# 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

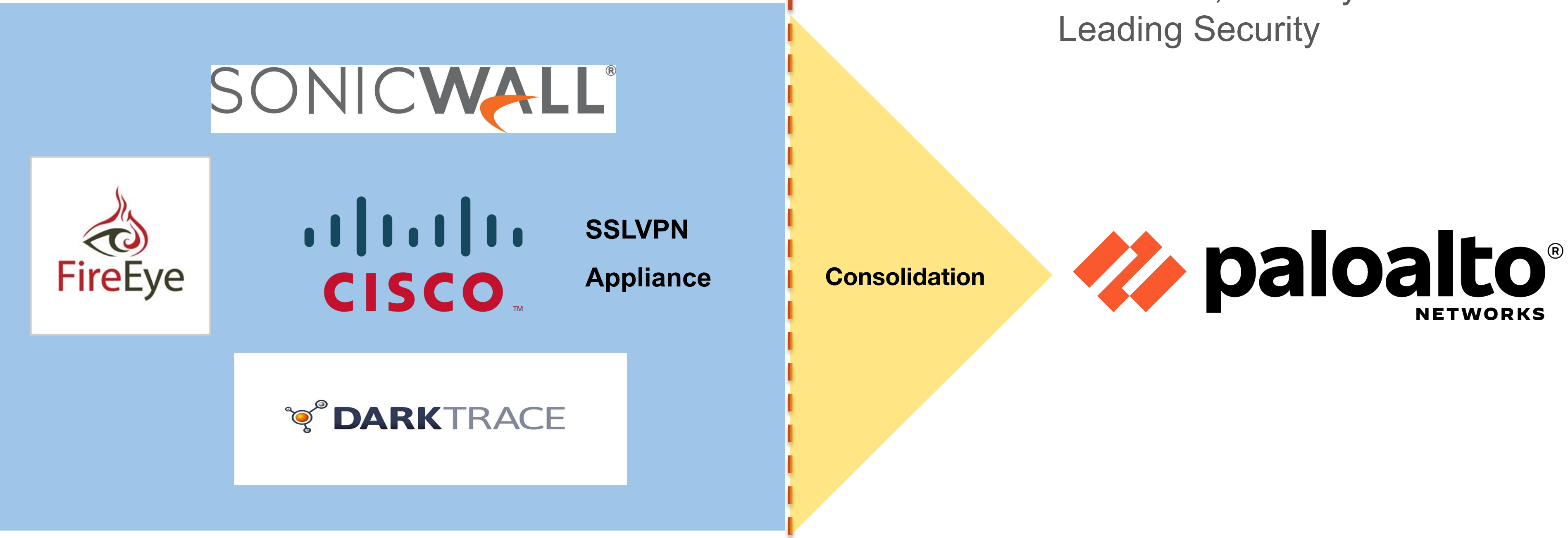
# Impact - 5 Point Solutions Consolidated

## Livingston County Government Current State

Multi-Point Solutions

## Proposed Future State

Consolidated, Industry-Leading Security



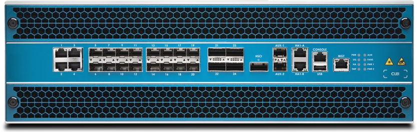
SSLVPN

Appliance

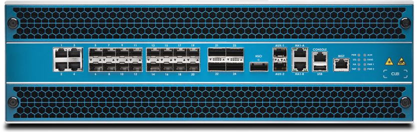
Consolidation

# Introducing the PA-5200 Series

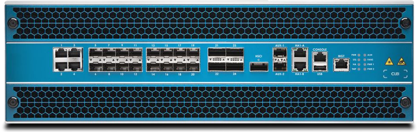
## PA-5200 Series



**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

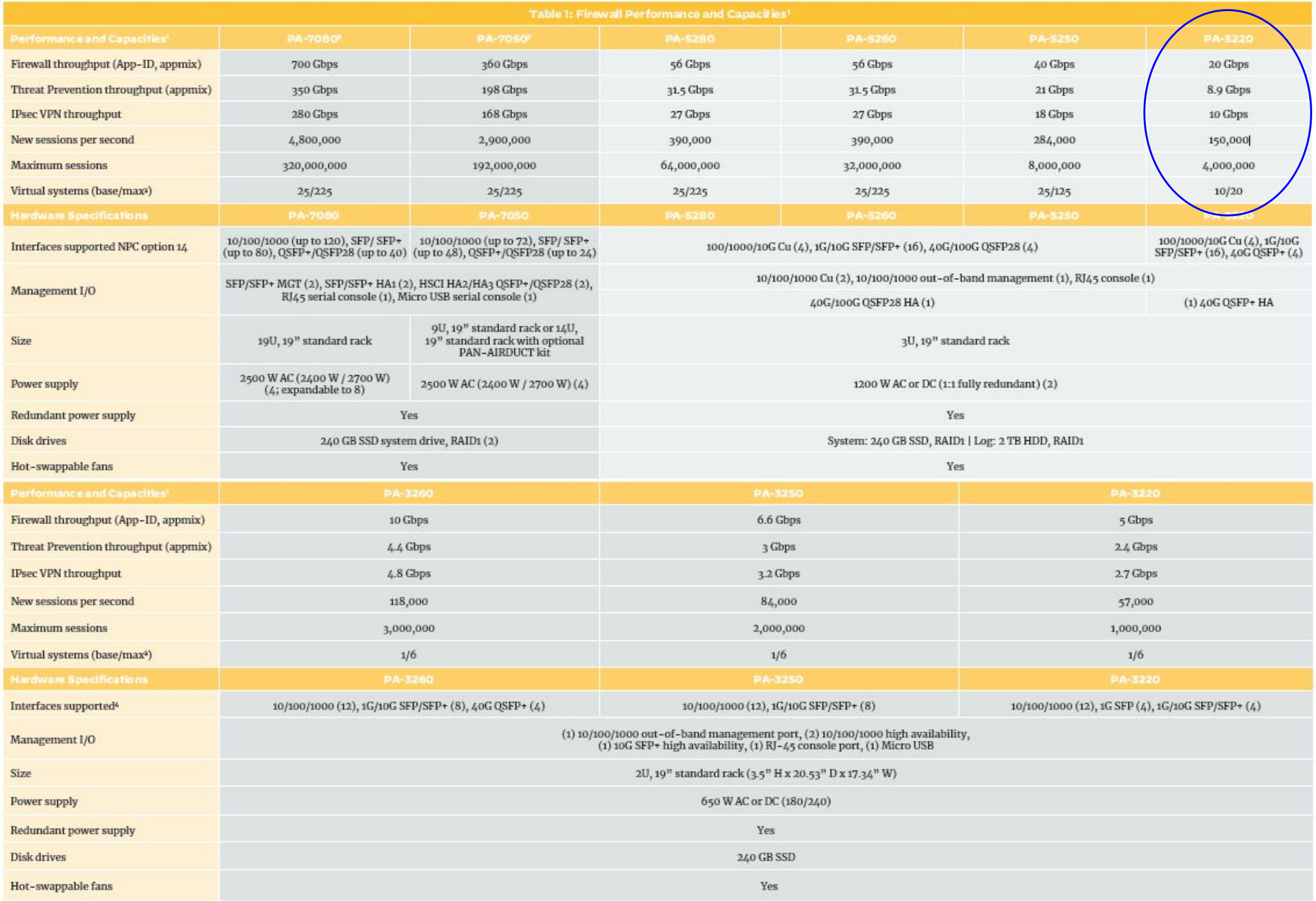
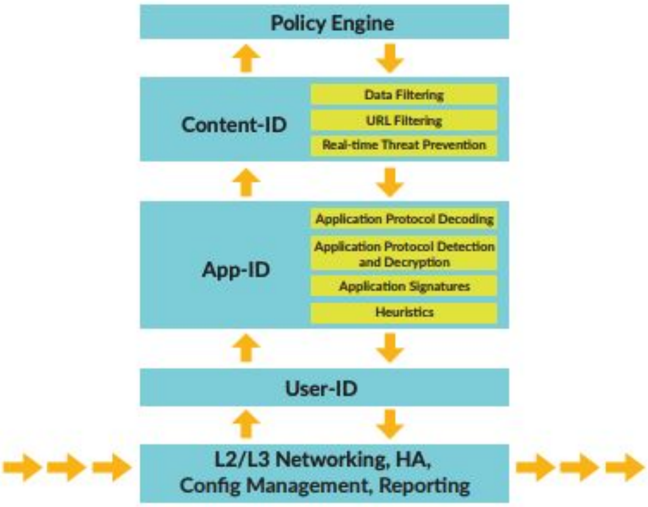


Table 1: Firewall Performance and Capacities[1]

| 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

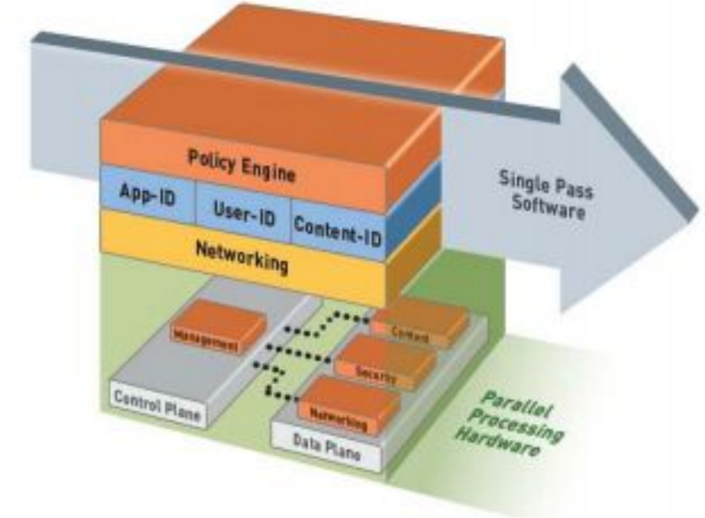
App-ID
- Application Protocol Decoding
- Application Protocol Detection and Decryption
- Application Signatures
- Heuristics

User-ID

L2/L3 Networking, HA, Config Management, Reporting

**Figure 1:** Single-Pass Architecture Traffic Flow

## Palo Alto Networks SP3 Architecture and Processing



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

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

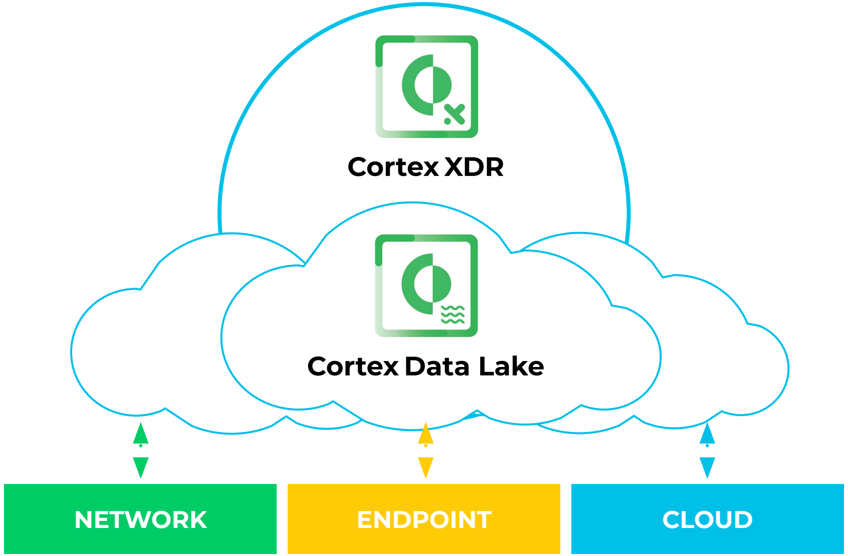
**Everything you can't prevent, detect and investigate fast**

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%

*“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”*

BRENT LOPEMAN

Senior Security Engineer

Ada County

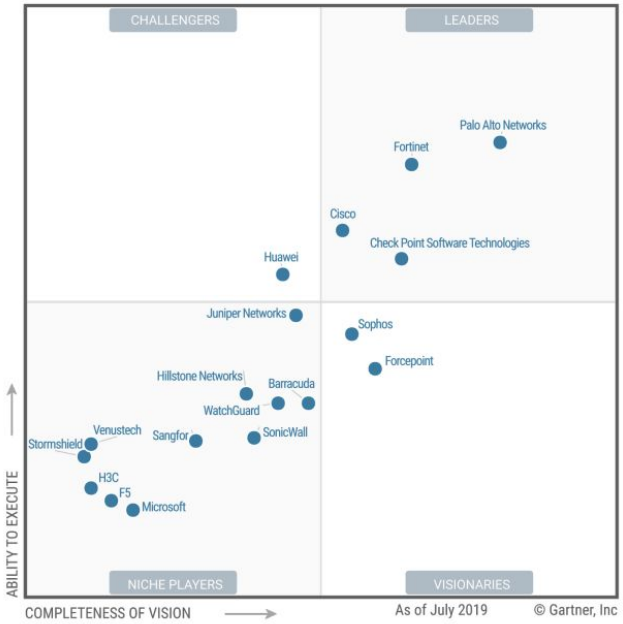
## Challenge

- 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**

PALO ALTO NETWORKS
PA-5220 PAN-OS 8.1.6-h2
NEXT GENERATION FIREWALL
NSS LABS
RECOMMENDED
JULY 2019
PALO ALTO NETWORKS
PA-5250 9.0.3-h2
NEXT GENERATION INTRUSION PREVENTION SYSTEM
NSS LABS
RECOMMENDED
OCTOBER 2019
PALO ALTO NETWORKS
PA-5250 9.0.3-h2
DATA CENTER SECURITY GATEWAY
NSS LABS
RECOMMENDED
NOVEMBER 2019

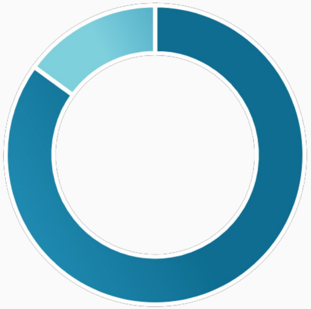
**NSS Labs Recommended**

# The World’s Leading Cybersecurity Company

## 95

### of Fortune 100

**Rely on Palo Alto Networks**



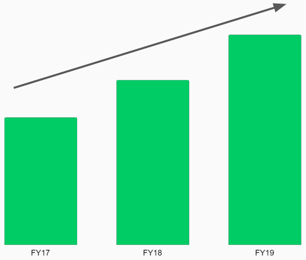
**71% of the Global 2K**

**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