

ENDPOINT SECURITY ([HTTPS://ENTERPRISE.COMODO.COM/BLOG/CATEGORY/ENDPOINT-SECURITY/?AF=7639](https://enterprise.comodo.com/blog/category/endpoint-security/?af=7639))

ENDPOINT PROTECTION ([HTTPS://ENTERPRISE.COMODO.COM/BLOG/CATEGORY/ENDPOINT-PROTECTION/?AF=7639](https://enterprise.comodo.com/blog/category/endpoint-protection/?af=7639))

GET IT FREE NOW (<https://platform.comodo.com/signup/?track=10225&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 instance 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 is 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.



Comodo AEP – Get Complete Protection!

Comodo Advanced Endpoint Protection (Comodo AEP), Get complete protection for every endpoint on your network.

- Free Trial for 30 days
- 7-Layers Endpoint Security Platform
- Default Deny Security
- Cloud-based Advanced Malware Analysis

Get Free Trial (<https://platform.comodo.com/signup/?track=10225&af=7639>)

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

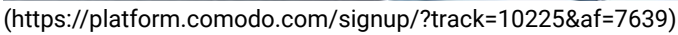
Comodo AEP is compatible with all versions of Windows. Be it Windows 10, Windows 8, Windows 7, Windows Vista or XP. Compatible with Android, Linux and Windows server editions (like Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2 etc.,) as well.

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.

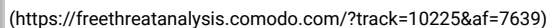
Secure Your Enterprise Endpoints!



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

[illegible]

Crucial
Today?
&af=2639=Endpoint
security



other

<https://enterprise.comodo.com/blog/what-is-endpoint-security/?af=7639>

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

devices.

Start Protecting Your Endpoints With 30-Day FREE Trial

Name*

includes

monitoring

status,

software,

and

activities.

Email*

The

endpoint

p&af=7639)

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

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

Comodo

@comododesktop

Comodo Announces BlueGrass Technologies as Partner for Middle East Cybersecurity Marketplace url-shortener.newsdirect.com/lyCv3uGI

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



Like Page

Learn More

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.facebook.com/ComodoHome/))  (<https://www.instagram.com/comododesktop/?key5sk1=5e49a46bc97623934f70b57f7f86aa935ffadf32&af=7639>)

 (<https://www.youtube.com/channel/UCMxfikDoQhg2KyOcyNb1CuW>)

© Comodo Group, Inc. 2020. All rights reserved. All trademarks displayed on this web site are the exclusive property of the respective holders.