SHOWCASE

JULY 2026

# The Role of Hardware in a Complete Security Strategy

Gabe Knuth, Principal Analyst, Omdia

Abstract: Most conversations around endpoint and server security begin and end with software, even though current software-centric approaches are struggling to keep up with the demands of increasing endpoint diversity, vulnerabilities, and sophisticated attacks. Additionally, management and security teams often use different tools and procedures, which further amplifies the problem.

This Showcase aims to shine a light on the problems that exist today across security and management teams, explore how organizations are consolidating teams and tools, and demonstrate the importance of hardware-based capabilities that can improve security posture, reduce exposure, and help organizations better protect increasingly distributed hardware environments.

## The problem: Management and security complexity

Organizations of all sizes are dealing with increased IT complexity coming from many different angles. While an increase in applications, devices, and remote work are factors, as is generative AI, the top drivers contributing to IT management complexity reported in recent research from Enterprise Strategy Group (now Omdia) were all related to security (see **Figure 1** and **Figure 2**).[1]

On the endpoint security side, the threat landscape (40%) and business-driven AI usage (40%) lead the list, but the number of endpoint vulnerabilities (31%), device diversity (32%), and remote/hybrid workers (36%) all contribute. On the endpoint management side, the picture is similar:

- The frequency of OS updates and patches (37%) is the top driver of increased management difficulty, reflecting a patching burden that automation has yet to relieve.
- Rising managed device counts (36%) and additional remote and/or hybrid workers (36%) continue to expand the management footprint.
- Device, OS, and application diversity (32%) compounds the problem, as organizations must manage an increasingly heterogeneous environment.

With these challenges in mind, it's no surprise that organizations are doubling down on investment. Fully 85% of organizations plan to increase endpoint management and security spending over the next 12 to 24 months, and roughly one-third expect significant increases in each area.

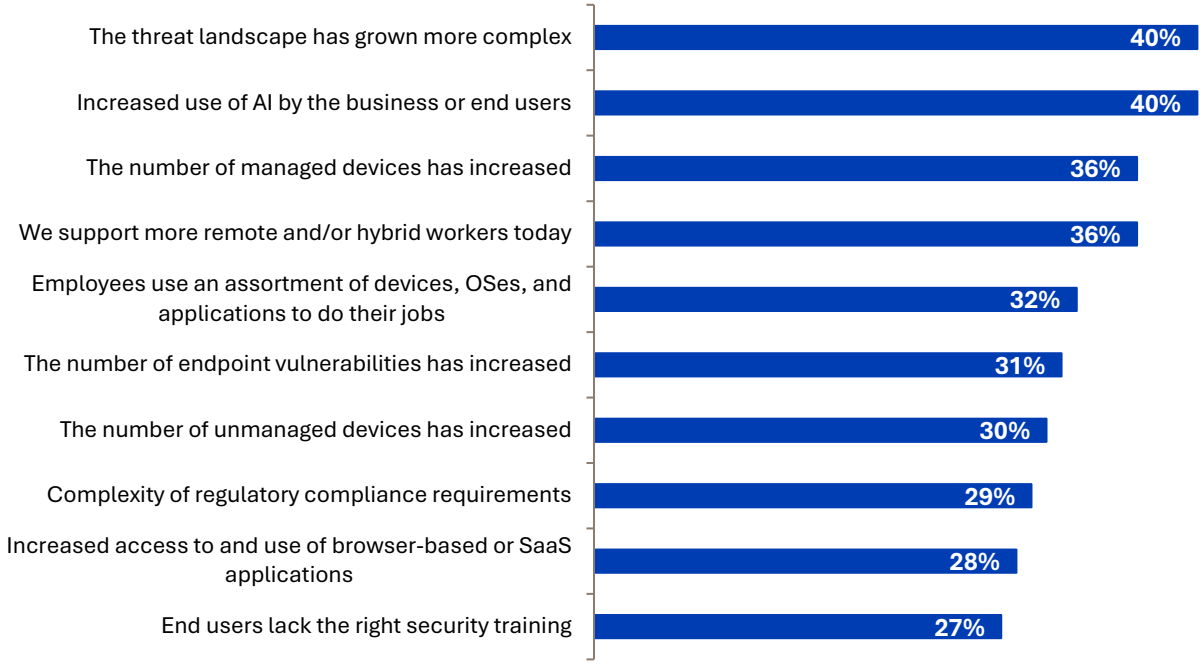
[1] Source: Enterprise Strategy Group (now Omdia) Research Report, *The Growing Role of AI in Endpoint Management and Security Convergence*, June 2025. All research references and charts in this Showcase have been taken from this research report.

This Showcase from Omdia was commissioned by AMD and is distributed under license from TechTarget, Inc.

© 2026 TechTarget, Inc. All Rights Reserved.

Figure 1. Top 10 drivers of increased endpoint security complexity

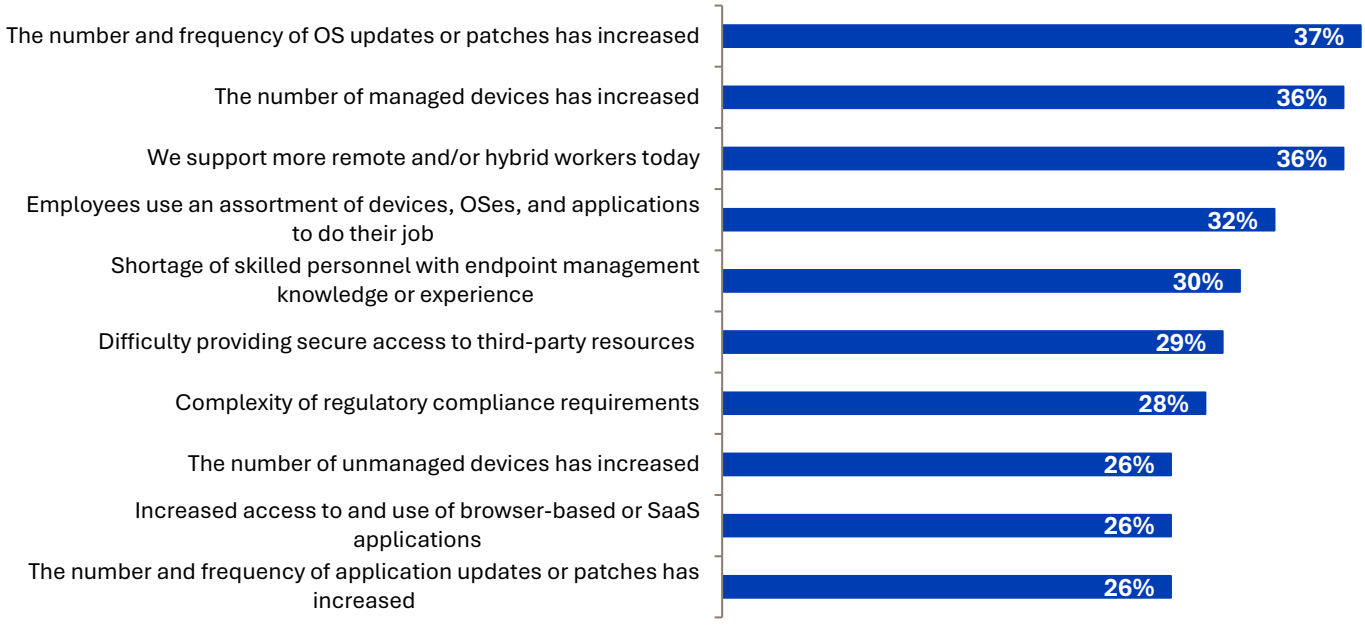
**Why do you believe that securing endpoints has become more difficult for your organization over the past two years? (Percent of respondents, n=154, multiple responses accepted)**




*Source: Omdia*

Figure 2. Top 10 drivers of increased endpoint management complexity

**Why do you believe that endpoint management has become more difficult for your organization over the past two years? (Percent of respondents, n=140, multiple responses accepted)**




*Source: Omdia*

©2026 TechTarget, Inc. All Rights Reserved.

While many organizations identify security optimization as a top priority, the tools they choose and how they deploy them are critical to success. One thing is clear, though: Tools alone are not enough. Research shows that 42% of organizations use more than 10 endpoint management tools and 49% use more than 10 endpoint security tools. Despite the number of tools, 54% of organizations said they'd experienced a cyberattack that began with the exploit of an unknown, unmanaged, or poorly managed endpoint, with 22% reporting this has happened several times. This is likely due to three primary issues:

- A lack of communication between management and security teams.
- Security and management tool sprawl due to reactive approaches.
- Blind spots due to a lack of information sharing and collaboration.

Ultimately, this leads to the "cycle of sprawl" (see **Figure 3**), whereby tactical solutions deployed as blind spots are discovered. For this reason, organizations are increasingly focused on consolidating tools and teams to increase visibility, optimize information collection and sharing, and make security and endpoint management more efficient.

**Figure 3.** The sprawl cycle that leads to the proliferation of endpoint management and security tools




*Source: Omdia*

While the data shown here is for endpoints, this division of security and management exists for data center and cloud workloads, too. Given the broad scope and importance of endpoint, server, and workload security, the path forward should focus on a strategy that avoids tactical solutions that often contribute to the overall problem of reactionary support, complexity, and sprawl. The new approach should prioritize purposeful consolidation of teams, tools, and processes to help ensure every stakeholder is marching in the same direction. Additionally, it should not ignore the role that hardware plays in helping secure workloads wherever they run.

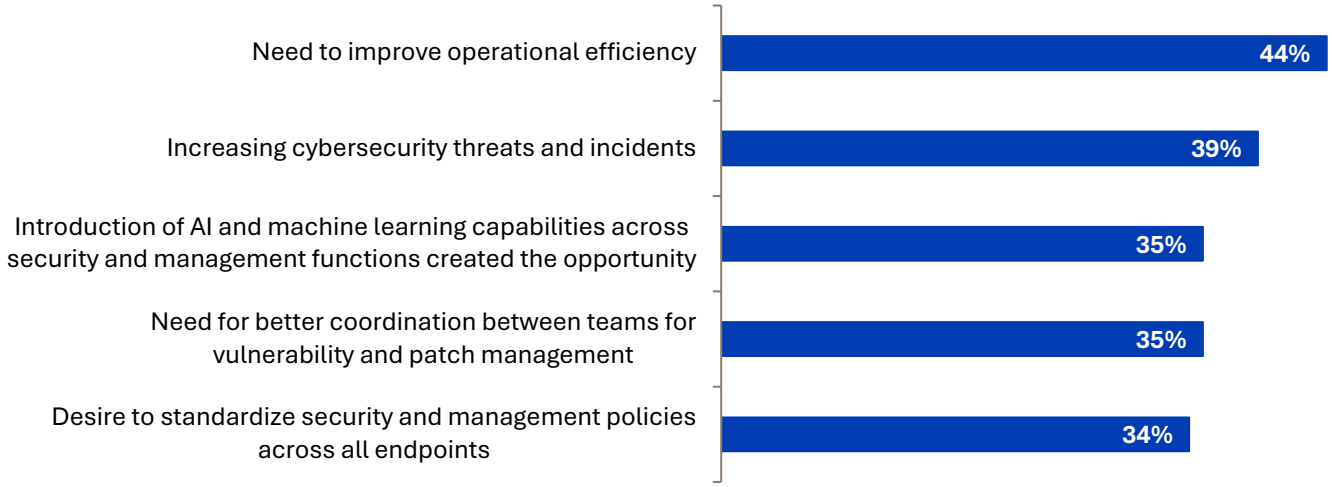
©2026 TechTarget, Inc. All Rights Reserved.

# A path forward

According to Enterprise Strategy Group (now Omdia) research, 82% of organizations have consolidated, or are making an effort to consolidate, their device management and security teams. The drivers behind this are plentiful and do a good job of highlighting the problems that need to be solved: the need to improve operational efficiency (44%), increasing cybersecurity threats and incidents (39%), and the need for better coordination between teams for vulnerability and patch management (35%) are at the top of the list (see **Figure 4**).

**Figure 4.** Operational efficiency and cybersecurity threats drive consolidation efforts

**What drove or is driving the consolidation of endpoint management and security at your organization? (Percent of respondents, n=334, multiple responses accepted)**




*Source: Omdia*

It's also important not to discount the role of hardware in an organization's overall management and security strategy. While much attention is given to software, teams often overlook the hardware benefits and features that can help protect users and reduce the chances of human error leading to security events and/or data breaches. For example, hardware today includes security features such as:

- Hardware-rooted capabilities designed to strengthen data protection across the stack, especially for data in use, while complementing software controls for data at rest and in flight.
- Confidential virtualization capabilities that can help protect existing workloads inside confidential VMs, often with little or no application code change.
- Trusted boot and platform integrity features that help verify firmware and boot components before allowing the system to proceed.

Overall, the combination of hardware, software, and team consolidation will be key to successfully addressing security and management sprawl. As these features, along with others, are being built in today's endpoints and servers alike, evaluating hardware in any consolidation or strategy decision is crucial if you want to move the needle.

©2026 TechTarget, Inc. All Rights Reserved.

# How hardware security features from AMD can help

As AI and new applications evolve, the amount of data used and shared across technologies continues to grow, and AI workloads, in particular, may keep more sensitive prompts, context, models, and intermediate data in the "in use" state for longer periods than many traditional workloads. Data protection is a top priority across AMD PRO commercial processor platforms, with security capabilities integrated at the silicon level to support robust, multifaceted protection.

AMD approaches security with two beliefs: Security should not be a feature that comes with a premium, and open standards beat proprietary approaches. AMD PRO platforms are designed to make enterprise-grade security capabilities broadly available across commercial PC portfolios. Across server and endpoint platforms, AMD brings a hardware-rooted approach to security, with capabilities such as:

- **Secure processor.** A dedicated security processor validates code before execution and checks for data and application integrity. This processor forms the foundation of AMD security architecture, acting as a root of trust anchored in hardware.
- **Shadow Stack.** On supported AMD processors and operating systems, Shadow Stack helps protect against control-flow attacks such as return-oriented programming by maintaining a protected copy of return addresses.
- **Secure boot.** AMD platform secure boot capabilities help establish a chain of trust from silicon through platform firmware and boot components, helping ensure authenticated code is loaded during system startup.

AMD has also built hardware-based security features specifically for their respective server and endpoint CPU product lines:

## Server CPU security

For servers and cloud instances, AMD Infinity Guard is a suite of hardware-based security features embedded at the silicon level that help protect data hosted on-premises or in the cloud. Central to the AMD server security approach is confidential computing, enabled by AMD Secure Encrypted Virtualization, or AMD SEV—a hardware-rooted approach to protecting data in use that creates hardware-enforced trusted execution environments (TEEs) at the processor level. Confidential virtual machines can protect entire workloads, including the application, data, and operating system, often without application code changes. The features outlined below build upon the common features listed above, forming the basis of this capability.

- **Transparent Secure Memory Encryption (TSME).** System memory is encrypted using a 128-bit AES key, helping protect data in RAM from unauthorized access and helping to mitigate risks like certain cold boot attacks. This happens transparently and without modification to existing x86 applications, which can help secure apps that lack inherent memory security.
- **AMD SEV.** SEV builds on AMD memory encryption technologies by enabling per-VM memory encryption, helping isolate guest memory from other VMs and from privileged host software.
- **SEV with Encrypted State.** SEV with Encrypted State helps protect CPU register contents when a VM exits or stops running, reducing the exposure of sensitive guest state to privileged software.

©2026 TechTarget, Inc. All Rights Reserved.

- **SEV with Secure Nested Paging.** SEV with Secure Nested Paging adds memory integrity protection, helping defend against malicious hypervisor actions such as memory remapping and replay attacks. Most recently, 5th Generation AMD EPYC™ processors introduced Trusted I/O support via the PCI-SIG TDISP standard, helping extend confidential-computing protections to supported PCIe®-attached devices such as accelerators, NICs, and storage, which is important for AI workloads where sensitive data can move across CPUs, accelerators, memory, and I/O devices.

These layered security measures help provide defense against a wide range of threats, from certain cold boot attacks to hypervisor-based intrusion to data replay. AMD SEV is supported across major cloud providers (AWS, Azure, Google Cloud, Oracle Cloud Infrastructure), operating systems, virtualization platforms, and server manufacturers. Plus, by integrating these hardware-based security features, AMD EPYC™ server CPUs offer a multilayered approach to security that enhances the protection of data and applications, addressing vulnerabilities that software alone cannot mitigate.

### Endpoint CPU security

For desktops, laptops, and workstations, AMD provides multilayered security features on AMD Ryzen™ PRO and AMD Ryzen™ Threadripper™ PRO CPUs, including:

- **Memory Guard.**[2] This feature delivers real-time encryption of system memory, helping to defend against physical attacks. If a laptop is lost or stolen, Memory Guard helps ensure that sensitive data stored in RAM is protected.
- **FIPS 140-3 Level 1 Certification.** This government encryption standard is widely adopted by the private sector as a best practice for validating the security of cryptographic hardware. The FIPS 140-3 Level 1 validation helps demonstrate that the relevant cryptographic module meets recognized security requirements for cryptographic functionality.

AMD designed these security features to work with existing and new software stacks, helping customers adopt strong protections with minimal application disruption, and to complement ecosystem partners at both the software and system levels. This integration of hardware, software, and services helps customers and partners quickly identify and address critical security issues.

## Conclusion

Hardware contributes to a complete security strategy by anchoring trust below the OS, helping protect data in use, isolating workloads from privileged software, and enabling evidence through attestation.

As organizations look to manage the complexity of their IT environments, leveraging hardware-based security features has become increasingly critical. AMD helps with this by building robust security capabilities, including memory encryption and confidential computing, directly into its CPUs across data center and endpoint platforms. This multilayered defense strategy strengthens the hardware foundation that software tools, platform services, and security operations depend on.

[2] 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.

©2026 TechTarget, Inc. All Rights Reserved.

AMD collaborates with ecosystem partners at both the software and system levels to enhance security across data center and endpoint solutions. Its commitment to industry standards and interoperability—from support for industry standards such as PCI-SIG TDISP to AMD's broader commitment to ecosystem collaboration and transparency—means organizations can adopt the security capabilities AMD provides within their existing infrastructure while maintaining freedom of vendor choice. These hardware-based security capabilities, coupled with close collaboration with OS, OEM, and ISV partners, helps organizations deploy a multilayered set of security features that help defend against many sophisticated attacks, both now and in the future.

AMD provides hardware-rooted security capabilities that help organizations safeguard data and maintain trust. With these tools, AMD demonstrates a strong commitment to security innovation and collaboration, making its solutions an excellent choice for any organization building a comprehensive, hardware-aware security strategy.

**Copyright notice and disclaimer**

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

**Get in touch:** www.omdia.com askananalyst@omdia.com

© 2026 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.