ComputerWeekly.com | TechTarget

E-guide

CW+ Content

Endpoint Security: from A to (N)Z

In this e-guide

In this e-guide:

The growing adoption of the internet of things and mobility among enterprises in Australia and New Zealand (ANZ) has without a doubt increased the attack surface that cyber criminals can exploit to conduct reconnaissance activities before launching a full-scale attack. This makes endpoint security more critical than ever– by providing a means for enterprises to identify potential vulnerabilities in devices that sit on the edge of a network, malicious activity that could lead to danger, as well as enforce strong end-user security practices. In this e-guide, find out how ANZ enterprises are approaching endpoint security and the tools you can add to your endpoint security arsenal.

In this e-guide

Endpoint security management

Margaret Rouse, WhatIs.com

Endpoint security management is a policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources. Endpoints can include PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point of sale (POS) terminals.

Endpoint security management systems, which can be purchased as software or as a dedicated appliance, discover, manage and control computing devices that request access to the corporate network. Required elements may include an approved operating system, a VPN client and anti-virus software with current updates. Devices that do not comply with policy are given limited access or quarantined on a virtual LAN (VLAN). Endpoints that do not comply with policy can be controlled by the system to varying degrees. For example, the system may remove local administrative rights or restrict Internet browsing capabilities.

Endpoint security systems work on a client/server model in which a centrally managed server or gateway hosts the security program and an accompanying client program is installed on each network device. In a software-as-a-service (SaaS) delivery model, the host server and its security programs are maintained

In this e-guide

remotely by the vendor. In either delivery model, when a client attempts to log onto the network, the server program validates user credentials and scans the device to make sure that it complies with defined corporate security policies before allowing access to the network.

In this e-guide

Frame founder talks up VDI approaches in Australia

Beverley Head,

When Nutanix paid $165m for Frame last year, the virtual desktop infrastructure (VDI) specialist didn't have an office in Australia – but it did have Australian customers who were using its software.

During a whistlestop visit to Australia to attend Nutanix's Next On Tour conference, Nikola Bozinovic, the founder of Frame and now vice-president of Nutanix, declined to name or quantify local users, but said universities and software companies had been among the early adopters locally.

The potential fly in the ointment for Frame's future success in Australia is the issue of bandwidth, which is critical for a seamless VDI or desktop-as-a-service (DaaS) offering. Without fast reliable connectivity, VDI and DaaS fall over as a concept.

"There is a little bit of sentiment that bandwidth-wise, it's not as good as was promised," said Bozinovic.

"Australia is not the best in bandwidth, but it is far from the worst. The national broadband network over promised and under delivered," he added,

acknowledging that bandwidth was a particular challenge for rural and regional businesses.

According to the *Speedtest Global Index*, Australia ranked 5th in the world for mobile internet access in February 2019. Its ranking plunged to 59th when it came to fixed broadband access which most enterprises would use to support VDI.

The drivers to use VDI are pretty much the same whatever the location. Bozinovic said the initial attraction was economy as VDI makes it cheaper to access centralised content. "But I think that has evolved," he said.

"The use cases are now primarily around security and to allow bring your own device. People travel and they want access to a centralised solution."

Business agility and flexibility with no compromise of security are key characteristics of a VDI approach.
At the same time, VDI allows enterprise to account for "data gravity", which is a growing issue for organisations managing large information collections. Centralising processing and keeping it close to corporate data stores helps rein in latency.

There are also cost advantages – especially for organisations which have highly elastic workloads. VDI allows enterprises which may hire seasonal workers, for example, to provide them with secure access to central systems through their

own device, a thin client, or an ageing machine, rather than having to provide a state-of-the-art PC for every worker.

Asked whether he saw the rise of software as a service (SaaS) as any threat to the VDI model, Bozinovic said there were very few organisations that ran entirely on SaaS. Instead, most use a mix of cloud-based and legacy solutions. "A lot of customers are using SaaS delivered by VDI," he said.

Bozinovic also believes that although VDI has traditionally been the province of large enterprise customers, it is now being adopted more widely. "In the past, it has been so complex that it hasn't been for the faint of heart. But when you make it easy, it can work for companies with 50 or 100 people," he concluded.

In this e-guide

Toyota Australia under cyber attack

Aaron Tan, Executive Editor, APAC

Toyota's Australian subsidiary has been hit by a cyber attack, leaving employees without access to their email messages for days, according to local media reports.

In a statement today, Toyota Australia confirmed that it had been a victim of an "attempted cyber attack", and that no private employee or customer data had been accessed so far.

"The threat is being managed by our IT department who is working closely with international cyber security experts to get systems up and running again," it said, adding that it has no further details about the origin of the attack at this stage.

The incident was first reported by a local radio station, which claimed that the company's staff was sent home. Those who needed to carry out their duties were told to use other forms of communications such as telephone and face-to-face meetings instead.

At press time, the contact information on Toyota Australia's website was unavailable. The company apologised to customers for the inconvenience,

noting that it was experiencing technical difficulties and was unreachable via phone or email.

The latest cyber attack in Australia follows a breach of the federal parliament's IT network earlier this month. Australian prime minister Scott Morrison later told parliament that the country's cyber experts believed a sophisticated state actor was behind the breach.

"From the breach of Australia's parliament and political parties to an attack on the EU's diplomatic cables, there is a worrying global trend emerging of geopolitically fuelled cyber attacks," said Andrew Tsonchev, director of technology at Darktrace.

Noting that nation states and cyber criminals are ramping up in sophistication to infiltrate what is typically considered the world's most secure networks, Tsonchev said no system, even those belonging to government, are safe from cyber attacks.

"With Australia's election looming and those in the US next year, we can expect a hike in disruptive attacks that deliberately attempt to meddle with the instruments of democracy," he said. "Protecting data integrity has never been so critical and the public sector will need to leverage the strongest defences to overcome these skilled adversaries."

In this e-guide

How to address endpoint security issues caused by users

Kevin Beaver,

A crucial function of endpoint security is protecting users from their own mistakes and missteps.

From human error to technical oversights and weaknesses in business processes, there are many ways that users can cause endpoint security issues. Users can make mistakes even if they understand the risks to the business because their desire for expediency and instant gratification is too strong. Some of the problems are the same behaviors IT professionals have been fighting for decades, but others aren't as obvious.

There's no amount of security awareness and training that will make this go away completely, but IT professionals must understand each of the endpoint security issues users might cause and the best practices for handling them.

Endpoint security issues caused by users

Choosing weak passwords. Password policies for Windows domains, websites, applications and mobile devices are often lax. Users follow whatever

guidance they are given even if it's not good advice. This leads them to create passwords that hackers can easily guess or crack. Users share the passwords between systems sometimes -- mixing both personal and business passwords -- and might write them down and store them on sticky notes.

Ignoring patch notifications. Because most users don't see the value in running patches and rebooting their desktops and apps, they likely ignore notifications for patches whether the patches are for desktops, such as Microsoft Windows or Apple macOS, or third-party software, such as Java and Adobe Acrobat Reader. Doing so creates security vulnerabilities in the endpoints.

Clicking links and opening attachments without question. It's so simple for hackers to get into a network by phishing users. Users might click malicious links, open unknown attachments or even provide their login credentials when prompted. If phishing security is not up to snuff, no other security controls matter because once an attacker has a user's login information, he has full access to the endpoint.

If phishing security is not up to snuff, no other security controls matter.

Bypassing security controls. Most of the time, endpoints automatically give users local administrator rights. With these rights, users can perform tasks that are ultimately harmful to their endpoint's security, such as disabling antimalware software and installing their own questionable software.

Unfortunately, it can be difficult to detect the harmful changes a user might make on his device if he has local admin rights. As a result, IT might not realize that a user has done something dangerous, which could leave business assets exposed.

Connecting to unsecured Wi-Fi. Users might connect to practically any open wireless network without question if it means they can access the internet. Even if IT instructs users to verify their connections and to only use trusted Wi-Fi networks, all those teachings go out the window the second a user only needs to get online for a few minutes to check email or social media.

Buying and selling personal computers without resetting them. It's amazing how many people don't reset their computers by reinstalling the OS when they sell them. Users who do not reinstall the OS expose personal information and place business assets, such as virtual private network connections, at risk. It is dangerous to recycle old computers without taking precautions.

How can IT address these endpoint security issues?

Users can be careless and often take the path of least resistance simply because it's most convenient. In reality, a small number of people and choices cause the majority of endpoint security issues.

IT can't control user behavior, but it can control users' desktop permissions. IT professionals must enforce security policies that prevent users from taking harmful actions rather than only telling users how to avoid those actions.

To effectively prevent these endpoint security issues, IT must determine what specific user actions are undermining the security program. IT pros should create processes and controls to prevent user mistakes, evaluate how effective they are and make alterations when necessary to ensure that the policies can handle the latest security threats.

In this e-guide

In this e-guide

How EDR tools can improve endpoint security

Kevin Beaver,

When IT professionals don't use the proper endpoint security practices in a modern workplace, they can use the same old methods and expect different outcomes.

If users download malware on PCs, laptops or mobile devices, hackers can gain access to those assets and use them as an entry point to an organization's network. Endpoint detection and response (EDR) tools can help to prevent malware. EDR tools are relatively new to the market, however, and some organizations don't understand what these tools can do.

What are EDR tools?

EDR tools have evolved into excellent resources for fighting advanced threats and responding to incidents on network endpoints. With EDR tools, IT pros gain a proactive and adaptive approach to endpoint security, often focused on malware security.

These products combine features such as behavioral analysis, behavioral blocking, application control and app whitelisting, along with overall network monitoring and incident response. IT could find another security tool that offers these controls, but EDR tools provide unique value because IT can remediate any endpoint weaknesses and provide forensic details to help with a quick incident response.

EDR tools also integrate into other security tools to accomplish the following tasks:

- improve visibility into endpoint behaviors and processes;
- manage physical and information assets;
- enhance response and remediation efforts; and
- assist with ongoing data collection to provide IT with device analytics.

While some EDR tools integrate easily with other endpoint security tools, many EDR tools require specialized APIs to do so. EDR vendors provide their customers with these APIs to integrate with other tools for data visualization, incident reporting and ticketing.

Are EDR tools right for your organization?

With EDR tools, IT pros gain a proactive and adaptive approach to endpoint security, often focused on malware security.

Organizations can use either an on-premises EDR tool or an EDR service from a vendor. Cloud-based tools can perform the same functions that on-premises tools do without affecting local storage and memory resources.

Some EDR vendors, such as Carbon Black and CrowdStrike, focus more on cloud-centric approaches to minimize the workloads that run on device and on premises. Other options, such as those from Symantec and FireEye, run well on premises.

Before purchasing EDR tools, however, IT pros should ask themselves the following questions:

- Do we fully understand our current level of endpoint risk? Do we have all the right information from vulnerability and penetration testing, control audits and so on?
- Do we have proper standards for addressing the big security gaps? What do our policies say?
- What reasonable steps can we take to close the gaps and minimize the risks? Do we need to address our users, the technical areas of endpoint security or our business operations and workflows?

IT should come up with a plan to close the gaps and then roll out the fixes. As with most facets of security, there's always more that IT can do to keep endpoint threats in check.

In this e-guide

12 essential features of advanced endpoint security tools

Linda Rosencrance, Contributor

As endpoint threats become more sophisticated and abundant, so does the need for more advanced endpoint security tools. An organization can improve the security of its endpoints -- including laptops, desktop PCs, mobile devices and servers in the data center -- by using software that can rapidly detect, analyze, block and contain in-progress attacks. These security systems must collaborate with each other as well as with other security tools to enable administrators to more quickly detect and remediate these threats.

Endpoint security tools use encryption and application control to secure devices that are accessing an organization's network and monitor and block risky activities. Endpoint security systems typically employ a client-server security model, consisting of a centrally managed security tool to protect the network and client software that's installed on each endpoint that accesses the network. Some products are SaaS-based, allowing administrators to remotely maintain both the central and endpoint security systems.

In addition to securing endpoints, encrypting data on removable storage devices and endpoints helps secure them against data loss and data leaks. And

application control stops users from installing unauthorized applications that could create vulnerabilities in the company's network. BYOD policies and the ability of employees to connect from anywhere have intensified the need for endpoint security tools.

Features to look for in an endpoint security tool

Detecting threats as early as possible is crucial. The longer a threat sits in the environment, the more it spreads and the more damage it can do.

Endpoint protection of enterprise systems is an efficient method of managing software deployment and enforcing IT security operations' policies. However, it does more than protect a network from malware. IT administrators can use endpoint security for a number of operation monitoring functions and data backup strategies. An endpoint security product should include the following key features:

1. **Protection from threats spread via email.** An organization's endpoint protection must scan every email attachment to protect the company from attacks.

2. **Protection from malicious web downloads.** The technology should analyze incoming and outgoing traffic and provide browser protection to block malicious web downloads before they're executed on endpoints.
3. **Enable easy application and device control.** This enables organizations to control which devices can upload or download data, access hardware or access the registry.
4. **Advanced machine learning.** This analyzes massive amounts of good and bad files and blocks new malware variants before they're executed on endpoint devices.
5. **Protection from exploits.** This protects against zero-day vulnerabilities and memory-based attacks.
6. **Behavioral monitoring.** This technique uses machine learning to monitor behavior-based security to determine risks and block them.
7. **Data loss protection.** DLP prevents access violations caused by insiders, including employees, and intentional or unintentional data loss in the event of a system breach. DLP enables organizations to block files that are transmitted via email or instant message as well as files that are uploaded to the internet.
8. **Third-party integrations.** Endpoint security tools should communicate with other security systems in the organization's environment. These tools should share and ingest threat intelligence so they can learn from each other. Using open API systems, endpoint security products should integrate with other security tools, such as Active Directory, intrusion prevention, network monitoring and security information and event

management.

9. **Reports and alerts.** These provide prioritized warnings and alerts regarding vulnerabilities as well as dashboards and reports that offer visibility into endpoint security.

10. **Incident investigation and remediation.** This includes centralized and automated tools to provide automated incident response approaches and step-by-step workflows to investigate incidents.

11. **Flexible deployment options.** Endpoint security tools should adapt to the organization's needs and environment, offering on-premises or cloud deployment options. These tools should also offer protection for every endpoint in the company regardless if it's a PC, Mac, Linux, iOS or Android device.

12. **Rapid detection.** Detecting threats as early as possible is crucial. The longer a threat sits in the environment, the more it spreads and the more damage it can do.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com