PC Platform Security and Isolation Technology

For Retailers

HIGHLIGHTS

- IT Operations teams maximize IT efficiency and user productivity with platform-based security
- Security teams improve risk management outcomes with full stack security
- At the application layer, isolation technology minimizes threats from ransomware and phishing, freeing up security teams to address other security needs.

Overview

Retailers are facing greater security challenges protecting their customers' data from threat actors. Attacks may come in through back office PCs, online retailer PCs, or even at the Point of Sale (POS) systems leaving retailers with high costs resulting from identity theft, remediation of IT systems, business disruption, and loss of company reputation.

The biggest risks are associated with endpoints: PCs and POS systems. These endpoints are where people, data, and the Internet converge, creating a large attack surface that IT Security teams need to protect. When thinking about security at the endpoint, retailers need to consider security at the different layers of the PC or POS system. Retailers need to take a "full-stack" layered approach to securing endpoints.

HP's FULL-STACK APPROACH

- Applications
- Operating System
- BIOS
- Resilient Hardware
- Factory Services

Each layer needs security controls implemented commensurate with the risk. That risk is heightened because a compromise at one level almost always results in compromises in the layers above.

The IT / Security Win-Win

The lower levels of the retail endpoint stack are of great interest to both the IT and Security teams. The IT Operations team looks to maximize IT efficiency, availability and user productivity while Security teams manage risk.

HP builds a variety of capabilities into our retail endpoints that deliver business outcomes for both IT Operations and Security. With respect to IT Operations, the table below highlights the key outcomes (or use cases) supported by HP Platform Security.

OUTCOME	DESCRIPTION	CAPABILITIES
MODERN IT MANAGEMENT	Cloud-based PC or POS system management, often based on Microsoft Intune	Secure OS image management; Autopilot factory enrolment; remote BIOS configuration management
ENDPOINT LIFECYCLE MANAGEMENT	Efficient PC or POS system support from procurement to retirement	Initial installation and upgrades of custom OS images & firmware; BIOS resiliency; and device location services for PCs and POS systems that leave the office
INCIDENT & DISASTER RECOVERY	Re-establish employee productivity in case of PC or POS system corruption failure or disaster scenario	Recover clean OS image at scale on remote PCs and POS systems
INCREASED STAFF PRODUCTIVITY	Minimize PC or POS system downtime or upgrade service interruptions to maximize productivity	Rapid OS re-imaging; Seamless BIOS updates

Turning to Security, HP goes well beyond the obvious “fight hackers” requirement, and supports a number of outcomes that are of particular concern to retailers:

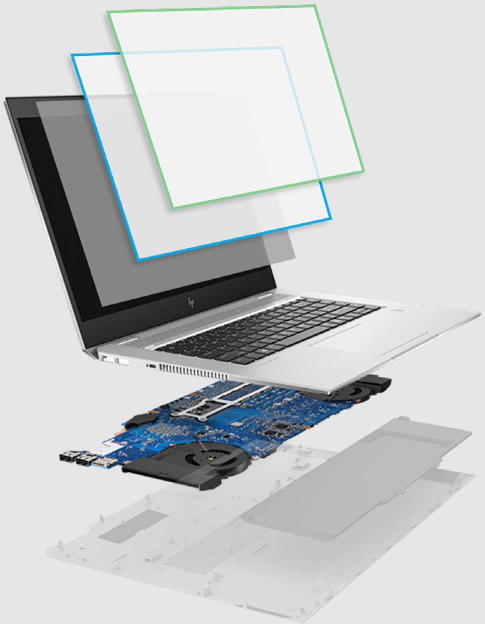
THREAT	RISK	CAPABILITIES
SUPPLY CHAIN RISK	Device compromise prior to onboarding, renders OS level security ineffective for PCs or POS systems	BIOS integrity; BIOS configuration integrity; Physical integrity
DEVICE LOSS OR THEFT	Loss of sensitive data for PCs	Remotely locate, lock or wipe PC
PC PLATFORM INTEGRITY	Malware compromises firmware causing persistent malware presence on PCs and POS systems	BIOS integrity; BIOS configuration integrity
PHYSICAL COMPROMISE	Unattended PC and POS system compromised via physical action	Secure BIOS; USB Controls
COMPLIANCE CONTROLS	Inadequate controls on in-scope infrastructure leads to audit findings	Software and configuration controls on underlying platform helps meet PCI compliance

Securing the Application Layer

Another aspect of endpoint security that retailers need to examine is the ability to protect PCs and POS systems from phishing and ransomware attacks at the application layer. This is seen most often in the back office of retail organizations. Corporate offices have employees receiving emails, browsing the web or using a USB device at a PC. The common aspect of these attacks is that they use social engineering to trick staff into assisting the attacker in their efforts to penetrate security defenses.

An effective solution to defeat this class of attacks is isolation technology. This threat containment method stops attacks at the endpoint by isolating each user task in a lightweight, micro-virtual machine (µVM). The isolation is enforced by the PC’s CPU, so that malware cannot escape. Each task from browsing the web to opening emails and downloading attachments is securely opened within its own µVM, completely containing the task. When the task is completed and closed, the µVM is destroyed eliminating any malware, allowing employees to click with confidence.

PC Platform Security



Sure Admin[1]

A modern BIOS management tool, eliminates the need for a password by creating a digital signature that allows IT administrators to securely manage PC and POS systems' BIOS settings over a network

Sure Start[2]

Protects PC and POS systems' BIOS firmware from malware or corruption by ensuring only trusted code is executed. If firmware deviation is detected, HP Sure Start quarantines the BIOS and replaces it with a gold copy of the BIOS stored in the HP Endpoint Security Controller.

Sure Run[3]

Monitors and keeps critical retail processes running when users or even advanced malware tries to shut them down. Software network isolation prevents malware from spreading and guards against changes to device settings.

Sure Recover[4]

Reduces downtime and lost productivity by leveraging the power of the HP Endpoint Security Controller to quickly restore the operating system when the hard drive has been compromised or corrupted.

Protect & Trace[5]

Protects lost or stolen PCs by locating the device, locking the device to prevent unauthorized access, and erasing data on lost devices to prevent malicious use.

Application Layer Security

Sure Access Enterprise[6]

Protects privileged user activity by isolating such activity from potential threats.

Sure Click Enterprise[7]

Prevents malicious websites and attachments from attacking the PC by isolating malware within a virtual container.

Wolf Pro Security[8]

A simple full-suite endpoint security solution that includes hardware-enforced isolation technology, anti-phishing credential protection, and next-generation antivirus.

Summary

Retailers have long known that strong security is fundamental to business success. However, the continuous threat of cyberattacks on these organizations suggest that new approaches are needed. HP Wolf Security uses two innovative strategies to protect retailers. Full-stack security builds protection from the hardware up, while Isolation defeats social engineering attacks. Both approaches are designed to reduce Security Operations overhead by decreasing ticket volumes. Working together, these approaches help meet retailer's risk management goals while also minimizing operational overhead.

[1] HP Sure Admin requires HP Manageability Integration Kit and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

[2] HP Sure Start is available on select HP products.

[3] HP Sure Run is available on select Windows 10 Pro, Windows for IoT, and higher HP products.

[4] HP Sure Recover is available on select HP products and requires an open network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

[5] HP Services are sold separately. 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.

[6] HP Sure Access Enterprise is sold separately and requires Windows 10 Pro or Enterprise. 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. For full system requirements, please visit www.hpdaas.com/requirements.

[7] HP Sure Click Enterprise is sold separately and requires Windows 8 or 10 Pro and higher and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.

[8] HP Wolf Pro Security is available preloaded on select HP devices, is available as a subscription and in term licenses. See HP Wolf Security.

4AA8-1581ENW, May 2022