

The time has come for PC purchasers to elevate platform security as a priority.

PC Firmware Integrity Protection and Recovery Foundational to Cyber-Resiliency and Business Resiliency

September 2023

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

Organizations know that business resiliency is linked to cyber-resiliency.

Highlighting the criticality that businesses place on cyber-resiliency, 60% of organizations currently have a cyber-resilience strategy and an additional 18% are planning to have a strategy in the next 12 months, according to IDC's February 2023 *Worldwide Security Survey*. IDC defines a cyber-resilient organization as being able to minimize the damage during a cyberattack and to rapidly return to being able to perform the minimal viable functions needed to operate.

IDC research also revealed that a cyber-resilience strategy consists of multiple activities (see Figure 1). Organizations' views on the relative importance of these activities vary. The activity identified as important or worthy of improvement by the highest percentage of survey respondents was verifying software, firmware, and information integrity through integrity-checking mechanisms.

AT A GLANCE

WHAT'S IMPORTANT

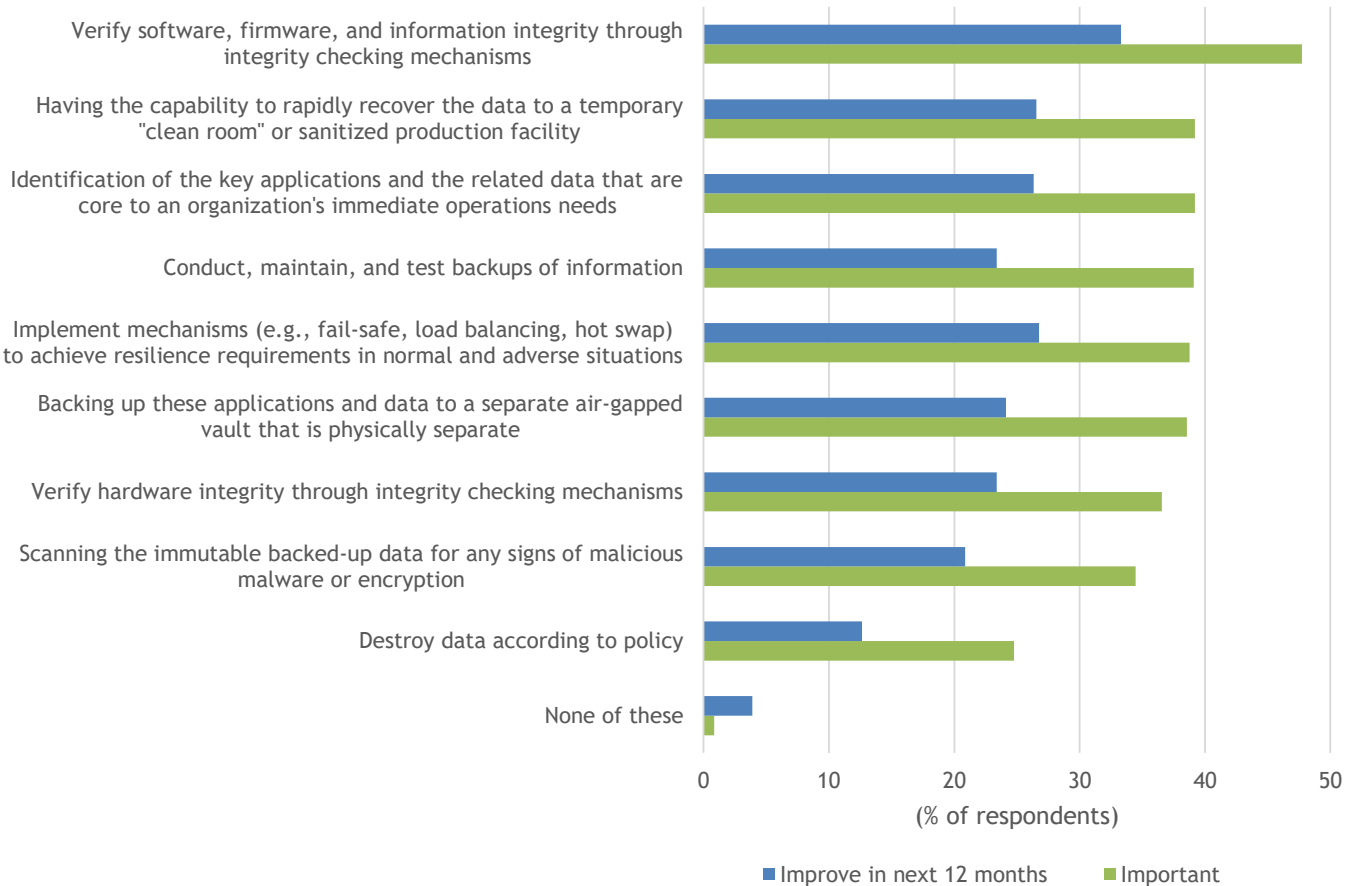
Cyberadversaries are ceaseless innovators, and PCs are lucrative targets that can place the business in a no-win, compromised position. While attacks targeting vulnerabilities in the OS and software applications are most common, attackers will intensify their below-the-OS assaults to gain a sustainable advantage.

KEY TAKEAWAY

To directly combat attacks, organizations must evolve their PC purchasing criteria to include protections that fortify the integrity of the firmware and BIOS configurations and provide secure, remotely executable mechanisms to recover to an authenticated state.

FIGURE 1: **Important Activities in a Cyber-Resilience Strategy**

Q Which of the following are considered as important activities of your cyber-resilience strategy?



Source: IDC's Worldwide Security Services Primary Research 2022–2023 Survey, February 2023

While the mix of IT assets used by organizations also varies, personal computers ([PCs]; i.e., laptops and workstations) are a ubiquitous asset. Furthermore, considering PCs' criticality to business functions and employee productivity, PCs are among the most important IT asset category. With that importance, the ability to monitor and maintain PC integrity is critical to any cyber-resilience strategy.

Pertaining to PC cyberintegrity, firmware integrity takes center stage. PC firmware is the foundational layer from which operating system (OS) and application software run. If PC firmware integrity cannot be assured, the integrity of the OS, applications, and data is at risk. As such, organizations must prioritize PC firmware integrity in their cyber-resilience strategies and operations.

Yet we suspect that when it comes to their PC purchasing decisions, many organizations have not prioritized PC firmware integrity or even firmware vulnerability management on par with other PC attributes, such as unit price, performance, manageability, expected life, and form factors.

Fortunately, reprioritization is possible without sacrificing other sought-after PC attributes. In addition, conducting firmware vulnerability management and checking its integrity are only subsets of firmware-related cyber-resilience activities that should be built directly into PCs. Other features include checking the integrity of BIOS configurations and OS images, having a secure means to change BIOS configurations and update the firmware and, most importantly, possessing firmware self-healing and OS recovery capabilities. Determining with certainty that either the firmware or OS has been compromised, while vital, is an incomplete approach to cyber-resiliency. Each must be returned to its authenticated state with expediency and without overburdening IT staff or impinging on end-user productivity.

This IDC Spotlight lays out the reasons why organizations should factor in firmware cyberintegrity and prioritize it when making PC purchasing and fleet updating decisions.

Why PCs Need Built-In Firmware Integrity Features to Support Cyber-Resiliency

No organization should have lingering doubts as to the criticality of PC firmware integrity. Those that do should pay heed to the considerations examined in the sections that follow.

For Cyberadversaries, End Users and Their Devices Are Attractive Targets, and the Consequences Are Often Severe

IDC research confirms that end users and their devices are heavily targeted by cyberadversaries (source: IDC's *Future Enterprise Resiliency and Spending Survey*, December 2021, August 2022, and March 2023):

- » For the preceding 12 months when each of the three surveys was conducted, 1 out of 7 organizations stated it suffered a ransomware attack, and that attack disrupted business operations for a week or more.
- » For nearly all ransomware attacks, the initial point of compromise entailed end users and their devices.

Hybrid Work Arrangements Add to Cyberadversaries' Attraction to End-User Devices

Operating outside the blanket protections of in-office perimeter defenses, end-user devices are more directly exposed to online and physical attacks. Consider the very real scenarios of traveling employees and employees working in public spaces, such as coffee shops. A lapse in physical possession of a few minutes at a coffee shop or hours in a hotel room provides a determined adversary the opportunity to clandestinely plant firmware-attacking malware or modify firmware configurations. Lacking the ability to immediately detect and remediate, the employee has become an unwitting partner in a cyberattack.

Regarding work arrangements, if hybrid work arrangements were subsiding, cyber-risk would also be subsiding. But this is not the case, as hybrid remains prevalent. IDC's December 2022 *Endpoint Security Survey* revealed that while shifts between full-time remote and hybrid work arrangements are occurring, 98% of surveyed organizations have a portion of their PC-provided employees in full-time remote and hybrid working arrangements in 2022 and expect the same in 2023. Moreover, with business travel rebounding from the COVID-19 pandemic lows and employees toting their PCs with them during vacation, hybrid exposure further expands.

An additional hybrid consideration is remote access by IT personnel. A necessity of systematic remote working is IT remote access into end-user devices in response to help desk tickets or to conduct routine servicing. With high-level admin privileges and the potential scenario of reused and default passwords or passwords exfiltrated in a data breach, a legitimate IT means to access employees' remote PCs is also a viable vector for bad actors.

PCs Are the End-User Devices That Organizations View as Having the Greatest Cyber-Risk

IDC research experience confirms that the cybersecurity spending of organizations is aligned with their assessment of cyber-risk. Spending flows to where cyber-risk is the greatest. Pertaining to end-user devices, smartphones and tablets are also used for work tasks. However, according to IDC's *Endpoint Security Survey*, 98% of all end-user devices with deployed endpoint security software are PCs. Also highlighting the importance organizations place on protecting their end-user devices from cyberthreats, commercial expenditures on endpoint security software solutions (e.g., next-generation antivirus and endpoint detection and response) have been increasing at an accelerating pace since 2018. For 2022, IDC estimates worldwide commercial spending on endpoint security software solutions to protect end-user devices increased 31% over 2021 and totaled \$10.3 billion (see *Worldwide Corporate Endpoint Security Market Shares, 2022: Pace of Growth Accelerated Through 2022*, IDC #US49349323, June 2023).

Possibly less considered by buyers of endpoint security software is that threat detection visibility above the OS does not translate to the same visibility below the OS. Compromised firmware, maliciously changed firmware configurations, and exploited firmware vulnerabilities have less chance of being detected than events occurring above the OS. Moreover, given the system-level control of firmware, the consequences can also be wider in scope. The remedy is to equip PCs with both firmware integrity and endpoint security software.

PC Firmware Attacks Become More Common

Historically, cyberadversaries are innovators and adaptors, and history will repeat itself. Although attacks targeting the OS and software applications garner greater notoriety today and spending on endpoint security has increased, firmware attacks will become more common. There are two main reasons for this.

First, threat actors will direct their efforts to negate efficacy gains in above-the-OS endpoint security software. Doing that from beneath in the firmware allows threat actors to disable this software and clandestinely modify how it performs. As cyberadversaries have done in the past, they will reverse engineer security software, OS, and firmware to uncover and exploit zero-day vulnerabilities. Given this likelihood and the OS and security software dependency on the firmware and its configurations, the advisable defense is to have firmware integrity and configurations protections built directly into the PC.

Second, compromising firmware strengthens cyberadversaries' advantage in three ways. The first was previously noted: exerting control over the OS and over hosted applications like endpoint security. Second, but no less important, is persistence. If the firmware including the booting sequence is compromised, rebooting the PC does not return the firmware to its pre-compromised state. Fold in the circumstance of hybrid work arrangements, and the direness of the situation becomes more evident as the end user will need to physically relinquish the PC for reimaging. Third, detection of firmware compromises is difficult. Endpoint security software is not tuned to detect firmware compromises. There is the possibility that the firmware compromise will not be detected by overlay threat detection software. Even if detectable, time becomes a factor in assembling and interpreting the signals that point to a firmware compromise. This detection delay is a time advantage for adversaries.

Benefits of Platform-Based Firmware Integrity

Organizations need to get ahead of the looming risk of firmware attacks. Waiting for evidence before taking action to mitigate this risk can be perilous. Often with cyberattacks, the threat actors use the first compromised PC to reach and compromise other systems to broaden and fortify their infiltration. By the time the first firmware-compromised PC is

detected, other PCs are likely impacted. The tip of the iceberg is the sign of a larger danger. Correspondingly, the benefit of firmware security is in steering clear of the iceberg.

Firmware integrity benefits will differ across PCs based on the capabilities the OEM has built in. So it is advisable to investigate differences. Among the differences are security for third-party firmware (e.g., running third-party firmware in isolation to contain potential malware spread), a secure mechanism for managing OEM BIOS configurations and updates, and included firmware vulnerability management and patching capabilities.

Last, the benefits of firmware integrity extend beyond the direct security benefits to include protecting PC availability. Although stated previously, it is worth repeating: Business resiliency is tied to an effective cyber-resilience strategy. By protecting the PC from threats targeting the firmware and with a built-in means to automatically recover from compromised firmware, business resiliency is served. Organizations benefit by reducing incidents that lead to end-user downtime and, accordingly, save IT teams' time.

Considering HP Inc.'s Approach to Firmware Integrity: Holistically Protect and Recover

PC-purchasing decisions have long-term implications. Firmware integrity should be a priority as IT teams debate the merits of PC OEMs. Discounting the risk and wide-ranging damage and disruption attacks targeting firmware can cause would be a mistake. At the same time, other PC attributes – performance, price, manageability, and form factor – remain critically important. The challenge is choosing the PC OEM that can deliver on all of these. While this research is not a PC buyer's guide, we can, nevertheless, highlight attributes of HP Inc.'s focus on platform security that can fold into an organization's PC-purchasing decisions. Those attributes are:

- » **Longevity.** Platform security, of which firmware integrity is a core element, is not a start-up endeavor. HP Inc. has been evolving and expanding its capabilities in secure platforms (PCs being just one) for over two decades. Moreover, with cyberadversaries continuously seeking new avenues to exploit and new approaches to evade threat detection software solutions, dedication to platform security is not limited to protecting against exploits currently in the wild but those that have the potential to surface in the future. Long-term substantiated commitment is a critical credential for any OEM promoting platform security.
- » **Hardware-based root of trust (RoT).** Security is built on trust. The foundation of HP Inc.'s platform security is the HP Endpoint Security Controller (ESC). ESC is a tamper-resistive, hardware-based root of trust. Other technologies in HP Inc.'s platform security portfolio and in collaboration with its technology partners (e.g., Trusted Platform Module [TPM]) integrate with the ESC to extend RoT to additional functions.
- » **Protection from physical tampering.** Hybrid work arrangements and mobility place PCs at risk of physical tampering. Designed into HP Inc. PCs is detection of physical tampering (e.g., cover removal) with configurable automatic response options, such as wiping sensitive information, disabling, and alerting.
- » **Lockdown of BIOS configurations.** The risk of unauthorized access to BIOS configurations must be eliminated. Yet for operational expediency, IT teams face perpetual risk by using a single password for all PCs or, worse, no password to access BIOS configurations. HP Inc. elevates protection of BIOS configurations without operational overhead through the use of digital signatures.

- » **Self-healing recovery.** A compromise in HP Inc.'s firmware and BIOS configurations cannot be fully eliminated from the realm of possibilities. Therefore, it is essential to have a turnkey mechanism to confidently (an attribute of the hard-based ESC) detect compromises and return to a safe and authenticated state independent of the PC location (on premises or remote) and without end-user involvement. With HP Inc. PCs, the OS golden image is also recoverable.
- » **Ability to serve multiple internal constituents.** IT, security, and auditing operational teams are inundated with "solutions" that only serve narrow objectives. While effective in purpose, this approach is inefficient in practice as restrictions and friction in tool proliferation mount. HP Inc.'s approach to platform security is its one-to-many attribute. SecOps need to mitigate cyber-risk. ITOps need a stable platform that contributes to business outcomes and, when a direct touch is needed, end-user transparency and scalability across the PC fleet. Auditing and compliance teams need easily attainable, trustworthy documentation rather than manual-intensive data collection. Each of these internal constituents is served by HP Inc.
- » **Non-HP Inc. firmware security.** Virtually any hardware add-on introduces third-party firmware, which adds to the attack surface. Representing a vector for malware to be introduced and propagated, HP Inc. PCs have a solution. They run third-party firmware in a protected virtual machine (VM) so that malware, if it exists, is structurally contained.

Challenges

Reprioritizing PC-buying criteria to have a greater emphasis on platform security, while necessary, may not always be straightforward. Context can add to confusion and uncertainty. Two areas of context that a company will likely encounter as it moves forward on PC-purchasing decisions are:

- » **Cybersecurity's operational burden.** Cybersecurity is a complex discipline consisting of multiple tools from multiple vendors. The implication is organizations have an oversized operational burden of managing existing cybersecurity tools for the threats they view as most imminent. Consequently, until the organization experiences a serious security incident attributable to inadequate platform security, platform security will not become a priority.
- » **Competitive alternatives.** Other PC vendors, chip manufacturers, and OS vendors promote their approaches to ensuring PCs are protected from silicon up through the operating system. Like HP Inc., they are highly recognizable technology brands and will, in a competitive market, continue to innovate.

Conclusion

Being prepared to effectively deflect a PC firmware attack not only is vital to an organization's cyber-resilience strategy but also requires IT teams to broaden their PC evaluation criteria. Waiting until a firmware compromise occurs to prompt a change in PC evaluation criteria can have devastating business consequences. With decades of delivering hardware-enforced protection in its PCs and a robust developmental road map, HP Inc. should be under consideration in establishing a fleet of PCs designed for today's and tomorrow's cyberthreats.

As cyberadversaries leverage every available avenue, organizations must prioritize firmware integrity protection and recovery or risk adversaries seizing system-level control of their PCs.

About the Analyst



Michael Suby, Research Vice President, Security and Trust

Michael Suby is a research vice president in IDC's Security and Trust research discipline. In this role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in topics spanning a wide and evolving spectrum of security and trust topics. In the broad endpoint security landscape, Mr. Suby focuses on impactful developments in solutions, markets, cyberthreats, and end-user requirements in the following endpoint security categories: modern endpoint security, server security, and consumer digital life protection.

MESSAGE FROM THE SPONSOR

HP Wolf Security gives you comprehensive endpoint protection and resiliency that starts at the hardware level and extends through the application layer. HP Wolf Security reduces the addressable attack surface and enables remote recovery from firmware attacks.

Our capabilities provide robust IT and Security outcomes from modern endpoint management, supply chain integrity to PC Platform Integrity and physical PC compromises, building a robust endpoint security platform.

HP Wolf Security capabilities help you minimize risks, boost IT efficiency, and enhance user productivity, making it easy to safeguard your PC endpoints.

Learn more about HP Wolf Security providing layers of protection on your PCs; visit us at hp.com/security.



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2023 IDC. Reproduction without written permission is completely forbidden.