000	3,000
GlobalProtect Client VPN		
Max tunnels (SSL, IPSec, and IKE with XAUTH)	30,000	15,000
GlobalProtect Clientless VPN		
Max SSL tunnels	5,000	2,500
Multicast		
Replication (egress interfaces)	2,000	1,000
Routes	4,000	4,000
Product Notes		
End-of-sale	NA	NA