DELL Technologies AMD

Solution Brief

Controlling Security in an Out-of-Control World

Server Security with Dell EMC PowerEdge™ Servers Powered by AMD EPYC™ Processors

Being in business today requires sophisticated attention to detail where data and device security is concerned. Dell Technologies and AMD are building for today's multi-faceted threat landscape. This brief looks at some of the risks and how comprehensive hardware and software innovation helps organizations regain control without slowing down.

Contents

Good news and bad news 2

The new shape of risk and opportunity..................3

Memory is the new disk..4

The silicon layer..5

Across the server lifecycle....................................6

Building smarter (and more securely)....................7

Good news and bad news

We all know what we're up against. The technological ecosystem of hyperconvergence, virtual machines, and software-defined everything and anything-as-a-service is as appealing in its drive towards agility and adaptability as it is inescapable. But as businesses and the technologies that keep them competitive evolve, so do the threats they face. Determined enemies are increasingly aiming complex multistage attacks at the heart of the information economy.

Everything is turned on. Everything is connected. Everything is at risk, and the old perimeters we used to rely on aren't enough to hold off new threats. Until recently, white hats spent their time countering malware, viruses, denial of service attacks, and the like. These threats still exist, but today's world of complex connectivity also faces more sophisticated attacks—side channel, return-oriented programming (ROP), cold boot, and code injection, to name a few.

The bad news is that modernization is complicated and time-consuming, requiring organizations to secure and build out their infrastructure in real time, across a hybrid and multi-cloud world that's taking on new applications and workloads every day. It's hard work and requires both technical capacity and expertise to snap it all together and keep things humming.

The good news is that technology is always evolving and rising to the challenge. Dell Technologies built a line of servers powered by AMD processors that help organizations find that elusive sweet spot where speed and control come together, thanks to a full stack of innovative features enabled by Dell, AMD, Microsoft, and our respective ISV partners.

Built for moving forward, securely

The new security paradigm is dynamic, multilayered, and deep-seated. This is why a network of partners collaborated to embed server security into the stack at every layer, from silicon to end-user, integrating control from the chip up. The result is a fundamental transformation that gives you the power to build while in motion.

- From reactive to proactive
  As organizations learn they don't have to wait for a risk to turn into a breach, they can work to actively sense, scan, understand, and adapt in real-time. This requires broad visibility and the ability to quickly deploy resources and intelligence precisely to where they're needed.

- From rigid to resilient
  Traditional security requires that broken pieces be fixed before a problem can be solved. Resilience helps enable a self-healing, self-scaling network where security needn't compromise performance demands. With a modular architecture, carefully optimized building blocks of compute, storage, and network can be deployed with security already built in.

Dell and AMD: Proactive Resilience, at Your Service

Why are you building out your IT infrastructure, anyway? Typically, it's because your business is growing and changing, expanding, or adapting to new demands. Traditionally, IT has been forced into a false choice: performance or manageability. An integrated full-stack approach bringing together Dell Cyber Resilient Security and AMD Infinity Guard[1] innovations helps you move past false constraints, deploying server performance that's responsive while managing risk.

Dell EMC PowerEdge™ Servers Powered by AMD EPYC™ Processors

XE8545	C6525	R7525	R6525	R7515	R6515
Optimized for: • AI / ML / DL • HPC • vGPUs	*Optimized for:* • Industry Solutions • Data Analytics • HPC	*Optimized for:* • Data Analytics • All Flash SDS • VDI	*Optimized for:* • HPC • Dense VDI • Virtualization	*Optimized for:* • Data Analytics • Virtualization • SDS	*Optimized for:* • Virtualization • HCI • NFV

Platform-based security features:

Protect

- Silicon-based root of trust
- Secure Boot
- Digitally signed firmware packages
- Dynamic system lockdown
- Hard drive encryption and enterprise key management

Detect

- Drift detection
- Persistent event logging
- Audit logging and alerts
- Chassis intrusion detection

Recover

- Automated BIOS recovery
- Rapid OS recovery
- Firmware rollback
- Ability to wipe all data from storage media with Rapid System Erase

The new shape of risk and opportunity

The ultimate promise of information is action. If we know more, sooner, our reactions can be smarter and faster.

But working up from raw data to an actionable insight is hard, with each phase of the information lifecycle—collect, input, process, and output—posing its own unique performance demands. Each hand-off, each systems integration, complicates not just security but also performance. IT and business teams must work together to build new kinds of connections, especially for advanced tools such AI and ML platforms that require work to be done as close as possible to the information itself.

The result is a new paradigm for building and managing enterprise networks across modern hybrid multi-cloud infrastructure. But even as organizations work to abstract as much managerial complexity as possible into a single consolidated set of lenses and levers, they must be careful not to reduce the ability to address the following:

An escalating volume of threats

This rise is driven by both the larger attack vector created by a more dynamic, distributed workforce and the rise of sophisticated automated tools available to bad actors. Even as ransomware and other newer exploits are getting lots of attention, malware incidents were reported to be up nearly 358% in 2020[2] over the previous year.

Multiplying variety

As environments get more complex, so do threats, including supply chain and third-party vulnerabilities, ransomware, and other attacks on users, applications, and networks. AI-driven bot swarms and weaponized 5G show us that bad actors can take fast advantage of new innovations while the good actors are still learning to neutralize old threats.[3]

Exponential value of loss

As organizations work to manage the true cost of security breaches, the costs go beyond dollars and cents. In addition to lost revenue, downtime, and compliance fines, security problems can have a corrosive long-term effect on brand image as well as vendor and customer trust.

And it's not just data-intensive applications that are at risk. Today's inescapable cloud environment is home to many other mission-critical workloads that demand an intelligent balance of performance and security. High-performance computing, secure databases, and HCI/VDI—these and other hybrid workloads are often an organization's biggest opportunity for meaningful transformation. That can only happen, of course, if it's all kept secure.

Dell Technologies and AMD help protect data in the cloud—making sensitive data opaque to the cloud provider and to administrators with direct access to the server. Data is encrypted while it is being processed, isolating it from malicious users, the hypervisor, and even admins.

AN ELEVATED, INTEGRATED APPROACH TO DATA CENTER SECURITY

Dell EMC PowerEdge servers powered by AMD EPYC™ processors are designed to help organizations deliver secure breakthrough compute performance precisely where it's needed, in a manner that is proactive and resilient.

AMD INFINITY GUARD: BUILT-IN CAPABILITIES AGAINST INTERNAL AND EXTERNAL THREATS

Every AMD EPYC processor is built with security in mind. Starting at the silicon level, this keeps your data private, maintains system memory isolation from would-be snoopers, and provides strong protection against modern-day hacks.

Memory is the new disk: helping secure your information in the hybrid multi-cloud

While attacks on static customer information or credentials garner most of the media attention, attacks on server memory continue to rise. As memory becomes the new disk, unencrypted data-in-use is increasingly vulnerable to exploitation. This risk is even more complex as organizations try to secure in-memory computing across on-premises, virtualized, and cloud machines. PowerEdge servers featuring AMD EPYC processors support up to 4TB of system memory, and the capability to fully encrypt it, helping protect the thousands of files or millions of lines of code stored which you need to run your business.

Memory is no longer merely a resource—it's a place adversaries can target to seize valuable information using the new tactics, including ROP exploits. In return-oriented attacks, hackers take control of the call stack and use small chunks of legitimate code already in memory to manipulate the system. To defend themselves, businesses are building better security for data-in-use, with controls they can manage consistently no matter where data is being processed.

Locally, AMD Secure Memory Encryption (SME) helps keep information in memory (and in use) protected via a dedicated cryptographic security processor integrated into each AMD EPYC processor. Every AMD EPYC processor supports up to eight memory channels, and each memory channel has a 128-bit AES encryption engine embedded in the memory controller. This architecture supports security that doesn't get in the way of doing business—there is minimal impact on performance and no need to rewrite code.

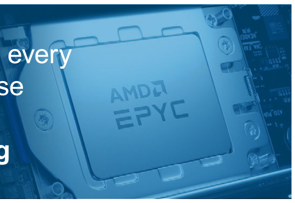
Extending security capabilities to cloud or virtual machines

For organizations processing information virtually or in the cloud, Secure Encrypted Virtualization (SEV) operates in a similar manner, with each virtual machine receiving a key that's also managed by the AMD Secure Processor.

As the need has emerged to secure workloads run in the cloud, a new paradigm has emerged, called **confidential computing**. It's a way to create a hardware-based trusted execution environment (TEE). PowerEdge servers featuring AMD EPYC processors are equipped to help support a trusted execution environment between the server and virtual or cloud machines. This is done by leveraging in-memory security controls across all environments, and by using SEV, which employs the same hardware root of trust to encrypt and manage up to 509 uniquely encrypted guest virtual machines.

Inside the base SEV features, there are two additional layers of security:

- SEV-Encrypted State (SEV-ES) helps add confidentiality and integrity protection for virtual machine registers by encrypting CPU register contents when a VM stops running. *Supported on AMD EPYC 7003 series and 7002 series processors.*
- SEV-Secure Nested Paging (SEV-SNP) adds yet another layer of protection by introducing memory integrity protection, helping to defend against a malicious hypervisor attempting to hijack virtualized or cloud workloads. *Supported only on AMD EPYC 7003 series processors.*



> “AMD EPYC™ processors are designed with security in mind, and with AMD Infinity Guard on every AMD EPYC processor, customers get a set of modern security features that can help decrease potential attack surfaces as software is booted, executed, and processes critical data.”
> **—Raghu Nambiar, AMD Corp VP of Datacenter Ecosystems & Application Engineering**

No compromise on performance

In a world where speed matters, security has traditionally been seen as a drag on performance. It can be a tricky trade-off, particularly for workloads optimized for performance. AMD EPYC processors help deliver both performance and strong security features—with both SME and SEV enabled on a PowerEdge™ R6525 server, a study showed the impact on OLTP database performance was negligible.[4]

Added layer of security: AMD Shadow Stack

AMD Shadow Stack gives servers hardware-based capabilities against software exploits like control-flow and ROP attacks. By validating a running program stack against a copy already stored in hardware, the AMD Shadow Stack helps organizations block attacks that use the control-flow hijacking tactic or ROP exploits. *Supported only on AMD EPYC 7003 series processors.*

DELL TECHNOLOGIES: CYBER RESILIENT SECURITY

Dell Technologies takes a layered approach to server security, with a Cyber Resilient Architecture that integrates strong defenses at every stage of platform development. Chip-level security features combined with critical controls help organizations safeguard their most important assets.

The silicon layer: Dell’s expanding root of trust

Dell EMC PowerEdge servers were first to implement an immutable, silicon-based root of trust to help validate the integrity of firmware or code being executed. It’s the initial, and probably most important, line of defense against spoiled or compromised code. If the root of trust detects a problem, notifications are made, and BIOS recovery begins.

While most attempted security breaches are software exploits, advanced attackers can target silicon in an effort to end-run critical BIOS and firmware controls. Dell and AMD are innovators in hardware-driven security features, and that intrinsic product leadership continues with the current line of PowerEdge servers powered by AMD EPYC processors.

Available Dell server features such as BIOS Live Scanning (which verifies the authenticity of the BIOS image in the primary ROM) and UEFI Secure Boot Customization (which prevents untrusted UEFI devices from being loaded) help protect your data and devices, from the moment you boot up.

Beyond the BIOS

Beyond the first critical hardware check, Dell has expanded the hardware root of trust with UEFI Secure Boot for PowerEdge servers. A customizable, certificate-based process verifies the cryptographic signature beyond the BIOS, including PCIe cards, mass storage devices, and other OS boot loaders. PowerEdge servers also validate firmware signatures in accordance with NIST SP800-147B guidance.

TPM (Trusted Platform Module) can be leveraged for cryptographic functions; generating, managing, and storing keys; and attestation. iDRAC (Integrated Dell Remote Access Controller) not only streamlines server management but also provides security features such as a Credential Vault of user credentials and private keys.

The data layer: protecting your most critical asset

Once we know we can trust the hardware and we've verified it hasn't been tampered with or reconfigured, it's time to solve for data-at-rest security on the device.

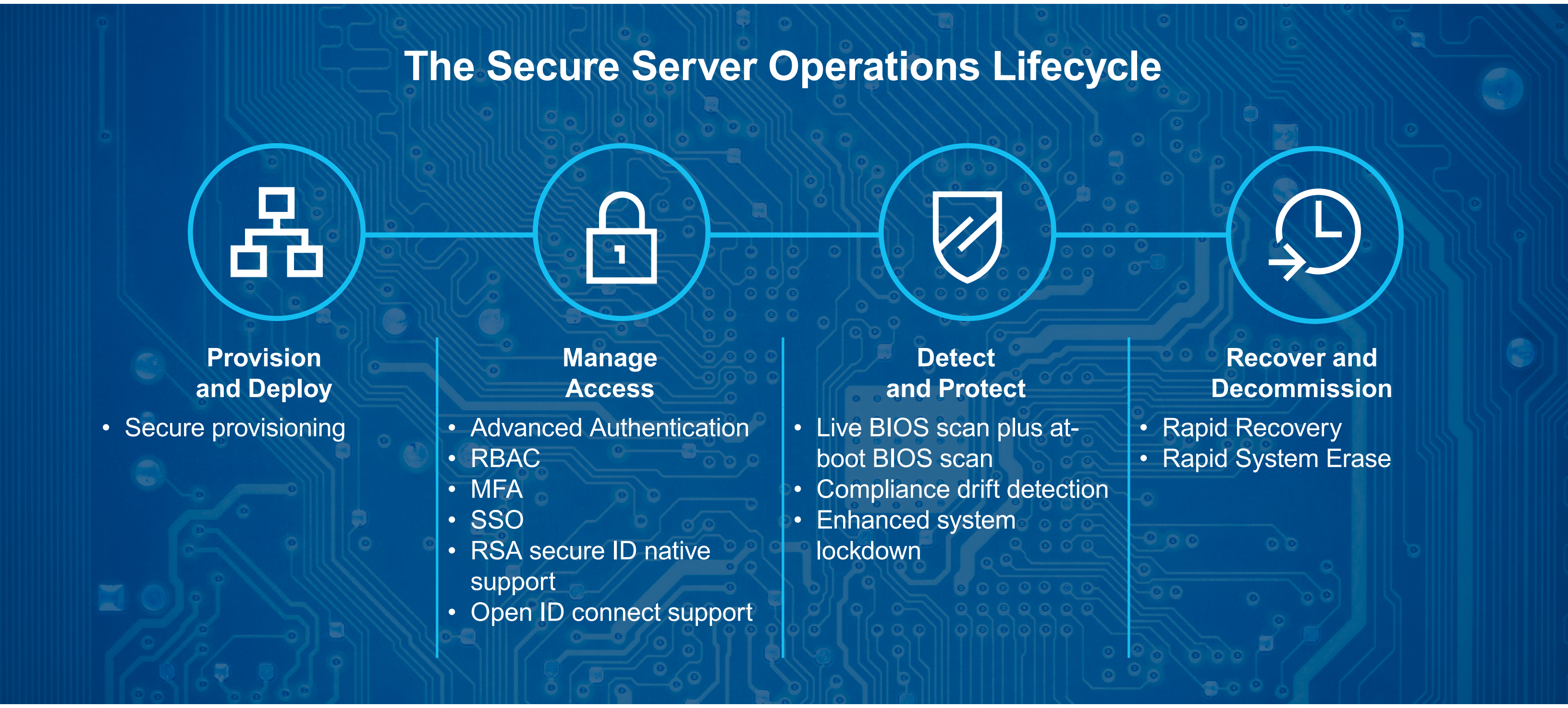
Dell EMC PowerEdge™ servers with AMD EPYC™ processors support the use of self-encrypting drives (SEDs) to help automatically encrypt data-at-rest, in the background, with no user intervention. This enables teams to deploy storage into an environment as needed without having to encrypt the drive first. SEDs also enable two other important Dell security features: Rapid System Erase, which enables you to irrevocably wipe data, and Secure DAR (data at rest), which locks the drive if it's lost or misplaced.

The final piece here is the OpenManage Secure Enterprise Key, which helps organizations centralize the building, managing, and monitoring of the cryptographic keys used to secure data. It's built around industry best practice and open standards, and it's a solution that evolves along with the technology and risk landscape.

Across the server lifecycle: secure, automated operations and administration

Protecting servers from external threats is only half the fight. Compliance and security best practices require that server access and administration are tightly controlled. The most effective way to accomplish this is via clear, consistent, policy-driven protocols. The ability to automate this provisioning and configuration not only saves time, but it also reduces the chance of errors or accidental noncompliance.

The Dell OpenManage suite gives organizations smarter, simpler tools for securing server operations and administration. The platform strengthens internal security by restricting access and strengthening authentication, as well as automatically scanning for changes to the configuration validation in the original root of trust.



The Secure Server Operations Lifecycle

Provision and Deploy
- Secure provisioning

Manage Access
- Advanced Authentication
- RBAC
- MFA
- SSO
- RSA secure ID native support
- Open ID connect support

Detect and Protect
- Live BIOS scan plus at-boot BIOS scan
- Compliance drift detection
- Enhanced system lockdown

Recover and Decommission
- Rapid Recovery
- Rapid System Erase

Provisioning and deploying

OpenManage automates the server provisioning, giving teams a centralized, integrated console for deploying, monitoring, and updating servers. The ability to drive access via policy from provisioning onward strengthens server security across the rest of the lifecycle.

Managing access

Authentication and access control are essential to security, so OpenManage gives users more options for embracing stronger multifactor authentication right out of the box. Organizations can leverage leading 2FA standards (including RSA Secure ID and Open ID Connect) and support for role-based access control (RBAC).

Detecting and protecting

Once servers are configured, Dell OpenManage Compliance Drift Detection automates the hard work of finding and remediating configuration across firmware and hardware. When errors are found, notifications are sent with remediation next steps, and embedded reporting creates shared visibility and continuous compliance at scale. Additionally, Dell EMC OpenManage Ansible Modules help IT teams automate threat hunting and incident response.

Some organizations may also choose the stronger protection of Enhanced System Lockdown, which guards against unauthorized configuration changes while still allowing critical operational features to be performed.

Recovering from attack

Organizations can leverage Dell Rapid Recovery to quickly bounce back with minimal business downtime or disruption. This gives IT teams the ability to automate BIOS and OS recovery on an impacted server, and rollback firmware when vulnerabilities are detected.

If the system detects that server drives have been compromised, Dell Rapid System Erase lets organizations permanently erase all the data on an encryption-capable physical disk. This instantaneously deletes all data from the drive to keep it out of the hands of attackers. It can also be used to sanitize a disk for decommissioning.

Building smarter (and more securely)

Businesses need a technology supply chain they can trust. That means finding partners who carefully vet and validate their own vendors, and who can demonstrate they've found meaningful ways to inject a security mindset deep into every aspect of their business—starting with the basics, like physical location and workforce security, and extending to how solutions are ideated and executed.

For Dell Technologies and AMD, this means orchestrating product development lifecycles, with security in mind, from platform design through manufacturing and QA and validation. This includes third-party audits and testing of both code and hardware. We also work with independent labs as well as internal research teams to evaluate the performance and security of our products once manufactured.

Secure Component Verification

The manufacturing and distribution processes must be similarly guarded. Dell and AMD implement careful inventory and parts control, including the use of component UIDs and specialized anti-tampering packaging to protect devices in transit. Using Dell Technologies Secure Component Verification, customers can verify cryptographically that every server they receive is exactly what was ordered, configured, and shipped. Additionally, Dell Technologies maintains ISO 9001 certification for all global manufacturing sites, minimizing the risk of counterfeiting.

Reacting faster (and at scale)

Dell Technologies and AMD are committed to proactively responding to new threats and challenges as they emerge, and helping our customers do the same.

> "Security is the foundation of everything we do, and our intrinsic security approach addresses our customers' need for trusted technology and partners to help them fend off attacks and lower business risk."
> **—John Roese, Dell Technologies Global CTO**

Impatiently (and painstakingly) innovating

Even as Dell and AMD work with today's virtualization and cloud leaders, we're also working to extend our approach to reducing attack surfaces of a server with minimal impact to productivity of the newest applications and workloads. Increasingly, this means optimizing our solutions for a world that builds and runs software differently, especially with the rise of Kubernetes and related orchestration tools.

Superior network intelligence

No matter your DevOps flavor, Dell EMC PowerEdge™ servers with AMD EPYC™ processors can generate and stream powerful data via iDRAC telemetry. Data can be shared to subscribed external clients or applications as required by IT or compliance teams. This flexibility helps extend automated management capabilities to physical servers across an organization, not just software deployments.

A bolder, future-ready way to run workloads

The data center has historically been a field of compromise. Density versus distribution, speed versus control, availability versus security, performance versus manageability. As we move into the second decade of mainstream cloud computing, we continue to see critical workloads and infrastructure services fluidly move between data centers and networks in response to business demands.

With the rise of edge computing and the unfolding promise of 5G, the future continues to evolve. Likely, we will continue to virtualize more and more of the applications and services that keep business engines running. It used to be that virtualization required sacrificing one of the three levers of optimization: scale, performance, or security. Dell Technologies and AMD are building technology for a world where businesses can dream and build beyond compromise.

Performance leadership with 3rd Gen AMD EPYC processors	Proven server dominance with Dell PowerEdge based on 3rd Gen AMD EPYC processors
• World's highest-performing server processor[5] • Best hyperscale density: 42% more throughput in the cloud vs. the competition[6] • Accelerated computing: 33% faster HPC performance vs. the competition[7] • Boosting enterprise productivity: 112% more simultaneous active VDI sessions vs. the competition[8]	• World-record benchmarks across critical modern workloads including big data, virtualization, IoT gateways, sales/distribution for SAP, Hadoop, VM environment[9] • Robust selection of validated designs including ready-made configurations optimized for compute-heavy workloads, vSAN Ready Nodes, VxRail, and more[10]

Learn more about how Dell EMC PowerEdge servers optimized for AMD EPYC processors can help secure your organization.

Explore AMD Infinity Guard—a modern, multi-faceted approach to data center security.

Contact a Dell Technologies Expert.

[1] AMD Infinity Guard features vary by AMD EPYC processor generations. Infinity Guard security features must be enabled by server OEMs and/or Cloud Service Providers to operate. Check with your OEM or provider to confirm support of these features. Learn more about Infinity Guard at https://www.amd.com/en/technologies/infinity-guard.

[2] Brooks, C. “Alarming Cybersecurity Stats: What You Need To Know For 2021.” Forbes.com, March 2, 2021.

[3] Hurst, A. “What are the newest cyber attacks to look out for?” Information Age. February 11, 2020.

[4] Principled Technologies, “The science behind the report: Enabling two security features on 3rd Gen AMD EPYC processors minimally affected OLTP performance on a Dell EMC PowerEdge R6525 system.” March, 2021.

[5] AMD EPYC™ Family of Processors Claim Information: MLN-016B

[6] AMD EPYC™ Family of Processors Claim Information: MLN-088B

[7] AMD EPYC™ Family of Processors Claim Information: MLN-086B

[8] AMD EPYC™ Family of Processors Claim Information: MLN-004

[9] https://www.delltechnologies.com/resources/en-us/asset/tech-notes/products/servers/direct-from-development-key-benchmarks.pdf

[10] https://www.delltechnologies.com/en-us/servers/amd.htm