AMD CSO

SPONSORED CONTENT

Responding to Today's Cyberthreats with Layered Security from AMD and Microsoft

WITH RESEARCH AND ANALYSIS BY IDC

Chip-to-Cloud Security Starts with Built-in, Hardware-based Defenses

Introduction

Cyberattacks continue to increase in number annually. In 2021, the FBI Internet Crime Complaint Center received a record number of complaints: 847,376, a 7% increase from 2020, with potential losses exceeding $6.9 billion. Leading complaints included phishing, identity theft, data breaches, and ransomware.

Despite all the time and energy directed at securing endpoint computers, they still represent a high-risk target. According to Vedere Labs, computers are the sixth riskiest IT asset with an 8.5 out of 10 average Common Vulnerability Scoring System (CVSS) score.

What can security and IT teams do to increase protections of endpoint devices? To answer this, we looked at some major trends driving heightened security awareness.

Situational overview

Security and IT professionals have high expectations for endpoint security solutions and those expectations are increasing. This is expected. Endpoint threats are a big concern; security breaches are common with many due to endpoint compromises. The dramatic rise in employees working from home (WFH), and the outlook that many will not return to the office, are also contributing factors.

Considering these circumstances, organizations need to reassess their cybersecurity hygiene and evaluate the benefits of adopting a chip-to-cloud approach for device security. Aftermarket, bolted-on endpoint security software is no longer sufficient. Hardware-based device security below the OS needs to be part of the security stack to defend against current and future threats.

Hybrid workplaces are not inherently secure

One result of the COVID-19 pandemic is that many employees have moved from a protected business work location to WFH. And as hybrid work becomes the norm, endpoint devices become increasingly difficult to defend.

Operating outside the carefully managed network of the enterprise means that end users and their devices may be more vulnerable to threat actors and their attacks. These threat actors know from experience that compromising endpoint devices and manipulating human behavior is a tried and true pathway to stealing sensitive information, instituting ransomware attacks, and disrupting business operations.

According to IDC, 53% of North American technology leaders agree that hybrid work will remain part of the corporate culture even after the pandemic is over. Protecting WFH employees and their devices is a top priority. Ensuring the security of corporate resources across all locations was another crucial consideration.

Firmware as an attack vector

UEFI (Unified Extensible Firmware Interface) plays a crucial role in loading the OS and securing the pre-OS environment. Since attacks on PC firmware through UEFI bootkits, which are malicious code planted in firmware, are more challenging, they have not been as common as other endpoint cyberthreats. But this is changing quickly, because such a widespread technology presents a tempting target for threat actors.

Prior to 2021, there were only two real-world cases of UEFI malware: MosaicRegressor (2019) and LoJax (2018). By late 2021, that number had more than doubled. Two new bootkits, FinSpy and MoonBounce, were uncovered by Kaspersky and a third, the ESPecter bootkit was discovered by ESET. According to ESET, all machines infected with the UEFI bootkit had the Windows Boot Manager replaced with a malicious one that allows the malicious boot manager to bypass all security checks.

The attack surface mushrooms with digital transformation and Industry 4.0

The digital transformation of businesses and Industry 4.0 means more devices, types of devices, and systems are being connected to the internet than ever before, tremendously increasing the size and complexity of the attack surface and exposing companies to significantly more potential cyberattacks. Endpoint security needs to be able to scale at the same velocity as the devices and systems that are being connected. Solutions that centralize the provisioning and deployment of security patches and software updates would help streamline these processes.

US government warns of increased security risks

With geopolitical tensions rising, concerns about cybersecurity have reached the highest levels of the U.S. government. In 2021, U.S. President Biden signed several executive orders which called for the government and private companies to harden the security of their computers systems, whether they are cloud-based, on-premises, or hybrid. According to one order, the scope of protection and security must include systems that process data and those that run the vital machines that play a role in our safety. Protecting the endpoint computers and the confidential data that is processed and stored is an essential component of national and economic security.

Beware of supply chain attacks

With the SolarWinds cyberattack in late 2020, supply chain security made headlines. According to Mandiant, supply chain compromise was the second most prevalent initial infection vector identified in 2021, accounting for 17% of intrusions compared to less than 1% in 2020. Further, 86% of supply chain compromise intrusions were related to the SolarWinds breach.

In the digital world, software from multiple suppliers is inevitable. Threat actors seek to insert their malicious code into the legitimate code of trusted software vendors/suppliers. Riding through the same delivery/update channel as the legitimate code, the threat actors' code is delivered to the vendor clients' environments. Once in the clients' environments, the contaminated software code can spread across multiple assets and devices and attempt to alter the firmware and the OS from which to gain persistence and system level administration rights. If the initial intrusions are not discovered and fixed quickly, they could lead to the injection of malware and ransomware attacks.

Software is just one source of supply chain attacks. Malicious code inserted into CPU firmware delivered from the factory or through third-party suppliers is another potential source.

A call to action

A layered approach — chip-to-cloud security

For all businesses, security should not be an afterthought. It should be built in from the beginning. Good security hygiene comes from strong collaboration between silicon vendors, PC hardware manufacturers, and independent software vendors. Chip-to-cloud security involves a layered approach which starts at the chip level and builds through firmware, the OS,

applications, and then to cloud processes. To establish a chain of trust, each layer attests and authenticates to the next layer in the stack that it is operating as intended.

For many organizations, their current approach to endpoint security includes an insufficient number of layers. Despite advancements and inclusion of machine learning and artificial intelligence into endpoint protection platforms and the layered addition of endpoint detection and response, organizations continue to operate 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 has a structural limitation as endpoint security software products lack visibility into firmware integrity.

Protection below the OS

A better alternative is to approach endpoint security holistically, starting with devices equipped with hardware-based root-of-trust technologies that help deliver security below and in the OS. A holistic approach to endpoint security may help address the inherent blind spots of bolted-on endpoint security software; 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 reduces IT-involved reimaging and minimizes disruptions to end-user productivity. Hardware-based security can also lessen security operation center (SOC) analysts' alert fatigue, number of incident investigations, and post-incident

remediations. Finally, hardware-based root-of-trust devices fold nicely into zero-trust architectures.

One recent example of a hardware-based layered security approach is Microsoft's requirement that a Trusted Platform Module 2.0, which stores encryption keys, security certificates, and passwords, be present and activated to install Windows 11 OS.

Protect against firmware/boot malware

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

- **Exploitable:** Because firmware functions below the OS and is established before endpoint security software loads, endpoint security software can only make inferences on whether firmware has been compromised. A PC that lacks a direct line-of-sight mechanism to detect firmware compromises as the PC is powered on or to certify the firmware's integrity once loaded, makes the PC an exploitable system.
- **Leverage:** A UEFI bootkit is malicious code planted in the firmware and is designed to load before everything else, including the OS. Accordingly, a UEFI bootkit is invisible to security software that runs within the OS because it loads before security software is running. Corrupted firmware resides in nonvolatile memory, is not erasable from the PC's hard drive and, therefore, is persistent. The corrupted firmware exists each time the PC powers up. This provides threat actors with persistence and control over an OS's boot process, making it possible to sabotage OS defenses, even bypassing a Secure Boot mechanism.

Protect against physical attacks

Hybrid work is here to stay. So, organizations must ensure that the devices that connect to their IT networks and contain confidential company data are protected as much as possible. Once outside the corporate walls, the chance that devices will be lost, stolen, or accessed by an unauthorized person increases.

Once in physical possession of a laptop, thieves can extract confidential cryptographic keys, certificates, and data. Security solutions integrated into the CPU exist that are designed to help prevent this type of attack.

Challenges

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

- **Threat prioritization:** Attacks on PC firmware (i.e., UEFI bootkits) are not as prevalent as other cyberthreats, but the number of UEFI bootkits has doubled in just the last year. Some organizations may still choose to prioritize defending against other cyberthreats that they are experiencing now and forgo PC refreshes until firmware attacks reach a critical level.

- **Digital transformations may obviate need:** Organizations that have taken a cloud-first approach 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.

- **Threat actor innovation:** There is no guarantee that any vendor's built-in device security is 100% effective in defending against all potential threats. The uncertainty of long-term effectiveness may contribute to organizations choosing to delay PC refreshes.

Advice to technology buyers

To secure companies' networks, data, and confidential information, employees must practice good cyber hygiene, i.e., implementing strong password practices, using multi-factor authentication, maintaining a secure network/VPN, keeping application and virus software up to date, and awareness of social engineering attacks, particularly phishing.

IT is responsible for the next security layer. When IT chooses built-in solutions to protect endpoint devices below the OS, hardware-based security defenses may require new hardware. PCs purchased in the last few years will have some hardware-based security, but the newest laptops have the highest potential to unlock several layers of security from chip to cloud.

IDC believes that enterprises should complete a hardware inventory to discover which computers qualify to be replaced, where they are located, how they are

being used, and who is using them. Then, a thorough risk assessment should be conducted prioritizing the computers that are in less-secure physical environments, are running sensitive applications, or handling confidential data; these PCs should be upgraded first.

Conclusion

Organizations are conditioned to protect PCs from cyberthreats solely with endpoint security software that runs above the OS. Unfortunately, bolted-on security software is not designed to defend against firmware attacks nor does this it have direct visibility into software running beneath the OS. Hardware-based security helps alleviate this blind spot so organizations can have holistic endpoint security below the OS.

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 to mitigate those attacks. Another relevant consideration for hardware-based security is in support of zero-trust architectures where the trustworthiness of a connected PC is confirmed by hardware-enforced root of trust. ■

Layered Security Combines the Power of Software, Firmware, and Hardware

In a London cafe, a journalist leaves a laptop unattended. While he's away, another patron inserts a USB drive into the laptop. By the time the journalist returns, the cyberthief has gotten what they needed: a backdoor connection to gather information about confidential sources the next time the journalist goes online.

Though this scenario is fictional, it illustrates the real risks inherent in today's hybrid work world, where unattended devices, whether company-owned or personal, pose security challenges for organizations of every description, size, and location.

Any effective approach to security must take in the complete system, from chip to cloud, not just select hardware or software components. Organizations need a layered approach to security, in which software, firmware, and hardware work together to block attacks at every level.

Fortunately, software, hardware, and OEM (original equipment manufacturer) vendors are responding to the threat with advanced, layered security protections that work seamlessly in the background so employees can go about their work without sacrificing efficiency.

New work realities, new exploits

Sophisticated attackers have found ways to exploit the gaps between hardware, firmware, and OS and application-based security. By intercepting authentication data as it transitions between hardware and software, bad actors can:

- Tap into the communications bus on device hardware to capture data before it has a chance to undergo encryption via software
- Repurpose legitimate snippets of boot-up code to force devices to execute malware as part of autoimmune attacks
- Capture login and encryption keys as they transit between hardware, firmware, and software layers.

Such attacks may start with physical access to a device, such as when an attacker plugs a USB device into an unattended laptop. These opportunities increase in the context of a remote and hybrid workforce.

"In an unsecured network, your device becomes the last line of defense," says Akash Malhotra, head of security product management at AMD. That's because devices such as laptops must fend for themselves away from the security of corporate networks.

"It can be stolen," Malhotra says of a corporate laptop or personal device used for work. "You can leave it for a couple of minutes, and people can plug some kind of malware into the USB port." But threats aren't limited to public places. "If people come to your house where you're working, the system is accessible," Malhotra says.

Clearly, security designed in the always-in-office era of work can no longer reliably keep sensitive company, employee, and customer data safe. Instead, a new approach is needed, grounded in the way people work today, and designed to counter emerging threats.

Layered security – in which hardware and software work together to help keep data safe – provides such an approach.

Closing the door on the bus

Layered security works through hardware and software features that enhance one another to form a whole greater than their parts. In contrast to older, separate security functions enabled by individual, disparate components, integration is the key to success.

For example, conventional software encryption can protect data on a laptop. But when the system passes that data through the communications bus, such as when it moves data to and from RAM and a hard drive, encryption keys protecting the information become exposed. And someone with physical access to the computer can exploit that vulnerability to extract the keys and use them to decrypt the data wherever it resides. That's why a robust security solution integrates both hardware and software components.

However, such integration represents a challenge because hardware and software vendors typically take separate development paths. "No one provider controls enough of the product stack to provide a fully comprehensive solution," explains Chuck Schalm, commercial business development manager at AMD.

Effective solutions require hardware and software developers to work in tandem to reduce security gaps. "By working together and providing some elements in silicon, some in firmware, and some in the OS, you have a combination of one plus one plus one that gets you more than three," Schalm says.

In other words, with integrated hardware and software protections, each layer of security provides more protection than any one of them on their own. Ideally, hardware and software security integration happens on the chip, with secure software elements running on processors versus passing through the bus. "It's a combination of hardware, software, and silicon coming together to provide a robust solution," Malhotra says.

The collaborative efforts between AMD and Microsoft provides just such capabilities.

AMD and Microsoft, integrated security features

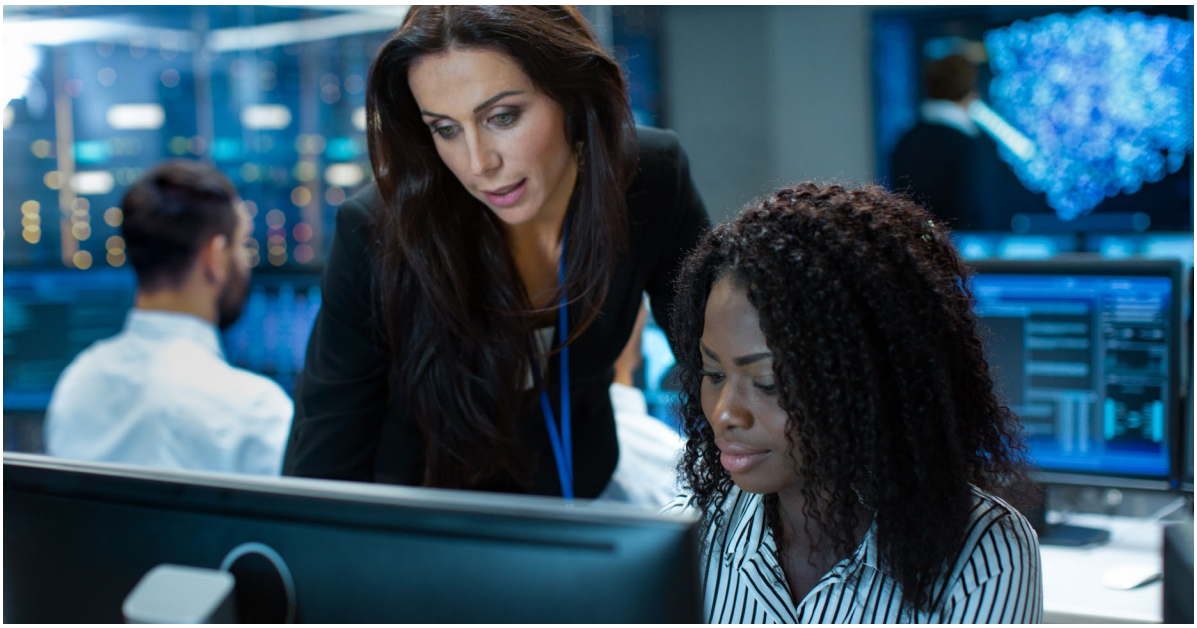
Meeting the critical need for layered security features and working in partnership with Microsoft, AMD has helped close the gap between hardware and software with AMD PRO technologies and AMD Ryzen™ PRO 6000 Series processors.

A key innovation is providing robust security features with little sacrifice of performance. "Performance has always been key," Schalm says. "But security features are getting more discussed and asked for by the end user."

Security features from AMD and Microsoft are integrated in such a way that they work together to help secure devices at every level, even from physical attack. That means AMD Ryzen™ PRO 6000 Series processors work with hardware and software from Microsoft to help protect data at every level, from the chip to the cloud.

For example, AMD Ryzen™ PRO 6000 Series processors integrate a Microsoft Pluton™[1] security processor for chip-to-cloud production – the first x86 commercial processors to do so[2]. Thanks to ongoing security updates, Microsoft Pluton™ helps defend new Windows 11 PCs with continuous protection for user identity and data.

"We are reducing attack vectors by confining authentication data to a very strict box," Malhotra explains. That box keeps communication used for authenticating users on chips rather than passing it over the communications bus to the operating system. In addition, full system memory encryption helps keep data safe as a standard feature. It's another first for a commercial processor family.



[1] Microsoft Pluton is a technology owned by Microsoft and licensed to AMD. Microsoft Pluton is a registered trademark of Microsoft Corporation in the United States and/or other countries. Learn more at https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/

[2] As of January 2022, only AMD Ryzen™ 6000 Series processors include the Microsoft Pluton security processor, while AMD Ryzen™ 5000 Series processors and Intel's latest 11th and 12th Gen processors do not. RMB-24

Full system memory encryption

AMD Memory Guard[3] delivers real-time system memory encryption. It's made possible by a dedicated security coprocessor – the AMD Secure Processor (ASP) – inside every AMD Ryzen™ PRO 6000 Series processor. The ASP provides a root of trust for many critical security functions, not just AMD Memory Guard.

AMD Memory Guard helps defend against physical attacks if a laptop is lost or stolen. "We encrypt the system memory itself so that the keys – which were originally in clear text – are encrypted, and attackers cannot find the keys," Malhotra explains. "Hardware and software integration is so close-knit that the data doesn't go out on the bus at all. Communication remains between AMD silicon and hardware."

Dynamic encryption makes hacking encryption keys a target that moves every time a computer boots up. "The beauty of this solution is that the encryption keys change with every boot," Malhotra says. Encryption each time a computer starts up drastically curtails the time an attacker has to try to get through, especially if they have limited access to a user's computer.

Flow control protection and more

Hardware and software integration for security on AMD Ryzen™ PRO 6000 Series processors doesn't stop with encryption.

For example, AMD Shadow Stack provides hardware-based data protection to help defeat control-flow malware attacks. In these attacks, malware attempts to redirect the flow of computational steps executed by legitimate software. To help prevent this, AMD Shadow Stack checks the software stack against a copy stored in hardware. Deviations that indicate an attack is in progress enable the system to stop software – and malware – from executing.

Nor does AMD leave IT departments behind. Making administration easier for busy IT teams, AMD Ryzen™ PRO 6000 Series processors also provide full support for modern enterprise mobility management solutions, including Microsoft Endpoint Manager. AMD PRO technologies help IT teams simplify the management of PCs by streamlining the deployment, imaging, and ongoing maintenance of their ever-changing fleets, no matter how large they grow.

[3] Full system memory encryption with AMD Memory Guard is included in AMD Ryzen PRO, AMD Ryzen Threadripper PRO, and AMD Athlon PRO processors. Requires OEM enablement. Check with the system manufacturer prior to purchase. GD-206.

Lastly, AMD collaborations with leading OEMs have resulted in support for features such as HP Sure Start, Sure Run, and Sure Click, and Lenovo features including ThinkShield and Self-Healing BIOs.

Secure for the future

The only constant in today's work world is change as threats continue to evolve. That's why layered security features that incorporate frequently updated software built into hardware is critical now and will continue to be so well into the future.

"If you marry hardware and software, the hardware provides another layer of security," Malhotra says. "If the software wall is broken, hardware is there to help protect it." And that makes all the difference for securing devices deployed in hybrid work environments.

Click here to learn more about how layered security protects devices from the chip to the cloud.

Foundational Security Benefits

Layered security features provide enhanced foundational security benefits in these critical areas:

- Hardware root of trust. A system built from the ground up with layered security features from AMD and Microsoft first establishes a hardware root of trust. That means the system bakes in trust at the most foundational level, where a system on a chip technology provides the touchstone for all other security measures.

- AMD Memory Guard, a first-to-market capability for commercial processors from AMD, encrypts data at the hardware level, helping eliminate opportunities for attackers to compromise data in transit, even if they gain physical access to the computer.

- Secured-core PC technology from Microsoft integrates security software at the firmware level, providing a layer of protection that can keep up with evolving threats thanks to continuous updates from the cloud to secure data and user identities.

- Firmware security ties other security functions together to complete a comprehensive layered security stack, hardening both hardware and software against threats, no matter where they originate or what form they take.