SOLUTION BRIEF

DELIVERING SUPERB IT AND SECURITY OUTCOMES

PC Platform Security from HP

HP WOLF SECURITY

INTRODUCTION

The PC is where people, data, and the cloud converge. With the rise of remote working and hybrid computing, the endpoint is the crucial component that must be available and secure. HP has been at the forefront of PC platform integrity for nearly two decades, and is focused on two goals:

- Maximizing IT efficiency
- Maintaining a resilient computing platform

HP offers a broad set of security capabilities that are included on most of its business-class PCs that provide Platform Security[1]. The capabilities are built using unique hardware and software unavailable from other vendors. This solution brief outlines how these capabilities support the goals of efficiency and resiliency.

"The devices which make up the platform are crucial to integrity and availability of the systems built upon the platform... Attacks which aim to damage or remove platform firmware have the potential to render systems permanently damaged, incurring substantial costs to the affected parties."

NIST: Special Publication 800-193

THE ROLE OF PC PLATFORM SECURITY IN MAXIMIZING IT EFFICIENCY

Remote and hybrid working are forcing changes in IT support strategies. There is less reliance on IT staff physically accessing endpoint computers, and more focus on remote management, without active VPN connections. This shift is happening in parallel with the ongoing drive to maximize IT efficiency and shift budget to applications and data, and away from infrastructure.

HP PC security capabilities are designed to support these initiatives, with IT efficiency and high user productivity as the key business outcomes. The following table lists the IT outcomes supported by Platform Security, and the corresponding capabilities for each.

OUTCOME	DESCRIPTION	SUPPORTING CAPABILITIES
ENDPOINT MODERN MANAGEMENT[2]	Cloud-based endpoint management, often based on Microsoft Intune	Secure OS image management; Autopilot factory enrolment; remote BIOS configuration management
LIFECYCLE MANAGEMENT[2]	Efficient PC support from procurement to retirement	Initial installation and upgrades of custom OS images & firmware; BIOS resiliency; Device location & data wipe
INCIDENT & DISASTER RECOVERY	Re-establish employee productivity in case of endpoint corruption failure or disaster scenario	Recover clean OS image at scale on remote PCs
STAFF PRODUCTIVITY	Minimize downtime or upgrade service interruptions to maximize productivity	Rapid OS re-imaging; Seamless BIOS updates

FULL-STACK PC PLATFORM SECURITY REDUCES RISK

HP has long recognized the need to build security into its hardware and firmware, as it's impossible to secure applications and data on an insecure platform. Most organizations focus on OS and application level security, without adequate consideration of the underlying platform. Threat actors are aware of this fact and have developed exploits to take advantage of platform vulnerabilities. And there continues to be risk associated with everyday events such as device procurement or a PC going missing or being stolen.

HP's PC Platform Security creates a robust compute platform that helps reduce risk. The table below describes the relevant risk areas and corresponding solution capabilities.

IMPROVING USER EXPERIENCE THROUGH THREAT CONTAINMENT

To better secure the PC application environment, HP offers HP Wolf Enterprise Security[3] to complement PC Platform Security. Using hardware-enforced micro-virtualization, SCE isolates and contains malware or ransomware that may be trying to get in via common user actions like clicking on a link or opening an attachment. SCE is transparent to the user, lowers ticket volume to the SOC, provides threat intelligence to the Security team, and has protected over 10 billion user actions without a reported compromise.[4]

THREAT	RISK	SUPPORTING CAPABILITIES
SUPPLY CHAIN RISK	Device compromise prior to onboarding renders OS level security ineffective	BIOS integrity; BIOS configuration integrity Physical integrity
DEVICE LOSS OR THEFT[2]	Loss of sensitive data	Remotely locate, lock or wipe PC
PC PLATFORM INTEGRITY	Malware compromises firmware causing persistent malware presence	BIOS integrity; BIOS configuration integrity;
PHYSICAL COMPROMISE[5]	Unattended PC compromised via physical action	Tamper protection; Secure BIOS; USB Controls
COMPLIANCE CONTROLS	Inadequate controls on in-scope infrastructure leads to findings	Software and configuration controls on underlying platform

DELIVERING SUPERB IT AND SECURITY OUTCOMES WITH FULL-STACK PC SECURITY

Contrary to expectations, the rise of cloud computing has not resulted in a decrease in importance of the endpoint PC. Instead, the move towards more flexible working makes the PC the critical IT platform for end user enablement and productivity. By adopting more efficient system management and full-stack risk controls, enterprises can achieve their business outcomes while meeting their risk management and IT efficiency objectives.

DISCLAIMERS

[1] Platform Security requires Windows 10 or higher, includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.
[2] Requires separately purchased service and/or third party management software.
[3] HP Wolf Enterprise is sold separately and requires Windows 8 or 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.
[4] Assumptions based on HP internal analysis of customer reported insights and installed base.
[5] HP Tamper Lock requires a supervisor password be established prior to use.

Learn more at hp.com/wolfsecurityforbusiness.

HP WOLF SECURITY

4AA8-1050ENW , January 2022