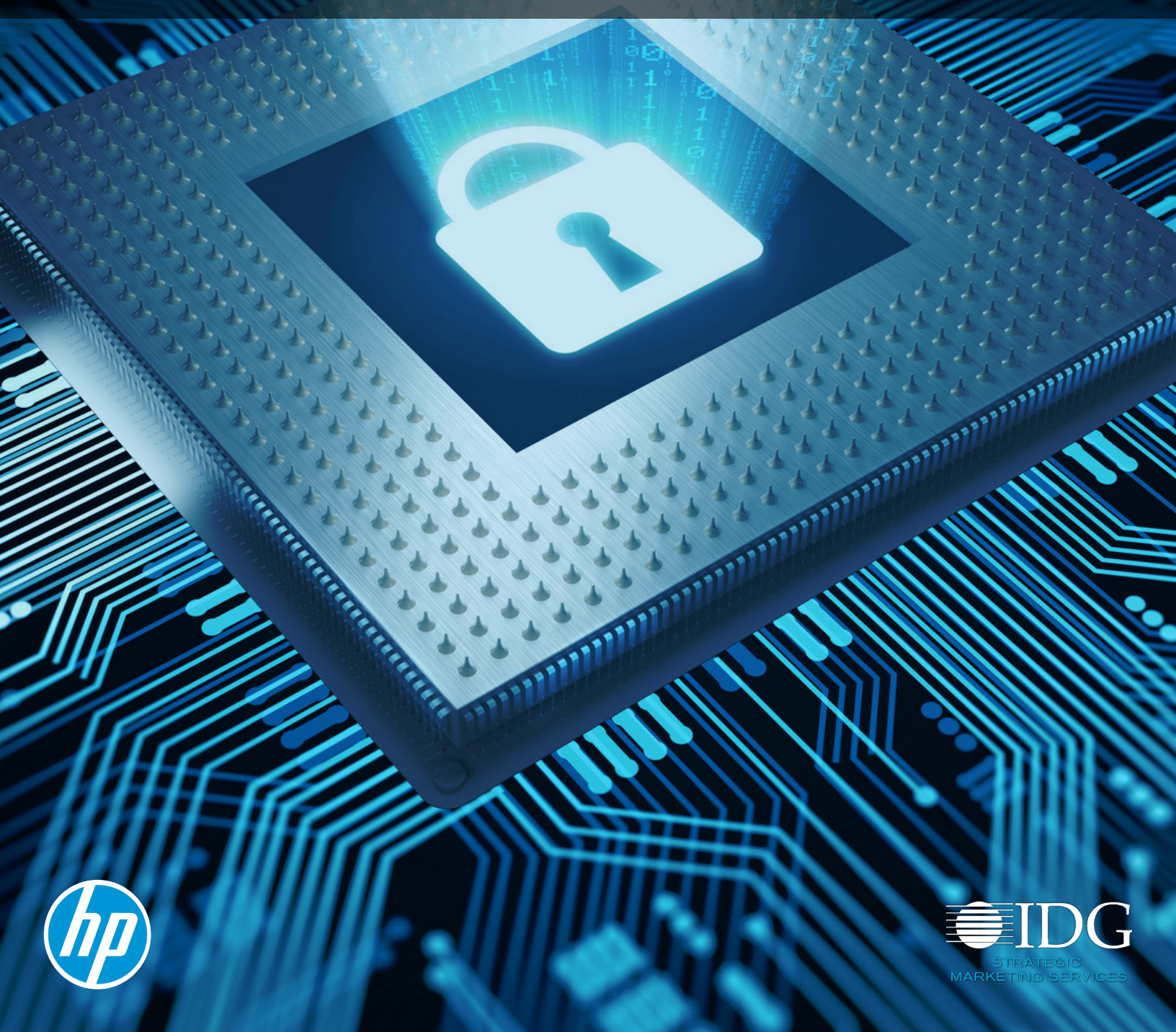
Sponsored content

Closing the Endpoint Security Gap at Federal Agencies

Learn why a more proactive and systematic approach to U.S. cyberdeterrence is urgently needed



IDG
STRATEGIC MARKETING SERVICES

Closing the Endpoint Security Gap at Federal Agencies

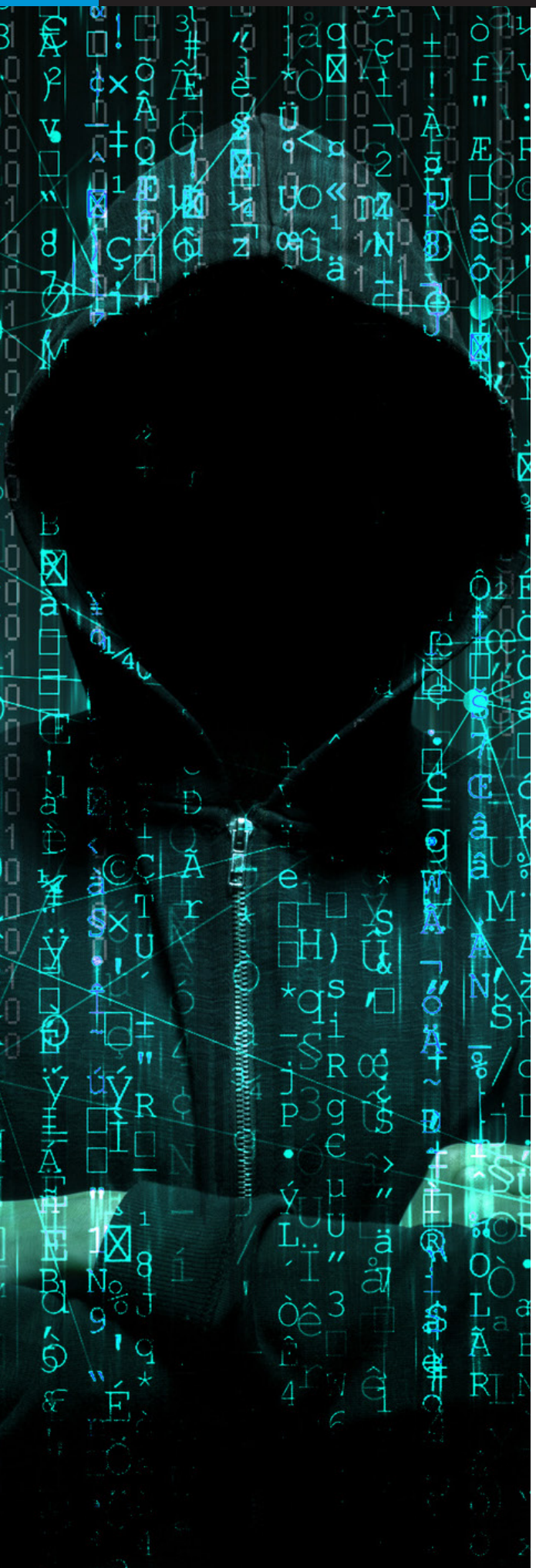
A BROAD VARIETY OF ACTORS, ranging from state-sponsored espionage teams to employee or contractor insiders, are intent on discovering and exploiting cyber and physical security gaps across the broad spectrum of federal agencies. Incidents span military, intelligence, regulatory, and public services agencies.[1]

Traditional firewall defenses don't cut it

In light of potential threats and actual attacks, endpoint security is a growing preoccupation of IT and network admin teams. Their task is growing ever more expansive, especially with the increasing number of connected Internet of Things (IoT) devices, everything from printers to an evolving array of fixed and mobile sensors. Traditional firewall defenses are insufficient to keep up with the expanding threat environment, so it's incumbent on agencies to implement a layered defense strategy that includes added endpoint protections.

continued >

CONTENTS



"The Task Force notes that the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed." [2]

– Craig Fields,
Chairman, Defense Science Board (DSB),
U.S. Department of Defense (DoD)

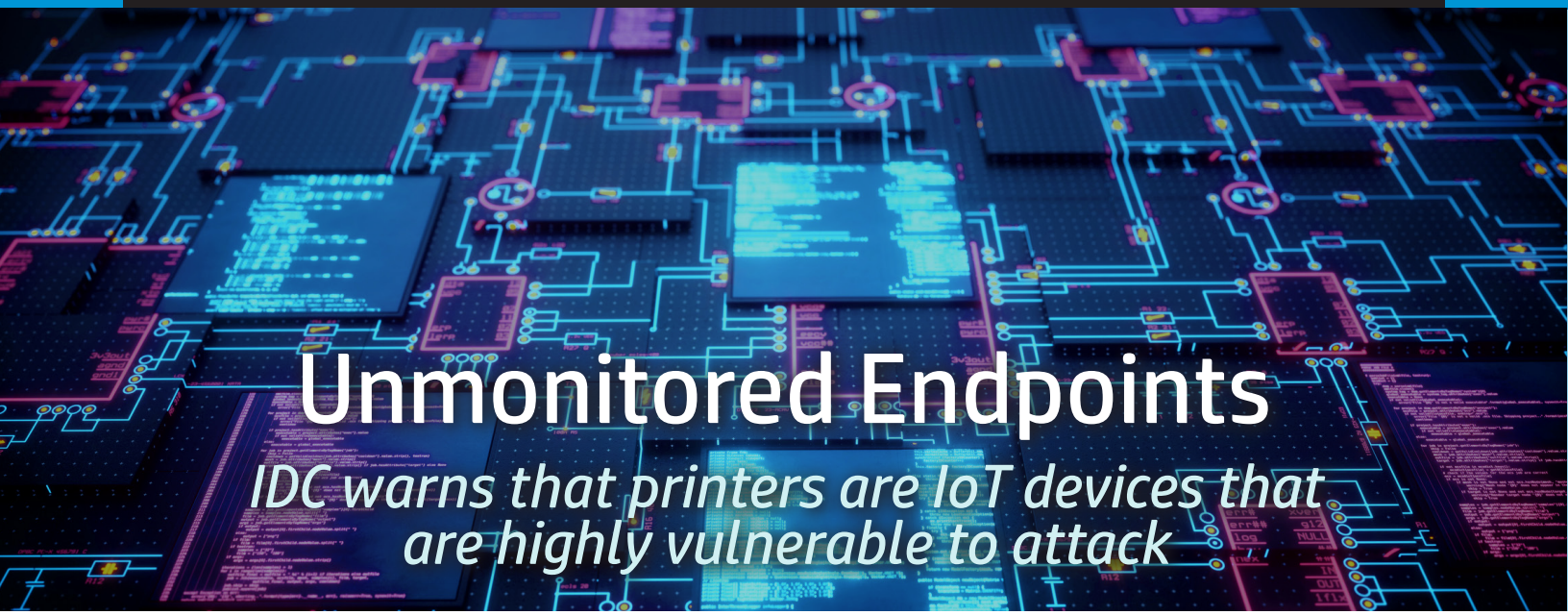
The DoD's DSB Task Force's report on Cyber Deterrence issued in February 2017 was a clarion call to action in defending the U.S. from cyberattacks and cyberintrusions perpetrated by major powers (Russia and China), regional powers (Iran, North Korea), and a range of state and nonstate actors.

In 2016 federal agencies were subjected to more than 30,899 cyberincidents that led to the compromise of information or system functionality, 16 of which were deemed "major incidents," according to the Office of Management and Budget (OMB) annual report to Congress on efforts to meet cybersecurity performance goals. Despite progress in areas such as vulnerability management, the OMB reported that only 61% of hardware assets across all agencies were compliant with asset management performance metrics; the number of agencies meeting performance goals in that category actually declined to 32 in 2016, from 35 in 2015.[3]

A growing target

Gregory C. Wilshusen, director of Information Security Issues with the Government Accountability Office (GAO), testified before a House of Representatives panel in February 2017 that "we routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment."[4]

It's a long-standing adage in cybersecurity that defenders need to be right all the time, whereas attackers need to be right—or lucky—only once. The vast number of endpoint devices, such as printers, PCs, and mobile devices, represents an environment that is a growing target. Because of the persistent nature of cyberthreats, endpoint devices need to be better secured with an array of protective measures, including automated threat monitoring, configuration maintenance, and attack detection and remediation. Agencies also need to protect against insider threats that can result in the compromise of electronic and printed documents.



Unmonitored Endpoints

IDC warns that printers are IoT devices that are highly vulnerable to attack

Even though IT teams in government and industry are focused on cyberdefense, industry surveys consistently reveal that printer security is often overlooked (if not completely ignored) in that effort. According to the research firm Quocirca, a survey of large enterprises found that 61% have suffered at least one data breach as a result of unsecured printing.[5]

According to IDC, printers are a vulnerable endpoint that can provide hackers with access to the enterprise network.[6] Even though they are relatively easy to use, printers and imaging devices, just like PCs, incorporate computing components such as firmware, software, and networking protocols. When unprotected, these valuable tools can also give cyberthieves access to information and a gateway to internal networks. With more than three-quarters of government IT funds spent on operating and maintaining legacy systems[7], managers may be tempted to continue operating aging printers as long as possible.

In addition, printers may be viewed as low risk by security teams that assume that, because they sit behind firewalls, they are automatically protected. But even advanced firewall security is no guarantee that you'll be able to spot a cyberattack. One test of next-generation firewall products found that more than 80% of them missed evasions intended to bypass security measures.[8] Printers, just like PCs, can and should be protected from viruses and malware.

Opportunities for exploitation

Printers and imaging devices are particularly vulnerable, because they often are unconfigured, unmonitored, and even outside of the scope of established security policies and processes. That provides multiple opportunities for exploitation:

- Cybercriminals can gain access through a network-connected device, such as a printer, to steal credentials that enable them to get at data and servers on the same subnet—thus compromising the organization's network.
- Print jobs stored to the printer's cache can enable hackers to gain access to sensitive information, including internal memos and documents.

> *"Attackers seize on the lack of attention given to printer security relative to other devices and peripherals on enterprise networks."*[6]
>
> —*IDC*

- Insiders can illicitly print out classified information, as the U.S. Department of Justice alleged[9] occurred at a government agency facility in 2017.

The dangers of poor security hygiene

A team of IDC analysts warned that "Printers are IoT devices that are highly vulnerable to attack because of the requirements of keeping them open and accessible to the entire organization. Attackers seize on the lack of attention given to printer security relative to other devices and peripherals on enterprise networks."[10]

These devices often ship with a multitude of open communications ports that make them susceptible to distributed-denial-of-service attacks. Poor security hygiene—ranging from configuration errors to failure to implement software or firmware patches or even change default passwords—can make it all too easy for bad actors to exploit manageable vulnerabilities.

Ensuring Printer Security

A checklist of measures that every agency needs to consider

THE FIRST STEP IN TIGHTENING printer security is to ensure that all endpoints are factored into your security policies and that protective measures are implemented at any point of vulnerability; moreover, given that printers and other devices may be moved, repaired, and replaced, managing that security policy requires implementation of automated monitoring, updating, and maintaining of configurations.

Some key measures that every government agency should consider:

Disabling ports/protocols: Unauthorized users can access a printer or a multifunction printer device via unsecured USB or network ports or unsecured protocols (such as FTP or Telnet); USB ports can potentially be used to upload malware, and unsecured protocols can be exploited for exfiltration of information to servers outside the organization. It's critical that IT and security teams have a full understanding of what ports and protocols are in use, disable those that are not needed, and establish authentication for those that are in use for legitimate purposes.

Encryption: Any sensitive information stored on an internal drive or hard disk is potentially vulnerable to interception or theft. Built-in encryption is available for many HP devices to protect data. When stored data is no longer needed, built-in device capabilities can securely overwrite data and safely remove sensitive information.

Data erasure: Imaging and printing devices store sensitive information on internal drives or hard disks, which can be accessed if not protected. Devices equipped with built-in encrypted hard drives can help protect sensitive information. IT should set autoerase procedures and use devices that can securely overwrite stored data. In the disposal or return of leased equipment, ensure that the hard disk is fully wiped.

It's critical that IT and security teams have a full understanding of what ports and protocols are in use, disable those that are not needed, and establish authentication for those that are in use for legitimate purposes.

Authentication and access control: Secure authentication and access controls can restrict output and ensure that only authorized users are able to access and operate devices. This can prevent unauthorized users from accessing printer features—such as using a USB port to gain access to the network or exfiltrating files via a certain protocol such as Telnet. When incorporated into security policy management, authentication and access controls can give government organizations the ability to secure and track operation of their print devices regardless of where data travels and how it is printed.

Activation of secure pull or push printing: To prevent unattended printing, agencies can implement PIN printing, so that when users send confidential print jobs, they assign a PIN, which they must enter at the device to release the job. Another secure option is pull printing, where print jobs are stored in the cloud or on users' PCs until users authenticate at their chosen print location to pull and print their jobs.

Productivity benefits of updated printers

INTERRUPTIONS AND COMPLEX MAINTENANCE can slow down printing and, ultimately, the pace of business. Built-in technology from HP can anticipate problems, schedule maintenance, and ensure that printers are consistently up and running. Advanced technology available from HP transforms printers, including multifunction printers (MFPs), into smart devices that ensure maximum uptime, fewer service interventions, and enhanced collaboration.

HP's vast data lake of printer performance data enables organizations to be proactive and predictive about the management of the printer fleet, allowing for faster diagnosis, dispatch, and resolution of service events.

Big data analysis of many types of data—user profiles, data types, and the duration of print jobs along with the composition of the existing printer fleet—makes it possible to create a plan for optimal device deployment and to update that plan as the office evolves. This enables precise printer placement in the office; determination of how many printers are needed for optimal productivity; and making decisions such as where a color printer is needed, versus black and white.

HP offers cloud-based continuous monitoring, remote resolution, and predictive service and supply fulfillment to keep printer fleets up and running. Continuous monitoring through HP Remote Management Centers can enable HP to address concerns before they have a negative impact on your operations.

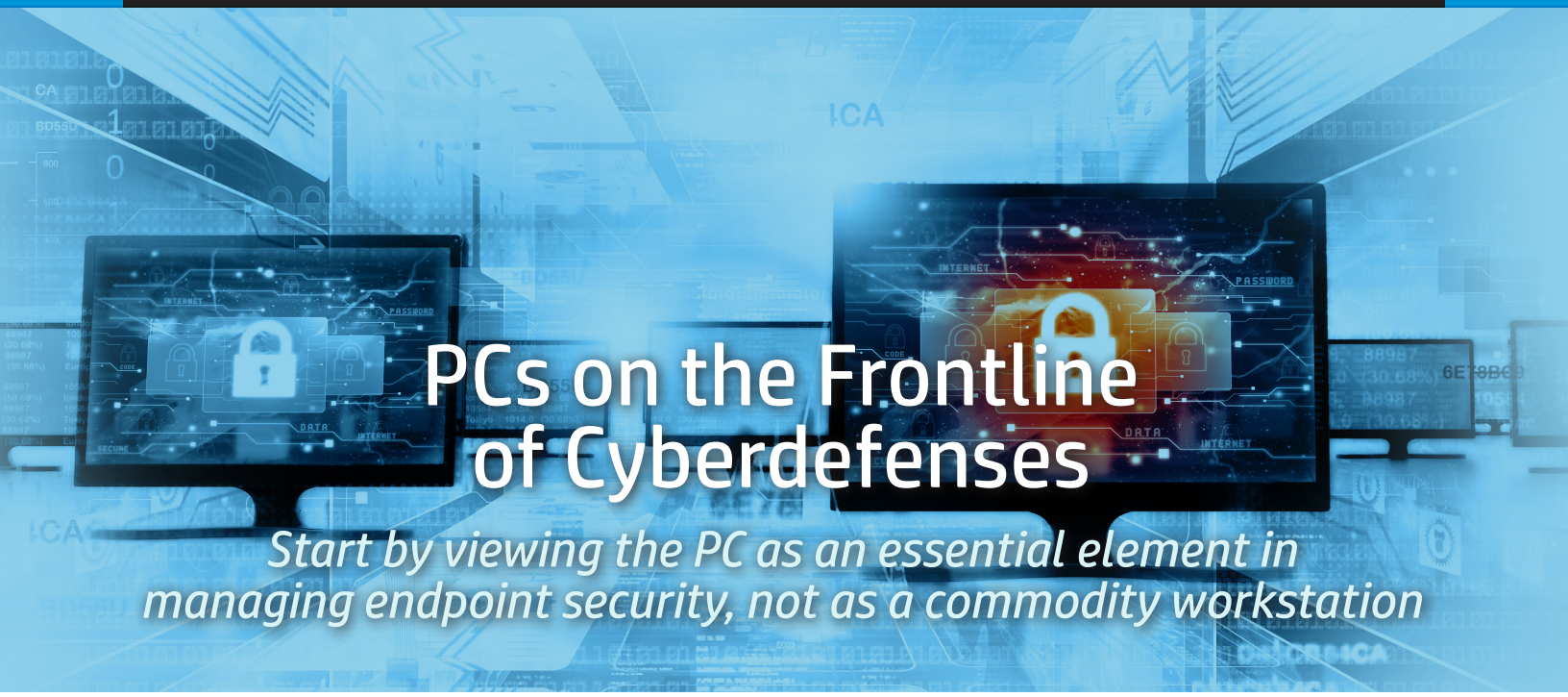
The HP JetAdvantage portfolio of workflow software and solutions is designed to capture, store, manage, share, find, and deliver information more efficiently, eliminating manual input and increasing operational effectiveness. HP document workflow solutions for government can help transform raw data into customized, compliant forms that can be easily distributed or printed to HP LaserJet printers and MFPs on demand.

Automated monitoring: Security monitoring and management solutions can help establish a unified policy-based approach to protecting data, strengthening compliance, and reducing risk. An effective monitoring solution can help identify configuration vulnerabilities, implement policies to resolve them, and generate compliance reports.

Fleet management: Centralized management makes it possible to apply a single security policy fleetwide to prevent protection gaps. HP JetAdvantage Security Manager, the industry's only policy-based imaging and printing compliance solution, automates print fleet security. Administrators can easily set security configuration policies and automatically set and maintain settings for every HP printer across the organization.

Protection through continuous self-monitoring

HP business printers are protected from attack by continuous self-monitoring. The printer's BIOS is checked on every startup to ensure that it is unaltered. A firmware check next ensures that only authentic HP software needed for running the printer loads to memory. And monitoring during operation stops attacks that might occur while a printer is running—all without intervention from IT personnel. In the event that a printer is compromised, HP runtime intrusion detection or HP Connection Inspector can detect the threat and then force the printer to immediately reboot to initiate the software checks and remove the malware.



PCs on the Frontline of Cyberdefenses

Start by viewing the PC as an essential element in managing endpoint security, not as a commodity workstation

Desktop and mobile personal computers are essential for government agency operations but represent targets of opportunity to a growing range of bad actors, including state-sponsored intelligence operations, terrorist groups, scam artists, and "hacktivists."

Before the days of widespread internet connectivity, IT cyberdefenses were typically overly reliant on the concept of a perimeter defense system designed to keep out all potential threats. This assumed that everything within the perimeter was protected by that barrier. But time has shown that cybercriminals are adept at bypassing these perimeters by finding gaps in defenses.

Government workers are targets of malware campaigns via email and website visits, and unattended PCs provide ports that can quickly be used to download electronic files to a thumb drive storage device or used to upload malicious code that can surreptitiously monitor network traffic or ransomware that locks up systems. Ransomware attacks in early 2018 paralyzed government public service operations in locations in the U.S.[11] and abroad.[12]

Remember, hackers seek the weakest link

In this growing threat environment, organizations are building interconnected, layered, and resilient defense systems designed to identify and snuff out risks before they become problems. The PC should be viewed as an essential element in managing endpoint security, not as a commodity workstation.

PCs have also evolved into dependable, long-lived productivity tools. In the U.S., the average age of an enterprise desktop computer was projected to be 4.4 years in 2018, and for enterprise mobile PCs an average of 3.5 years.[13] But security is a moving target, with hackers constantly discovering new vulnerabilities to exploit. In January 2018, for example, it was reported that chip design flaws had created vulnerabilities—labeled Spectre and Meltdown—that enable hackers to read information from chips that power most PCs.[14] Subsequently, Intel® announced that it would not be issuing patches for certain processors, including some produced as recently as 2015.[15]

> *"We routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. "*
>
> *– Testimony of Gregory C. Wilshusen, Director of Information Security Issues, GAO*[16]

The greatest danger to security is a gap between official security policies and procurement practices, which tend to focus on price. Hackers will always focus on the weakest link in the chain, and older devices or new devices lacking firmware protections present tempting targets.

HP PC Security Goes Beyond Software

A comprehensive range of hardware-enforced security provides strong protection

MOST COMPUTER USERS TODAY have some awareness of malware software protection, but hackers can bypass such protections by directly attacking the PC's BIOS, the firmware that initiates operating system control over computer components. In this manner, an attacker can get unlimited control of a PC to steal valuable data, insert ransomware, or render the PC inoperable. Because antivirus software is unable to monitor for attacks in the firmware, malware hiding in the BIOS can be virtually impossible to detect and incredibly difficult to remove.

Cyberresilient PCs should be able to quickly and automatically recover to a working state, even from unforeseen attacks that bypass existing protections and inject malicious software and/or firmware into the target platform. This kind of attack may also attempt to render the PC inoperable by removing or corrupting software and/or firmware on the device.

HP provides a comprehensive range of hardware-enforced security that provides strong protection. HP Sure Start, for example, is embedded in hardware to protect the BIOS with runtime intrusion detection and many other advanced firmware security features. In the event of a malware attack on the BIOS, HP Sure Start automatically detects the change, notifies the user and IT, and restores the most recent good version of the BIOS. Moreover, this protection can be managed centrally by IT teams and integrated with Microsoft® System Center Configuration Manager to monitor tamper alerts.

Exceeding NIST guidelines

HP business PCs with HP Sure Start exceed the National Institute of Standards and Technology (NIST) Platform Firmware Resiliency Guidelines[17] (Special Publication 800-193) for host processor boot firmware, which is one of the leading public sector efforts to formalize requirements for cyberresilient platforms.

HP offers several other key security enhancements:

- **HP Sure Run**[a], a hardware-enforced application persistence solution, can maintain communications with the policy enforcement hardware while the OS is running. It can continually monitor the presence of critical services and applications, even if the HP Sure Run agent in the OS is attacked or removed.
- **HP Sure Recover**[b] is an automated operating system recovery solution integrated into HP PC hardware and firmware. It can quickly recover the operating system whenever needed, even if the primary drive has been completely erased.
- **HP Sure View**[c] enables mobile PC users to quickly and easily enable privacy mode to minimize the potential of "visual hacking"—where unauthorized persons can visually read a screen or take photos of it with a smartphone to capture sensitive or classified information. Workers can instantly make the screen appear unreadable to those around them while still being able to view information themselves.
- **HP Sure Click**[d] Help protect your PC from infected websites, malware, ransomware, and viruses with HP Sure Click—hardware-enforced security for browsing the web and in-browser .pdf viewing.

HP computing devices are also designed for reliability. All HP Elite 2-in-1 and 3-in-1 devices, notebooks, tablets, and desktop PCs, plus select Thin Clients pass multiple MIL-STD-810G test procedures. This standard, although created specifically for the U.S. Department of Defense, is widely used as a benchmark for quality for commercial products in multiple industries. It outlines a broad range of tests that can be tailored to measure the reliability of specific pieces of equipment and includes multitiered climatic and environmental test methods.[18]

Extending the Security Net with Comprehensive Security from HP

Because every PC and printer decision is a security decision

Once a cyberattacker gains access

to a network endpoint device, it may take days, weeks, or even months for an organization to discover that it has been compromised. In the meantime, criminals may be siphoning off classified documents and personally identifiable information or surreptitiously navigating the network to implant malware for future exploitation.

It can be difficult to defend against attacks directed at the firmware level of devices, whose infections can spread to other devices and the network. Hardware-enforced security protections work to stop an attack the moment it starts, better equipping organizations to ward off attackers and realize immediately that an assault is under way. HP printers and PCs incorporate the HP Trusted Platform model, an embedded security controller that enables key security measures, including:

- **BIOS protection:** HP Sure Start validates (monitors) the BIOS for any deviations or tampering. If those are detected, Sure Start immediately quarantines the corrupted BIOS and replaces it with a "golden copy" stored in the HP Embedded Security Controller to reboot the device and provide self-healing capability.
- **Hardware-enforced application persistence:** HP Sure Run can maintain communications with the policy enforcement hardware while the OS is running. The presence of critical services and applications can be continually monitored even if the HP Sure Run agent in the OS is attacked or removed.
- **Whitelisting:** Implemented in firmware by HP, whitelisting validates the integrity of firmware system files during the load process. If that validation fails, protected devices will prevent execution of potential malware exploits.
- **Runtime intrusion detection:** Sure Start–capable HP enterprise printers can detect potential malware intrusions in system memory, take the configured policy action, and report these intrusion events.

It's critical to require embedded hardware-enforced protection in your endpoint hardware purchases. The protective tools and technologies discussed here should be considered essential features of devices for government agencies. Every PC and printer decision is a security decision, and HP provides the most-secure and most-manageable PCs[19] and printers[20] in the world.

For more information, go to www.hp.com/go/hpsecure.

Endnotes

1 Riley Walters, The Heritage Foundation, "Federal Cyber Breaches in 2017," January 3, 2018.

2 Defense Science Board, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence," February 23, 2017.

3 Office of Management and Budget, "Federal Information Security Modernization Act of 2014, Annual Report to Congress, Fiscal Year 2016," March 10, 2017.

4 Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office, "CYBERSECURITY:Actions Needed to Strengthen U.S. Capabilities." Testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives, February 14, 2017.

5 Quocirca, "Print Security: An imperative in the IoT Era," January 2017.

6 Tom Austin, et al., IDC, "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," November 2016.

7 U.S. Government Accountability Office, GAO-16-468, "Federal Agencies Need to Address Aging Legacy Systems," May 25, 2016.

8 Tara Seals, InfoSecurity Magazine, "80% of NGFWs Fail to Detect Evasions," June 6, 2017.

9 U.S. Department of Justice press release "Federal Government Contractor in Georgia Charged with Removing and Mailing Classified Materials to a News Outlet," June 5, 2017.

10 Tom Austin, et al., IDC, "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," November 2016.

11 Phil Hall, Westfair Online, "Ransomware: Hostage-taking, Cyber Style." April 29, 2018.

12 Simon Sharwood, The Register, "Death in paradise: 'Cyber attack' takes out national government's IT," April 10, 2018.

13 Daniels Research Group, "United States Computing and Telecommunications Personal Device Market Forecast: 2018-2022, Q4 2017 Update," January 2018.

14 Russell Brandom, The Verge, "KEEPING SPECTRE SECRET: How an industry-breaking bug stayed secret for seven months—and then leaked out," January 1, 2018.

15 Ashley Carman, The Verge, "Intel says it won't patch older chips for Spectre," April 4, 2018.

16 Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office, "CYBERSECURITY: Actions Needed to Strengthen U.S. Capabilities." Testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives, February 14, 2017.

17 Andrew Regenscheid (NIST), "SP 800-193 Platform Firmware Resiliency Guidelines," May 2018 https://csrc.nist.gov/publications/detail/sp/800-193/final

18 MIL-STD-810G testing is conducted on select HP products. Testing is not intended to demonstrate fitness for U.S. Department of Defense (DoD) contract requirements or for military use. Test results are not a guarantee of future performance under these test conditions. Coverage of accidental damage or damage under these test conditions requires an optional HP Accidental Damage Protection Care Pack.

19 Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC, including hardware, BIOS, and software management with Microsoft System Center Configuration Manager as of May 2017 on HP EliteOne PCs with seventh-generation and higher Intel® Core™ Processors, Intel integrated graphics, and Intel WLAN.

20 HP's most advanced embedded security features are available on HP Enterprise-class devices with FutureSmart firmware 4.5 or above, based on HP review of 2016–2017 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. For a list of compatible products, visit hp.com/go/PrintersThatProtect. For more information, visit www.hp.com/go/printersecurityclaims.

Disclosures

a HP Sure Run is available on HP Elite products equipped with 8th generation Intel® or AMD® processors.

b HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors and requires an open, wired network connection. Not available on platforms with multiple internal storage drives, Intel® Optane™. You must back up important files, data, photos, videos, etc. before use to avoid loss of data.

c HP Sure View integrated privacy screen is an optional feature that must be configured at purchase.

d HP Sure Click is available on select HP platforms and supports Microsoft® Internet Explorer, Google Chrome, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode. Check http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-0922ENW for all compatible platforms as they become available.