Enterprise Strategy Group by TechTarget

SHOWCASE

JULY 2024

The Role of Hardware in a Complete Security Strategy

Gabe Knuth, Senior Analyst

Abstract: Most conversations around endpoint and server security begin and end with software, even though current software-only 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 paper 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 and reduce the number of incidents in an increasingly distributed hardware environment.

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, and newer concepts such as generative AI (GenAI) are here, the top drivers contributing to IT complexity reported in recent research from TechTarget's Enterprise Strategy Group were all related to security (see Figure 1).[1]

Security can mean many things, and while the increasing and/or changing cybersecurity landscape (30%), incorporating new and emerging technologies (26%), and new data security and privacy regulations (23%) all featured prominently on the list of reasons IT complexity has risen, other adjacent areas also factored into the top 10 responses. For example:

- Supporting remote and hybrid work (24%) leads to an expanded and less clearly defined perimeter.
- Higher volumes of data and data sources (22%) increase the chances of data loss.
- An increase in the number of end-user devices (16%) expands both the management and security footprint that organizations must grapple with.

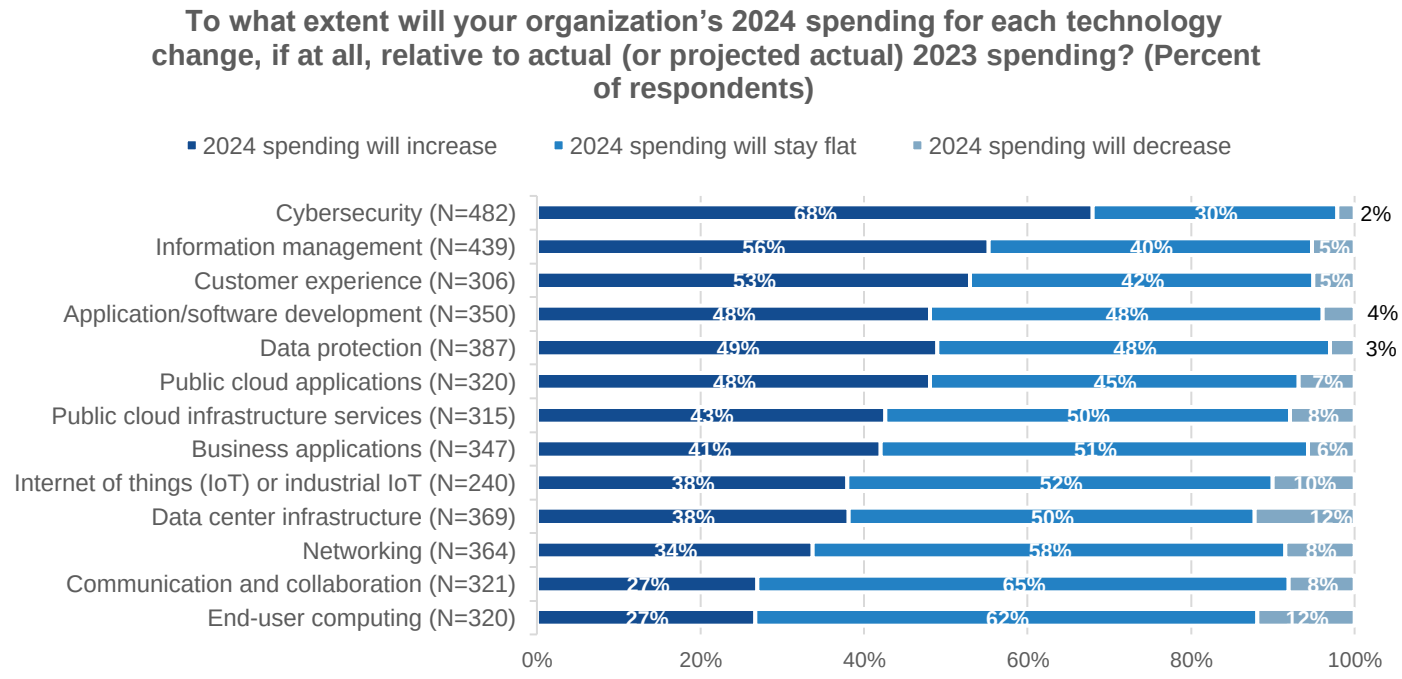
With these in mind, it's no surprise that cybersecurity continues to see the most investment across all IT priorities for 2024, with 68% of organizations noting increased spending in this area (up from 65% in 2023). Other related areas are also expected to see increased investments, like information management (56%), data protection (49%), and data center infrastructure (38%; see Figure 2).[2]

[1] Source: Enterprise Strategy Group Complete Survey Results, *2024 Technology Spending Intentions Survey*, February 2024.
[2] Ibid.

Figure 1. 6 of the Top 10 Reasons for Increased IT Complexity Are Related to Security

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

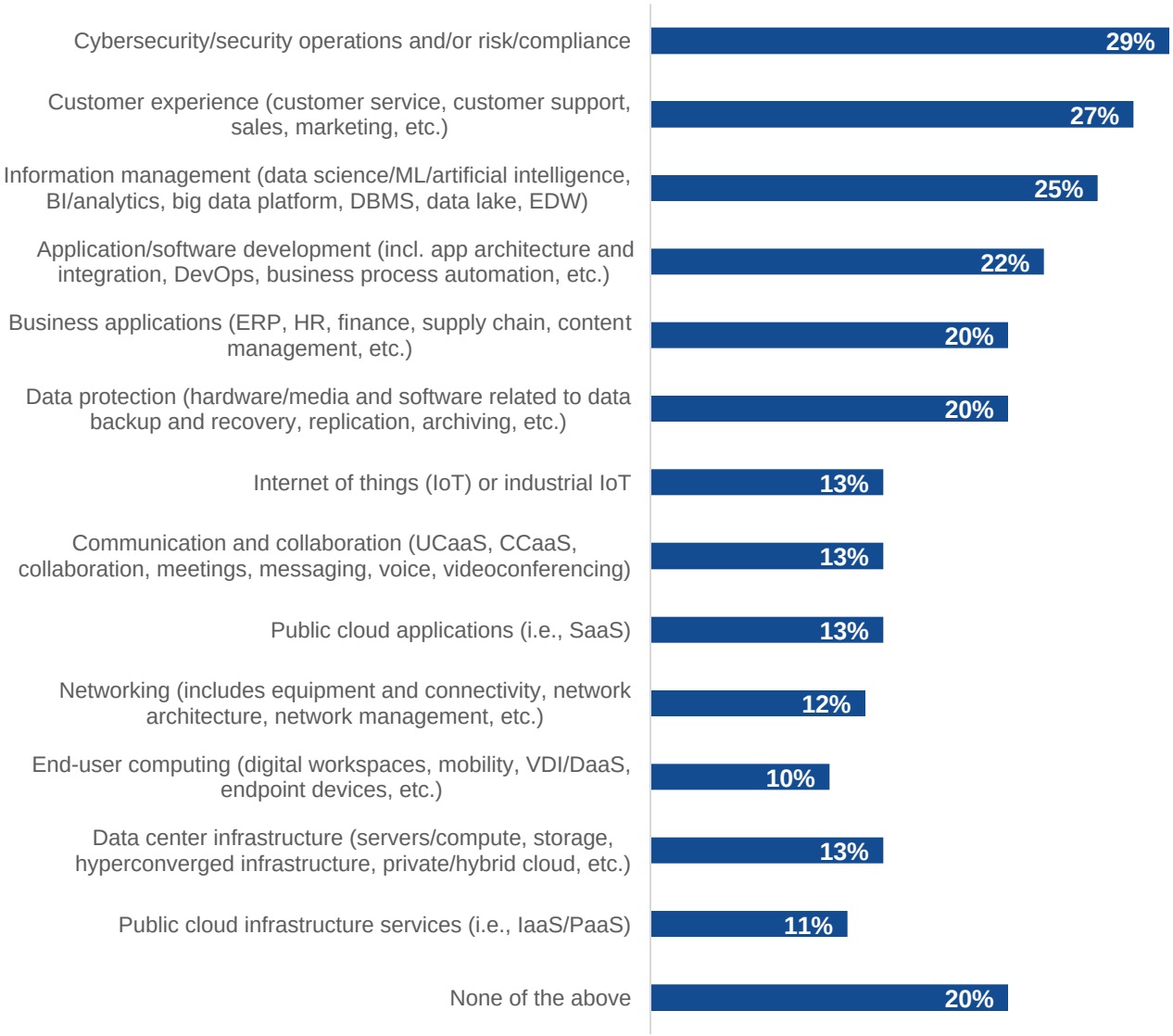
Figure 2. Security Spending and Adjacent Areas Are Set to Increase in 2024



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

With so many variables driving complexity and a variety of initiatives to undertake, organizations have far-reaching intentions for GenAI investments related to security. For example, 29% of organizations say they'll invest in tools that help bolster their cybersecurity, security operations, and/or risk and compliance efforts, while 20% are looking to employ it for data protection purposes (see Figure 3).[3]

Figure 3. GenAI Is Expected to Be Used in Many Areas,



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

While many organizations are identifying the need for security optimization, which tools will be implemented and how they will be deployed is critical to success. When Enterprise Strategy Group conducted research into the teams that manage and secure endpoints, we found that over two-thirds (68%) of organizations have deployed

[3] Ibid.

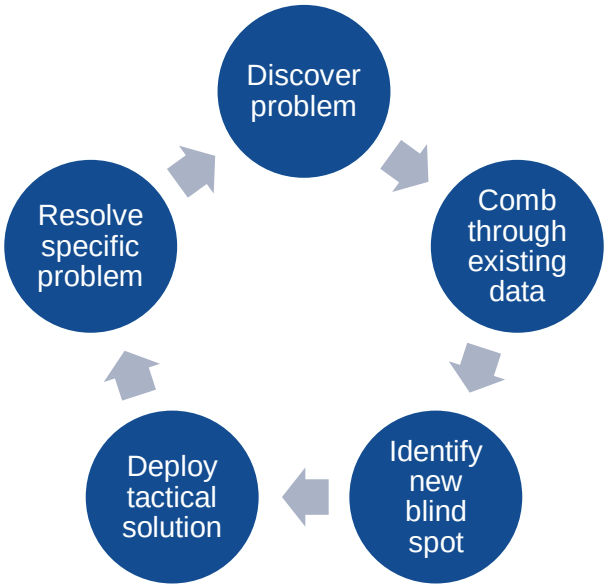
more than 10 tools for endpoint security and management purposes, with over one-third (35%) of those organizations reporting that they have deployed more than 15 tools.[4]

Interestingly enough, the number of tools deployed for management and security does not correspond to an increase in security. In fact, 53% of those organizations with more than 15 tools deployed noted that they'd experienced several cyberattacks related to unmanaged or poorly managed endpoints. This is due to three primary issues:

- Lack of communication between management and security teams.
- Security and management tool sprawl due to reactive approaches.
- Blind spots due to lack of information sharing and collaboration.[5]

Ultimately, this leads to the "cycle of sprawl" (see Figure 4), whereby tactical solutions deployed as blind spots are found without regard to an overall strategy or alignment with broader IT or business objectives. For this reason, organizations are increasingly focused on consolidating tools and teams to increase visibility and optimize information collection and sharing, with the ultimate goal of a more efficient security and endpoint management operation.

Figure 4. The Sprawl Cycle That Leads to the Proliferation of Endpoint Management and Security Tools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

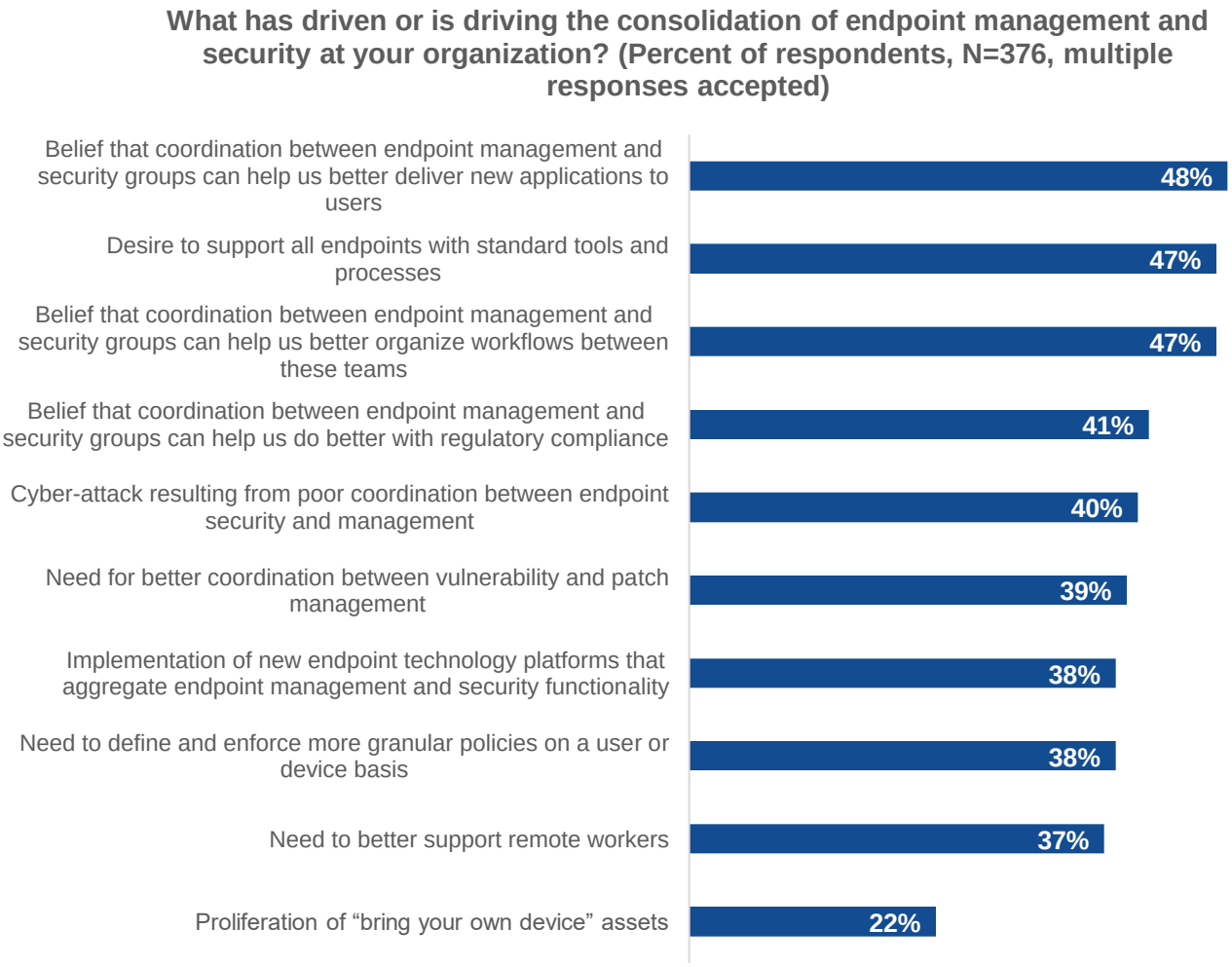
While the data shown here is for endpoints, this division of security and management exists for data center and cloud workloads, too. With this in mind, the path forward should focus on a higher-level strategy that avoids tactical solutions that often contribute to the overall problem of reactionary 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.

[4] Source: Enterprise Strategy Group Research Report, *Managing the Endpoint Vulnerability Gap*, May 2023.
[5] Ibid.

A Path Forward

According to Enterprise Strategy Group research, this consolidation is already top of mind for many organizations, with 58% of respondents noting that one of their goals is to completely consolidate their endpoint security and management teams and have one team responsible for both areas. Another 36% answered that this may happen but said that it was too early to tell.[6] The reasons for this are plentiful and do a good job of highlighting the problems that need to be solved (see Figure 5).

Figure 5. Coordination Among Security and Management Teams, Tools, and Platforms Is the Primary Driver of Consolidation Efforts



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

It's 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 like:

[6] Ibid.

- Data protection wherever the data resides (data in flight, data at rest, or data in use).
- Secure virtualization capabilities that can wrap legacy workloads in secure containers to help meet compliance goals.
- Trusted state features that verify the BIOS/firmware is unmodified before allowing system boot.

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.

How Hardware Security From AMD Can Help

As AI and new applications evolve, the amount of data used and shared across technologies continues to grow. In response, AMD has prioritized security across its commercial product portfolio through deeply integrated, robust, and efficient security capabilities built into the CPU level. For example, AMD CPUs enable confidential computing for both data centers and client devices. This technology encrypts data in use at the memory level, protecting it even if compromised. Additionally, AMD's server and client CPUs share many security features, including:

- **Secure Processor.** A dedicated security processor validates code before execution and checks for data and application integrity. This processor forms the foundation of AMD's security architecture, acting as a root of trust anchored in hardware.
- **Shadow Stack.** This helps protect against attacks that try to hijack an application's control flow, such as return-oriented programming (ROP) attacks, by maintaining a separate copy of return addresses and triggering alerts on mismatches. On desktops and laptops, Shadow Stack is integrated with Microsoft Hardware-enforced Stack Protection in Windows 11, helping enhance the overall security of PCs**.**
- **Secure Boot.** AMD's Secure Boot technology helps defend against firmware-level threats by establishing a chain of trust from the silicon to the BIOS and the operating system. This feature extends the AMD silicon root of trust to the BIOS and helps confirm that only authenticated firmware is executed. UEFI Secure Boot continues this chain of trust from the system BIOS to the OS boot loader, which helps protect against remote attackers attempting to embed malware into firmware.

Additionally, AMD has built hardware-based security features specifically for their respective server and desktop CPU product lines.

Server CPU Security

For servers and cloud instances, AMD Infinity Guard delivers hardware-based security features embedded at the silicon level that help protect data hosted on premises or in the cloud. On AMD-powered cloud instances, these features combine to help protect the data both from external threats and those that might originate from within the CSP. These features, outlined below, build upon the common features listed above, forming the basis of confidential computing.

- **Transparent secure memory encryption (TSME).** System memory is encrypted using a 128-bit AES key, protecting data in RAM from unauthorized access and helps mitigate risks like cold boot attacks. This happens transparently and without modification to existing applications, which can help secure apps that lack inherent memory security.
- **Secure encrypted virtualization (SEV).** This capability enhances TSME by offering encryption per virtual machine, isolating VMs from each other and the hypervisor, which is especially beneficial in multi-tenant cloud environments.
- **SEV-Encrypted State (SEV-ES).** This feature encrypts CPU registers of non-running VMs, helping prevent sensitive information leakage from data at rest and maintaining data integrity before the VM resumes.

- **SEV-Secure Nested Paging (SEV-SNP).** This adds memory integrity protection, helping prevent hypervisor-based attacks like data replay and memory remapping.

These layered security measures provide a comprehensive defense against a wide range of threats to help mitigate against common attacks even in the most demanding environments. By integrating these hardware-based security features, AMD EPYC processors 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 additional multilayered security features on AMD Ryzen™ PRO and AMD Ryzen™ Threadripper™ PRO CPUs, including:

- **Memory Guard.** This feature delivers real-time encryption of system memory, helping to defend against physical attacks. If a laptop is lost or stolen, Memory Guard ensures that sensitive data stored in RAM remains encrypted and secure.
- **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 certification means that AMD processors meet stringent security requirements, providing confidence in their cryptographic capabilities.

AMD built these security features to work seamlessly with legacy and new software without requiring modifications, 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

As organizations look to manage the complexity of their IT environments, leveraging hardware-based security features becomes increasingly crucial. AMD helps with this by building robust security capabilities directly into their CPUs that can prevent attacks before they happen. This multilayered defense strategy not only increases security but can reduce dependency on other tools and platforms that are overwhelming IT and security operations teams.

AMD collaborates with ecosystem partners at both the software and system levels to enhance security across data center and endpoint solutions. For client systems, AMD is expanding its security services, including the integration of on-chip AI/ML inference engines, to provide consistent, best-in-class security features across all PC types. This hardware-based security, coupled with close collaboration with OS, OEM, and ISV partners, helps organizations deploy a multilayered set of security features that defend against sophisticated attacks, both now and in the future. This proactive approach improves the time to value for any hardware investment and can add much-needed security around workloads that are critical to the business.

AMD's dedication to security innovation and collaboration makes it an excellent option in any organization's comprehensive security strategy, providing the tools needed to safeguard data and maintain trust in an increasingly complex digital landscape.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com