Learn about terminal security (endpoint security)

The world of modern information technology brings many benefits but also favorable conditions for bad guys to make use of.

What is endpoint?

Our information technology system is growing, the Internet has an increasing transmission speed, the information technology devices are also more and more diverse, but every transmission has two sides.The world of modern information technology brings many benefits but also a favorable condition for bad guys to take advantage of and carry out illegal acts.In that endpoint security solution means integrating security protection into informatics devices at all dispersal points, which can be an effective preventive solution.The most popular endpoint devices include PC (server, desktop, laptop), mobile device, storage device including via USB, Bluetooth devices, product code reader, machine sell….

What is endpoint security?

Endpoint security or Endpoint protection, temporary translation is terminal security or endpoint security, is a term referring to a technology that protects the network of computers connected remotely to users' devices.The use of laptops, tablets, mobile phones and other wireless devices is connected to the corporate network, creating vulnerable security holes and entailing security threats. securityTerminal security is an attempt to ensure that such devices are safe to a certain extent according to the requirements and standards.It includes monitoring status, software and activities.Endpoint protection software will be installed on all network servers and on all terminals.

Corresponding to the increase of mobile devices such as laptops, smartphones, tablets . is a sharp increase in the number of lost or stolen devices.These incidents have the potential to cause organizations and individuals to mislead sensitive data, especially for businesses that allow their employees to bring the above mobile devices into joint network systems. their career.

To solve this problem, businesses must provide enterprise data security measures on their employees' mobile devices in a way that even if the device falls into the wrong hands, Data will still be protected.Terminal security process for this business is called terminal security.

Terminal security management system is a software approach that helps identify and manage users' computers to access the company's network.This involves network administration to restrict access to certain websites for users to maintain and adhere to organization policies and standards.Components involved in arranging endpoint security management systems include a VPN computer, an operating system and a modern antivirus software.Computer devices that do not conform to the organization's policy can only provide limited access to a virtual LAN.It also helps businesses successfully prevent any data abuse by the employees they have provided data.Example: A disgruntled employee trying to annoy a business or a person may be an employee of an employee trying to illegally use available business data on the device.

Endpoint security is often confused with some other network security tools such as antivirus, firewall and even network security.

Why is it called endpoint security?

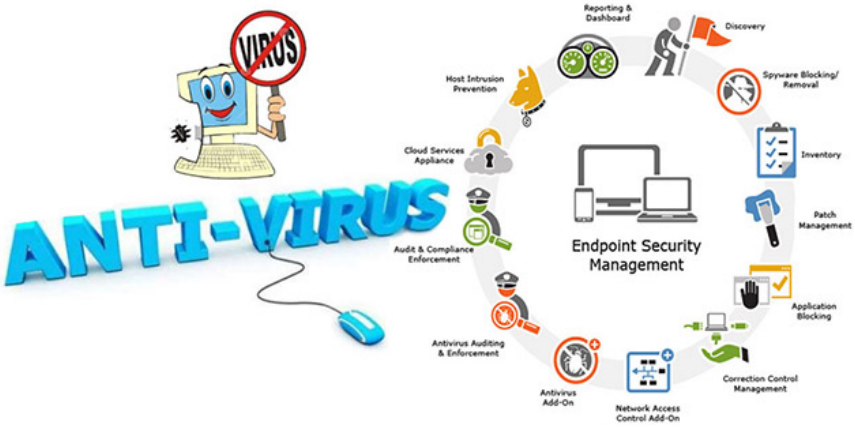
As you can see, every device that can connect to the network can cause significant security risks.And because these devices are located outside the company's firewall system, they are called end points.That means the end of that network.

As stated in the first section, the end point can be any mobile device, from a laptop to a tablet today, as long as they can be connected to the network, and your strategy Use in securing these endpoint devices is called endpoint security.

Endpoint security is not the same as antivirus

Although the goal of end-to-end security solutions is the same, that is to keep a device safe, there are still significant differences between endpoint security and antivirus software.Antivirus is more focused on protecting PCs (one or more depending on the type of antivirus software being deployed), while end-to-end security is 'concerned' with all relevant terminals. general.

Difference between Endpoint security and Antivirus?



Antivirus is one of the components of endpoint security.While endpoint security is a broader concept including not only antivirus but also many security tools (such as Firewall, HIPS system, whitelist tool, patching and logging tool .) to protect the various terminals of the enterprise (and the business itself) against various types of security threats.These are also things that are often not available in antivirus software.

More precisely, terminal security uses the server / client application model to protect the various terminals of the business.The server will have a main record of the security program and the clients (terminals) will have the 'agents' installed inside.These agents will contact and provide the server with the operation and status of the respective devices such as device health, user authentication / authorization . and therefore, help keep it safe. terminal.

Meanwhile, antivirus software is usually just a single program responsible for scanning, detecting and killing viruses, malware, adware, spyware . Simply put, antivirus is A suitable tool to protect your home network system and appropriate endpoint security to secure larger and more complex businesses in processing.It can also be said that anti-virus software is simple endpoint security.

The difference between endpoint security and network security

As mentioned, endpoint security is aimed at protecting corporate terminals (mobile devices like laptops, smartphones and many other things), and of course, businesses will also against the dangers created by these terminals.While network security focuses on implementing security measures to protect your entire network (the entire IT infrastructure) against various security threats.

The main difference between endpoint security and network security is that endpoint security focuses on terminal security, while for network security, the focus is on protecting the network system.Both types of security are very important.It is best to start with building the endpoint security system and then the network security system.Simply understand, your network will be safe only if your endpoints are strictly secure.You should note this before starting to look for end-to-end security and network security products.

The difference between endpoint security and firewall

The firewall will be responsible for filtering traffic into and out of your network based on 'a set of security rules', such as restricting traffic flowing into the network from a curing site. Specific hidden dangers.While endpoint security not only concerns network filtering, but also performs many other tasks such as patching, logging and monitoring . to protect the endpoints.

Both anti-virus and firewall are important factors in endpoint security.Their goal remains the same, although the applied model (client / server model) and the number of computers they protect are different, and in the endpoint security model, when operating with Other security tools, they will become much more efficient.

Endpoint security has many different forms

Depending on the criteria of consumers and businesses, we also have different endpoint security forms.In general, endpoint security solutions can be divided into 2 different categories.One for consumers and one for businesses.The biggest difference between these two types is that for consumers there will be no centralized management and management, while for businesses, centralized management is essential.The admin center (or server) will arrange reasonable configurations or install endpoint security software on individual terminals, then the log of performance and other warnings will sent to the central administration server for evaluation and analysis.

What do these end-to-end security solutions often contain?

Although there are certainly no limitations on the applications of endpoint security, and the list of applications will be further expanded in the future, there will still be some core applications for any any endpoint security solution

Some of these applications include firewalls, antivirus tools, internet security tools, mobile device management tools, encryption, intrusion detection tools, mobile security solutions. .

Modern and traditional endpoint security

To show the real differences between modern and traditional endpoint security is quite complicated because it is constantly being changed.While businesses are often reluctant and afraid to change, even if that change is beneficial to them.But end-to-end security is one area where businesses will have no choice but to adopt the latest modern endpoint security measures.Because endpoint security is not only an anti-malware tool, it can also take great steps in protecting corporate networks against ever-changing security threats. change every day.

Windows 10 and endpoint security

Although Windows 10 is claimed to be the safest Windows operating system, it still contains some security weaknesses.Security experts have proven that the integrated security features of Windows such as Windows Defender, Firewall . are also becoming ineffective in today's complex and constantly changing security situation.Therefore businesses using Windows 10 operating systems will still need endpoint security to protect the various terminals connected to the network and to protect their own network.

Security systems built into Windows will never be enough.Because today 's ways of attacking security are too diverse and changed too quickly.That means we no longer live in a world where email attachments or downloads are the only sources of malware infection.Simply put, your windows operating system needs additional protection in the form of antivirus for Windows or more if possible depending on your requirements.

With that in mind, let's take a look at the ways you can protect your Windows operating system from various security threats:

1. Keep your Windows operating system up to date with the latest version: Today is Windows 10 but there will be a new version tomorrow.Whatever the reason, make sure your PC is always updated to the latest version.This is probably one of the simplest measures you can take in addition to installing additional antivirus software, because the latest update is usually an update that will help protect users from all Security vulnerabilities have been discovered.
2. Ensure other applications are fully updated: One of the key components in a computer system is applications.Make sure all the applications in your system are up to date and contain the latest security patches, because there is a clear fact that hackers often try to exploit vulnerabilities from software. popular like Java, Adobe Flash, Adobe Acrobat . and then enter your system.
3. Using proactive security solutions: Unfortunately, traditional anti-virus software alone will not be enough in the current situation, especially when you are against modern, used malware. The methods are much more sophisticated than before.Therefore, to solve the ever-changing network security threats, users will need proactive security solutions such as Internet security (for family size) and endpoint security (for enterprise).
4. Use a local account instead of a Microsoft account: If you are using Windows 10, it is best to avoid using Microsoft accounts and instead choose a local account, because using a Microsoft account means is that you have put some of your personal information in the cloud and this is not a good way of security.To select a local account, go to Settings> Accounts> Your info and select 'Sign in with a local account'.
5. Ensure user account control is always enabled: UAC (User Account Control) is a Windows security measure, primarily responsible for preventing unauthorized changes (being initiated) by applications, users, viruses or other types of malware) for the operating system.UAC will ensure that changes will only be applied to the operating system when approved by the system administrator.So please always enable this feature.
6. Perform common post-save activities: Always be prepared for 'worst' situations when it comes to dealing with security threats, that is, your system is completely out of control. .Therefore, make regular backups of your system (both online and offline) so that all data will not be lost in case your computer is severely affected by threats. security or trouble cannot fix hardware.
7. Update your browser regularly: The browser is what we use to access the Internet.Therefore, security holes in the browser also mean that the path to 'entry' security threats into your system becomes more open.Therefore, just like with operating systems and other applications, always update your web browser to the latest versions.Other security measures you can take with your browser: 1)Choose a private browsing mode to prevent sensitive details from being stored.2)Prevent or block pop-up windows.3)Configure web browser security settings to improve security .

8. Turn off location tracking: If you are using Windows 10 or any other version that contains Location Tracking, it is best to turn it off or use it only when actually necessary.For example, if you want to know the weather information where you live or different nearby stores . To turn off location tracking, go to Privacy> Location click the Change button and then move the bar. Slide from On to Off.
9. Use the Internet more wisely: All security measures listed here will become useless if you are not cautious when operating online.Therefore, make sure that you don't click on a dangerous search link, download malicious attachments from unknown emails or from untrusted sites, as well as avoid access to websites. suspect…

The Windows operating system is probably one of the best operating systems available today, and that's why it has become so popular and widely used around the world, although some still contain some. security threat.To be fair, there is no operating system that is absolutely safe, it is only a matter of ensuring that you can equip yourself with the necessary knowledge of security as well as the use of products. Suitable security products and adhere to the best security methods.Doing these will ensure that your Windows operating system is always safe in any situation.

Wishing you a great security system!

See more:

1. The most scary computer viruses ever
2. How to kill virus automatically delete Unikey, Vietkey, Zalo on the computer
3. How do I know if someone has accessed and used your computer?
4. No need to install any software, this is how to protect your folders safely