DELL Technologies

AMD
together we advance_

Whitepaper

Securing the Digital Frontier: Inside Dell and AMD's Zero Trust Approach

Protect Your Organization with Dell and AMD's End-to-End Security

Table of contents

Introduction

The devices that connect us make incredible things possible, but these connections also provide additional points of vulnerability that malicious actors can exploit. In fact, some estimates predict that cyber attacks will cost organizations as much as $10.5 trillion USD by 2025.[1] And according to one estimate, recovering from the damage of a cyber attack takes about 277 days.[2]

While newer tech such as artificial intelligence (AI) offers improvements in productivity and business operations for many organizations, it also leaves data vulnerable to more sophisticated cyber attacks. With each advancement in technology, tech industry leaders must shift strategies to effectively counter cyber criminals as they find new ways to attain and exploit data. To thwart these threats and keep data safe, every data center component—from servers and storage to networks, software, and firmware–needs built-in protection. Protection starts with supply chain tampering mitigations on the manufacturing floor and continues through the transportation process and customer use. And attacks no longer stop at the data center walls. Organizations with a presence in the cloud face additional challenges in keeping data secure.

Together, Dell and AMD provide a purpose-built cyber resilient architecture that helps organizations adopt a Zero Trust strategy, embracing the idea that system components are vulnerable at each link in the chain and offering protection at every point. A Zero Trust strategy uses strong, identity-based policies for every IT asset along with "least privilege" principles for access. Dell Cyber Resilient Architecture includes in-depth features centered around boot integrity and data protection as well as security features in Integrated Dell Remote Access Controller (iDRAC). Dell PowerEdge servers are anchored with a silicon-based Root of Trust (RoT) that establishes a chain of trust for cryptographic verification of hardware and software components on the server. AMD Infinity Guard provides an additional layer of security that decreases the potential of attack during software boot and execution. AMD Infinity Guard encompasses several additional security features, including Platform Secure Boot and Platform Secure Processor, that ensure PowerEdge servers are protected at each stage in their lifecycle.

Dell Cyber Resilient Architecture

Dell Cyber Resilient Architecture utilizes PowerEdge security features that work in concert to provide both resiliency and enable a zero trust strategy. Security features must protect against potential threats, detect suspicious activity, and recover quickly in case of a breach. At the same time, they must also maintain a "verify before trust" posture for a zero trust approach of least privilege, where users and devices are given access only to what they need to perform their tasks. By working together, these PowerEdge security controls provide a comprehensive security solution that ensures resiliency while enforcing a zero trust posture. For more details on the full Dell Cyber Resilient Architecture features and services, see the whitepaper.

Ensuring Boot Integrity

The pre-boot environment it often overlooked and, if safeguards aren't taken, could be open to attack. If a malicious actor compromises the BIOS, firmware, or a driver during boot, they could potentially obtain access to the entire system. Without the proper controls in place, they could successfully infiltrate the system at any point and reach their desired target: your data.

To mitigate vulnerabilities, the server vendor must protect the BIOS, but also verify and validate specific server components and firmware such as memory and processors. Server hardware manufacturers must ensure that their components integrate fully with the server architecture for security and validation checks to work seamlessly. Every Dell PowerEdge server offers multiple layers of security to protect the boot cycle: a silicon-based RoT, UEFI Secure Boot, and iDRAC security features, including Firmware Rollback and Rapid Operating System Recovery.

On top of these Dell PowerEdge server-based security layers, AMD processors feature Platform Secure Boot (PSB) and Platform Security Processor (PSP) to protect data in use. Combined, Dell and AMD cover every aspect of the boot cycle to ensure a secure foundation for your data and workloads.

[1] Chuck Brooks, "Cybersecurity Trends & Statistics For 2023; What You Need to Know," accessed December 4, 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=9885ce219dba.

[2] Ken Kizzee, "Cyber Attack Statistics to Know," accessed December 19, 2023,https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC and Root of Trust

The RoT concept assumes that if a system verifies a foundation or baseline as safe, then all subsequent validations and security checks are anchored in a continuous chain of trust. Imagine a house: If the foundation is unstable and beginning to crumble, the integrity of the wall supports matters little. Similarly, if your server's BIOS is compromised, protecting the server OS may be in vain.

The PowerEdge server chain of trust provides a seamless cryptographic verification across all server components from foundation to data. This ensures that the components of the system software stack (hypervisor, OS, applications) are aware that they can trust the underlying server when the server is operational. This layer establishes the foundation of a chain of trust within a server and creates a trusted and secure server platform. Dell servers use a unique silicon-based RoT burned into each server for cryptographic verification that ensures secure booting on every cold boot or A/C cycle. Starting with version 4.10.10.10, iDRAC provides an RoT mechanism to verify the BIOS image at boot and will not allow the server to boot until it verifies the BIOS image. For PowerEdge servers with AMD processors, integrated Dell Remote Access Controller (iDRAC) leverages AMD PSB technology to verify the BIOS code before the OS loads. AMD PSB scrutinizes the BIOS integrity, interfacing with the primary BIOS ROM and AMD fusion controller hub (FCH) for thorough RoT processing. This meticulous validation extends up to the OS bootloader, guaranteeing a continuous chain of trust.

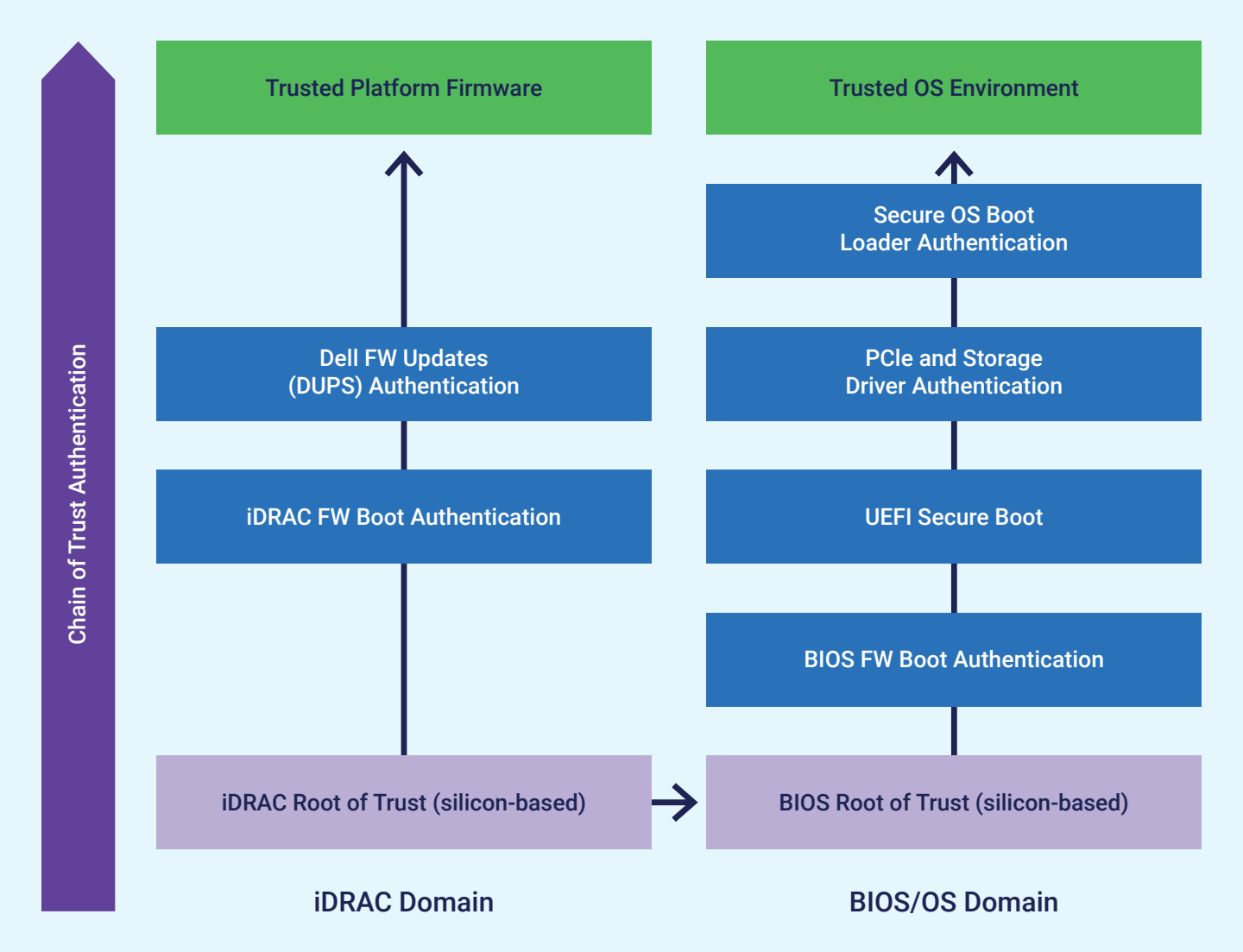

Figure 1: Silicon-based Root of Trust Domains in PowerEdge Servers with iDRAC9.

Should BIOS validation fail, iDRAC immediately shuts down the server and notifies the user, preventing the booting of unauthorized firmware. iDRAC also includes a backup and recovery system for BIOS and iDRAC firmware, which reinforces server reliability and safeguards server operations against potential firmware corruption. To provide additional protection, iDRAC also offers a live BIOS scan that users can run on demand or schedule to run regularly. This scan requires the iDRAC Datacenter license and allows users to catch potential issues before they reboot, allowing proactive mitigation.[3]

UEFI Secure Boot

Dell PowerEdge servers use the industry-standard UEFI Secure Boot to validate operating system-specific bootloaders, ensuring the integrity of the OS kernel and other critical components. UEFI acts as a shield from malware and ransomware in pre-boot environments. To ensure interoperability, both server and component manufacturers need to collaborate to ensure that the UEFI-enabled BIOS recognizes driver and firmware signatures for components. By validating cryptographic signatures of UEFI drivers and other pre-OS code, UEFI Secure Boot endeavors to ensure that any code loaded during boot is free of malicious content.

To heighten security customization, administrators can configure custom OS bootloader signing certificates for UEFI Secure Boot. (To learn more about UEFI Secure Boot Customization options, visit https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats.) This restricts execution to trusted secure OS bootloaders, which uphold the secure boot chain by authenticating the OS kernel and filesystem. This feature provides additional flexibility, particularly for Linux administrators who prefer to sign their own OS bootloaders rather than depend on third-party default UEFI Certificate Authorities. Administrators can upload custom certificates through the iDRAC API, enhancing authentication of their specific OS bootloaders. Uniquely, Dell PowerEdge servers support complete customization of Secure Boot, including the option to remove all standard certificates from Microsoft, VMware, or UEFI CA.[4]

CPLD Validation

Every Dell PowerEdge server validates the Complex Programmable Logic Device (CPLD) on every A/C boot. CPLD, a versatile programmable logic device,[5] comprises multiple simple PLDs connected by a programmable switching matrix. Its firmware, typically stored in EEPROM, flash memory, or SRAM, enables modifications to system board functions beyond BIOS capabilities, including the implementation of specific logic for system board device interactions. CPLD Validation ensures that system board modifications will not harm your servers or your data.

iDRAC Hardware Security

Extending the chain of trust to additional hardware components, iDRAC uses the Security Protocol and Data Model (SPDM), which standardizes how servers gather information about their components. Each component's identity, firmware, and configuration information is encrypted. iDRAC hardware security uses authenticated key exchanges to secure lines of communication between components and iDRAC. With SPDM, iDRAC can authenticate the validity of components such as PowerEdge RAID Controllers (PERC)12 and network interface cards (NICs), which not only enhances server security by authenticating components' Device Identity certificates, but also alerts users to any authentication failures.

[3] Dell, "Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning," accessed December 19, 2023, https://dl.dell.com/manuals/common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf.

[4] Dell, "Cyber Resilient Security in Dell PowerEdge Servers," accessed December 4, 2023, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

[5] Technopedia, "Complex Programmable Logic Device," accessed December 4, 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

AMD processors feature AMD Platform Secure Boot (PSB) to help counteract another growing concern in today's digital landscape: firmware-level threats. PSB leverages the AMD silicon RoT and verifies the boot process from the BIOS code to the OS Bootloader through UEFI secure boot.[6] Dell uses AMD PSB-enabled motherboards to permit only their cryptographically signed BIOS code to run. Additionally, Dell binds each AMD processor to a specific motherboard with one-time-programmable fuses that tie the processor to the Dell firmware code signing keys.[7] To protect against attacks aimed at embedding malware into firmware, PSB boots authorize only firmware authenticated by AMD Secure Processor.[8]

By cryptographically verifying the software stack, AMD Platform Secure Boot adds a substantial layer of defense against unauthorized intrusion across various platforms, particularly in virtualized environments or in the cloud.

AMD Platform Secure Processor

Together with PSB, AMD Platform Secure Processor (PSP) fortifies the Dell PowerEdge server boot process. When a CPU first powers on in the Dell factory, the AMD Platform Secure Processor embeds a unique Dell ID permanently into the CPU. This ID effectively ties the CPU to the PowerEdge server, creating a secure bond.[9]

This integration means that PSP will prevent a PowerEdge server from booting if it detects a CPU from a different server. However, CPU portability is still possible in the event of a hardware failure. The AMD processor is locked to the vendor's signing key rather than the motherboard, offering a balance between security and component mobility.[10]

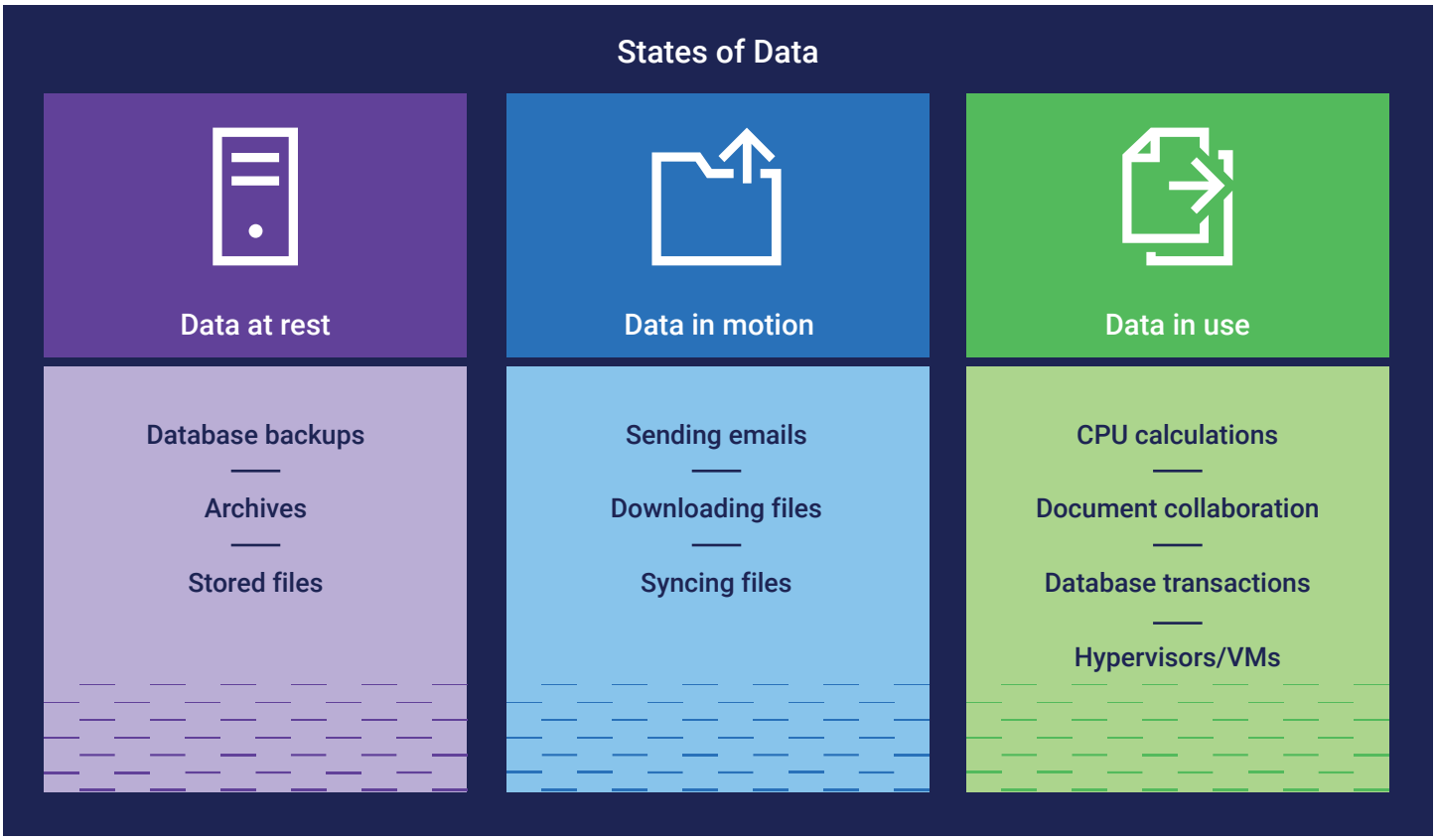

Figure 2: States of Data

[6] AMD, "AMD Pro Security," accessed December 4, 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, "AMD Infinity Guard," accessed December 4, 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, "4 Ways AMD Infinity Guard Helps Protect Your Data," accessed December 4, 2023, https://www.amd.com/system/files/documents/content-security-infographic.pdf.
[9] AMD, "AMD Infinity Guard."
[10] Dell, "Defense in-depth: Comprehensive Security on PowerEdge AMD EPYC Generation 2 (Rome) Servers," accessed December 4, 2023, https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Protecting Your Data

While attackers gain access to systems, the end goal is always the same: to find your data and steal, manipulate, sell, or destroy it. The physical server isn't the only point of vulnerability. Bad actors can attack networking, IT policies can contain errors, end-users can have weak passwords, and IT teams can set access permissions too broadly. Attackers may target users with phishing emails to distribute malware.

Dell enables customers to employ a Zero Trust approach that relies on multiple security layers to help protect against all these types of vulnerabilities. To guard against theft or compromise, you must secure data at rest, data in process, and data in flight, through to data decommissioning.[11] With features such as at-rest encryption, robust encryption key management, and automated certificate renewal, Dell PowerEdge servers work to block, deter, and mitigate malicious attacks after first boot. Dell PowerEdge servers with AMD processors offer additional features to bolster security, including AMD Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV).

Data at Rest

To protect data at rest, Dell provides three main security features: software-based encryption, enterprise key management, and hardware drive encryption. With drives that support Instant Secure Erase (ISE), Dell customers can cryptographically erase any data on self-encrypted drives (SEDs), ISE drives, and NVM devices such as NVDIMMs. SEDs protect data from attacks in instances where a disgruntled employee or other malicious actor physically removes drives from a server. Because the encrypted drive's locking key password ties it to the specific server and RAID controller it came from, another server cannot access the data. For further protection, iDRAC can use Dell OpenManage Secure Enterprise Key Manager with local key management (iLKM, LKM) which works in conjunction with an external third-party key manager to lock and unlock the storage controller at boot. If someone boots the server away from the key manager, iDRAC keeps the storage controller locked so that the data stored on the device remains encrypted. To find out more about other encryption key options, visit https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

Data in Flight

With data in flight, vulnerabilities in the network and data access control could allow attackers to intercept or modify data traveling over the network. The iDRAC web connection is one possible point of vulnerability—so Dell provides several options to secure the connection with a TLS/SSL certificate, thus mitigating the chance of attack. While this certificate is self-signed by default, admins can create a custom certificate, or one signed by a trusted Certificate Authority (CA). This certificate enables encrypted, secure connections for web browsers and tools such as command-line utilities to safely interact with the server via the iDRAC connection.

iDRAC also provides several controls for users to modify strict, narrow access rules that allow SSH access to the server. For iDRAC users with a Datacenter level license, iDRAC offers Simple Certificate Enrollment Protocol (SCEP), which maintains web server certificates with automatic renewal to avoid accidental lapses in coverage. A 2020 study from third party Principled Technologies found that this automatic renewal feature keeps servers more secure while saving IT staff valuable time—especially when it comes to maintaining a fleet of server certificates.[12]

Data in Use

To protect data in use, Dell PowerEdge servers enable AMD confidential compute features, including AMD Secure Memory Encryption (SME) and Secure Encrypted Virtualization (SEV) to protect data as it flows through memory and processing components.

[11] Dell, "Reduce Your Risk of Unauthorized Server Data Access," accessed January 24, 2024, https://infohub.delltechnologies.com/section-assets/data-protection-infographic.

[12] Principled Technologies, "Reduce hands-on deployment times to near zero with iDRAC9 automation," accessed December 4, 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME encrypts all data as it enters the memory, further securing your data. Without memory encryption, data is vulnerable to malicious software and other intrusions, especially with newer memory technology such as NVDIMMs that do not lose data when powered down. This protection extends to memory via high-performance encryption engines integrated into the memory channels, ensuring both security and speed. Because it's completely transparent to the host OS and application layers, AMD SME accomplishes this without necessitating any changes to application software, providing a user-friendly approach to enhanced memory security.[13]

AMD SME in-memory data encryption marks a departure from older memory encryption methods that were tailored to specific use cases. A key advantage of AMD SME is its flexibility, allowing software to utilize it in different ways: either by encrypting all of DRAM for comprehensive protection or selectively encrypting specific regions, such as those used by guest virtual machines (VMs).[14]

AMD Secure Encrypted Virtualization

AMD SEV enhances encryption for memory and virtual machines by implementing a virtual machine-based Trusted Execution Environment (TEE). Integrating with AMD-V architecture, AMD SEV encrypts each VM's memory separately, protecting the VMs from each other and from the hypervisor. This approach employs cryptography to safeguard code within a VM from potentially vulnerable higher-privileged code, such as the hypervisor. The added layer of security is especially crucial in cloud environments. This method ensures enhanced protection for VMs, fortifying them against external vulnerabilities. The encryption happens right at the memory controller, where it encrypts and decrypts data without slowing processing speed—thanks to the AMD Secure Processor handling all the encryption details invisibly.[15]

There are still some situations when a VM's data needs to communicate with other VMs or with the hypervisor. In these instances, AMD SEV allows the VM to choose which encryption key to apply to specific memory pages: a guest key that keeps the page private to the VM or a hypervisor key that allows the hypervisor and other VMs to decrypt the page. This flexibility allows for security and communication based on the needs of each VM.[16]

AMD SEV offers additional features that expand the cryptographic isolation of VMs: SEV-Encrypted State (SEV-ES) and SEV-Secure Nested Paging (SEV-SNP). SEV-ES further isolates VMs from each other and the hypervisor by encrypting CPU register content when a VM powers down, protecting it from unauthorized access via a neighbor VM or the hypervisor. SEV-SNP builds on SEV and SEV-ES, adding memory integrity protection and optional additional security features for VMs. The memory integrity enhancement makes it so that a VM can access data in memory only if it can read the last value it wrote. If another entity modified the data in the memory, the VM cannot access the data. This protects the VM from running compromised data or code.

Encryption and Encryption Keys

AMD SEV uses a unique encryption key for each VM, cryptographically isolating VMs and the hypervisor. This encryption engine secures data on write and decrypts it on read. Each VM, upon creation, receives a unique key, ensuring that any unauthorized attempt to access its memory results in incomprehensible data. Every 4th Generation AMD EPYC™ processor offers up to one thousand encryption keys. This architecture doesn't alter applications within the VM; instead, it operates at the operating system level and elevates data security. Designed to protect data in use, including memory contents, the encryption hardware built into the memory controller manages VRAM traffic encryption and decryption, strengthening protection of data in use.[17]

[13] AMD, "AMD Infinity Guard."
[14] AMD, "AMD Memory Encryption," accessed December 4, 2023, https://www.amd.com/content/dam/amd/en/ documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[15] AMD, "AMD Secure Encrypted Virtualization," accessed December 4, 2023, https://www.amd.com/en/developer/sev.html
[16] AMD, "AMD Memory Encryption." https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf
[17] AMD, "AMD Secure Encrypted Virtualization."

Conclusion

From the moment you order Dell PowerEdge servers with AMD processors to the time you retire them and every moment in between, Dell and AMD offer numerous layers of security to keep your data safe. With tightly integrated layers of silicon-based RoT and multiple layers of boot protection to weed out suspect drivers, firmware, BIOS versions, server components are secure from the moment of manufacture. Additionally, by encrypting SED and ISE drives, your data is safe even if malicious actors physically remove disks or servers from your data center. Through other security features such as processor-based AMD SME and SEV technology, which protect data in process, and state-of-the-art software checks through iDRAC, Dell PowerEdge servers with AMD processors help ensure business continues without a hitch—no matter what new methods of attack cybercriminals may come up with. To learn more about Dell PowerEdge Servers with 4th Gen AMD EPYC processors, visit www.dell.com/servers/amd.

Learn more about Dell and AMD solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation with #PowerEdge

DELL Technologies

AMD together we advance_