Business white paper

Create a solid healthcare security position

Security risks and recommendations for healthcare organizations

Table of contents

Protect patient data

Given the wealth of sensitive personal data that healthcare organizations process and store, it's no surprise that hospitals, medical offices, and other healthcare organizations are prime targets for cybercrime. As attacks get more sophisticated and the consequences of a breach more severe, hardening security across the operation becomes imperative. Fortunately, HP offers devices with built-in security features and add-on solutions that can help reduce risk and increase efficiencies.

Vulnerable endpoints can put the network and data at risk

Healthcare organizations spend a lot of time and money making sure firewalls are strong and their server infrastructure is protected. But what about endpoints like PCs and printers? These devices are connected to the network. If they become compromised, the entire network—and patient data connected to it—can be at risk.

Although today's printers and MFPs are networked, they are still often overlooked in security measures. In a recent study, print infrastructure is now viewed as one of the top security risks by organizations.[1] Even something as simple as an unclaimed print job can put sensitive patient data in the wrong hands.

End users pose another security risk that is often neglected. End users should be your first and last line of defense and educated with security awareness, such as social engineering and phishing attacks. For instance, PC users can be tricked into browsing a fraudulent website that can infect their machine with malware.

Common attack scenarios

An administrative staffer receives a seemingly innocuous email that leads to a malicious website that installs malware. When the PC misbehaves, the helpdesk logs into the device to resolve the issue. The malware steals the helpdesk user's credentials. The attacker uses those credentials to access more endpoints and steal more credentials, then launch several kinds of malicious attacks—from pranks to ransomware schemes to data theft. Stopping the cycle can be very difficult, and attempts are relentless: in 2017, users received an average of 16 malicious emails per month.[3]

Or, a nurse receives an email with an attached PDF coupon—with malware attached. When the nurse sends the PDF to the printer, the malware infects the printer, and then enters the firmware. From there, the malware could create all kinds of problems, from simple pranks (such as changing the front panel to a different language) to opening printer ports (thus allowing hackers to upload compromised firmware).

Other scenarios involve physical theft. A doctor sends a confidential medical record to the printer but then is distracted by an important phone call. By the time she arrives at the printer, the document has been picked up by someone else. Or, a laptop is stolen from a hospice nurse's car. The default password is easily guessed, giving the thief access to thousands of unencrypted patient records.

40% of healthcare agencies hit by single ransomware in 6 months

Healthcare organizations tend to use legacy apps and outdated operating systems. That makes them easy prey for ransomware—even old versions that can be blocked by patches.

According to a report by cybersecurity firm Armis, 1.7 million devices worldwide are still vulnerable to the WannaCry ransomware released in 2017. It attacks 3,500 devices every hour, with 145,000 devices currently compromised.[2]

Costs of a security breach

- IT time and infrastructure updates to fix the issue and recover data
- Regulatory fines
- Civil actions
- Identity theft monitoring services
- Loss of business
- Loss of brand or share value

= $13 million

(Average annual cost of a breach)[4]

HP can help

Security must be built into PCs and printers, not bolted on as an afterthought. By designing for cyber resilience, healthcare organizations can help reduce the risk of attacks, increase user productivity by helping to eliminate downtime, cut IT costs, improve compliance, and get back to what they do best—patient care.

This white paper explores some of the security challenges faced by healthcare organizations today and discusses recommended processes, including HP hardware and solutions, that can help reduce risk.

The costs of a breach can be staggering

A data breach can inflict huge costs on organizations and their patients. The ramifications of a security breach could include identity theft, stolen competitive information, a tarnished brand image and reputation, and litigation. Plus, regulatory and legal noncompliance can result in heavy fines.

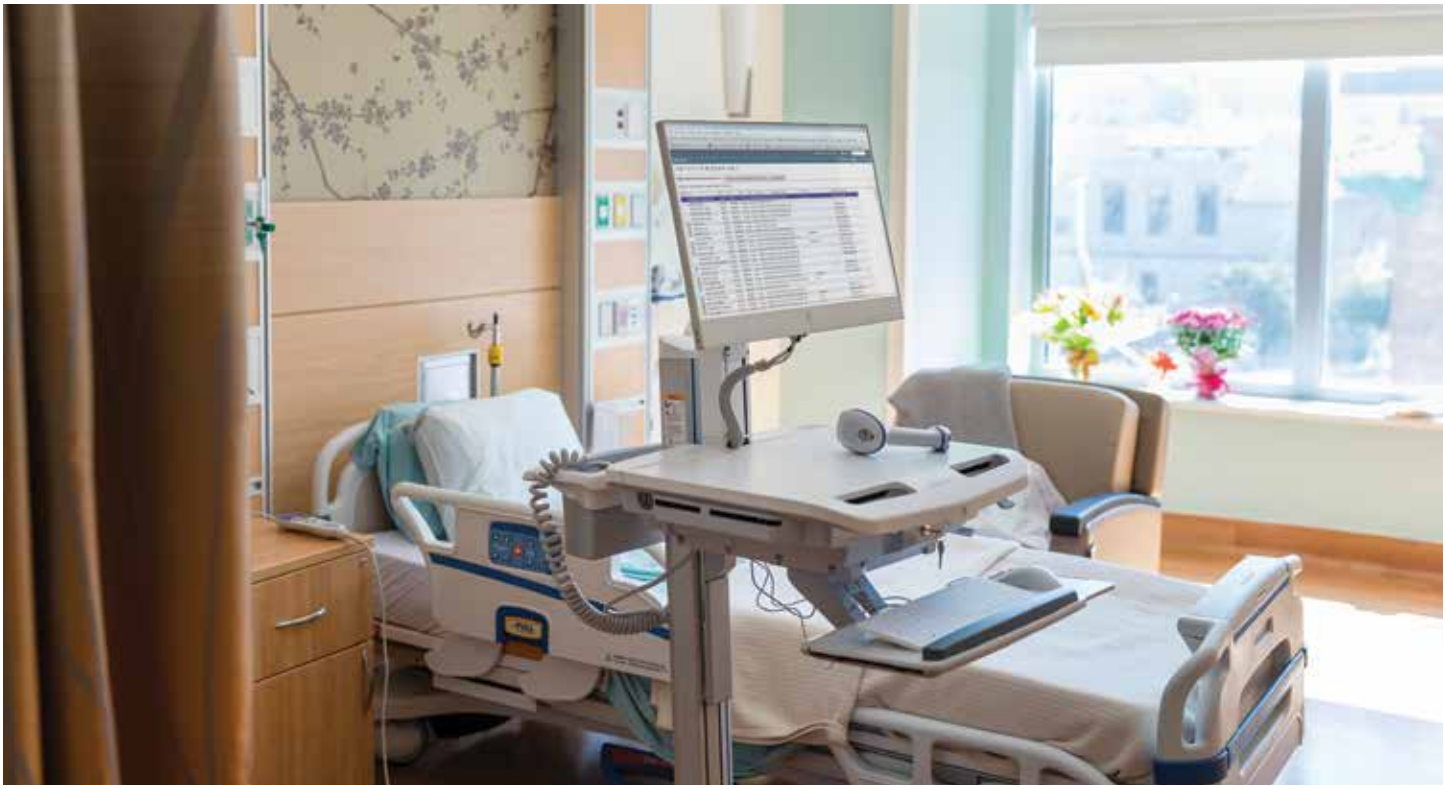
Medical patient records are covered by particularly strict regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the US. Healthcare breaches remain the most costly per record because of their high visibility and multiple downstream impacts. The healthcare industry has the highest per-capita data breach cost, at $408 per compromised record—nearly twice the cost per record for financial organizations.[5]

Security breaches are increasing in frequency. According to Risk Based Security, 2017 saw more than 5,200 breaches that exposed nearly 7.9 billion records.[6] That figure rose to 6,500 breaches in 2018.[7] Medical patient records are particularly lucrative targets.

In addition to the financial costs of a security breach, loss of productivity can also cause big problems. Malicious attacks can make PCs unusable or can cut off providers from the data they need to treat patients safely. An attack at the BIOS level can take hundreds or even thousands of devices down, bringing operations to a halt across an organization.

Healthcare organizations have specific security concerns

Security is important for all companies, but healthcare organizations have additional concerns. These organizations must meet the challenges of protecting Electronic Medical Records (EMR) while, at the same time, providing authorized personnel access to the information they need. To keep patients safe, information must be accurate and delivered quickly. In a public environment—with patients, clinicians, staff, visitors, and suppliers coming and going—the devices that healthcare professionals use must be protected from theft and malicious activity like visual hacking. When time and budgets are tight, IT must find ways to streamline management and monitoring of device fleets. And strict compliance requirements request healthcare organizations to be ready to prove they have protected sensitive information in the case of an audit. This includes safeguarding against internal accidental or malicious breaches by constantly monitoring and analyzing content for data loss detection.



Impacts of a security breach to a healthcare organization

- Loss of critical patient data
- HIPAA breach resulting in fines and litigation
- Loss of productive patient care
- Loss of established brand

The firewall isn't enough to protect the network

Many organizations are counting on their firewalls to protect the data and devices within the network, but this isn't enough. It's becoming much easier for hackers to break into networks through under-secured endpoints like IoT devices, PCs, and printers. In a typical organization, the number of endpoints is much greater than the number of servers, sometimes as many as two devices per employee. Consider all the computers and printers healthcare workers use throughout the day—including portable devices used in patient rooms and laptops taken home for use after hours. The sheer volume of endpoints increases the risk. Just one stolen or vulnerable device can provide entry to the network, expose sensitive data, and put the entire infrastructure at risk. That's why it's so important to deploy devices with built-in security protections that can detect and automatically recover from attacks.

HP designs layers of security to help protect devices and the network

HP is revolutionizing security with a whole new approach: help protect the network and reduce risk by building layers of security into endpoint hardware. HP printers and PCs are designed to protect the device, identity, data, and document. A comprehensive mix of built-in features and add-on solutions helps protect each of these from below (hardware-enforced), within, and above the operating system.

And, of course, any protection needs to be manageable, because security without manageability is unsustainable. HP's unique management solutions help organizations improve endpoint device security without over-burdening their IT staff. Many monitoring and management tasks can be handled automatically, without IT intervention. HP devices are also designed to seamlessly connect to Security Information and Event Monitoring (SIEM) tools to provide real-time security-event analysis.

HP understands healthcare security challenges and how to meet them. Whether it's in a clinic, a visit room, a doctor's office, the back office, a provider's home office, or a health insurance company, HP has the devices and solutions to help organizations reduce risk while improving efficiencies.

Healthcare security challenges and HP solutions

Securing the device

Vulnerabilities

Vulnerable endpoints can open the entire network—and any data stored on it—to attack. If devices are rendered unusable by malware, or "bricked", organizations can suffer loss of productivity or even their entire operations.

Printers and MFPs are similar to PCs when it comes to their components, capabilities, and risks. Both PCs and printers start up using firmware called BIOS (Basic Input Output System). The BIOS is responsible for controlling the basic functions of a computing device. It holds the time, date, and configuration settings such as the boot order and the speeds at which the processor and memory run. This is core to how the PC and printer operate, so an unsecured BIOS can offer a dangerous amount of access to a hacker.

BIOS-level attacks are very difficult to detect because they control the device below the operating system and cannot be removed or modified by anti-virus software. Malware targeting the BIOS can continually supply data and reinstate itself after network defenses deploy. It can even survive a disk wipe and operating-system reinstallation.

Unsecured wireless connections, open ports, and outdated protocols can all give hackers access to devices and the sensitive patient data stored on them.

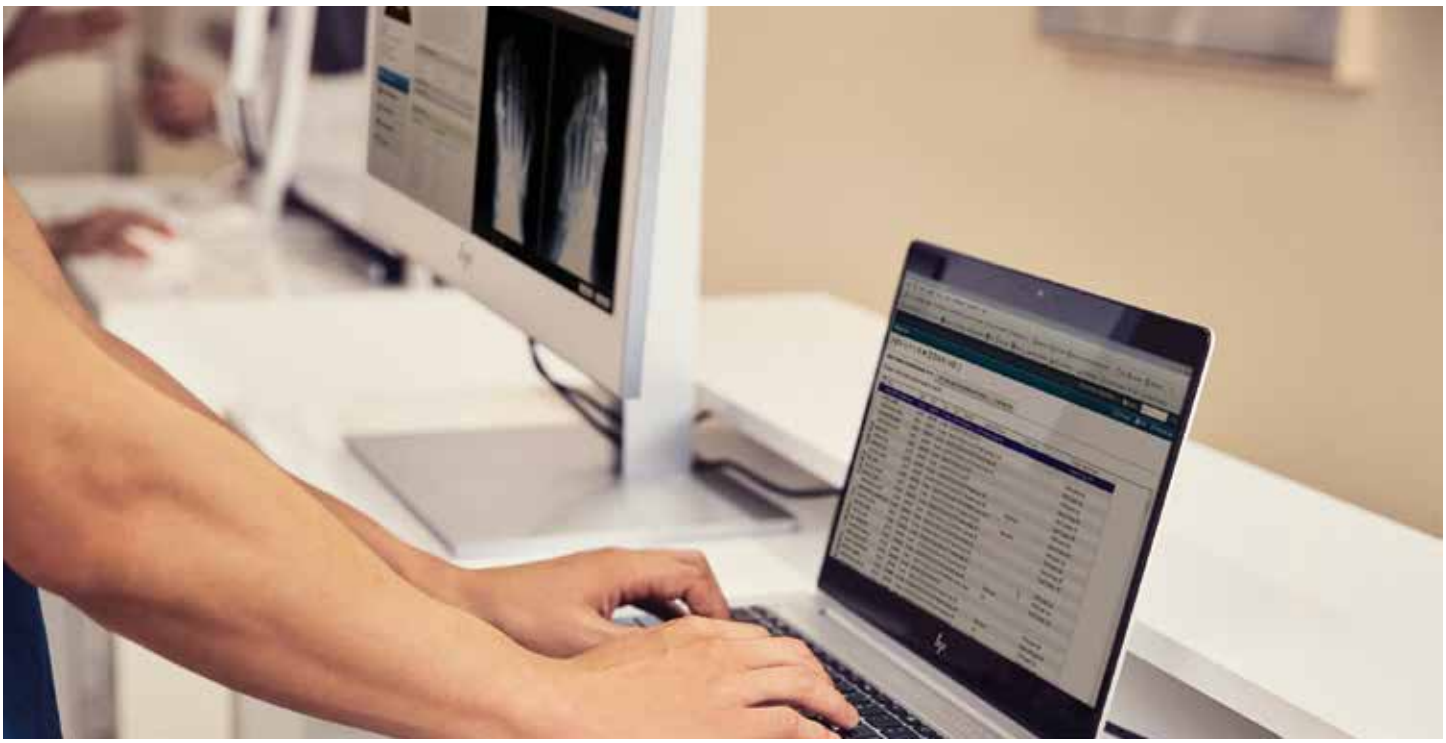
Recommendations

To protect against malware, HP Elite PCs offer HP Sure Start Gen 5,[8] which uses always-on monitoring to automatically detect, stop, and recover from a BIOS attack or corruption without IT intervention and with little or no interruption to user productivity. HP Sure Start automatically validates the integrity of the BIOS code at startup and during operation to help ensure that the PC is safeguarded from malicious attacks. Run-time intrusion detection constantly monitors memory while the device is running. In the case of an attack, the PC can self-heal using a safe "golden copy" of the BIOS in less than a minute. Plus, BIOS-setting protection safeguards and restores BIOS setup variables, policies, and data. It's the industry's first and only self-healing BIOS with run-time intrusion detection—and it's built into HP Elite PCs.[8]

HP Sure Start and run-time intrusion detection are also included on HP Enterprise printers and MFPs to protect at startup and during operation. If malware is detected, the printer automatically shuts down and reboots the device. Every time a printer is turned on or restarts with an error, HP Sure Start automatically validates the integrity of the BIOS code and self-heals if necessary. There's no need for IT to intervene. HP Enterprise printers and MFPs also include whitelisting to help ensure that only authentic, known-good HP firmware and approved third-party applications are digitally signed by HP and loaded into memory. HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and thwart malware by automatically triggering a reboot. Only HP print security offers real-time detection, automated monitoring, and built-in software validation to stop threats the moment they start.[9]

It's important to keep the OS updated to the latest version. HP Enterprise printers and MFPs are powered by upgradeable FutureSmart firmware, which allows organizations to update printers with new security features as they become available. HP Elite PCs come with Windows® 10, the most secure Windows version ever. HP hardware is designed together with Windows to help secure the device. HP Sure Run[10] interfaces with the HP Endpoint Security Controller at the hardware level (below the OS) to ensure OS security. It builds upon the existing HP Endpoint Security Controller hardware foundation to continually maintain a desired state of the operating system. This can include particular security services and specific functionality that must be present at all times. HP Endpoint Security Controller is enabled by unique HP security hardware.

IT departments can save time with management tools that allow them to check firmware versions and update firmware across the printer and PC fleets. Plus, HP offers Managed Print Services to further reduce the burden.



9 assisted living facilities affected by ransomware

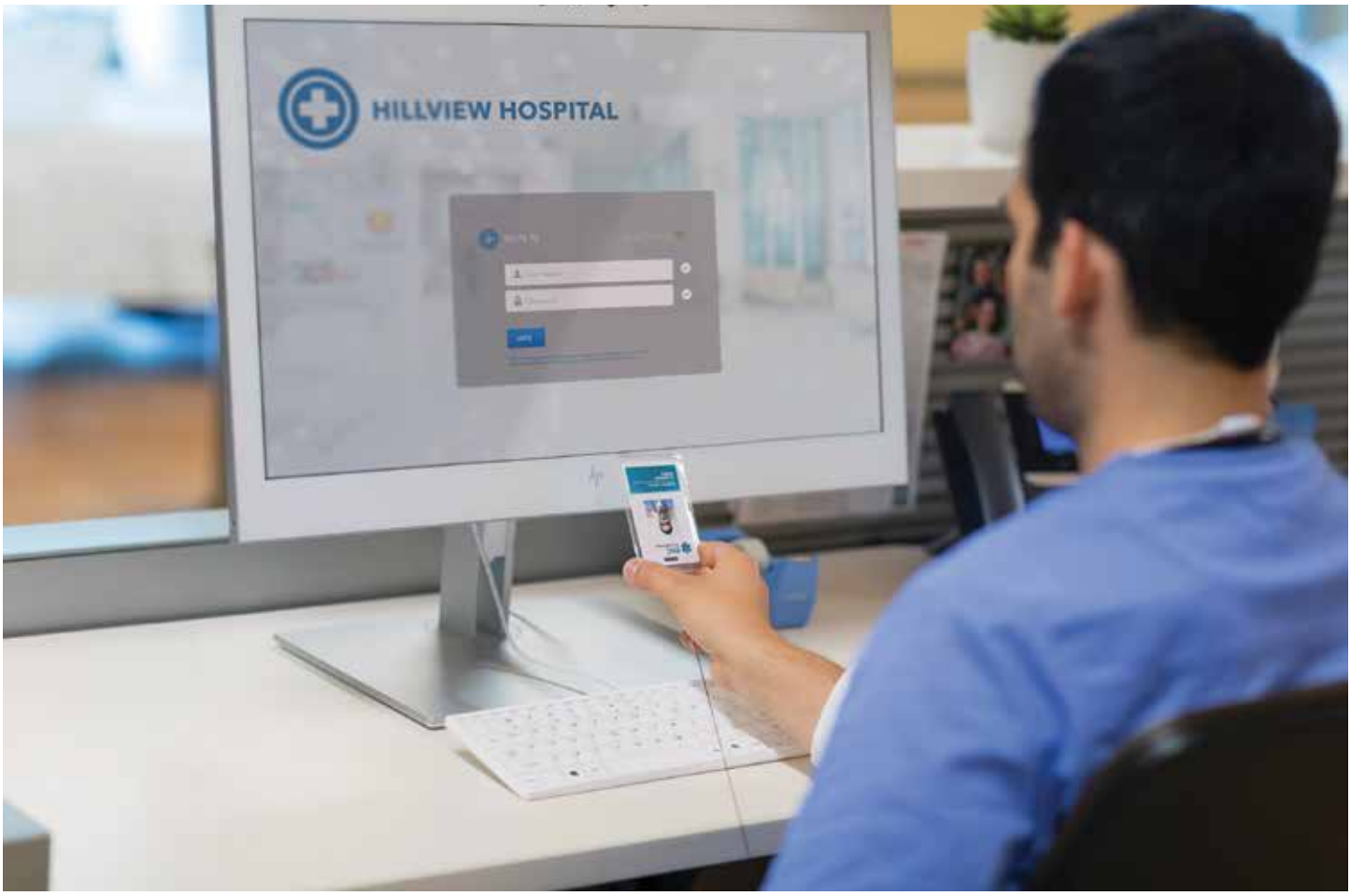
In March 2019, ransomware attacked records at nine assisted living facilities. The attack was promptly detected—but that did not prevent widespread file encryption for purposes of extortion. Compromised data included names, addresses, social security numbers, financial information, diagnoses, lab test results, and prescriptions.[14]

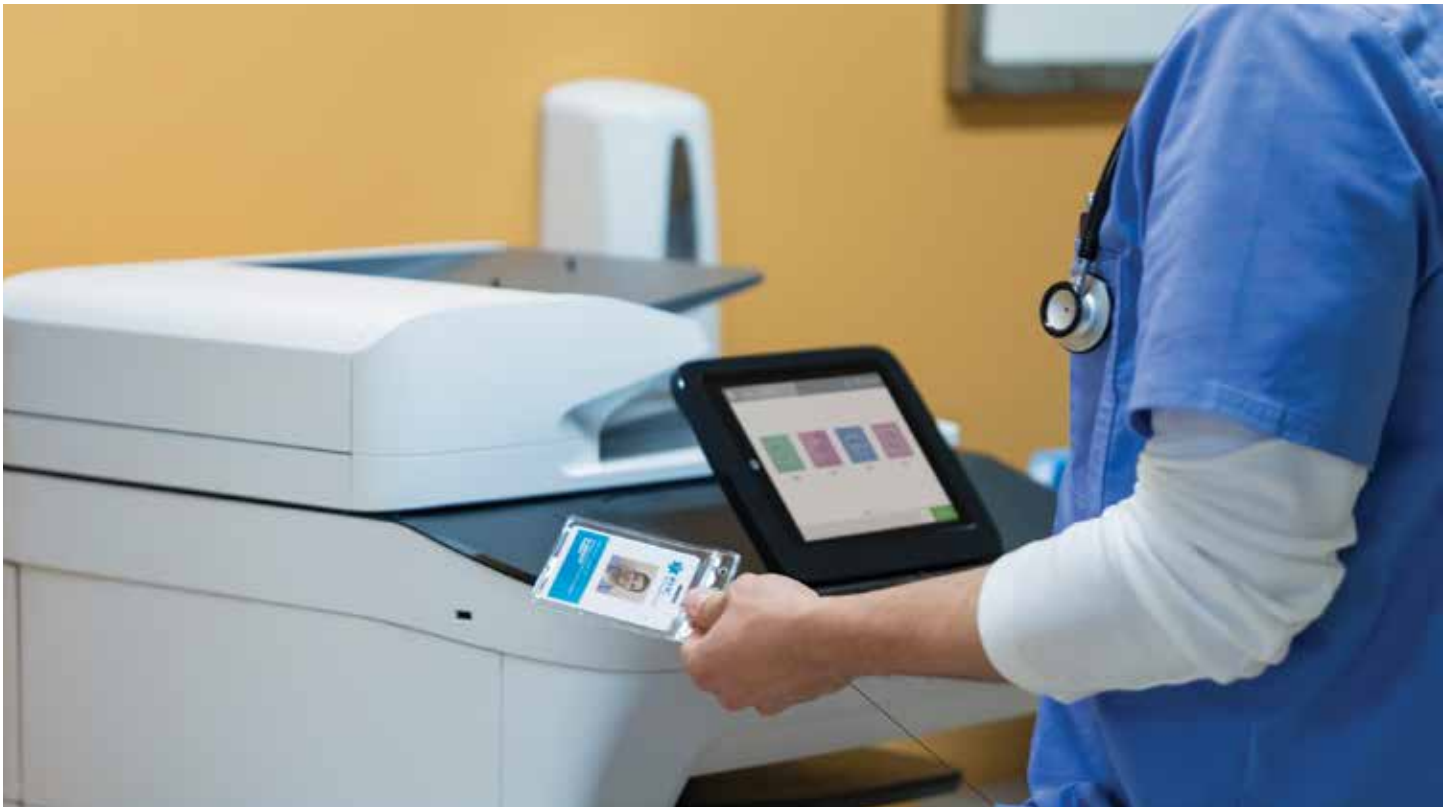
In addition to Sure Start and Sure Run, HP Elite PCs have other features built in to ensure resiliency (the ability to self-heal after an attack). HP Biosphere keeps a copy of the boot sector in firmware, enabling automatic detection and recovery from the most destructive malware that renders other PCs inoperable. HP Sure Recover[11] is a PC OS recovery solution built into the hardware and firmware that can fully recover the HP OS image from a network connection, even if recovery software isn't present on the machine. HP Sure Recover can be configured to use healthcare provider custom, securely signed software images hosted on an internal private network or the public internet. And, the HP Sure Recover configuration can be managed either locally or remotely, with the HP Sure Recover configuration for each PC protected in isolated, non-volatile memory managed by the HP Endpoint Security Controller hardware.

For both printers and PCs, administrators should close unused ports and protocols—for example, to prevent malware being uploaded from or data being downloaded to a USB drive. For printers, IT can manage USB ports and removable media with HP Web Jetadmin.[12] Manage print security across the HP fleet using HP JetAdvantage Security Manager to create proof-of-compliance reports that demonstrate adherence to security and data-protection policies. HP JetAdvantage Security Manager can automatically assess, monitor, and remediate devices, allowing IT staff to focus on other tasks.[13] For PCs, the HP Device Access Manager allows administrators to establish approved users who authenticate and then are granted access to specific PC features for a predetermined period.

From a print policy point of view, organizations can set policies to enforce that only network-approved, secured devices are connected to the network, to reduce the risk of non-compliant devices.

Administrators can also automatically track the location of assets (such as PCs, laptops, printers, or servers) with RFID asset monitoring. HP Healthcare Edition Notebooks and Healthcare Edition AiO PCs now offer embedded RFID for location services, which transmits a signal to a hospital's real-time location services or geofencing infrastructure.





Securing identity

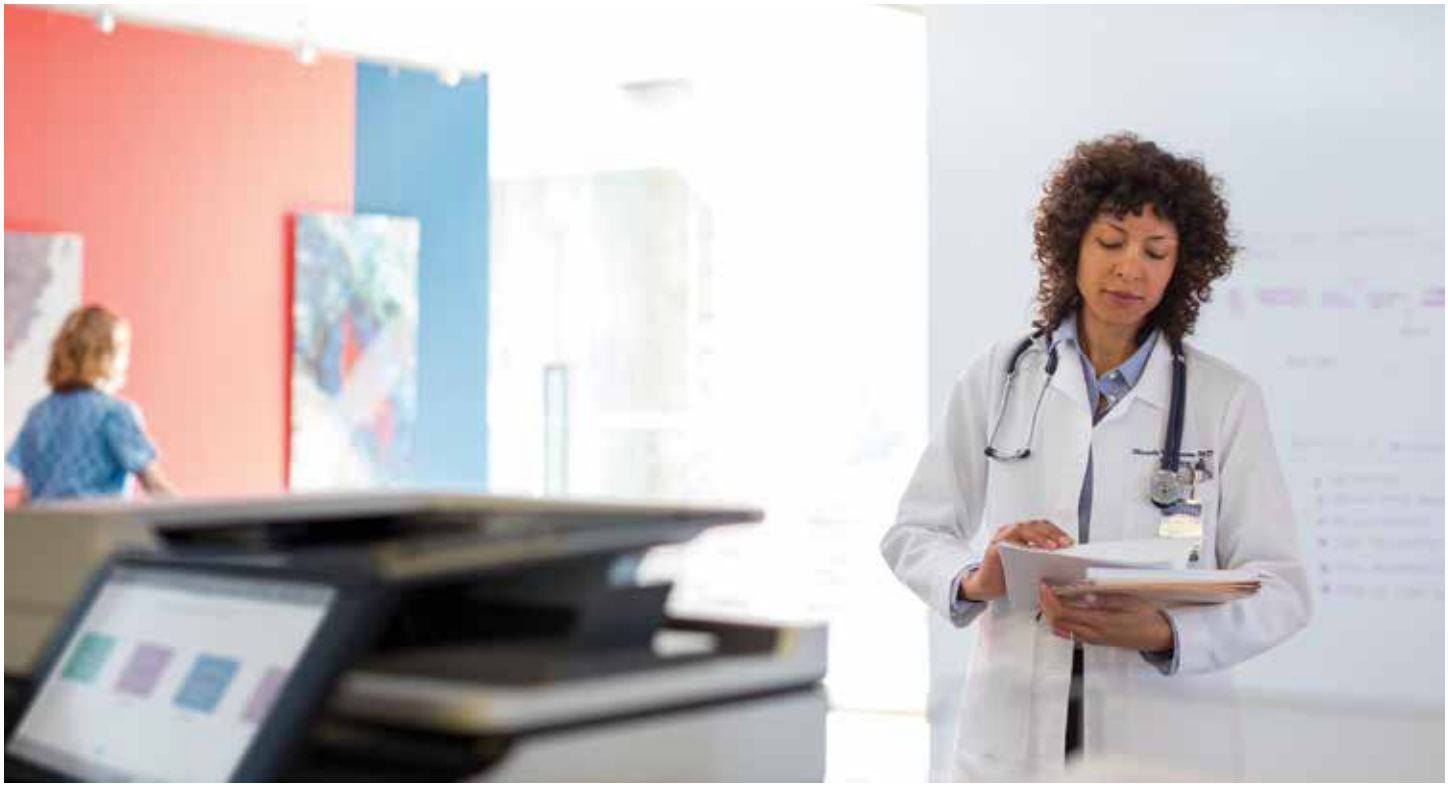
Vulnerabilities

PC and printer credentials are top targets for thieves, because they can provide hackers an entry point to the IT infrastructure. Passwords alone no longer provide the level of security required for today's threats, and users often take shortcuts that reduce the integrity of passwords. According to a recent report by Clearwater, deficiency in user authentication (including weak or default passwords) is the most common security vulnerability in healthcare.[15] Authentication should be required when completing patient charts or when sending scanned patient documents, either internally or externally.

Recommendations

Good password security makes the user's life easy while making the attacker's job difficult. HP Client Security Manager multi-factor authentication is a software-based approach that gives admins the ability to increase security by requiring two authentication factors. For HP PCs with Intel® processors, HP Client Security Manager with Intel Authenticate support offers three-factor authentication, including hardware-enhanced factors.[16] By requiring more than one factor, such as what a user knows (password, PIN), what a user is (fingerprint, facial recognition), and what a user has (proximity card, smartcard, contactless card), users get a faster, more seamless login experience that is one million times more secure than a single, non-hardened password. This is more secure than conventional Windows 10 security, which only gives different options for single-factor authentication. Furthermore, HP's Management Integration Toolkit enables configuration and enforcement of PC authentication policies, making it easier for administrators to secure their fleet.

HP MFPs offer a multi-protocol, proximity-embedded RFID Card Reader with Seos technology for improved identity verification. HP Healthcare Edition personal systems and printers offer the RFID card reader, plus a FIPS 201-compliant fingerprint reader.



Health insurer fined $16M for data breach

A major health-benefits company reached a record $16M settlement with the U.S. HHS Office for Civil Rights (OCR) in October 2018 after the largest-ever U.S. health data breach.

The 2015 breach lasted nearly two months and compromised the personal information of nearly 79 million individuals, including names, social security numbers, addresses, medical ID numbers, birthdates, email addresses, and employment information.

The OCR's investigation concluded that the company lacked sufficient security measures and failed to identify and respond to the cyberattack.[17]

Securing data

Vulnerabilities

Keeping patient data safe is one of the most important duties of healthcare organizations. When a breach occurs, the costs can be high—both financially and to the organization's reputation. Even without an actual breach, organizations that fail to meet compliance requirements can face steep regulatory fines.

Without a strong authentication system and administrative controls, devices—and the data they're connected to—can become available to unauthorized users.

As attacks become more sophisticated, hackers can often gain access to the system through its users, whether through an innocent-looking link in an email or fraudulent use of printer credentials. A 2019 Quocirca report calls print security "the gateway to valuable, confidential and sensitive information."[18]

In public healthcare environments, notebook computers can be susceptible to visual hacking. A visual hacker—say, a "patient" who observes a doctor entering credentials—may only need one piece of valuable information to start a data breach. According to studies by the Ponemon Institute, nine out of ten attempts to steal sensitive business information using only visual means were successful, with nearly four pieces of private information visually hacked per trial. In 68% of the visual hacking attempts, the visual hacker went unnoticed or unchallenged. Nearly half of the visual hacking attempts were successful in less than 15 minutes.[19]

Data can also be at risk if a device is lost or stolen, or when an organization is ready to decommission devices. Organizations often fail to completely wipe data from drives when disposing of PCs or printers at end of life or end of lease.

Recommendations

Only authorized users should be able to access devices and networks. As discussed above, multi-factor authentication can help protect PCs and identities. For printers and MFPs, fleet-wide authentication solutions can require users to enter a password or PIN, or scan their badge or fingerprint. HP solutions include HP Universal Print Driver[20] and HP Access Control[21] for PC network printing, and HP PrinterOn Enterprise and HP Roam for Business[22] for mobile users.

Admins can protect devices by using strong administrative controls to prevent configuration changes. HP JetAdvantage Security Manager[13] can automatically apply these controls across the print fleet. Role-based access can limit access to only those users who need specific features. For example, HP Access Control[21] allows IT to prevent users from sending emails from MFPs without authorization. HP Healthcare Edition products offer integrated dual-band RFID readers for authentication and single sign-on.

Encryption helps make stolen data unreadable, which can help meet compliance requirements. When equipped with hard drives from the factory, all HP Enterprise printers and MFPs utilize AES 256-bit self-encrypting drives to protect data at rest. FIPS-certified drives are also offered optionally. HP Elite PCs come with BitLocker Drive Encryption, which integrates with the Windows 10 operating system to help mitigate unauthorized data access by enhancing file and system protections. It also helps protect against data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

Data in transit should also be encrypted. Data traveling between PCs and the network is often encrypted, but data flowing to and especially from printers is often overlooked. Administrators should use Wi-Fi and network-encryption protocols along with solutions like HP Universal Print Driver[20] or HP Access Control.[21] Apply CA signed certificates to network printers and MFPs. Save time by using HP JetAdvantage Security Manager[13] to automatically install and renew certificates.

Hardware-based virtualization can protect devices when users need to visit unfamiliar websites or open attachments from unfamiliar sources. With HP Sure Click[23] enabled on a supported browser, users are protected if they accidentally click on bad links in phishing emails. Because untrusted websites will always be opened in their own isolated micro-VMs, users can explore the Internet safely—any malware they encounter remains isolated from the rest of the system and destroyed when the browser tab is closed. The latest version of Sure Click now offers protected viewing for PDFs, Microsoft® Word, Microsoft Excel, and Microsoft PowerPoint files to help prevent damage from potentially malicious attachments.

The HP Sure View integrated privacy screen protects against visual hacking in public environments.[24] Users can block out wandering eyes with just the push of a button. The HC241p and HC271p clinical review displays have integrated passive privacy filters behind the glass, making them easy to clean and disinfect, and allowing for much nicer aesthetics than add-on privacy filters that have to be frequently replaced due to wear and tear.

Healthcare organizations should make sure that data on storage drives is made unreadable and unrecoverable before disposing of or repurposing hardware. HP Secure Erase[25] meets various industry regulations to permanently erase data on PC and printer storage drives. HP also offers on-site data destruction and off-site recycling to erase sensitive information and help keep organizations in compliance.

The HP EliteOne 800 G5 and EliteBook 840 G6 Healthcare Edition PCs use HP Sure Sense to recognize and protect against malware—even never-before-seen attacks that traditional antivirus solutions may not recognize. With cyberattackers targeting valuable healthcare information, protecting against the newest threats is vital to safeguarding sensitive patient data.

Securing the document

Vulnerabilities

Unclaimed print jobs are one of the simplest and most common ways sensitive patient data can be exposed. Any printed document is at risk of being stolen by an unauthorized person if the intended recipient isn't there when it comes out of the printer. Additionally, documents are often sent to the printer and forgotten—left unattended for anyone to claim.

While many health systems are moving towards a completely digitized environment, only five percent of hospitals in the U.S. and one percent worldwide achieved HIMSS Stage 7 by 2017.[26] That means that patient charts, critical lab results, treatment plans, discharge papers, and other stats are still frequently printed on paper. In the wrong hands, these paper records can expose protected health information, medical courses of action, or post-discharge treatment plans. Printed stats, when stolen, can have a devastating effect on patients' privacy and can cause the liable institution significant financial harm.

Even when health information is not printed, it still must be protected. Without proper tracking and control, sensitive records—including scanned content like patient admissions forms or lab results—can become available to unauthorized users. This kind of breach can put organizations at risk of noncompliance. Printer input trays can also present a risk. Special paper used for printing checks, prescriptions, or other sensitive documents can be stolen if not protected.

Recommendations

Healthcare organizations should deploy a pull-print and user-authentication solution fleet-wide so that documents are not printed until the user authenticates at the device using hospital identification security protocols. HP offers several authentication and pull-print solutions for a variety of situations and IT environments:

- HP Access Control Secure Pull Print is a server-based, pull-print software solution that can be set to require all users to authenticate before retrieving their job.[21]
- HP JetAdvantage Secure Print provides an option for print jobs to be sent and stored in a secure cloud queue until the user authenticates and prints the job.[27]
- HP Universal Print Driver is a free print driver solution that includes a secure encrypted printing feature for sensitive documents.[20] It allows users to send a print job to be held until they release the job via a PIN at the device.
- The HP Proximity Card Reader lets users quickly authenticate and print securely at a printer or MFP using their existing ID badge.[28]

Capturing digital information can support record retention and privacy requirements. Securely track and control distribution of scanned content with HP Capture and Route. This HP JetAdvantage Workflow Solution makes it easy to manage, update, and route information—accurately and efficiently. HP Capture and Route is a secure and compliant solution that not only utilizes user authentication and validation, but data-at-rest encryption, along with a number of other security features.

Detect and help prevent intentional or unintentional data breaches by preventing scanning, faxing, or printing of sensitive or confidential documents in real time. The HP Capture and Route Data Loss Prevention solution allows you to set policies and choose how the solution will respond if a user initiates a scan or fax job that violates those policies, from stopping delivery to quarantining the document for review by an Admin. The HP Access Control Print Data Loss Prevention solution allows you to set policies to prevent printing of confidential documents and customize actions based on the rules you create. This solution can be incorporated into your existing HP Access Control installation or deployed as a standalone solution.[21]

Control access to preprinted forms. Equip your printers and MFPs with locking input trays to help prevent theft of special paper used for printing checks, prescriptions, or other sensitive documents.

Protecting the patient

Vulnerabilities

Safeguarding patient identification is a regulation set by healthcare-accreditation agencies across the globe. In fact, proper patient identification is the foundation of patient safety. But patient admissions can be complex, manual, multi-step processes that can easily lead to errors. New regulations and smaller budgets are causing undue burden on nursing, managerial, and intake staff. To help these people do their jobs accurately, healthcare organizations need to reduce administrative complexity even while they're focusing on improving patient safety and reducing medical errors. Wristbands that stay on the patient and remain readable after repeated use and extended treatments must be easy to print and cost effective to deploy.

Recommendations

The HP Patient Identification Printing Solution for Healthcare increases efficiency and patient safety by allowing healthcare organizations to leverage their investment in existing printers. Consolidate devices by using a broad range of HP devices approved for printing LaserBand® patient identification wristbands and labels.

The solution can help organizations meet Electronic Medical Records protocol without having to invest in new equipment. It allows admissions departments to print a complete patient admissions packet—including not only color-coded wristbands, but privacy notices, consent forms, barcoded labels, and documents for lab work, X-rays, or other procedures—from one device, at one time.

Since it is self-laminating, the information on the band is protected against fluids, scratching, or other physical damage throughout the hospital stay. Clinical staff can use a portable barcode scanner to instantly access a wealth of patient information—including photographs, standard medical records, allergy warnings, and so on. This can greatly reduce the potential for error, helping to improve patient safety.

Protecting the prescription

Vulnerabilities

Today's hospital systems need more control over unauthorized prescription access than what's provided by physician's orders on prescription pads or on costly pre-printed specialty prescription paper. As theft of prescription pads becomes more frequent, lucrative prescription fraud threatens to turn healthcare institutions into unwilling enablers for abuse of controlled substances. Secure, tamper-resistant, practical, and cost-conscious alternatives to pre-printed prescription forms are essential.

Recommendations

The HP Prescription Printing Security Solution enables healthcare providers to use HP Enterprise LaserJet and PageWide printers and MFPs—and plain paper—to print high-value, black-and-white documents with anti-fraud security features. Or, proven security features can be added to documents printed on security-forms paper. The server-based application lets administrators define settings for security printing queues, adding anti-fraud features to print files before they are routed to the printer:

Copy-evident pantograph	Reveals a special pattern when any unauthorized copying or scanning occurs.
Variable-data watermark	Prints unique user-defined data across the back of each document to protect against alteration.
MicroPrint optimized	Reveals secondary authentication under simple magnification.
Intelligent warning box	Allows first-line inspectors to easily verify document authenticity.

The HP Prescription Printing Security Solution also includes EMR system-generated features for added security. The FIPS-201 compliant fingerprint reader included on the HP Healthcare Edition Notebook (G6) and AiO (G4 but not G5) for electronic prescriptions for controlled substances (EPCS) helps improve authentication security.

Streamlining management and monitoring

Vulnerabilities

Unsecured endpoints like printers and PCs can open the entire network to attack. But managing the security of printers and PCs can take a lot of time and expertise. Many IT administrators still use laborious, manual processes, which can drive up costs. Across a large fleet of devices, this inevitably leaves individual devices out of compliance and at higher risk.

Recommendations

HP offers management solutions that save time and help reduce costs and resources to maintain security across the fleet of HP printers/MFPs and PCs.

- For HP PC fleet security, the HP Manageability Integration Kit (MIK) is the world's first and only management toolkit certified for Microsoft System Center Configuration Manager (SCCM).[29] Microsoft SCCM is a widely used management solution to remotely plan, deploy, configure, and monitor a fleet of PCs. MIK is an SCCM plug-in that streamlines security and BIOS administration, as well as image creation, through a modern and intuitive user interface. Even new devices can have security policies automatically applied as soon as they are added to the network. MIK can also prevent users or malware from turning off security protection, and can manage roles.
- For HP printer fleet security, administrators can manage basic printer security settings with the HP Printer Security Plug-in for Microsoft SCCM. The HP Printer Security Plug-in can discover, assess, and remediate the top 15 security settings and report on the results. For comprehensive printer fleet security management, HP JetAdvantage Security Manager is a policy-based, print-security compliance tool that allows administrators to easily establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates.[13] Security Manager can even automatically assess and reconfigure security policies every time a device reboots or when a new device is added to the network. Plus, it can create fleet-wide compliance reports so the security team can see how many printers are at risk.

IT should regularly monitor and audit its environment to make sure no endpoints—including PCs and printers—are left unsecured.

- HP printers and PCs have syslog capabilities to create event notifications for security issues such as intrusion detection, whitelisting, or BIOS events.
- Printer and PC syslog capabilities can be integrated with SIEM (Security Information and Event Management) tools to provide real-time endpoint monitoring to help IT detect and resolve issues. In contrast to most printer manufacturers, HP's print devices can be configured to send security alerts to select SIEM tools, including ArcSight, Splunk, SIEMonster, and McAfee.
- Data in SIEM tools can be extracted into an Enterprise Governance, Risk and Compliance (EGRC) solution for compliance reporting.

HP Print Security Services and specialists can help with print-security assessments, planning, deployment, and ongoing management. HP Print Security Advisory Services can help organizations assess vulnerabilities and compliance, develop a custom print-security policy, and make process and technology recommendations for improved security. HP Print Security Governance and Compliance can help organizations maintain security settings compliance across the printer fleet.

Build a better defense today

It's time to take proactive steps to reduce risk and help secure patient data. Security can be complicated, but HP offers hardware and solutions that make it easier for healthcare organizations to protect patients, secure data, address user vulnerabilities, streamline management, improve compliance, and reduce costs.

For more information, or to schedule a thorough risk assessment, contact your HP representative today.

Learn more

HP PC Security: hp.com/go/ComputerSecurity

HP Print Security: hp.com/go/secureprinting

Printing and workflow solutions for healthcare providers: hp.com/go/healthcareprint

[1] Quocirca Global Print Security Study, Louella Fernandes, January 2019. For more information, see hp.com/go/analystscorner.

[2] HIPAA Journal, "40% of Healthcare Delivery Organizations Attacked with WannaCry Ransomware in the Past 6 Months", May 31, 2019. hipaajournal.com/40-of-healthcare-delivery-organizations-attacked-with-wannacry-ransomware-in-the-past-6-months/.

[3] Symantec Internet Security Threat Report, Vol 23: "In 2017, the number of malicious emails sent to the average user each month increased from 9 in January, to 16 by the end of the year."

[4] Study conducted by Accenture and Ponemon Institute, "2019 Cost of Cybercrime Study", accenture.com/us-en/insights/security/cost-cybercrime-study.

[5] Ponemon 2018 Cost of a Data Breach Study, sponsored by IBM: public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf.

[6] 2017 Year End Data Breach QuickView Report by Risk Based Security / Cyber Risk Analytics, January 2018.

[7] 2018 Year End Data Breach QuickView Report by Risk Based Security / Cyber Risk Analytics, pages.riskbasedsecurity.com/2018-ye-breach-quickview-report, February 2019.

[8] HP Sure Start Gen5 is available on select HP PCs with Intel processors. See product specifications for availability.

[9] HP's most advanced embedded security features are available on HP Enterprise-class devices with FutureSmart firmware 4.5 or above and is based on HP review of 2018 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, see hp.com/go/PrintersThatProtect. For more information, visit hp.com/go/printersecurityclaims.

[10] HP Sure Run is available on HP Elite products equipped with Intel or AMD 8th generation processors.

[11] HP Sure Recover is available on HP Elite PCs with 8th generation Intel or AMD processors and requires an open, wired network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

[12] HP Web Jetadmin is available for download at no additional charge at hp.com/go/webjetadmin.

[13] HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

[14] HIPAA Journal, "Ransomware Attack Reported by American Baptist Homes of the Midwest", May 8, 2019. hipaajournal.com/ransomware-attack-reported-by-american-baptist-homes-of-the-midwest/.

[15] HIPAA Journal, "Most Common Security Weaknesses in Healthcare Identified", December 28, 2018. hipaajournal.com/most-common-security-weaknesses-in-healthcare/

[16] HP Client Security Manager with Intel Authenticate support is available on select HP business PCs with 7th Generation Intel® Core™ vPro™ processors.

[17] DistilNFO HITRUST Advisory, "Largest Health Breach Results in Largest HIPAA Settlement", October 22, 2018. distilnfo.com/hitrust/2018/10/22/largest-health-breach-results-in-largest-hipaa-settlement/.

[18] Quocirca Business and IT Analysis, Louella Fernandes, "Global Print Security Landscape, 2019", February 2019. For more information, see hp.com/go/analystscorner.

[19] Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment", 2015, and the "Global Visual Hacking Experiment", 2016, both sponsored by 3M.

[20] The HP Universal Print Driver is available for download at no additional charge at hp.com/go/upd.

[21] HP Access Control must be purchased separately. To learn more, please visit hp.com/go/hpac.

[22] Subscription or accessory may be required. For more information, visit hp.com/go/roam. To enable HP Roam, some devices may require firmware to be upgraded and an optional accessory to add Bluetooth® Low Energy (BLE) beaconing capabilities. Customer can purchase the HP Jetdirect 3100w BLE/NFC/Wireless accessory or the RadBeacon USB.

[23] 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, when Microsoft Office or Adobe Acrobat are installed.

[24] HP Sure View Gen3 integrated privacy screen is an optional feature that must be configured at purchase and is designed to function in landscape orientation. HP Sure View is optional on HP EliteBook 840 G6 Healthcare Edition Notebook and EliteOne 800 G5 Healthcare Edition AiO.

[25] HP Secure Erase is for the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method. HP Secure Erase does not support platforms with Intel® Optane™.

[26] Nemours, "Nemours Recognized for its Electronic Health Record", October 2017. nemours.org/about/mediaroom/press/dv/nemours-recognized-for-its-electronic-health-record.html.

[27] HP JetAdvantage Secure Print: Pull printing works with any network-connected printer or MFP. On-device authentication is available for many HP LaserJet, PageWide, and OfficeJet Pro devices and selected non-HP devices. Some devices may require a firmware upgrade. Internet connection required for cloud storage and retrieval of print jobs. Print-job release from a mobile device requires a network connection and QR code. For more information and a list of supported printers and MFPs, see hp.com/go/JetAdvantageSecurePrint.

[28] HP Proximity Card Reader (CZ208a) is available for separate purchase for select HP devices with Hardware Integration Pocket (HIP) and touchscreen display.

[29] As of December 5, 2016. See partnercenter.microsoft.com/en-us/pcv/solution-providers/hp-inc_4299709950/1221645_1?k=hp. HP Manageability Integration Kit is not preinstalled, available at hp.com/go/clientmanagement.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-0931ENW, November 2020. Rev. 3