White Paper, sponsored by Dell Technologies and Advanced Micro Devices

Cyber-Resilient Infrastructure Starts with Server Security

RESEARCH BY:

Heather West, PhD
Senior Research Analyst, Infrastructure Systems, Platforms and Technologies Group, IDC

Ashish Nadkarni
Group Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Kuba Stolarski
Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

January 2023 | IDC #US49954422

Table of Contents

Click on titles or page numbers to navigate to each section.

IDC Opinion

In the digital-first era, firms employ a technology-based business strategy that underpins all aspects of their business, be it the way they engage with customers or the way they operate their business. This technology strategy enables firms to reinvent themselves, create or extend their market differentiation, and future-proof their business. Businesses that embark on digital transformation initiatives glean rich insights from data, which itself is considered the lifeblood of the digital economy. These insights enable businesses to make faster and more informed decisions, to create competitive advantage through new products and services, to improve customer experience, and to increase operational efficiencies. A modern IT infrastructure serves as the foundation upon which businesses can ensure the timely use of data.

In any IT infrastructure — especially one that supports digital transformation for firms not born in the digital age — legacy systems and dated operating models are pervasive and challenging to maintain. Approaches to security are often pieced together. Such systems can hinder strategic transformation initiatives and objectives.

With cyberthreats looming large, businesses cannot take infrastructure security for granted. Ad hoc approaches are not just limiting — they can also be dangerous. The infrastructure hosts the data businesses rely on. Further, this data can include sensitive information and be part of the firm’s intellectual property. The security of infrastructure, and specifically that of compute (server) and storage hardware, is therefore as important today as that of applications and networks. With so much focus on the latter, infrastructure security often gets ignored.

A firm's cyber-resiliency strategy must therefore include the modernization of its infrastructure, automating IT service delivery, transforming IT operations, and taking active measures to maintain the security, integrity, and availability of the hardware and software assets that host business-critical data. IT organizations must focus on updating or closing the knowledge gap by partnering with trusted vendors to ensure that their infrastructure is secure and compliant.

The era of hardware-based — and specifically processor-based — security is finally here. Approaches offered by Advanced Micro Devices (AMD) in its EPYC line of datacenter processors enable IT organizations to encrypt data in use in addition to data in flight and data at rest. Dell offers AMD's EPYC line of x86-based processors in its PowerEdge line of servers, enabling organizations to benefit from complete hardware-based security without the need to make any changes to their workloads. Furthermore, AMD EPYC processors are highly capable, thus allowing IT organizations to reduce their compute footprint by way of workload consolidation.

Methodology

This white paper discusses the findings of a study commissioned by Dell Technologies and AMD. The study sought to investigate the continuing need for server security and the challenges organizations face in fully securing their servers. For its analysis, IDC relied on empirical data obtained via a web survey of 1,524 IT and line-of-business decision makers who represent IT departments with at least one function dedicated to cybersecurity and who have familiarity with the organization’s evaluation, management, and implementation of server security infrastructure. Additionally, IDC’s observations, insights, and recommendations are based on over six decades of research and intelligence on the IT infrastructure industry and markets. All monetary values are in U.S. dollars.

Situational Overview

To maintain competitive differentiation, businesses must be able to transform their revenue operations through data-driven decision making. Gaining actionable insights through data enables them to optimize business processes, decrease time to market for new products and services, better leverage research and development investments, and transform their customer engagement.

The key to this success is not only a company's ability to conduct timely data analysis of large, diverse data sets but also its ability to protect its intellectual property as well as sensitive customer data from leaking into the open. Further, when there are security breaches, the organization must be able to limit the exposure and bounce back to normalcy within its operational service-level objectives. In other words, the business must have a comprehensive cyber-resiliency structure in place that enables it to preemptively protect its data and infrastructure from a security breach or attack, swiftly detect an attack or breach once it occurs, and minimize interruptions and costs during the recovery process. To be cyber-resilient, organizations must continuously update and modernize their infrastructure and data security in the face of an ever-increasing number of internal and external IT threats.

So far, many of the cyber-resiliency mechanisms have focused on data in flight and data at rest; they have centered on protecting the networks that carry this data and the storage systems in which this data resides. Protecting data in use — which requires processor-based security features — completes the circle of trust, enabling businesses to build a tamper-proof, cyber-resilient infrastructure.

The Prevalence and Costs of Infrastructure Security Breaches

No organization is immune from an infrastructure or data security breach. While a small percentage (10%) of organizations do not acknowledge or realize that they have been the victim of a security breach, the majority (90%) report having been attacked by malware specifically (see *AI and Its Evolutionary Impact on Data Protection When Building a Future of Trust*, IDC #US48974722, May 2022). In many instances, an infrastructure security attack or breach (which can also include phishing, ransomware, accidental exposure of sensitive data, compromised insider threats, unsecured networks, SQL injections, and more) takes time to detect, due to challenges that hinder an IT department's ability to maintain the physical security of the system as well as software and firmware currency, monitor across all server components, and filter through multiple alarms to identify the most critical alerts. Such delays can significantly impact a business's bottom line: IDC found that over half (53%) of infrastructure security attacks and breaches result in an estimated 5.6 unplanned downtime incidents that affect about 15% of internal users and reduce productivity by 26% (see **Figure 1**). Overall, one of these revenue-impacting events results in an average loss of $37,000.

FIGURE 1

Organizational Impacts of Infrastructure Attacks and Breaches

Q: When infrastructure attacks and breaches occur, what impacts do these events have on the following items?

Average number of unplanned downtime incidents

5.6

Average percentage of internal users impacted by each incident

15%

Average productivity loss among impacted users

26%

Average revenue loss per incident

$37,000

Average percentage of incidents that are revenue impacting

53%

n = 914, Source: IDC's *Dell Technologies PowerEdge Server Security Survey,* July 2022

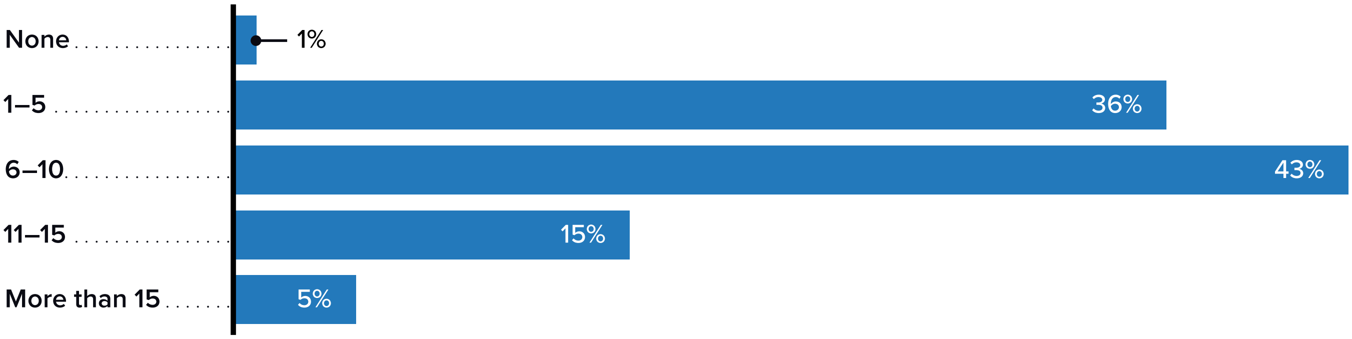
Making these events even more detrimental to an organization is the fact that these events tend not to be a one-time occurrence: 79.1% of organizations reported experiencing up to 10 infrastructure security attacks or breaches in the last 6 to 12 months, and another 20% reported being attacked 11 or more times (see **Figure 2**, next page).

FIGURE 2

Frequency of Organizational Infrastructure Security Attacks or Breaches Within the Last 6 to 12 Months

(% of respondents)

Q: In the last 6 to 12 months, approximately how many infrastructure security attacks or breaches has your organization experienced?



n = 914, Source: IDC's *Dell Technologies PowerEdge Server Security Survey*, July 2022

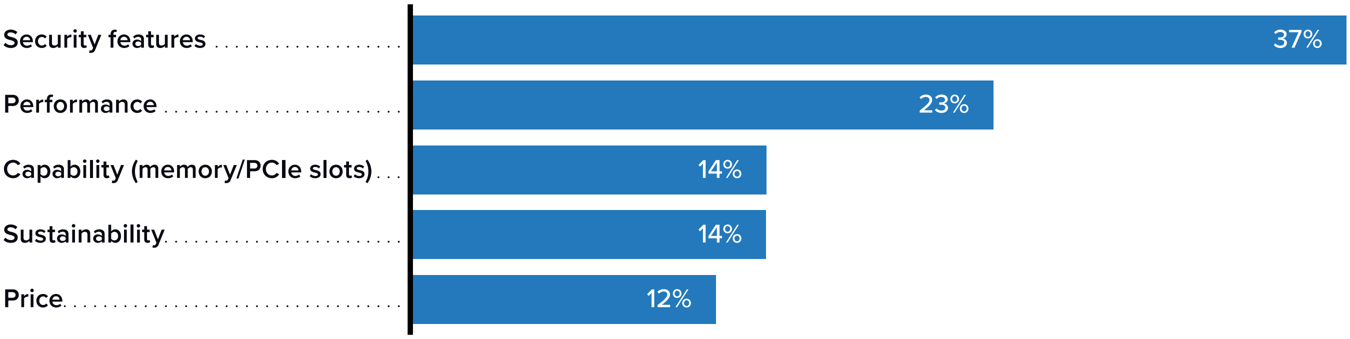
Most organizations understand the importance of implementing infrastructure security, as security features are the number 1 most important feature organizations consider when procuring servers (see **Figure 3**). Consequently, almost all organizations (85.9%) prioritize these investments, with almost three-quarters (72%) of IT spend being allocated to infrastructure security (35%) and data security (37%), an amount that is expected to increase. Further, organizations reported a willingness to pay a premium for server hardware that meets their organization's security requirements.

FIGURE 3

The Top Server Features Organizations Consider During the Server Procurement Process

(% of respondents)

Q: In order of importance, please select and rank the top 3 server features that your organization considers during the server procurement process. (% respondents answering "the most important")



n = 1,524, Source: IDC's *Dell Technologies PowerEdge Server Security Survey*, July 2022

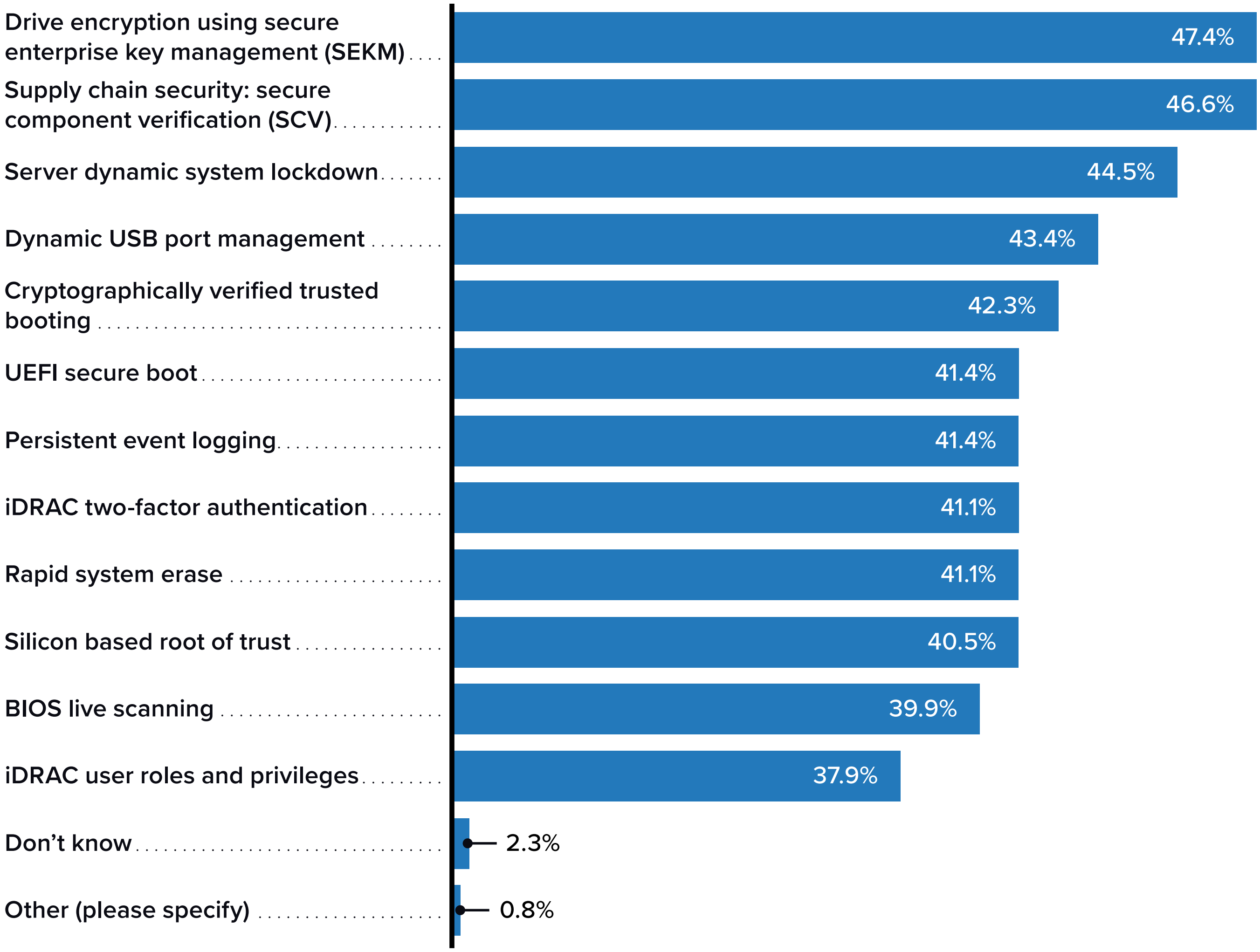
However, despite a financial commitment to being cyber-resilient, many IT decision makers are often unaware or fail to take advantage of the cyber-resiliency architecture employed by leading server vendors. For example, less than half of current Dell customers reported that they currently or plan to take advantage of any one of the OEM's server security features (see **Figure 4**) and therefore are or will be more likely to see improvements in application security, the ability to keep server and application software updated, physical security, and more. Consequently, CIOs and enterprise architects need to view infrastructure and data security as strategic investments that can assure the security of data and intellectual property at the infrastructure hardware and software layer by delivering a secure infrastructure foundation with built-in security at the processor layer.

FIGURE 4

Server Security Capabilities of Which Dell Customers Currently Take Advantage

(% of respondents)

Q: Which of the following server capabilities does your organization currently take advantage of? Plan to take advantage of in the future? (Check all that apply)



n = 914, Source: IDC's *Dell Technologies PowerEdge Server Security Survey*, July 2022

Key Pillars of Infrastructure Security

Implementing and managing infrastructure security is a complex task and requires the IT organization to hold itself accountable for ensuring that the firm's digital assets are secured. Using a simple Protect-Detect-Recover framework, based on the recommendations of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), IT organizations can build a secure infrastructure and maintain its integrity by incorporating these key areas of server security into the "people, process, and technology" fabric of the IT organization:

- **Physical security:** This involves the physical protection of IT assets and deployment locations. With the shift to a core-edge model for distributed IT, the physical security of the datacenter is not the only thing that matters; the physical security of edge locations (which could include remote and branch offices, retail locations, manufacturing facilities, and point-of-presence locations) is equally important. This is especially true if these locations are in a "lights-out" location and in places where operator control is remote.
- **Platform security:** This includes the ability to protect data in use, data at rest, and data in flight. It starts at the lowest level (firmware and boot), working its way up into the operating environment or hypervisor and eventually the application stack. In highly virtualized environments — especially in hybrid cloud operating models — software security introduces additional complexity.
- **Application and data security:** The security of workloads (applications and their associated data sets) is the next pillar of infrastructure security. It requires ensuring application currency, that any software vulnerabilities are patched, and that any external attacks to steal data or code are rendered ineffective. Often, organizations address security considerations during application development and design and institute simulations to protect apps after they are deployed. Application security also includes procedures that identify or minimize security vulnerabilities.

Best Practices for Securing Your Server Infrastructure

IT organizations must ensure that infrastructure, and specifically server security, is an ongoing process-and-policy workflow, not an afterthought or a one-time activity. In the digital-first era, IT organizations have a fiduciary responsibility to their business and must secure the firm's IT infrastructure as part of their duties.

IDC recommends a simple Protect-Detect-Recover framework (based on NIST recommendations) that IT organizations can use to build a secure server infrastructure.

- To protect is to build security into all aspects of the infrastructure.
- To detect is to uncover any compromises as they occur.
- To recover is to return to a verified known good state within an operational recovery window.

IT organizations can maintain the integrity of server infrastructure by incorporating five key areas of server security into the "people, process, and technology" fabric of their organization:

- **Physical server security:** This involves protecting the physical server racks, enclosures, power supplies, components, and fabric interconnection from being intentionally tampered with, damaged, or altered.
- **Firmware and software security:** This includes the ability to efficiently conduct complex encryption and cryptographic algorithms to protect both server data and application data in storage devices attached to the server, and the ability to monitor changes made to firmware and software.
- **Attestation trust features:** These capabilities are built into the server using special-purpose processor features and cryptographic onboard elements. These provide a root of trust (preferably based on an immutable authentication element) that enables checking at start-up and at other points in the server life cycle, whether or not the server has been altered from its expected configuration. Administrators can set policies to take the server offline and send a notification of the error to IT staff. This ensures that the components of the system software stack (hypervisor, OS, applications) are aware that the underlying server can be trusted when the server is operational. This layer establishes the foundation of a chain of trust among servers and creates a trusted and secure distributed server platform.
- **Processor security:** The security and integrity of a server start with the selection of a processor in which cryptographic functions are performed more effectively and efficiently in hardware. Further, cryptographic functions should provide robust hardware instructions and functions that can be easily leveraged by application developers, including the Advanced Encryption Standard, Secure Hash Algorithms, and truly random number generators.
In looking to differentiate processors based on cryptographic features, their capabilities should entail not only the fundamental functions but also the enablement of those functions to be actively leveraged. For example, hardware support for memory encryption has become one such differentiating feature, providing system-level memory encryption and securely isolated/encrypted VMs. Such encryption support helps protect against malicious administrator type attacks, among others. As a result, the feature would be implemented at the OS and/or the hypervisor level. Additionally, support should be provided for platform devices such as network, storage, and graphics cards to access encrypted pages seamlessly through direct memory access (DMA).
- **Secure server management:** This is conducted using an embedded baseboard management controller to manage server firmware, software updates, and other operations for server security across the datacenter.

An effective way to deal with security-related organizational and infrastructure challenges is to move the organization toward IT automation. This makes large-scale asset management and auditing easier, automates routine activities (reducing the risk of human errors), and tags and identifies potential vulnerabilities (like out-of-date patches) before they become issues.
Any automation solution should include comprehensive application peformance indicators (APIs) and the ability to simplify complex tasks through software functionality.

Dell and AMD Value Proposition

AMD's Approach to Processor Security: EPYC Processor Architecture

AMD has built security into the core EPYC architecture and has enhanced it further in the second-generation EPYC processor. A dedicated encryption offload sub-processor provides encryption without any overhead on the processor or the software stack. Servers built with second-generation EPYC processors can take advantage of built-in security technologies such as secure root of trust, secure memory encryption, and secure encrypted virtualization.

- **Secure root of trust** creates a hardware root of trust, enabling only known/trusted code to be loaded and run through the Basic Input/Output System (BIOS) load, thus helping prevent the injection of malicious code prior to the loading of the operating environment. It is managed by a dedicated security processor (called the AMD Secure Processor, an integrated processor that sits alongside CPU cores). AMD says its security architecture makes AMD EPYC processors not susceptible to Foreshadow, Spoiler, Meltdown, and Lazy floating-point unit (FPU).

- **Secure memory encryption (SME)** protects data in use by encrypting the contents of the main system memory. SME is different from data-at-rest encryption at disk in that it also protects data in use — which is held in unencrypted memory by default. This situation can open the door to the snooping of sensitive data, passwords, and secret keys by unauthorized administrators or software or by hardware probes. Cold boot attacks can exacerbate this problem. SME is best utilized in situations where the server cannot be physically secured (like edge deployments) or in situations where unauthorized individuals can physically remove DIMMs or NVDIMMs from a server.

- **Secure encrypted virtualization (SEV/SEV2)** provides workload-to-hypervisor isolation with 509 unique keys per system. IDC considers SEV to be a new virtualization security paradigm designed for the cloud era — where virtual machines in a shared and multitenant environment have selective trust with the hypervisor and management layer of their host system. Initially, support for AMD SEV was limited to KVM-based hypervisors from vendors including Red Hat, SUSE, Canonical, and Oracle. In August 2019, VMware became the latest virtualization vendor to commit to offering full support for AMD's encryption stack in its flagship vSphere virtualization platform.

Both SME and SEV require no application software modifications. They require only the operating system and/or the hypervisor to be enabled.

Dell PowerEdge Security

Dell Technologies takes a comprehensive end-to-end approach to security. Dell's PowerEdge servers with AMD EPYC processors have featured robust security for several generations, including the use of silicon-based data security. This has been further strengthened in the latest generation of PowerEdge servers with a cryptographic hardware root of trust during the server boot process.

Dell builds security into every design step in response to the security threats faced in modern IT environments.

This includes incorporating security features into the hardware to prevent malicious attacks as well as developing, testing, and verifying the integrity of the firmware prior to installing it. Dell's security measures include the following:

- **Adhering to NIST cybersecurity guidelines,** which provide a standardized approach for delivering server security. For example, NIST-approved crypto techniques like the secure system erase enable the erasure of sensitive data securely and instantly.
- **Employing a cyber-resilient architecture,** based on three design goals:

Protect, which provides secure and granular access control, cryptographic authentication, and data protection at rest and in flight

Detect, which includes audit logging and secure alerting, intrusion detection, firmware drift detection, and software change detection

Recover, which includes BIOS and OS recovery, easy restore, and rapid response to new vulnerabilities

- **Incorporating silicon-based root-of-trust design,** which is based on immutable trust factors for the authentication of BIOS, iDRAC, and a secure-boot OS environment. A cryptographically signed firmware enforces a secure platform environment, while the iDRAC serves as an always-on vigilant security sentinel that can thwart cyberattacks.

- **Following a security development life cycle (SDL),** which requires implementing a rigorous six-step process that continuously integrates security-related software features into the product build cycle (i.e., the server supply chain). Through SDL, security features are developed and deployed as configuration, firmware, or software updates for the PowerEdge server installed base. Only duly authorized individuals or processes can modify the server itself by altering its firmware or software, or by changing its configuration or identity. This layer preserves the integrity of the server and firmware throughout the life cycle.
- **Assuring end-to-end supply chain integrity,** meaning the entire build environment — starting from the components through to the delivery of products to the end customer — is based on a chain of trust.

Dell also provides proactive updates and system recovery. This includes proactively patching firmware bugs or vulnerabilities, ensuring that updates are delivered and applied in a timely fashion, and providing a restore to a known good state when a system recovery is necessary.

Dell PowerEdge servers with AMD EPYC processors conform to key industry standards on cryptography and security and perform ongoing tracking and management of new vulnerabilities. Dell has implemented the security development life cycle process with security as a key element in every aspect of development, procurement, manufacturing, shipping, and support, resulting in a cyber-resilient architecture.

Benefits of Purchasing Dell PowerEdge Servers with AMD EPYC Processors

Survey respondents' initial decisions to procure Dell servers with AMD EPYC processors were less focused on security and more focused on factors such as performance (50%), technical support and services (44%), and system management tools (43%). However, after adopting Dell servers and taking advantage of Dell capabilities such as Enterprise Key Management (EKM) and cryptographically verified Trusted Booting, Secure Boot, and Dynamic System Lockdown (to name a few), more than a third of organizations experienced reductions in server security breaches (38%), earlier detection of security breaches (37%), and a quicker recovery to a known good state (35%). Further, customers that invested in Dell servers with AMD CPUs and took advantage of AMD capabilities such as SME, SEV, and Secure Encrypted Virtualization–Secure Nested Paging (SEV-SNP) reported reductions in server security breaches (37%), earlier detection of security breaches (36%), and a quicker recovery to a known good state (34%).

Essential Guidance for IT Buyers

End-to-end security is necessary for firms to protect themselves from data breaches, which can be extremely costly should they occur. When a breach does occur, detecting and recovering from it in a timely fashion is equally important. A secure infrastructure forms the foundational layer for end-to-end security. It starts with the choice of a server platform that has built-in security features with standards-based building blocks and is backed by a vendor that designs and develops these features with a secure development life cycle and extends supply chain security to third-party suppliers to ensure that its products are free of potential threat elements. Furthermore, firms should seek a vendor that provides technologies to their IT staff for efficient and secure ongoing server management. These important considerations should factor into the total-cost-of-ownership analysis during production purchasing decisions.

Here are the key objectives that firms must keep in mind when evaluating the capabilities of a vendor and its server portfolio:

- **Platform security:** Vendors must incorporate server security into the core architecture, not bolt it on. Add-on mechanisms hardly work and can in fact make a platform more vulnerable. The platform must be based on a cyber-resilient architecture and must provide granular (i.e., role-based) access control.
- **Service and support:** The vendor must have documented security standards and diligently follow security-related best practices. It must provide a monitoring solution that can detect malicious attacks on an "always-on" basis. Furthermore, it must provide mechanisms to protect against physical intrusion, such as chassis intrusion protection. In the event of a data breach, the vendor must help the firm recover quickly. Finally, the vendor must provide a mechanism to securely decommission servers.

A final comment: Not all servers and server vendors are the same. Firms must be wary when purchasing equipment from white-box server manufacturers. Several vendors have limited resources and do not invest heavily into resources for developing and managing firmware-level security; they instead rely on their partners or ODM clients to provide such functionality on their own. These vendors also lack the setup to meet the requirements of enterprise IT such as the ability to meet stringent service-level agreements for feature updates and bug fixes. They lack the systems or resources to prevent or respond to threats on their own. This means the vendor's ability to aid with post-incident recovery is limited at best. Buying servers from such vendors can expose firms and make their investments in servers more expensive overall.

Challenges and Opportunities for Dell Technologies and AMD

The level of trust that firms place in an infrastructure vendor is directly related to the vendor's ability to build and deliver a performant and secure server platform.

For a vendor, delivering a quality product means having the ability to:

- **Maintain a secure supply chain:** Verifying the authenticity of components or parts, procuring them from trusted suppliers, and physically securing the build environment, the system build process, and the process of shipping the system to the customer. Dell's cyber-resilient design uses a cryptographically trusted booting cycle and immutable silicon root of trust, starting at Dell's factory.
- **Build security into every design step:** Incorporating security features in the hardware to prevent malicious attacks as well as developing, testing, and verifying the integrity of the firmware prior to installing it. Dell's servers enable IT organizations to wipe all data securely and quickly from storage media, including hard drives, SSDs, and system memory, with System Erase.
- **Provide proactive updates and system recovery:** Proactively patching firmware bugs or vulnerabilities and ensuring that updates are delivered and applied in a timely fashion; when a system recovery is necessary, providing a restore to a known good state. Dell Repository Manager and Update Manager plug-ins automate driver, BIOS, firmware, and software updates. Dell also offers these updates via a public site without requiring any special support contract.

IT organizations are generally open to working with a vendor that expends the extra effort to make key influencers and buyers aware of the build integrity, and strongly affirm the need for individuals and teams involved in making or influencing purchasing decisions to be fully aware of the vendor's build process. Furthermore, firms hold vendors to high standards when it comes to the vendor's ability to protect (prevent), detect, and recover from security breaches. This is where the vendor's ability to stand behind its product with an equally competent services organization comes into play.

Maintaining a trusted roster of infrastructure vendors is a key practice in most modern IT organizations. Firms can add a vendor to this trusted list in return for the vendor's demonstrating consistent product and service quality. Firms can disqualify or change server vendors should the vendor fail to deliver on its commitments.

Examples that can lead firms to switch vendors include:

- Dissatisfaction with the quality of services and support, as well as inadequate or lacking security capabilities of the server platform
- Discovery of bugs in the security of the platform, a lack of or poor security features in the product, a lack of guarantees from the vendor on the integrity of its end-to-end build environment, and its inability to support security-related situations
- Security certification, a critical factor which could be the sole cause of vendor disqualification in some industries

Conclusion

In a digital economy, data is capital. Top-to-bottom and end-to-end security is important for firms to protect themselves from data breaches. When a breach does occur, detecting and recovering from it in a timely fashion is equally important.

IDC recommends that organizations take a security-focused approach when investing in the next wave of IT infrastructure. The focus of this investment must be on a workload-optimized, innovation-focused infrastructure platform or service from a trusted vendor. One-size-fits-all approaches to infrastructure platforms can put business outcomes at risk due to performance and scalability issues manifested by the inherent limitations of the platform. And by not upgrading in a timely manner, IT organizations put their business at risk due to the unreliability of aging infrastructure. Older or generic infrastructure platforms, which may be left open due to a lack of vendor support, are also vulnerable to data breaches.

Finally, firms with organizational readiness and robust security-related response mechanisms are better prepared to prevent or deal with infrastructure security breaches. With the right choice of processors to power their infrastructure, dedicated security teams, well-documented security-related handling and recovery processes, and strong relationships with their infrastructure vendor, firms are better prepared to keep their server infrastructure up-to-date, actively monitor for security breaches, and promptly recover to a known good state should a breach occur.

About the Analysts

Heather West, PhD

Senior Research Analyst, Infrastructure Systems, Platforms and Technologies Group, IDC

Heather West is a Senior Research Analyst within IDC's Enterprise Infrastructure practice. In this role, Heather contributes to semi-annual Server and Storage Workloads Trackers, primary market research, and custom data modelling.

More about Heather West

Ashish Nadkarni

Group Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Ashish Nadkarni is Group Vice President within IDC's Worldwide Infrastructure Practice. He leads a team of analysts who engage in delivering qualitative and quantitative research on computing, storage, and data management infrastructure platforms and technologies, via syndicated research programs (subscription services), data products (IDC Trackers), and custom engagements. Ashish's vision for his team is to take a holistic, forwarding-looking, and long-term view on emerging as well as established infrastructure-related areas in the datacenter, in the cloud, and at the edge. His core research starts with an objective assessment of heterogeneous, accelerated, fog, edge, and quantum computing architectures, silicon, memory, and data persistence technologies, composable and disaggregated systems, rackscale design, software-defined infrastructure, modern operating system environments, and physical, virtual, and cloud computing software. It is complemented by research on current and next-gen applications and workloads, vertical and industry-specific use cases, emerging storage and server form factors and deployment models, and upcoming IT vendors. Ashish also takes a keen interest in tracking the ongoing influence of open and open- source communities like OpenStack and Open Compute Project on infrastructure.

More about Ashish Nadkarni

Kuba Stolarski

Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Kuba Stolarski is a Research Vice President within IDC's Enterprise Infrastructure Practice focused on research in the computing platforms and cloud infrastructure space, including the Core and Edge Computing Platforms CIS, the Enterprise Infrastructure: Buyer and Cloud Deployment Tracker, and the Cloud Infrastructure Index. Kuba oversees the research for ODM infrastructure supply chain and contributes to IDC's research in topic areas such as workloads, virtualization, containers, and dedicated cloud infrastructure as a service. Kuba also oversees the global server forecast and is IDC's SME for the server market.

More about Kuba Stolarski

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc @idc idc.com