Closing the Endpoint Security Gap in State and Local Government

Technology and best practices improve protections for PCs and printers.

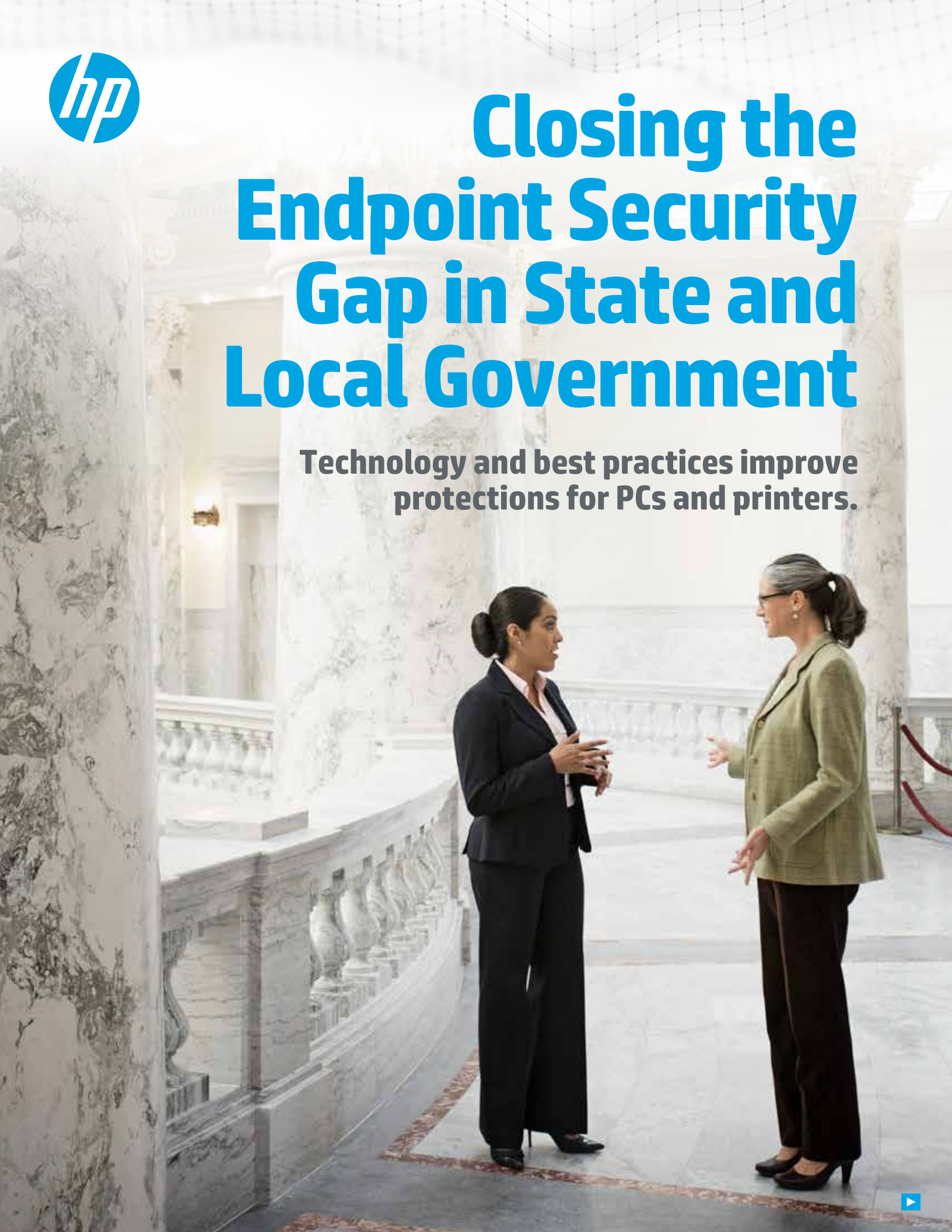

TABLE OF CONTENTS

THE IMPORTANCE OF SECURITY EVERYWHERE

Cyber attacks on government agencies are happening at an alarming rate. These attacks cost U.S. state and local governments millions of dollars in remediation and disrupt employee work and citizen services.

For example, after a ransomware attack in Atlanta, employees couldn't use their computers, citizens couldn't pay bills or tickets online, and police had to write reports by hand. The immediate cost to fix it was estimated at $2.7 million,[1] and the total cost to taxpayers could be closer to $17 million, according to the *Atlanta-Journal Constitution*.[2] Similarly, in Colorado, the Department of Transportation spent $1.5 million to get its computers back up and running after two ransomware attacks in early 2018.[3]

Large cities and state governments aren't the only targets. Town governments in Ohio, a library system in South Carolina and a housing agency in Indiana have all experienced ransomware attacks.[4]

Governments also need to be concerned about the loss of sensitive citizen, client and employee information, whether through a cyber event on a PC or unauthorized access to documents at the printer. According to a Verizon study, personal information is the top type of data lost in public sector breaches.[5] The costs of such a breach can quickly escalate. One study estimates an organization will incur $2.2 million in costs for a data breach that involves less than 10,000 compromised records.[6]

One study estimates an organization will incur $2.2 million in costs for a data breach that involves less than 10,000 compromised records.

Several factors make government agencies easy targets. Budget constraints may require some agencies to use outdated computers and printers that cannot support the security features needed to protect against current threats. Many agencies lack funding to develop, implement and manage robust security policies. And the mix of technologies in most government agencies makes security management more challenging, which may inadvertently provide an opening for attacks.

"Everyone is taking cybersecurity a lot more seriously now because they realize the stakes are getting higher and the game is getting harder," says Dan Lohrmann, former chief security officer (CSO) for Michigan and now CSO and chief strategist for Security Mentor, Inc.

ENDPOINTS: AN ENTRY POINT FOR BREACHES AND ATTACKS

Agencies across Washington state have experienced an increase of more than 300 percent in endpoint attacks.

A major source of security vulnerabilities lies in endpoints — the PCs and printers employees use to do the everyday work of government. Although an agency may not have full awareness of endpoint vulnerabilities, hackers certainly do. As one example, a county IT director noted an increase of more than 300 percent in endpoint attacks at agencies across Washington state.[7]

A lack of control or inability to monitor endpoints creates significant security risks and may lead to:

- ✓ Unauthorized people seeing sensitive information due to careless user actions
- ✓ Cybercriminals stealing data or holding computer files for ransom or blackmail
- ✓ An attack on critical agency systems through an endpoint's network connection

Multiple factors contribute to these potential scenarios, but perhaps the most common is **inadequate security settings and lack of proactive monitoring.** Printers in particular often receive limited security configurations initially, making them a point of vulnerability from the moment they connect to the agency network. Over time, infrequent monitoring and inconsistent installation of software patches can increase the risk of both PCs and printers.

Another common factor for security vulnerability is **password sharing**. Multiple employees may share user or administrative passwords as a matter of convenience for getting work done. However, shared passwords make it difficult for IT to prevent unauthorized access and to pinpoint the source if a breach does occur.

The **valuable data** stored in PC and printer memory or hard drives may be easily viewed or stolen unless strong security measures are in place. These measures include defining strong security policies at the agency level and educating users to consistently follow good security practices.

When default security settings aren't optimized, the device becomes a "weakest link," giving hackers an easy entry point into the organization's network. Printers are often installed with defaults such as open ports and simple passwords.

Sometimes it's just a matter of **incomplete endpoint awareness**. When an agency has hundreds or thousands of PCs and printers to track, it can be hard to maintain up-to-date knowledge of all endpoints. One analysis found that a government organization typically doesn't know about 12 percent of its network-connected endpoints.[8] If the IT team doesn't have visibility and control of an endpoint, it can't be certain it is adequately secured.

IT can address these vulnerabilities with a combination of security technology, policies and practices. However, Lohrmann notes, "It's important to understand that implementing stronger cybersecurity isn't a one-time thing. You need to be able to sustain the improved security with the teams and resources you have."

HP'S MEASURES TO IMPROVE PC SECURITY

It's easy to assume that a firewall application and anti-virus software are all that's needed to secure a PC. Although these measures remain important, they cannot deliver full protection against today's sophisticated attacks.

Achieving this higher level of protection involves both best practices and technology tools. Best practices begin with basic measures such as requiring strong passwords and not allowing users to share accounts. Many governments are also choosing to adopt the extensive best practices in the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework.

As a supplement to cybersecurity practices, advanced security tools provide stronger protection than traditional tools for PC applications, data and network connections.

Hardware-enforced application persistence. Sometimes the firewall, antivirus and other security applications on an endpoint become the target of an attack. Operating from a secure position in the PC hardware, HP Sure Run[a] software guards these critical security processes against malware attacks that try to disable them. Sure Run acts as a security controller that is embedded in the endpoint hardware and enables IT to continuously monitor the presence of vital services and applications on the device.

Hardware-enforced browsing isolation security. One click on a malicious link in an infected website can be enough to launch ransomware, viruses and other malware. HP Sure Click[b] delivers hardware-enforced isolation security for web pages and PDF files viewed within an individual browser window. Because each window is isolated from other browser windows, HP Sure Click can quarantine detected security threats and risks and prevent them from infecting the entire browsing session on multiple sites.

Automated operating system recovery. If a computer's hard drive is completely erased, HP Sure Recover[c] is integrated into PC hardware and firmware to quickly and automatically recover the operating system.

Screen privacy for mobile PCs. Information theft can happen with just a glance or a smartphone photo of an unobscured computer screen. With HP Sure View,[d] users can easily enable a visual privacy mode on their mobile PC, making the screen unreadable to people around them.

Single system for endpoint management. One way to overcome the challenge of endpoint visibility and management is to consolidate all PCs and printers in a managed service delivered by a single expert vendor. In the HP Device as a Service (DaaS)[e] offering, HP proactively configures, monitors and manages all devices, including their security settings. When devices are removed from service, the HP service for secure and responsible disposal includes a rigorous data wiping protocol.

PCs aren't the only endpoint type that needs comprehensive security protections — office printers need them as well.

HP'S MEASURES TO IMPROVE PRINTER SECURITY

Advanced, network-connected printers used in many work environments often present security gaps.

Printers may seem like an unlikely entry point for an application attack or data breach. But the advanced, network-connected printers used in many work environments often present security gaps. Mitigating those gaps is possible with a combination of best practices and technology tools.

Printer-focused security best practices. An initial step is to fully implement best practices that focus on printer security, including:

- ✓ Checking each printer to disable open ports and unsecured protocols, such as Wi-Fi or Bluetooth access that doesn't require a user login and password
- ✓ Verifying the data sent to and stored in the printer memory is encrypted, then erased when the job is complete
- ✓ Requiring "pull" printing for sensitive documents, where a user must authenticate at the printer before printing starts
- ✓ Monitoring and managing the entire printer fleet, including timely distribution of new software versions and patches
- ✓ Assuring proper decommissioning and disposal so documents cannot be accessed later in the printer's memory or hard drive

Printers designed for security. Some printers have minimal options to configure and manage security. Others have extensive security built in and offer security management software with comprehensive options for customization.

Why Firmware-Level Protection Is Essential

For both PCs and printers, the device's firmware (also called BIOS) controls the most fundamental level of operation. Firmware must be secure every time the device powers on and it must remain secure while the device is in use.

Tools that attack firmware are now readily available to any hacker and have the appeal of allowing a stealthy, severe and persistent breach. For IT, detecting and recovering from a firmware attack is extremely difficult — it may even involve replacing the device's system board.

An embedded feature of HP computers and printers, HP Sure Start automatically validates the integrity of BIOS code at startup and allows the device to boot only with genuine HP BIOS code. During PC operation, HP Sure Start runtime intrusion-detection capabilities continuously monitor the device memory to automatically detect, stop and recover from a BIOS attack or corruption. If the device is compromised, HP Sure Start forces an immediate reboot and overwrites corrupted BIOS code with an embedded safe copy. For printers, HP Sure Start keeps the BIOS safe while whitelisting ensures only digitally signed, good code is used. Runtime intrusion detection identifies anomalies during complex firmware and memory operations, and Connection Inspector monitors for anomalies of outgoing packets. All of these self-healing capabilities are performed without IT intervention and with little or no interruption to user productivity.

In addition, PCs managed by HP DaaS and printers covered by HP Managed Print Services can automatically receive firmware updates, so they continually operate with the latest security patches and features.

For example, the HP JetAdvantage Security Manager software enables IT to establish and maintain security settings such as configuring ports and access protocols, in accordance with agency policy, on an individual printer or across the fleet. HP printers also support the security features of HP Sure Start, application whitelisting and real-time intrusion detection.

Additionally, the HP Connection Inspector feature on enterprise printers blocks suspicious network requests to thwart malware. The printer also uses this feature to detect and prevent unexpected changes to its memory that could signal a cyber attack.

Finally, to make sure sensitive documents are retrieved only by the right person, HP printers require user authentication and access codes.

Closing gaps in security policy. Strengthening policies is an important part of ongoing security management. Yet without a high level of security expertise, it can be difficult to identify needed improvements. HP Security Advisory Services for Printers and PCs offer security assessments by credentialed security experts to evaluate security, including security vulnerabilities. As an outcome of security assessment, the HP security advisor provides a roadmap detailing how to improve the agency's security posture based on its current printer fleet or PC fleet.

HP security advisors will work with the agency's respective key stakeholders and teams to review the current environment and better understand security concerns, processes, practices, gaps and vulnerabilities.

A security environment engagement will bring together key stakeholders, educate the client on security threats, and help the client reach consensus on the goals of a new security strategy — one that strikes the right balance between security, cost and ease of use.

HP security advisors gather detailed information and conduct inquiries and interviews with a variety of teams — including print, infrastructure, network and security teams — about the client's security practices and how they are applied to print devices or PCs. The security advisors help identify and validate risks, estimate their likelihood and potential impact, and present recommendations to improve the client's security posture as it relates to the printer or PC environment.

Printing as a service. A managed service for printers from an external vendor may better serve the agency's technology and security needs than buying and managing printers directly. HP Secure MPS is a managed print services offering that implements secure printers, then protects them with layers of defense including device hardening, data encryption and built-in malware protection.

These practices are important for every printer in the agency, not just the most sophisticated models or the ones with the highest use.

IMPROVING SECURITY WITH EVERY REFRESH

Cybersecurity today means protecting every endpoint with robust technologies and practices. The goal is to keep hackers from breaking in and limit the chance of accidental breaches. How can a public sector organization make these security improvements given the constraints of staffing and budgets? Either of two strategies can help.

One strategy is to use a planned technology refresh as the opportunity to move to a managed device service. An agency can leverage a vendor's staff, expertise and tools to deploy, secure and manage all PCs and printers with timeliness and consistency. This strategy also has the benefit of predictable costs that are applied to operations budgets.

The other strategy is to take an incremental approach to implementing new endpoints in a scheduled technology refresh. Some agencies replace mission-critical devices or those at highest risk initially, then prioritize the remaining devices. This strategy can add complexity for months or years depending on the organization's fleet refresh cycle because different endpoints will have different security protections. However, those differences will diminish with the eventual replacement of all endpoints.

Executive support is essential for either strategy. Unfortunately, some leaders don't see the need for strong security until a data breach or ransomware attack occurs. Begin by educating agency

Making the Case for Investment in Endpoint Security

Former Michigan State CSO Dan Lohrmann provided the following tips to educate agency leaders about the importance of investing in cybersecurity for endpoints:

- Use benchmarks to compare the agency's security position and investment with peers
- Conduct on-site education and conversation sessions with leaders throughout the agency to obtain both bottom-up and top-down engagement
- Provide regularly scheduled briefings to agency leaders about current security trends, as well as success stories, best practices and lessons from other states or localities
- Promote understanding of applicable security regulations and mandates and the importance of compliance

stakeholders and leaders about the importance of endpoint security to the organization. Provide information that helps them see how it's much easier and less costly to improve security proactively, especially for endpoints.

For an incremental refresh, the next area for attention is the procurement process. Examine RFP specifications and procurement criteria to verify they adequately address the organization's security requirements for endpoints. Nearly 30 percent of public sector RFPs for PCs and printers don't specify security requirements. Of greater concern is that when security requirements are included, they are typically outdated and weak.[9]

Educating all procurement decision-makers and staff about the importance of security requirements avoids the situation where a product with inadequate security is chosen simply because it has the low cost. It's also important to understand that many equipment vendors offer security only as an add-on option. This approach means extra cost and a printer or PC that's more complex to monitor and manage.

Finally, consider how security capabilities will need to adapt in the future. An endpoint that has a roadmap to add security features and tools over the solution's life cycle will deliver long-term value.

HP delivers solutions in a comprehensive line of PCs and printers that are designed to help meet the security requirements of government. These solutions are based on HP's recognized work in conducting cybersecurity research, participating in security standard setting bodies and driving security innovation. The comprehensive HP roadmap will continue to help government agencies detect, protect and recover from incidents with built-in security features that employ technologies such as intelligent machine learning, automated BIOS protection and intrusion detection.

Automating device security with current and future HP solutions will help improve an agency's cyber resiliency and solve the problems created by staffing shortages. HP's automated features free time for cybersecurity professionals, allowing them to meet other agency needs. The HP roadmap will help agencies stay at the forefront of technology innovations, best practices and industry standards for security.

This piece was created by the Government Technology Content Studio, with input from HP.

Endnotes

1. https://www.ajc.com/news/local/ransomware-attack-cost-city-million-records-show/fQsFupoLl9Zzmt1OsnTIIM/
2. https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/?icmp=np_inform_variation-control
3. http://www.govtech.com/security/As-Government-Hacks-Intensify-Mounting-Costs-Prompt-Concern.html
4. http://www.govtech.com/security/Ohio-cities-face-increasing-ransomware-cyber-attacks.html
5. Verizon: 2018 Data Breach Incident Report, https://www.verizonenterprise.com/verizon-insights-lab/dbir/
6. Security Intelligence: Calculating the Cost of a Data Breach in 2018, the age of AI and the IoT, https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
7. http://www.govtech.com/security/Lewis-County-Wash-IT-Official-Cybersecurity-Is-Not-Going-to-Get-Any-Easier.html
8. Cisco/Lumeta: Cisco 2018 Annual Cybersecurity Report, https://www.cisco.com/c/en/us/products/security/security-reports.html#~download-the-report
9. IDC: Government Procurement Device Security Index 2018

Disclosures

a HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® or AMD processors.

b HP Sure Click is available on most HP PCs and supports Microsoft® Internet Explorer and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.

c 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.

d HP Sure View integrated privacy screen is an optional feature that must be configured at purchase and functions in landscape orientation.

e HP DaaS plans and/or included components may vary by region or by Authorized HP DaaS Service Partner. Please contact your local HP Representative or Authorized DaaS Partner for specific details in your location. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

Sponsored by: hp

For more information, visit: **www.hp.com/go/nationalipa**