Business white paper

HP Client Security delivers multi-level protection

Keep point-of-sale data safe on all sides

Table of contents

Customer details hold value – and risk

70% of all breaches occurring in retail were POS breaches.

73% of all breaches occurring in entertainment were POS breaches.

91% of all breaches occurring in accommodation were POS breaches.

The technologies at work in today's retail point-of-sale (POS) environment capture more – and more valuable – customer data than ever before, allowing retailers to provide seamless and highly personalised shopping experiences.

From interactive surveys and activities offered at in-store kiosks to opt-in loyalty programmes at the checkout register, intelligent POS computing systems create compelling benefits for retailers and customers alike. Instant access to payment and shipping information enables faster, more accurate service. Details about a shopper's age, interests, purchase history, and other characteristics help the business personalise its marketing to build a stronger emotional connection with each customer.

However, storing and managing all of this confidential, personally identifiable information also brings greater potential risk. An accidental leak or malicious attack can quickly erode the trust and loyalty you've worked so hard to build.

No business, large or small, can afford to underestimate its risk of being attacked. In 2015, retailers around the world experienced at least 370 data breaches – 70% of which targeted POS systems.[1] Analysts predict that by 2020, more than **1.5 billion** people globally will be affected by data breaches.[2]

The hackers behind these intrusions are using ever-more sophisticated methods and increasingly powerful technologies to steal personally identifiable information, including financial data. You need POS client security that can protect data across all your computing layers and enable you to recover quickly, with minimal damage, in the event of a breach.

[1] *2016 Data Breach Investigations Report*, Verizon.

[2] Christian A. Christiansen et al., *IDC FutureScape: Worldwide IT Security Products and Services 2016 Predictions*, International Data Corporation, November 2015.

Multi-layered security from HP

HP has the comprehensive, in-depth PC security framework – backed by our industry-leading support services and efficient management tools – to help your retail business stay secure.

Our client security strategy includes creating multiple layers of protection across devices, data, and identity. Along with delivering HP security tools through software, we provide additional features in hardware and embed strong protections all the way down to the BIOS level. IT managers can centrally configure, deploy, and update these tools without interrupting employee productivity.

Figure 1. HP Client Security delivers end-to-end protection at all levels of the business IT environment.

Protect devices and data at the core

BIOS attacks are among the hardest to detect, and by the time they are found, your devices and data may already be compromised. However, constantly monitoring and troubleshooting to keep devices secure diverts time and money into routine tasks instead of productivity to move businesses forward.

HP BIOSphere provides enhanced, end-to-end protection against malicious attacks and accidental errors that can compromise the BIOS. It provides a self-healing architecture designed to prevent, detect, and repair attacks. Simple to set up and customise, HP BIOSphere helps your business streamline management tasks and safeguard device firmware so that you can stay productive while still protecting sensitive information. The solution can be integrated with existing security protections, configured remotely, and easily managed via automated updates.

HP Sure Start – a BIOS-level, self-healing technology solution – works alongside HP BIOSphere to provide an added level of security. It helps ensure all systems and data are secure before starting the boot-up process. HP Sure Start stores a clean version of the BIOS in memory that third-party software or firmware can't access. The hardware-based solution also protects a device's unique data, such as its serial number and factory settings. And with HP Sure Start's audit-log capabilities, you can find details about the attempted BIOS attack.

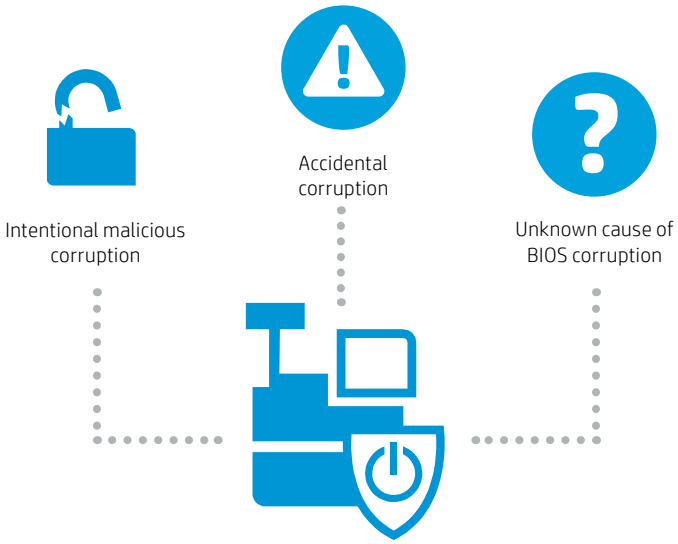

Figure 2. HP Sure Start recovers the BIOS for uninterrupted productivity – anytime, anywhere.

Keep trusted users productive – and keep intruders out

False user authentication can happen from multiple points in retail POS systems, exposing your systems and data to misuse. Unencrypted data is also vulnerable as it sits on device hard drives or travels between systems. HP Client Security creates a strong barrier against these types of intrusions.

HP Trusted Platform Module (TPM) security chip is an industry-standard chip that securely stores user identification information – passwords, certificates, or encryption keys – to authenticate devices and ensure they haven't been breached. It automatically seals off sensitive data on the device's hard drive if platform configuration is changed because of unauthorised access.

Windows 10 Credential Guard[3] enables multi-factor authentication to prevent unauthorised access or data removal on POS systems by keeping sensitive information only on privileged software. For example, virtualisation-based security holds credentials in a protected environment separated from the OS, keeping them safe from advanced threats.

HP self-encrypting drive (SED) technology encrypts and decrypts data faster and more securely than software-based solutions. When needed, the SED can erase data in seconds, as opposed to traditional wiping methods that can take hours.

Intel® Data Protection Technology for Transactions (DPTT) helps safeguard customers' information from the moment it's captured by edge peripherals before entering the CPU or the OS – all the way through to storing the data. Once a transaction is initiated, DPTT creates a path that directly routes encrypted data from the payment terminal to bank servers – keeping sensitive information out of the POS platform, OS, and memory.

Windows 10 Device Guard[4] lets IT managers create rules to run only signed, trusted, and approved applications on the POS system to help protect against walk-up and low-level attacks through USB ports.

[3] Windows 10 Enterprise and Credential Guard are available for installation only through HP Custom Integration Services to enterprise customers with a volume licence to use Windows 10 Enterprise. Credential Guard is not available with Windows 10 Pro.

[4] Windows 10 Enterprise and Device Guard are available for installation only through HP Custom Integration Services to enterprise customers with a volume licence to use Windows 10 Enterprise. Device Guard is not available with Windows 10 Pro.

Secure and manage all devices with ease

Performing routine security tasks and audits can be a costly distraction for in-demand IT personnel and strain your limited budget. Our client security solutions help automate and streamline day-to-day management so that the IT team can focus on supporting employees and creating better experiences for your customers.

HP Client Security Manager provides enhanced Windows® login and website single-sign-on capabilities. Administrators can use these tools to manage unique security features for POS systems as well as monitor and diagnose problems within the hardware. HP Client Security Manager also lets you assess password strength and use fingerprint credentials to protect devices throughout your system.

Remote deployment tools from HP help you save time and money managing and deploying security settings to your POS systems. IT administrators can capture the current settings on a central device and replicate them across all other systems within the business. As a result, IT administrators can monitor devices, upgrade firmware, and even get advanced reporting and more – all remotely.

HP input/output port control helps you easily configure and manage device ports. BIOS-controlled port lock/unlock capabilities help protect against attacks through portable media storage units.

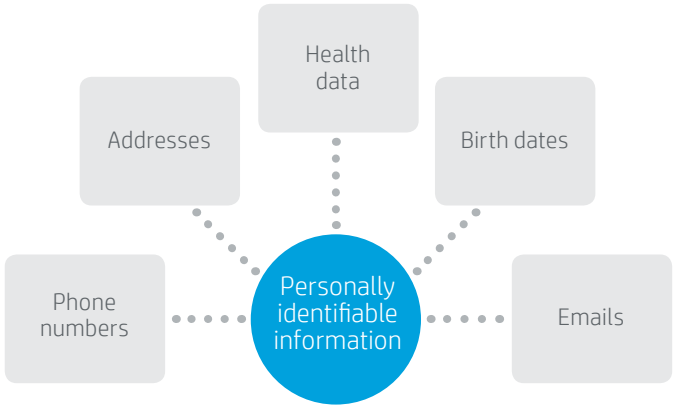

Figure 3. Attackers target more than just credit card data. Personally identifiable information has a lifespan of months, days, years, or even decades.

Retire devices and data on a secure note

As part of gathering the information you need to build strong customer relationships and better business results, it's essential to securely dispose of that data once it's no longer needed. HP offers two tools that help you easily and securely destroy old data to keep your devices, your reputation, and customers' identities safe.

HP Secure Erase completely rewrites all data on the Intel® Solid-State Drive (SSD) or standard hard drive, with no possibility of recovery. Simply select "Secure Erase" from the Security menu and confirm the drive you want to erase.[5]

[5] For the use cases outlined in the Department of Defense 5220.22-M Supplement. Does not support SSDs. Requires Windows on business desktops. Not available on business desktop BIOS. Network connection to the management server is required. With Windows 8.1, user must turn off Enhanced Protection Mode in IE11 for shred on browser close feature.

Gain peace of mind with help from a trusted leader

Earning and maintaining customer loyalty are essential for helping your retail business thrive. The better you know your customers, the more opportunities and personalised experiences you can offer.

Maintain that trust – while staying ahead of hackers, thieves, and unauthorised users – with industry-leading security that is built in, not bolted on. HP Client Security features help you repel an ever-changing world of threats with protection to cover multiple entry points, from the BIOS and hardware through POS software applications. Our experienced consultants can help identify your specific security needs and recommend customised solutions to fit your environment.

Contact your HP representative to get started, or learn more at www8.hp.com/us/en/solutions/business-solutions/computing.html#computer-security.

Table 1. Suite of HP security features

Feature	Description	Device	Data	Identity
HP BIOSphere with Sure Start	BIOS-level, self-healing technology solution created to protect against malware and security attacks aimed at the BIOS	X	X	X
HP Trusted Platform Module (TPM)	Cryptographic processor that validates integrity of the platform and provides secure credential storage to aid in peripheral component interconnect compliance	X	X	X
Windows 10 Credential Guard[3]	Utilises TPM to enable multi-factor authentication, increasing protection against credential theft	X	X	
HP self-encrypting drive (SED)	Hardware-based solution that encrypts and decrypts data as it is written or read from the hard drive; secures data while minimising overhead		X	X
Intel® Data Protection Technology for Transactions (DPTT)	Safeguards payment and nonpayment transaction data from point of entry (model-specific register swipe or barcode scan); examples include loyalty cards, employee badge-ins, and driver's licences		X	X
Windows 10 Device Guard[4]	Windows 10 IOT Enterprise Virtualization-Based Security feature that enables a lockdown of the POS client to only run signed, trusted, and approved applications	X	X	X
HP Client Security Manager	Framework for managing and configuring security features available on their retail POS and business PC platforms		X	X
Remote deployment tools from HP	Capture current image and replicate across management suite to all other systems	X	X	
HP input/output port control	BIOS-controlled port lock/unlock to prevent attacks from USB-bootable media and strengthen integrity of IT	X	X	X
HP Secure Erase[5]	Permanently destroys data on hard drive in preparation for system disposal/redeployment; all data on SSD or standard hard drive will be completely rewritten and cannot be recovered even with advanced data-recovery tools		X	X

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA6-9041ENN, January 2017

This is an HP Indigo digital print.