HACKER COMBAT COMMUNITY

Hackercombat.com

Endpoint Security, Antivirus, Firewall: Everything You Need To Know!

Swipe Now

Introduction

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 that 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

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'. Hackercombat.com

Endpoint Security Is Not The Same As 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,' 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. 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.

Difference between Endpoint Security and Antivirus

Antivirus is one of the components of endpoint security. At the same time, 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, endpoint 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 health, user authentication/authorization, etc., thus keeping the endpoints secure.

Antivirus is usually a single program responsible for scanning, detecting, and removing viruses, malware, adware, spyware, ransomware, and other malware. Simply put, antivirus is a one-stop shop for securing your home networks, and endpoint security is suitable for securing enterprises that 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. In contrast, network security is about security measures to protect your entire network (IT infrastructure) against various security threats.

The main difference between endpoint security and network security is that in the case of the former, the focus is on securing endpoints, and in the case of the latter, the focus is on securing the network. Both types of security are important. Ideally, it's best to start by securing the endpoints and building them 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 were secured first. This you should make a 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. For example, restricting traffic flowing into the network from a potentially dangerous website.

Whereas endpoint security concerns itself not just with network filtering but performs many other tasks like patching, logging, monitoring, etc., to safeguard 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.

Swipe Now

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 that has to be installed on the network for deployment and a cloud-based solution is one that 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., to 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 11 — Needs Endpoint Security?

Inbuilt Windows Security will never be sufficient because today's security attack vectors are just too many to handle. This 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 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:

Keep Your Windows OS Up-to-Date:

Today it's Windows 11. 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.

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.,

Use Proactive Security Solution:

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.,

Use Local Account Instead Of Microsoft Account:

If you are using Windows 11, it's best to avoid a Microsoft account and instead opt for a Local account, as using a Microsoft account means saving some of your personal details on the cloud, which is not 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".

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.

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.

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.,

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.

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, which is why it is hugely popular and has so much following — despite 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 Endpoint Protection and follow the security best practices. These will ensure your Windows OS stays safe no matter what.

Hackercombat.com

Follow. Learn. Share

Save For Later

Follow us!

Find us Online

Like and Comment