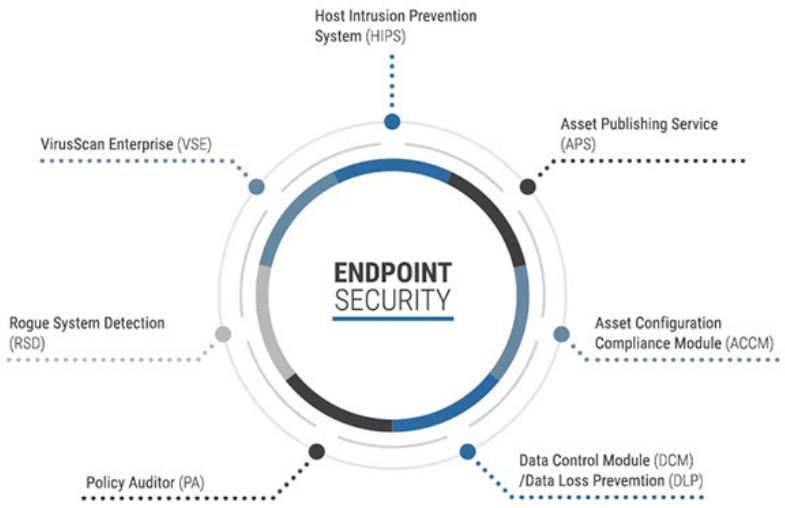
Top 5 trends in endpoint security for 2018

Endpoint security is a type of security that is growing rapidly.

Endpoint security is a type of security that is growing rapidly.Today, agencies and organizations are constantly pushing for ways to coordinate the control of computers, servers and phones on their networks to eliminate malicious software and intruders. permissions as well as other potential security risks.

It can be said that endpoint security in many ways is considered as a direct descendant of the forms of computer protection that appeared in the dawn of the information technology (IT), but with speed extremely fast development.Take a look at the achievements this security method has achieved in recent years, so we can easily recognize that.Security technology developers have also now considered endpoint security to be an important area, able to bring a stable source of revenue for years to come.

What is endpoint security?



A little bit of theory, endpoint security is a security method that focuses on keeping the endpoint devices secure (including personal computers, phones, tablets and support devices). Other network connections) to keep the entire network secure.This sounds like no other than the concept of firewall and antivirus software on computers that we already know, and actually in the first few days, people once suspected that security points The end is just a marketing term to make the antivirus service sound more professional, something more 'specialized'.

But the factors that help us distinguish end-to-end security services from simple home computer protection processes are the fact that security tools on endpoints are often managed. and the use of focus on the scale of

enterprises and organizations is essential.Endpoint security measures run on two floors: There is agentsthat software running in the background on endpoint devices and a terminal security management system that focuses on monitoring and controlling the agents in the server.This entire management system can be monitored by IT staff or another automated system, or it can be both.

Sometimes you will hear the endpoint protection term used to replace endpoint security.Gartner defined the endpoint protection platform as "a solution that converges the security functionality of terminals into a single product, providing services such as anti-virus, anti-spyware, wall personal fire, application control and server intrusion prevention types (such as blocking behavior), and linking these services into a unified and coherent solution ".So seriously, the term endpoint protection can include security products that are not centrally managed, although these security products are also marketed and targeted at enterprise-level customers. .And, yes, sometimes security companies can also offer their antivirus products as "endpoint security."This is a fuzzy marketing concept, fraudulent, so if you are a person who needs security services, be wary!

Trends in endpoint security

Of course, when threats are constantly evolving in a more dangerous, more sophisticated way, endpoint security measures will have to be developed as well.In 2018, and also in the first half of 2019, end-to-end security service providers will have to work seriously to keep up with the following five trends:

Machine learning and artificial intelligence (AI). As threats increase, they will become popular, and the speed of transmission is so fast that the already passive containment measures are now more difficult to keep up.Therefore, now, most of the security processes of each endpoint security will have to be increasingly enhanced with automation, combined with machine learning and artificial intelligence to check traffic and corpses. identify threats, and only the most urgent, urgent needs are informed and need human hands.For example, machine learning capabilities have been fully utilized in Microsoft endpoint security services.

Endpoint security based on SaaS. Traditionally, central endpoint security management systems are often operated on a server or even a device, and deployed as well as held accountable by organizations and businesses.But with the fact that cloud-based or SaaS services are becoming more and more reliable as an integral part of IT, we can see that endpoint security management can be provided as a service. , with well-known suppliers such as FireEye, Webroot, Carbon Black, Cybereason and Morphick.In certain ways (unlike switching to machine learning), companies are reducing the responsibility of endpoint security management for their internal employees, in other words, they are trying to trying to limit internal staff intervention into endpoint security management systems, which is why they need security providers, and of course many SaaS services are also on the trend. Apply machine learning and AI to their services as mentioned above.The result is a rapid increase in the number of security service providers by each market segment.

Protection against anonymous attacks. Anonymous attacks (caused by malware that are entirely in the RAM system and never written to the hard drive) are a growing attack method at an alarming rate. .End-to-end security service providers are also rushing to provide the necessary protection against this type of attack.It is often necessary to combine this with automation and machine learning, because existing tools can not distinguish fake attacks, and pursuing them will only consume precious IT resources.Looking at them, this will be an important feature that any end-to-end security service provider will need to provide to its customers in the future.

Place IoT devices (Internet of Things) under protective shields .One of the big stories about Internet security over the past few years is that billions of internet connections come from many different devices like cameras, sensors, routers . and other devices, which are quietly perform your work without any protection that should have been.A simple example can be obtained from Mirai botnet, a device that university students create by seizing control of thousands of sealed camcorders to launch DDoS attacks against their servers. Minecraft player, causing some of the biggest denial of service attacks ever recorded.Although there are many IoT devices running separate operating systems that are difficult to manage, most are being operated on popular platforms like Linux, iOS, Android or even Windows variants. , and endpoint management service providers are beginning to develop software that can run on these devices to establish the necessary protections.

Minimize complexity and increase proactivity

As the market segment has gradually shaped and started to grow, many end-to-end security service providers have provided a wide range of specific security tools, each targeting one type of attack. public or a specific type of vulnerability.As a result, companies with up to seven different child security software run on each endpoint device, and importantly they all need to be managed separately.End-to-end security companies are aiming to unify their services into unified and seamless models.

So what do we need to do in the future?The ESG study surveyed network security and IT professionals about the biggest end-to-end security challenges they face.In addition to false alarms and a lack of automation, many surveyed people expressed their desire for an integrated troubleshooting capability, including the process of terminating, deleting files and restoring images. The system . all of this will help IT staff limit the need to reconstruct compromised systems.Hopefully the service providers can listen to these practical ideas.

Endpoint security software and tools.

You can consult Gartner's award winning security applications of customers in 2017 to get an overview of end-to-end security service providers.You'll find familiar names like Microsoft and Symantec, along with other specialized companies, such as Cylance, CrowdStrike and Carbon Black.Gartner also provides links so you can make comparisons between endpoint security software.

Below is a list of some of the excellent endpoint security services selected by consumers in 2017:

1. **Digital Guardian:** Guardian Threat Aware Data Protection Platform is at the forefront of efforts to combat complex threats, provide an endpoint security service that can be deployed on-site or as a support consulting service. Extremely good with optimization and automation.
2. **enSilo:** The enSilo platform provides traditional endpoint security with the ability to provide additional protection after being attacked.It can also 'trap' threats, keep them in place and make them harmless until experts can analyze and investigate.
3. **Minerva** : **Minerva's** Anti-Evasion platform aims to identify new types of malware.The idea here is that most normal threats will be prevented by traditional anti-virus software and Minerva will try to prevent and detect remote threats.
4. **Promisec:** Organizations may need assistance in managing the detection of potential threats and their appropriate responses to threats as well as many problems that arise every day in the size of the business. career.Promisec can provide such help.Bringing the terminal into a strict and fully automated security platform and can be managed easily and flexibly.

See more:

1. Hack SIM: Things to know and how to avoid
2. The most basic insights to becoming a Hacker - Part 1
3. Free online virus scanning tools online
4. Some free "hack" tools