Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

appreciation. Even a simple 'thank you' goes a long way. Further to this, investment in your team's continued development is another way to improve satisfaction levels, and an opportunity that can improve its knowledge on security.

Offering training – such as courses on cyber security and how to protect the business – is another tack to take. By doing this, the organisation is showing that it is willing to invest finances and time into individuals in order to help them grow as professionals. Meanwhile, it is also benefiting the company in its continued fight against insider threat. There are positives on both sides of the equation, and employees will not only come away from training sessions feeling valued, but better equipped to protect their employer.

Being ready as an organisation

Only when every employee is fully trained and understanding of necessary security procedures, and is 'on board' with those procedures, can an organisation begin to properly protect itself from insider threat.

Organisational readiness is a factor that too many overlook in their pursuit of complete security. The right foundations need to be set before any business can expect to produce a top-drawer security system. Once employees understand the importance of their role in protecting their company and when they feel valued enough and buy into a secure culture, at that point businesses can expect to see vast differences with the technology that they're introducing.

Staff need to know their own worth. Too many have access to data that they shouldn't have, and this is something that they often won't recognise. There are, of course, ways to revoke this access in order to remove any risk, but where that isn't possible, staff need to be happy in their role and aware of any possible security risks. Adequate training and a vigilant attitude are integral to the fight against insider threats and it all begins with organisational readiness.

About the author

Mark Rodbert is CEO of Idax Identity Analytics. He has over 20 years' experience of running technology for large organisations. He has delivered global, business-critical, technology change addressing IT and operational risk, big data, analytics and IT security. He founded Idax in 2014 as he saw the opportunity to use the emerging techniques of analytics to address the endemic issues of identity management and insider threat. Prior to Idax he was head of IT strategy for Barclays Wealth, and head of identity management, IT risk and control for Credit Suisse. He is visiting professor in computer science at the University of York, a fellow of the Royal Society for the Encouragement of Arts, Manufactures and Commerce, and speaks regularly on many topics associated with identity risk.

References

1. 'Insider Threat Report'. Securonix. Accessed Jul 2020. https://pages.securonix.com/rs/179-DJP-142/images/2019-Insider-Threat-Report-Securonix.pdf.
2. 'The engaged employer'. Moorepay. Accessed Jul 2020. www.moorepay.co.uk/resource/engaged-employer-report/.
3. 'Company culture and employee engagement statistics'. CultureIQ, 4 Jan 2018. Accessed Jul 2020. https://cultureiq.com/blog/company-culture-employee-engagement-statistics/.
4. Kashyap, Vartika. 'Surprising Stats on Employee Recognition You Need to Know (+ Key Insights)'. ProofHub, 9 Jul 2019. Accessed Jul 2020. www.proofhub.com/articles/employee-recognition.

Managing endpoints, the weakest link in the security chain


Dave Waterson

Dave Waterson, SentryBay

Endpoint security is a term open to interpretation. Traditionally, an endpoint would be any device or node connected to the LAN or WAN, such as a workstation or end-user PC, or a modem, a hub or a switch. But now endpoints incorporate a multitude of additional digital devices from laptops, tablets and mobile phones, which sit on the edge of the network, through to network printers, consumer and industrial IoT devices and point-of-sale systems.

Inevitably, securing this ever-expanding portfolio of endpoint technology has become an urgent necessity, not least because these devices represent a significant risk to the cloud ecosystem and the increasing number of global enterprises that are moving inexorably towards it.

Endpoints are the weakest link in the security chain. According to a recent report, 70% of breaches originate at the endpoint, and 42% of endpoints are unprotected at any given time.[1] Since

the end of March, when businesses were obliged to ask their employees to work from home in order to contain the spread of Covid-19, the regular use of unprotected endpoints to access corporate applications will doubtless have grown further. Last year the business endpoint security solution market was predicted to grow in revenues by 20% from 2019 to 2023, taking it from $7.1bn to over $13.3bn. But in light of the global lockdown, and the necessity to quickly protect new devices, this figure could rise even more sharply.[2,3]

Understanding the risks

To decide how best to tackle breaches at the endpoint, it's important first to understand the actual risks that they pose. First, unprotected devices tend to be those that are used by remote workers, or as part of a BYOD agreement. This means that they have a lower security posture from the start, partly due to out-of-date anti-virus or Internet security software or because they are shared. In addition, they have a higher risk of compromise because they could be running counterfeit or unlicensed solutions, or they are operating from an untrusted network.

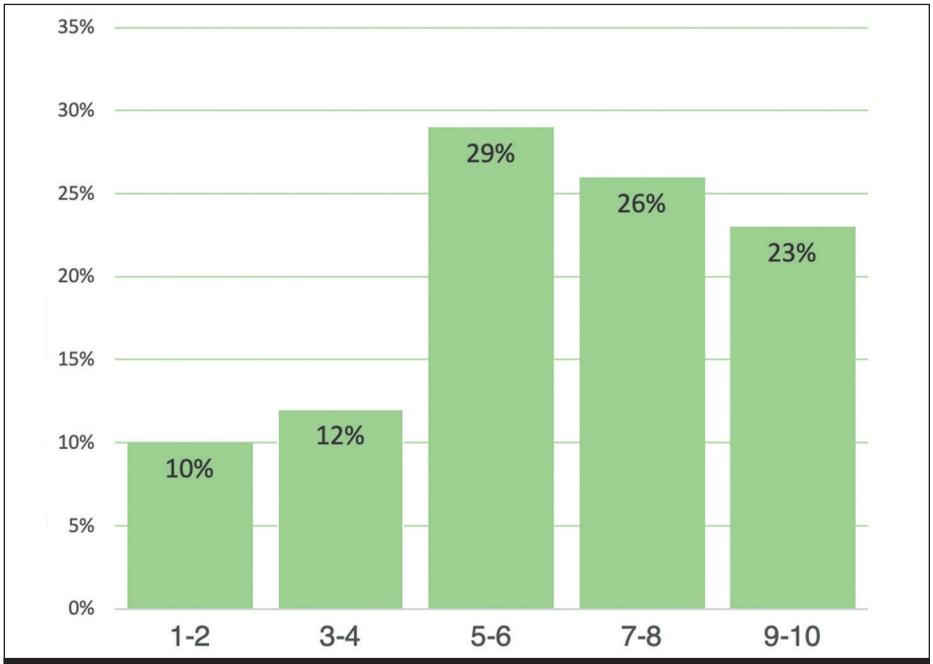
"A survey carried out in April found that already 42% of people working remotely had received suspicious emails and 18% had tackled a security breach"

In recent months, the move to coronavirus lockdown happened quickly and organisations had virtually no time to prepare. Their ability to rapidly deploy security on all devices that employees would be using from home, or remotely, was limited, as was the opportunity to assess, let alone address, any security deficiencies. A survey carried out in April found that already 42% of people working remotely had received suspicious emails and 18% had tackled a security breach.[4] In addition, 49% of employees felt vulnerable due to the insecurity of the endpoint devices they were using.

Answers to the question, 'Why is your security team not effective in detecting endpoint attacks?'. Source: Ponemon/Sullivan.

Unmanaged devices accessing a network remotely usually present a higher risk in terms of sensitive data – including corporate login credentials – being stolen via attacks involving keylogging. Along with spyware, keylogging is ranked as the highest-ranking global malware by the NTT 'Security Threat Intelligence Report'.[5] Other types of attacks to which endpoints are vulnerable include screen capture/screen grabbing, man-in-the-browser, saved account detail harvesting, screen mirroring, man-in-the-middle, DLL injection and RDP double-hop. At the moment, with so few people working within the security of an on-premise network, the risk is increased hugely.

When it comes to endpoint security, protection against keylogging should be a priority. With a keylogger installed, it makes no difference how secure the data of an organisation is, a breach can take place from the moment a user logs in. While API-based keyloggers are the most common and work by infiltrating the keyboard API to log the keys that



Answers to the question, 'How effective is your security team's ability to detect endpoint attacks?', where 1 = 'not effective' and 10 = 'highly effective'. Source: Ponemon/Sullivan.

are pressed and store a record of this to be accessed by cyber criminals later, the more dangerous are kernel-based keyloggers. These not only sit deeper in the system and record key strokes as they pass through the system, but they are also considerably more difficult to identify and to eliminate.

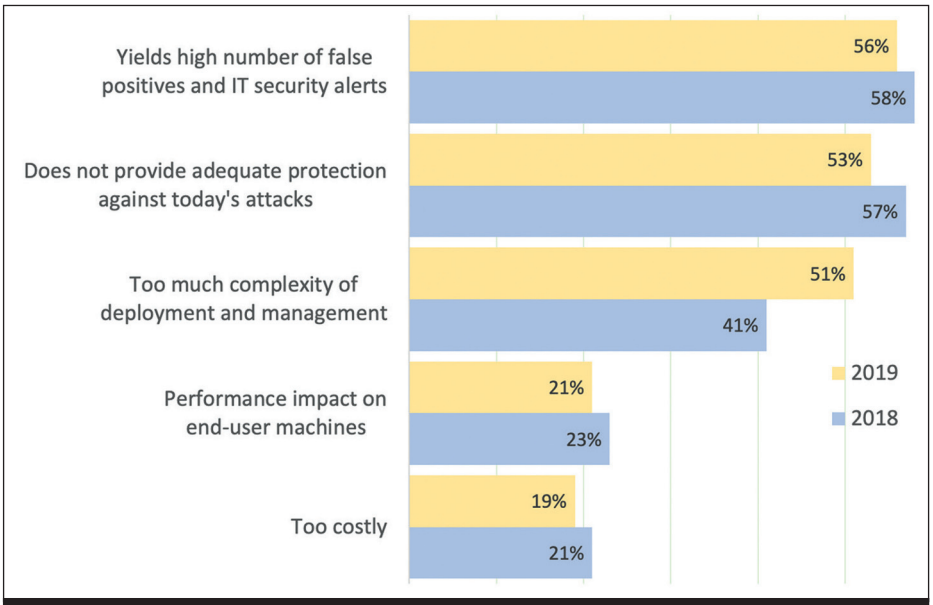
"Malware detection, particularly detection of newly released kernel-level malware, is now incredibly difficult and increasingly complex"

Other keyloggers include those that are built into the keyboard or installed by a USB device, others that analyse the different sounds that keys make in order to determine which ones were used, and form grabbers that record data entered onto web forms, which then attack websites to gain access to names, addresses and credit card details. It was this technique that was used when British Airways was attacked in 2018, resulting in 380,000 passenger details being compromised and a fine for the airline of £183m.

Prevalent protections

The most prevalent protections against endpoint keylogging currently are solutions such as anti-virus (AV) and endpoint detection and response (EDR). Integral to both these technologies is malware detection. However, malware detection, particularly detection of newly released kernel-level malware, is now incredibly difficult and increasingly complex. The SANS Institute concluded that less than 50% of cyber attacks are detected by anti-virus software.[6] Detection evasion techniques such as polymorphism and stealth-mode activation during sandboxing, result in fewer and fewer instances of new malware being detected.

While AV and EDR may have their limitations, malware detection still has a place; however, it should not be relied upon exclusively. Rather, a layered approach to security should be taken



Answers to the question, 'What are the biggest challenges with your traditional anti-virus solutions?'. Source: Ponemon/Sullivan.

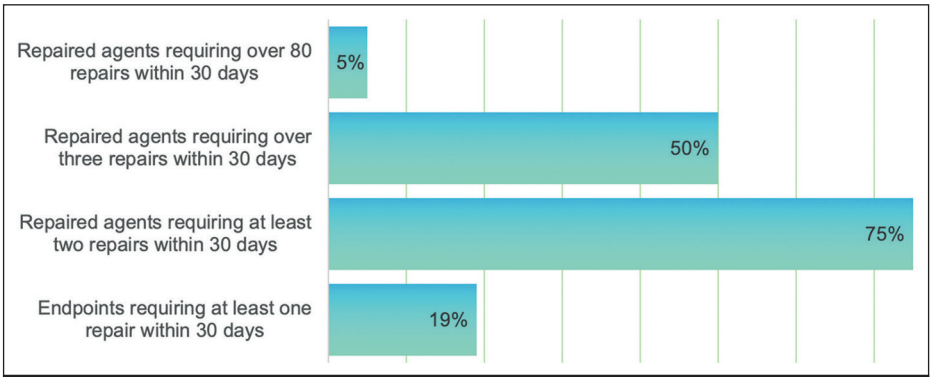
(defence in depth), where multiple security controls complement and reinforce each other. A layered approach provides strength and depth, ensuring that although a specific attack may bypass one security measure, it will be thwarted by another. The most precious asset – data, and the specific applications that handle sensitive data – should be placed at the centre, with security layers wrapping it protectively.

New protection techniques that do not rely on detection but securely wrap sensitive data and applications that process data, are beginning to emerge to become 'best of breed'. These do not wrap around the entire endpoint device, just the applications – those that interact with data going into the cloud.

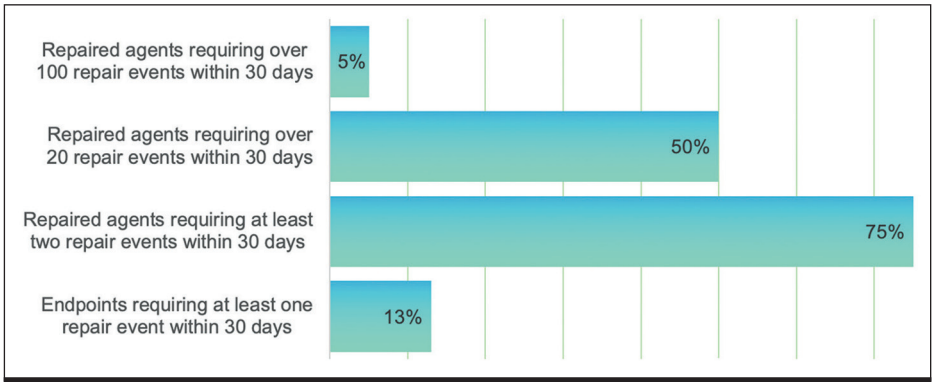
Consider just how extensive the list of applications is, and what needs to be wrapped or secured in order to protect it: online office tools; SaaS application access; enterprise applications such as accounting, personnel and CRM; SAP or Oracle applications and those remote access solutions such as Citrix, VMware and RDP. By securing the data that is entered into these applications, organisations are, in effect, ensuring that the unmanaged devices being deployed outside the corporate perimeter are as secure (and in some case more secure) than standard managed corporate devices.

Containerisation

One approach is to use containerisation and virtualisation, both of which encapsulate an application in its own operating system environment. While containerisation shares the operating system with its host, a virtual environment incorporates its own operating system. Containerisation is a form of fast, lightweight virtualisation (it has a smaller file



Rates of failure for endpoint client/patch management agents. Source: Absolute.



Rates of failure for endpoint encryption agents. Source: Absolute.

size, consumes fewer resources and is faster to provision). This is why containerisation is sometimes called operating system virtualisation. Both containerisation and virtualisation share the host's kernel components, which opens up the potential for vulnerabilities.

Applications that run within a container need all the resources that are likely to be required to be inside the container (dependencies, libraries, configuration files and all other related files). There are different ways of creating containers, all requiring varying degrees of complexity to be provisioned. Utilising the Windows operating system to provision a new user or new desktop are low-overhead, easily provisioned methods. Docker containers were originally developed for Linux and there are now Windows versions as well and these share the host operating system.[7] Windows Defender Application Guard creates single-purpose containers for running untrusted websites, isolating potential threats from the website from other applications and the rest of the operating system.[8] The method chosen for creating the container should be appropriate to the situation.

"Containerisation means that applications are executed in a controlled, clean environment, which narrows the attack vector – only the minimum services can be included in the container"

An application running inside a container has no access to applications or environment settings outside the container (ie, both those on the host operating system as well as those in another container), and likewise, applications outside the container cannot access applications inside. This provides two-way security benefits, as applications within a container have a degree of isolation from malicious applications residing on the host or in other containers, and any malicious code inside the container is isolated from outside.

Containerisation means that applications are executed in a controlled, clean environment, which narrows the attack vector – only the minimum services can be included in the container. These environments are consistent, predictable and replicable. Containers only exist while they are needed, and environmental parity of containerisation allows laboratory testing to be extended to real-world situations with higher levels of confidence.

Additional measures

While containers offer many advantages for organisations, it's important to recognise that there are limitations. Containerisation security can potentially be compromised through malicious applications designed to gain permissions to execute inside the container or through the kernel – such as kernel-level keyloggers or screen capture. Docker containers may also allow network traffic to move between containers by default, which opens the door to hackers.

The answer to this is to ensure that the applications involving sensitive data within a container are bolstered with additional security measures to those built into the container itself. The most effective and comprehensive way to do this is by using a combination of simple containerisation, injected security and anti-keylogging which can securely wrap remote access, enterprise and SaaS applications being used by endpoint devices.

Unfortunately, as mentioned above, most AV and EDR solutions fall short of the mark. Rather than identifying 100% of threats, they barely cover half because they were designed to work on devices within the corporate perimeter rather than on the unmanaged remote and BYOD endpoints that are currently being widely relied upon to connect to the network. EDR can detect malware that it has prior knowledge of, or which demonstrates common behavioural techniques that mark it as malware, but cyber criminals have built tools designed specifically to evade detection and they test these on EDR solutions before releasing them.

In addition, EDR is impractical to deploy on unmanaged devices because this type of defence requires large and experienced teams of analysts working around the clock to investigate the more than 10,000 alerts per day that are generated. The cost of this and intensity of management, plus the challenges inherent for end-users, are prohibitive.

What is needed, therefore, to protect endpoints is a baseline security profile that does not rely solely on detection, but instead neutralises the effectiveness of any malware that gets through other protections that have been put onto the device. It should offer techniques to tackle the key threats to endpoints and applications including keylogging, screen capture, session hijacking and common malware, man-in-the-browser, man-in-the-middle, DLL injection and browser-saved account detail harvesting. It should protect logon credentials and extend across an entire session while also securing sensitive data into local applications, and it should also eliminate browser compatibility issues.

Other considerations

There are also other considerations that must be taken into account, which have become particularly acute in the current lockdown environment and will remain

so as we move into the 'new normal' of the post-Covid-19 workplace. To be effective, deploying security solutions for endpoints must be easy and updates should be automatic.

"Endpoints need not continue to be the weakest point in the organisation cloud ecosystem. Organisations can implement measures to minimise the likelihood of a high-profile breach"

It is unlikely that one solution can cover all threats, so if standard anti-virus and EDR protection is already in-place, subsequent protections based on containerisation, anti-keylogging and anti-screen scraping, must be complementary and compatible. Finally, the importance of regulatory compliance must be taken into account. Security solutions should meet with PCI, PSD2, HIPAA and General Data Protection Regulation (GDPR) regulations. The fact that an organisation's employees are working from home will be no defence if a GDPR breach occurs and it is facing a hefty financial penalty for want of endpoint security that is fit for purpose.

The technology exists to ensure that endpoints need not continue to be the weakest point in the organisation cloud ecosystem. Organisations can implement measures to minimise the likelihood of a high-profile breach. By securing the input of sensitive data and by wrapping security around the applications that handle sensitive data, organisations can add another layer, boosting the protection of endpoint devices. In today's world with more and more data being handled outside of the protection of the corporate perimeter, with BYOD and working from home, emerging technologies can help with both compliance and the overall security posture.

About the author

Dave Waterson is CEO at SentryBay and an expert in endpoint and application security. His technical focus areas are anti-keylogging, anti-phishing, data security, secure browsing, IoT, mobile security, identity theft and cloud-based security. He was included among the top 10 tech thought leaders identified by AT Kearney at the World Economic Forum in Davos and is a winner of the Great British Entrepreneur of the Year Award for cyber security.

References

1. 'Endpoint Security Trends Report 2019'. Absolute. Accessed Jul 2020. www.absolute.com/go/study/2019-endpoint-security-trends/.
2. 'Endpoint Security Market 2019 – 2023'. The Radicati Group, Nov 2019. Accessed Jul 2020. www.radicati.com/wp/wp-content/uploads/2019/01/Endpoint_Security_Market_2019-2023_Executive_Summary.pdf.
3. 'The state of endpoint security risk: it's skyrocketing'. Ponemon & Sullivan, 12 May 2020. Accessed Jul 2020. https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/.
4. Canter, Lily. 'Coronavirus: Half of remote workers victims of cybercrime'. Yahoo Finance, 29 Apr 2020. Accessed Jul 2020. https://uk.finance.yahoo.com/news/coronavirus-half-of-remote-workers-victims-of-cybercrime-144200532.html.
5. 'Global Threat Intelligence Report'. NTT Security, 2020. Accessed Jul 2020. www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf.
6. Bond, Robert. 'SANS Institute – Less than 50% of cyber attacks detected by anti-virus software'. SecureOps, 8 Aug 2018. Accessed Jul 2020. https://secureops.com/security/anti-virus-ineffective/.
7. 'What is a container?'. Docker. Accessed Jul 2020. www.docker.com/resources/what-container.
8. 'Windows Defender Application Guard'. Microsoft, 28 Mar 2019. Accessed Jul 2020. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview.

Zoombombing – the end-to-end fallacy

Ion-Alexandru Secara

Ion-Alexandru Secara

Zoombombing, a trend in recent months, has quickly moved from online classroom pranks to organised disruption efforts, which the FBI has threatened to punish with jail time. "The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language." the agency stated in a recent press release.[1]

As shelter-in-place and lockdown orders were enforced around the world, Zoom meetings replaced classrooms, offices, gaming lobbies and even concert halls. Throughout the month of March alone, over 200 million people used the conferencing platform, compared to the previous monthly maximum of 10 million.[2]

An investigation carried out by the *New York Times* in April has revealed that a considerable number of social media accounts, including Instagram accounts, Twitter accounts, message boards on Reddit and 4Chan, are