MANAGING EUC THREATS

3 SIMPLE WAYS TO IMPROVE ENDPOINT SECURITY

CONTENTS

EMERGING THREATS: THE ENDPOINT EXPLOSION

INFORMATION IS BIG BUSINESS. ARE YOU PREPARED TO PROTECT YOURS?

Today's end user computing (EUC) environment is complex — and growing exponentially. Tablets. Smartphones. Cloud applications. The list of EUC endpoints goes on and on. To protect valuable company information, which can be accessed at any number of these EUC endpoints, it's imperative companies keep pace with rapid user-level technology growth and an increasingly mobile workforce to pro-actively protect against EUC threats.

So how do you manage EUC threats to your company's information? There are 3 simple ways you can improve endpoint security. Read on.

The average cost of a data breach[1]

THE UNIVERSE OF ENDPOINTS

Simply put, endpoints are devices and applications that connect to your company network. Take a guess: How many do you have? Dozens? Hundreds? Thousands? There are likely more than you think.

The Internet of Things (IoT), and its accelerated technology advancements, has expanded the list of potential endpoints at a mind-blowing rate, to include devices like security cameras, thermostats, refrigerators, and more. Of course, digital business environments are more focused on the list of EUC endpoints — including devices and applications — employees use every day to access organizational data and information.

The use of commercial cloud applications, BYOD, and employees who work remotely have significantly increased endpoint risk[2]

HOW MANY EUC ENDPOINTS DO YOU HAVE?

Without a doubt, the sheer number of EUC endpoints makes it more and more challenging to effectively manage, secure, and protect your company's valuable information. How many of your company employees are mobile and work remotely due to travel, movement between offices or locations, flex arrangements, nontraditional work spaces, time off, or even just logging after-hours time at home? How many devices and applications are they using?

The list of EUC endpoints includes:

- ☑ Physical desktop and notebook computers
- ☑ Desktop operating systems and applications
- ☑ Smartphones, tablets, and other mobile devices
- ☑ Printers and copiers
- ☑ VoIP phones
- ☑ Mobile, web, and cloud applications
- ☑ Virtual desktops and applications

Now that you've seen the list, take another guess: How many EUC endpoints do you have? Dozens? Hundreds? Thousands?

LEARNING FROM A CYBERSECURITY BREACH

WITH 71% OF DATA BREACHES TARGETING THE ENDPOINT TODAY,[3] IT IS MORE CRITICAL THAN EVER TO PROTECT YOUR EUC ENVIRONMENT.

In a major cybersecurity breach in December 2014, Sony was targeted by hackers who wiped critical data from its systems and stole confidential information, sensitive documents, and pre-release movies — and made it public. It was a havoc-wreaking, headline-making breach that impacted Sony's reputation and relationships, eroding trust and confidence among consumers, partners, and employees.

Some asked the question: Had Sony protected its data, assets, and information with the same tenacity as its physical locations, like movie sets and its corporate headquarters? There's no question protecting that data was critically important. Yet Sony's security unfortunately fell short, exposing the company to a massive cyberattack.

So what about your company? Is it easier to access your network or your front lobby? Is your data as secure as the product in your warehouse?

The lesson: Give cybersecurity the respect it deserves. Be proactive in investing in and establishing systems, processes, and protocols to protect your company's valuable data and information. If you don't, are you willing to accept the risks — and the consequences?

ENDPOINT THREAT DETECTION & RESPONSE

Large or small. Domestic or international. Every company is a target. Yes, every company. Every company has information somebody wants — or wants to disrupt. Proprietary information. Intellectual property. Product specifications. Legal files. Employee data. Customer data. Partner data. Assets. Plans. Schematics. Systems. Secrets.

THERE ARE SEVERAL OPTIONS TO MINIMIZE, AND HOPEFULLY AVOID, EUC ENDPOINT THREATS, INCLUDING:

SOFTWARE

Some software is designed specifically to detect potential threats, without the need for maintenance by IT staff. Such software should feature behavior-based malware detection, rather than signature-based, which only identifies known malware. It should also include protection against fileless malware as well as remote administration, malware analysis, uptime alerts, performance optimization, automated realtime whitelist protection, software vulnerability updates, and reporting access through a single pane of glass. Look for software from a qualified security SA16 certified MSP like NWN, and security that's at least 95 percent effective in proactive and reactive protection and remediation.

HARDWARE

Choose hardware featuring built-in tools to protect against cyberattacks without the need for software or human user intervention. One example is HP's automatic runtime intrusion detection, which monitors memory activity to detect and stop hacker intrusions. Another is HP Sure Start, which validates the integrity of the BIOS when powering up and automatically self-heals from a known good version of the BIOS and restarts if it's compromised. There's also Intel Authenticate Solutions, which provides hardware-based multi-factor identity authentication that also works with the operating system (OS) to reduce exposure to software-level attacks.

81%

of hacking-related breaches leveraged either stolen and/ or weak passwords[5]

PHYSICAL DEVICES

Look for emerging technology in physical devices designed to enhance security. One example is the HP SureView, a privacy screen that prevents “visual hackers” from looking over your shoulder at your screen — a revolutionary industry first that has competitors scrambling to develop similar technology.

30%

of visual hacking attempts are successful[6]

IMPROVE YOUR EUC ENDPOINT SECURITY

SO, GETTING DOWN TO BUSINESS, HOW CAN YOU BETTER MANAGE EUC THREATS TO YOUR COMPANY'S INFORMATION?

Here are the 3 simple ways you can improve endpoint security:

UPGRADE

CONSOLIDATE

ASSESS

1. UPGRADE

First, take a close look at your hardware. How old are your computers, your laptops, your printers, and your copiers? If your company isn't using devices equipped with the latest security features, you need to make a change — and fast. Old, outdated devices are essentially a welcome mat for hackers.

Make it a priority to leverage the advanced security technology available in today's PCs and printers:

- ☑ ***Privacy screens*** offer protection from visual hackers.
- ☑ ***Integrated self-healing BIOS chips*** fend off sophisticated malware attacks — beyond the capabilities of even the most current antivirus app — by detecting and correcting issues, all without intervention from human users.
- ☑ ***Multi-factor authentication*** safeguards against weak and vulnerable password protection by creating a multi-layered defense utilizing two or more credentials — including passwords, one-time passwords (OTP), personal identification numbers (PINs), virtual private networks (VPNs), tokens, swipe cards, and biometric verification like fingerprints or voice waves — giving hackers more barriers to break through.
- ☑ ***Run-time intrusion detection*** protects printers and computers when they're powered on and connected to the network — when most cyberattacks occur — by monitoring memory activity, searching for anomalies, and automatically halting any intrusions that are discovered.
- ☑ ***Whitelisting*** automatically verifies authentic firmware — which, if compromised, could expose your entire network — and, if anomalies are detected, reboots the device to a secure, offline state and notifies IT of the issue.

For more efficient and effective management of company devices, consider Device as a Service (DaaS) opportunities to outsource procurement and lifecycle management to IT service providers, like HP. Beyond the advantage of utilizing devices with the latest advances in security, DaaS also enables companies to scale up or scale down devices as needed, more easily upgrade to new technologies, and more quickly refresh devices.

Finally, while upgrading your printers and copiers, consider Managed Print Services that provide mobile capabilities to print from multiple devices — like from an employee's tablet — without putting the company network at risk, and without compromising data security via a non-networked and potentially outdated printer or copier.

2. CONSOLIDATE

Sometimes less is more. And when it comes to managing EUC endpoints, less is also more secure. Consider simplifying device lifecycle management with a Unified Endpoint Management (UEM) system, a singular next-generation technology architecture designed to unify desktop, mobile, and application management. It's a solution that creates a more efficient, more connected, and more secure IT workspace architecture.

With UEM, you can manage the complete lifecycle of all EUC endpoints over the air and in real time, giving your security efforts a powerful boost. For example, configuration management empowers IT to push patches and policies, install software, and consolidate operational processes across all EUC endpoints — whether they're on the network or off. In addition, enhanced client health and security technologies built to block cyberattacks allow IT to designate trusted apps with permissions to open or encrypt data, configure safe locations for data protection, and create flexible enforcement levels impacting how user groups move and share data between work and personal endpoints.

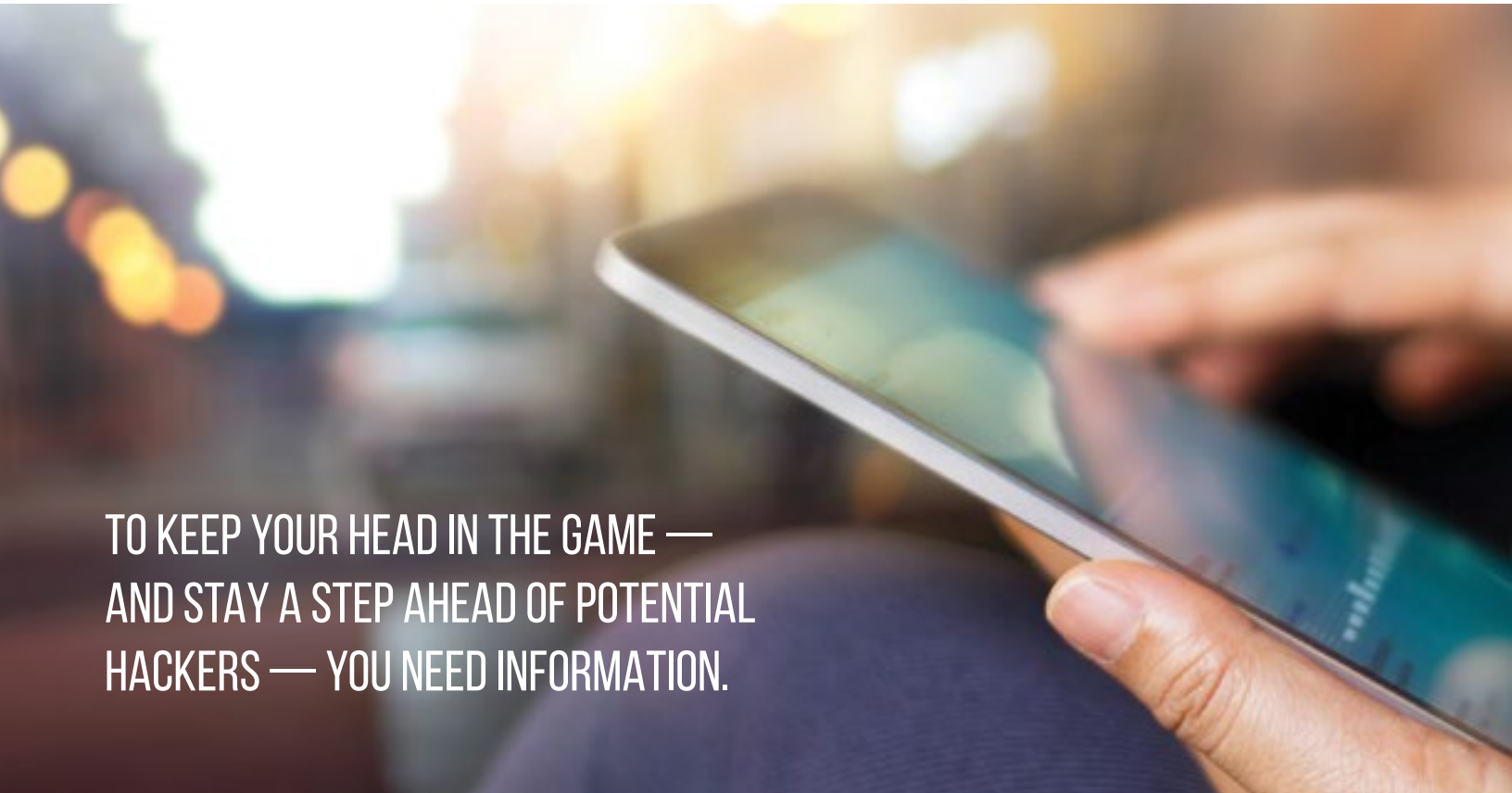
One example is Intel's Active Management Technology. Bonus points: HP DaaS incorporates VMware's UEM system, giving you the security benefits of both UPGRADE and CONSOLIDATE with one solution.

3. ASSESS — AND REASSESS

A regular IT security risk assessment will let you know just where you stand with EUC endpoint security. Where are your risks? Where are your threats? Where are your opportunities? Where are you vulnerable? Where are you hitting the mark? And where could you and should you do more?

Aim to perform a thorough risk assessment at least annually — or quarterly, depending on your level of risk tolerance — and stay focused on continuous improvement. Utilize these risk assessments to demonstrate your accomplishments, proactive efforts, and ongoing commitment to EUC endpoint security. In addition, leverage risk assessments to quantify and support corporate investment in additional software, hardware, devices, updates, and upgrades to strengthen EUC endpoint security and protect your company's assets and information.

How long has it been since your last IT security risk assessment? If you haven't done one in a while, or if you just don't have the resources to complete a thorough assessment, most technology consultants will perform a detailed IT security risk assessment for you at no charge. Your consultant will identify a detailed list of vulnerabilities and threats, and provide you with specific recommendations to secure them. For the best results, choose a technology vendor with demonstrated experience in your vertical market, who will best understand your unique business needs and security risks.



PROACTIVE PREVENTION & PROTECTION

With the speed at which today's complex EUC environment is growing, you can't afford outdated devices and obsolete systems and processes that put your company's information at risk. It's imperative to invest in proactive protection against EUC endpoint threats. By upgrading, consolidating, and thoroughly and regularly assessing your current digital business environment, on your own or in collaboration with an experienced IT security services provider, you'll not only improve your endpoint security, you'll have confidence you're taking the right steps to manage EUC threats — and avoid finding your company in the headlines as the target of the next cybersecurity breach.

Every company is a target. Every company has information somebody wants — or wants to disrupt. EVEN YOURS.

Don't wait. Get started today with a custom EUC assessment to help you identify vulnerabilities and possible entry points in your corporate environment. NWN will provide you with an inventory of active software and hardware as well as a detailed list of action items and recommendations to strengthen your company's endpoint security.

NWN helps customers solve business problems with proven IT solutions and services. We believe in helping customers stay ahead of the game in a world of ever-changing technology. Our practical, cost effective solutions — from data center optimization to cloud computing — are based upon your specific needs and environment, tailored to meet your business and financial objectives. Learn more about how NWN can help protect your company. Visit NWNIT.com

[1] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," 2016.
[2] Ponemon Institute, "2016 State of the Endpoint Report," 2016.
[3] Verizon, "Data Breach Investigations Report," 2013.
[4] Bitglass, "Lost & Stolen Devices Account for 1 in 4 Breaches in Financial Services," August 25, 2016.
[5] Verizon, "Data Breach Investigations Report," 2017.
[6] Verizon, "Data Breach Investigations Report," 2016.