White Paper

Holistic Endpoint Security Requires Built-In, Hardware-Based Defenses

Sponsored by: HP

Michael Suby
March 2021

IDC OPINION

The business criticality and cyber-risk of endpoint devices could not be greater. With the COVID-19 pandemic, many employees rapidly shifted from a protected business work location to work from home (WFH). Post-pandemic, evidence points to WFH being more prominent than pre-pandemic. According to IDC's *COVID-19 Impact on IT Spending Survey,* respondents said that 6% of their employees worked from home prior to the pandemic. During the pandemic, that number jumped to 53% of employees; and, in 2021, respondents expect that 30% of employees will work from home. Yet, operating outside the guarded network of the enterprise, threat actors have escalated their attacks on end users and their devices; these actors knew from experience that compromising endpoint devices and manipulating human behaviors is their golden pathway to steal sensitive information, ransom business continuity, and divert funds (see Figure 1). IDC's research shows that the importance of endpoint security, already high, increased with the sudden WFH migration.

For many organizations, their current approach to endpoint security is insufficient. Despite advancements and inclusion of machine learning and artificial intelligence (ML/AI) into endpoint protection platforms and the layered addition of endpoint detection and response, organizations are not fully removed from operating in a reactive mode. In addition, organizations are also reliant on endpoint security software products to thwart the next new or unknown threat. This reliance, however, has a structural limitation as endpoint security software products lack visibility into firmware integrity. Inferences on the actual state of firmware integrity may be possible but are subject to error.

A better alternative is to approach endpoint security holistically, starting with devices equipped with hardware-based root-of-trust (RoT) technologies that deliver security below and in the operating system (OS). This will address the inherent blind spots of bolted-on endpoint security software, and device self-healing will also be possible if deviations from a known good state occur. In addition to producing an immediate reduction in risk, self-healing also reduces IT desktop operations (IT-involved reimaging) and minimizes disruptions to end users' productivity. Hardware-based security can also lessen SOC analysts' alert fatigue, number of incident investigations, and post-incident remediations by inoculating through isolation the prominent endpoint attack vectors of web browsing and file downloads and email attachments. Finally, hardware-based root-of-trust devices fold nicely into organizations' zero-trust architectures.

PC buyers should, however, tread cautiously as manufacturers differ on the breadth, depth, experience, and certification of their hardware-based security capabilities. A little homework will pay

dividends. To assist in this homework, IDC describes the HP Wolf Security for Business feature set, which is engineered into HP Business PCs. This white paper also provides a baseline for comparing PCs from other vendors. In addition, the white paper explores the context around security professionals' expectations of endpoint security solutions as well as the threat landscape that crystalizes the justification for folding PCs equipped with hardware-based security into your PC inventory.

ENDPOINT SECURITY'S SITUATIONAL OVERVIEW

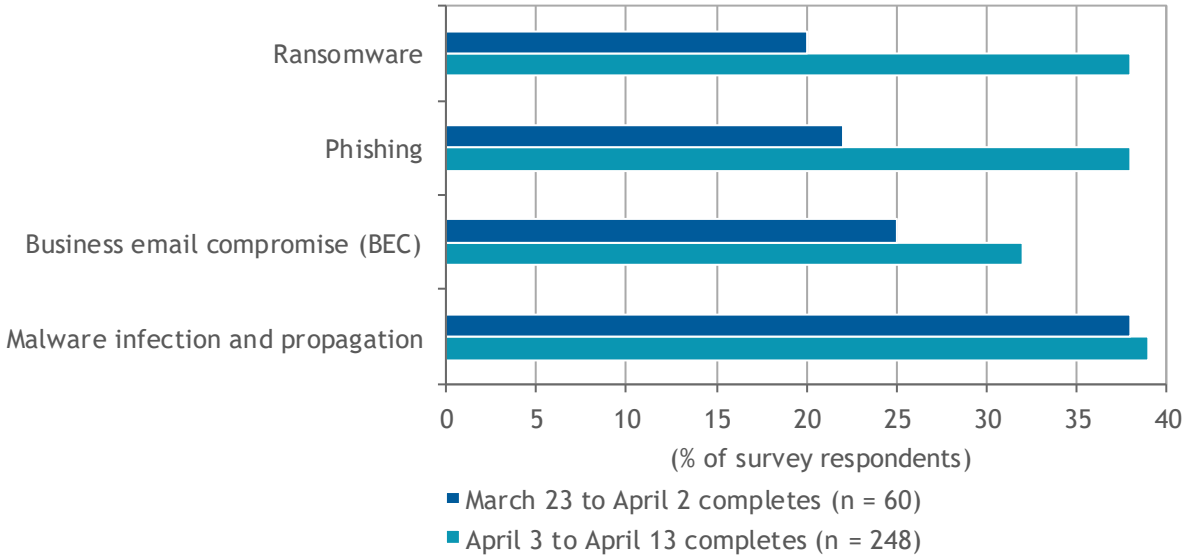
Security professionals have high expectations for endpoint security solutions and those expectations are increasing. This is logically expected. As highlighted in our survey findings, endpoint threats rank high among security professionals' concerns, security breaches are common with many due to endpoint compromises, high-risk URLs are on the rise, and the perceived risk of new and unknown threats aimed at endpoints is trending upward. Further increasing security professionals' expectations is the dramatic rise in employees working from their homes and expectations that work-from-home arrangements will not return to pre-pandemic levels in the foreseeable future. Considering these circumstances, organizations should question if aftermarket, bolted-on endpoint security software is sufficient or if they would be better served with overlaid security software paired with hardware-based device security.

Figure 1 shows the relevance of endpoint security in risk management.

FIGURE 1

For Security Decision Makers, Relevance of Endpoint Security in Risk Management Across Multiple Threats Is High, and the Pandemic Drove Relevance Even Higher

Q. Please rate the relevance of endpoint security products in mitigating the following risks.



n = 308

Survey respondents rated their relevance on a scale of 1 to 5, with 1 meaning not relevant to 5 meaning very relevant.

Data shows percentage of respondents selecting 5 = very relevant.

Source: IDC's *SMB Security Survey,* 2020

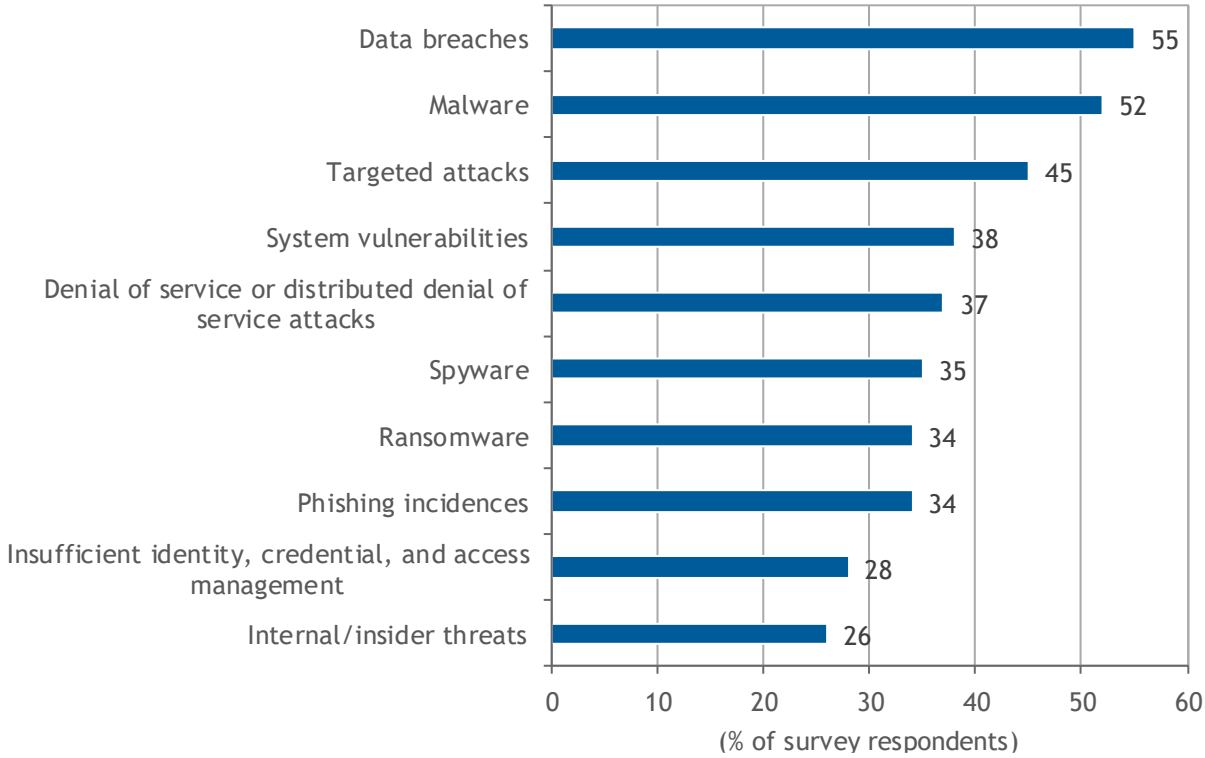
According to IDC's *2020 SMB Security Survey*, the relevance of auto-remediation as an endpoint security product feature rose materially. This rise corresponds to organizations migrating to work-from-home arrangements following the declaration of a national emergency caused by the COVID-19 pandemic. As employees rapidly shifted from working from corporate locations to their homes, their exposure to cyberattacks increased but IT support to remotely repair compromised endpoint devices could not scale at a similar pace. Consequently, the relevance of auto-remediation increased. In this survey, 55.0% of survey completions from March 23 to April 2 rated auto-remediation as a 4 or 5 (1 = not relevant to 5 = very relevant). This percentage rose to 68.1% for survey completions from April 3 to April 13.

A similar concern of endpoints' cyberexposure is reflected in IDC's *U.S. Managed Security Services/Managed Detection and Response Survey* conducted in May 2020. In a majority of the top security concerns (e.g., data breaches, malware, phishing, spyware, and ransomware), cyberthreats are directed at or conducted through endpoints (see Figure 2).

FIGURE 2

Security Professionals' Top Concerns Are Highly Concentrated on Threats Aimed at or Through Endpoints (Endpoint as the Initial Point of Compromise)

Q. *Which of the following five factors are your company's greatest concerns when it comes to securing your business operations and IT environments?*



n = 410

Source: IDC's *U.S. Managed Security Services/Managed Detection and Response Survey,* May 2020

Moreover, threats, if not thwarted, contribute to security breaches, which unfortunately are a common occurrence. According to IDC's *U.S. Managed Security Services/Managed Detection and Response Survey,* 90% of survey respondents stated their organizations sustained at least one security breach in the past 12-24 months. For 66% of the surveyed organizations, they sustained seven or more security breaches during the past 24-month period.

IT Security Professionals Are Increasingly Concerned About New and Unknown Threats

In three consecutive annual surveys conducted by Ponemon Institute and summarized in *The Third Annual Study on the State of Endpoint Security Risk,* the percentage of survey respondents choosing "strongly agree or agree" with the following statement — "new and unknown threats against our organization have significantly increased" – steadily increased from 69% in 2017 to 70% in 2018 and then 73% in 2019.

The Risk of End Users Encountering High-Risk URLs in Their Browsing Activities Continues to Increase

According to Webroot, an OpenText company, phishing URLs represented 45% of all high-risk URLs in 2019 and the number of phishing URLs increased by 640% over 2018 (source: *Webroot Threat Report, 2020*).

In 2020, the COVID-19 pandemic has further accelerated this trend as threat actors adjusted their themes to boost effectiveness. Illustrative of this, Google on April 21, 2020, posted the following, "During the last week, we saw 18 million daily malware and phishing emails related to COVID-19. This is in addition to more than 240 million COVID-19-related daily spam messages."

FIRMWARE'S ATTRACTIVENESS TO ATTACKERS AND BOLTED-ON SECURITY SOFTWARE LIMITATIONS

By the very nature of their nefarious objectives, cyberattackers target systems and layers within systems that are exploitable and provide attackers with leverage in terms of persistence and privilege. PC firmware has both of these attractive attributes:

- **Exploitable:** Functioning below the OS and established before endpoint security software loads, endpoint security software can only make inferences on whether firmware has been compromised. Lacking a direct line-of-sight mechanism to detect firmware compromises as the PC is powered on or certify the firmware's integrity once loaded, the PC is exploitable.
- **Leverage:** Residing in nonvolatile memory, corrupted firmware is not erasable from the PC's hard drive and, therefore, is persistent. The corrupted firmware will exist each time the PC powers up. And as a foundational system layer, corrupted firmware affords attackers the highest privilege level to orchestrate attack plans, including modifying security settings and applications to the attacker's benefit.

HP WOLF SECURITY FOR BUSINESS FEATURE SET

With over 15 years of hardware-based security innovation, which began with an industry-first certified Trusted Platform Module (TPM) in 2004, HP Inc. has systematically added and advanced features to deliver multilayered (below and in the OS) security that is enforced in hardware. These features, HP Wolf Security for Business, are included in HP Business PCs.

HP Wolf Security for Business includes:

- HP Sure Start
- HP Sure Run
- HP Sure Recover
- HP Sure Admin
- HP Tamper Lock
- HP Sure Click

Below the OS

HP Sure Start

HP Sure Start protects the firmware, including HP BIOS, from corruption, confirms authenticity when the PC powers up and during operation (i.e., health monitoring), and restores the firmware and settings if altered. The foundation to HP Sure Start is HP Endpoint Security Controller (ESC), a built-in hardware-based root of trust. To confirm the authenticity and integrity of platform firmware and HP BIOS before each executes as well as during operation, HP ESC maintains an isolated, cryptographically protected copy of the firmware and settings, which is critical in self-healing.

Beneficial to end users and IT, HP Sure Start self-healing is automatic and transparent. Self-healing is also comprehensive as all flash components and firmware settings essential to booting the PC and establishing PC security processes are restored and certified.

HP Sure Start is now in its sixth generation. Feature enhancements included in this generation are reduced time in flash updates and recovery and expanded attack protections — notably, protection against attacks targeting HP ESC and pre-boot direct memory attacks (DMAs).

Certifying its functionality, HP Sure Start has undergone testing by an independent accredited test lab (ANSSI) and was built to align with the NIST Framework and Resiliency Standard 800-193.

HP Sure Run

HP Sure Run, an OS software agent, continuously monitors and alerts on the operating status of critical security processes, services, and applications. The HP Sure Run agent includes kill prevention capabilities, and if the agent is interrupted, it is automatically reinstalled. In addition, authorized applications (e.g., antivirus), including custom applications, are automatically restarted if stopped by an attack. As with HP Sure Start, HP Sure Run is integrated with HP ESC to deliver hardware-based enforcement.

HP Sure Recover

Incorporated into the system's hardware and firmware, HP Sure Recover returns corrupted OS, drivers, and applications to their last approved images. Ranging from low to no IT involvement, three recovery methods are available with HP Sure Recover: automatic, scheduled, or user directed.

Limiting end-user disruption, OS and driver recovery time can be accomplished in as little as five minutes with the embedded recovery option. Recovery time for data, if required, will depend on the organization's data backup methods (e.g., from a cloud storage service).

Coupled with HP Sure Start, HP Sure Recover auto-remediates corrupted firmware, OS, drivers, and applications rapidly and easily. User downtime and IT involvement are minimized.

HP Sure Admin

An unadvisable but common practice with administrator passwords is the reuse of a single password to access multiple systems. While a single password for multiple systems is a convenience for end users, a serious security vulnerability is introduced. Whether shared, stolen, or guessed, an external threat actor or malicious insider can reuse a single password to access multiple systems, potentially more than PCs, and change settings and configurations even down to the BIOS level. HP Sure Admin erases this vulnerability by eliminating passwords for administrator access.

HP Sure Admin utilizes certificate-based public-key cryptography to deliver a passwordless access method. Emphasizing ease of use, local and remote management access is supported in HP Sure Admin and local access can be enabled through a smartphone application.

HP Tamper Lock

HP Tamper Lock solution combines the hardware-enforced security of the HP Endpoint Security Controller with sensors to detect if the PC case has been opened. Policies on a detected event include blocking boot until valid BIOS administration credentials are entered, clearing the TPM to delete all user keys such as BitLocker keys and powering off the system when the cover is removed.

In the OS

HP Sure Click

Enforced at the hardware level, HP Sure Click creates an isolated micro-virtual machine (micro-VM) for each browser tab and supported applications (MS Word and PDF). Operating in this fashion, HP Sure Click eliminates all judgement calls on whether a website/URL, web-downloaded file, or email attachment is malicious. Instead, any malicious code is fully contained within the micro-VM during the user session and completely wiped away when the session is terminated (e.g., closed browser tab or Microsoft Word document). In addition, as each micro-VM is self-contained, malicious code cannot seep from one browser session to another or among HP Sure Click–supported applications.

Even when files of unknown trustworthiness are opened in a micro-VM and then saved on the end user's PC, risk is mitigated. The file is marked as untrusted, and when opened again, the file is opened in a fresh micro-VM.

HP Sure Click is a standard feature of HP Business PCs and delivers a native end-user experience in performance speed and in browser and application features. No end-user training is required, and end users' routines are undisturbed.

Advanced HP Sure Click Security Options

As business needs vary, HP Sure Click offers additional capabilities in HP Wolf Pro Security Edition and HP Wolf Enterprise Security Suite. Designed for small and midsize businesses that want more protection without additional administrative overhead, HP Wolf Pro Security Edition extends isolated containers into additional use cases (e.g., editing of Microsoft Word, Excel, and PowerPoint documents) and defends against credential theft from phishing sites. Alternatively, HP Wolf Enterprise Security Suite is designed for organizations that want in-depth knowledge on malicious files and an ability to track down malicious files that may already exist within the organization, even in legacy PCs not running HP Sure Click.

With HP Wolf Enterprise Security Suite, HP Inc. offers HP Protected Apps. Instead of isolating untrusted applications and browsers inside an isolated container, HP Protected Apps places high-value applications inside protected virtual machines. The host OS and potential malware running on the host are unable to interact with the data, inputs/outputs, or systems inside the protected virtual machine. HP Protected Apps is useful for highly secure access to domain controllers, banking networks, and other high-value assets.

CHALLENGES

The benefits of hardware-based security will only materialize if organizations acquire PCs that are equipped with hardware-based security as, unlike software, these capabilities cannot be added after purchase. Consequently, purchases of hardware-based secure PCs are folded into organizations' PC-purchasing sequences and subject to several factors that may hinder the adoption of hardware-based secure PCs. Those factors include:

- **Threat prioritization:** Attacks on PC firmware are not as prevalent as other cyberthreats, yet the potential exists and there have been actual instances (e.g., LoJax and MosaicRegressor). Some organizations may choose to prioritize defending against other cyberthreats that they are experiencing now and forgo PC refreshes until firmware attacks become more prevalent.
- **Digital transformations that may obviate need:** Organizations that have taken a cloud-first or default position or are heading in this direction may question the need for full-function PCs and concentrate their security controls and defenses around and/or near their cloud-hosted assets and applications, in edge gateways or proxies, and in identity and access management systems instead.
- **Organizational disagreement:** Teams in charge of PC acquisition may not value the threat prevention capabilities of hardware-based secure PCs to the same degree as security teams. The time to nurture interteam concurrence may delay adoption.
- **PC vendor competition:** HP Inc. is not alone. Other PC vendors will also present the merits of their built-in security that can contribute to buyer uncertainty and debate in choosing a vendor, which can also delay adoption.
- **Threat actor innovation:** There is no guarantee that any vendor's built-in device security is 100% effective in defending against all potential threat actors. In addition, threat actors, as they have done in the past, will evolve their techniques to circumvent new forms of defenses. The uncertainty of long-term effectiveness may contribute to organizations choosing to delay PC refreshes until another, more advanced release becomes available.

CONCLUSION

Organizations have been conditioned to protect their PCs from cyberthreats solely with endpoint security software installed and run above the OS. The principle deficiency in this approach is that bolted-on security software is not designed to defend against attacks targeting firmware nor does this software have direct visibility beneath the OS.

Hardware-based security alleviates this blind spot so organizations can have holistic endpoint security below the OS. Plus, as present in HP Wolf Security for Business, a range of built-in security features grounded in root of trust are available to ensure the integrity and authenticity of the entire flash stack, enable rapid and seamless recovery of corrupted OS and BIOS settings, circumvent administrative access attacks with passwordless authorization, prevent the interruption of critical security processes and applications, and prevent malware delivered through the web or in email file attachments from being executed on end-user PCs and propagated to other systems.

IDC's recommendation to organizations, small and large, is to accept the threat of firmware and other attacks aimed below the OS as real and take steps now to mitigate those attacks. As highlighted with HP Wolf Security for Business, the protections afforded with its hardware-based security capabilities are not limited to firmware but also extend through the OS and into the browser and productivity

applications where many attacks occur today. Another relevant consideration for hardware-based security is in support of zero-trust architectures where the trustworthiness of a connecting PC is confirmed by hardware-enforced root of trust. We further recommend that organizations consider HP Inc.'s expanding range of hardware-based security capabilities as they conduct comparative analysis with other PC alternatives.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com
