Defense in-depth: Comprehensive Security on PowerEdge AMD EPYC Generation 2 (Rome) Servers

Tech Note by

Mukund Khatri
Craig Phelps

Summary

Security in servers is no longer an afterthought – it is a key consideration in the choice of a server provider and platform.

Dell EMC approaches security in multiple layers to best protect customer assets and data. This includes not just security built into the system and components, but also to manufacturing processes and ensuring a secure supply chain.

Introduction

In the wake of Spectre and Meltdown and endless other side-channel issues, and with predictive indicators showing that new forms of attack are likely – security is a critical requirement for servers. And it is important to ensure that server security is at layers within the systems so that malicious activity can be mitigated in numerous ways. PowerEdge servers with AMD Rome processors use a multi-layer, end-to-end approach of security to help ensure that users' data and assets are protected, see Figure 1.

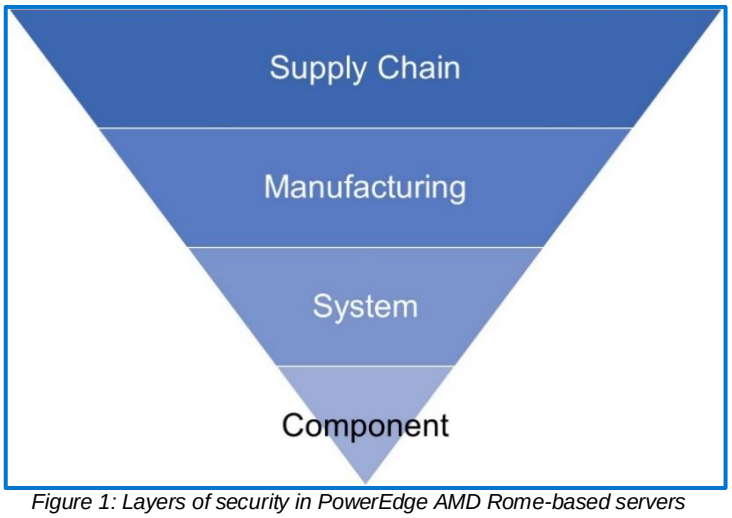

Figure 1: Layers of security in PowerEdge AMD Rome-based servers

Layer 1: AMD EPYC-based System Security for Processor, Memory and VMs on PowerEdge

The first generation of the AMD EPYC processors have the AMD Secure Processor – an independent processor core integrated in the CPU package alongside the main CPU cores. On system power-on or reset, the AMD Secure Processor executes its firmware while the main CPU cores are held in reset. One of the AMD Secure Processor's tasks is to provide a secure hardware root-of-trust by authenticating the initial PowerEdge BIOS firmware. If the initial PowerEdge BIOS is corrupted or compromised, the AMD Secure Processor will halt the system and prevent OS boot. If no corruption, the AMD Secure Processor starts the main CPU cores, and initial BIOS execution begins.

The very first time a CPU is powered on (typically in the Dell EMC factory) the AMD Secure Processor permanently stores a unique Dell EMC ID inside the CPU. This is also the case when a new off-the-shelf CPU is installed in a Dell EMC server. The unique Dell EMC ID inside the CPU binds the CPU to the Dell EMC server. Consequently, the AMD Secure Processor may not allow a PowerEdge server to boot if a CPU is transferred from a non-Dell EMC server (and CPU transferred from a Dell EMC server to a non-Dell EMC server may not boot).

AMD EPYC Generation 2 processors also offer the AMD Secure Processor --- for cryptographic functionality for secure key generation and key management. This provides full stack encryption without any overhead for the processor. In addition, for hardware-accelerated memory encryption for data-in-use protection, the security components in Rome processors include the AES-128 encryption engine, which is embedded in the memory controller and automatically encrypts and decrypts data in main memory with an appropriate key.

The AMD EPYC processors also include these two unique security features:

1. **Secure Memory Encryption (SME):**

   SME uses a single key to encrypt system memory, which is generated by the AMD Secure Processor at boot. SME requires enablement in the system BIOS or operating system; when enabled in the BIOS, memory encryption is transparent and can be run with any operating system

2. **Secure Encrypted Virtualization (SEV):**

   In addition to what SME capabilities, SEV provides Virtual Machine (VM) level encryption, which protects against hypervisor corruption with hardware protection – a more robust solution than software protection. The EPYC Generation 2 (Rome) processors also offer 509 keys per hypervisor for SEV, versus 16 in EPYC (Naples)-based servers

   a. **Secure Encrypted Virtualization – Encrypted State (SEV ES):**

      Encrypts all CPU register contents when a VM stops running, preventing leakage of information in CPU registers to components like the hypervisor, and it can detect malicious modifications to a CPU register state. Some technical details:

      - Guest register state is encrypted with guest encryption key and integrity protected
      - Only the guest can modify its register state
      - Guest must explicitly share register state with the hypervisor
      - Guest-Hypervisor Communication Block (GHCB)
      - Protects the guest register state from the hypervisor
      - Adds additional protection against VM state related attacks (exfiltration, control flow, rollback)

For more information, see this technical brief on EPYC first generation security:
AMD CPU Security Features in PowerEdge 14G Servers

Layer 2: PowerEdge Systems Security

All Dell EMC PowerEdge servers offer built-in security that supports customers with compliance, preventive security, and fast means to recover in the event of errors or breaches. This includes FIPs/Common Criteria Compliance, immutable silicon root of trust (PowerEdge CPUs have a Dell signature: once it is used in a Dell system if cannot be used in another server), digitally signed firmware updates, automatic BIOS recovery, firmware rollback, and more.

In addition, Dell EMC offers differentiated security features in every PowerEdge system:

- **Dell EMC OpenManage Secure Enterprise Key Manager –**embedded in Dell EMC PowerEdge servers and works in conjunction with leading Key Management Servers for enabling keys at scale
- **System Lockdown** – Locks down the configuration and firmware, protecting the server(s) from inadvertent or malicious changes, and is enabled or disabled by the IT Administrator… and prevents system/firmware "drift"
- **System erase** of all user drives, including NVMe – through a process that is not only fast, but enables the drives to be reused and meets NIST recommendations for data erasure
- **Rapid OS Recovery –** Allows users to boot a trusted backup OS image from a hidden boot device
- **Enhanced UEFI secure boot with custom certificates** – with UEFI Secure Boot, each component in the chain is validated and authorized against a specific certificate before it is allowed to load or run
- **Dynamically-enabled USB ports**
  - This feature allows administrators to disable all USB ports and then enable them dynamically to allow local crash cart usage (to let a local technician have temporary access)
  - The USB ports can be dynamically enabled and disabled without rebooting the server; normally changing the USB port state requires a reboot and takes down the workloads
- **Intrusion-switch included –** detection of chassis intrusion at no extra expense
- **Domain Isolation -** an important feature for multi-tenant hosting environments, hosting providers may want to block any re-configuration by tenants. Domain isolation is a configuration option that ensures that management applications in the host OS have no access to the out-of-band iDRAC or to Intel chipset functions

For more information, see this technical brief:
Security in Server Design

And this video for further information:
Server Security – Dell EMC PowerEdge Servers

Layer 3: Dell Technologies Factory Security

Factories where Dell products are built must meet specified Transported Asset Protection Association (TAPA) facility security requirements, including the use of closed-circuit cameras in key areas, access controls, and continuously guarded entries and exits. Additional controls are applied at Dell and supplier-managed facilities and for air, rail, and ocean shipments to address the variety of risks faced across transportation modes and regions. Some of these protections include tamper-evident packaging, security reviews of shipping lanes, locks or hardware meeting required specifications, and container integrity requirements. GPS tracking devices may also be placed on any container and monitored 24x7 until confirmation of delivery.

Dell also maintains certification with the United States Customs and Border Patrol's Customs-Trade Partnership Against Terrorist (C-TPAT). This logistics security program is recognized as compatible with similar programs around the world, including the Authorized Economic Operator (AEO), Canada's Supply Chain Assurance v4.0 | Dell Inc., 2018 4 Partners in Protection, and Singapore's Secure Trade Partnership programs. While the primary focus of these programs is to prevent contraband, the required protections also guard against tampering with products being imported.

Layer 4: Dell Technologies Supply Chain Security

The goal of Dell's supply chain security processes is to provide continuous security risk assessment and improvement. Dell's Supply Chain Risk Management framework mirrors that of the comprehensive risk management framework of the National Infrastructure Protection Plan (NIPP), which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Dell's framework incorporates an open feedback loop (see Figure 2) that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle.

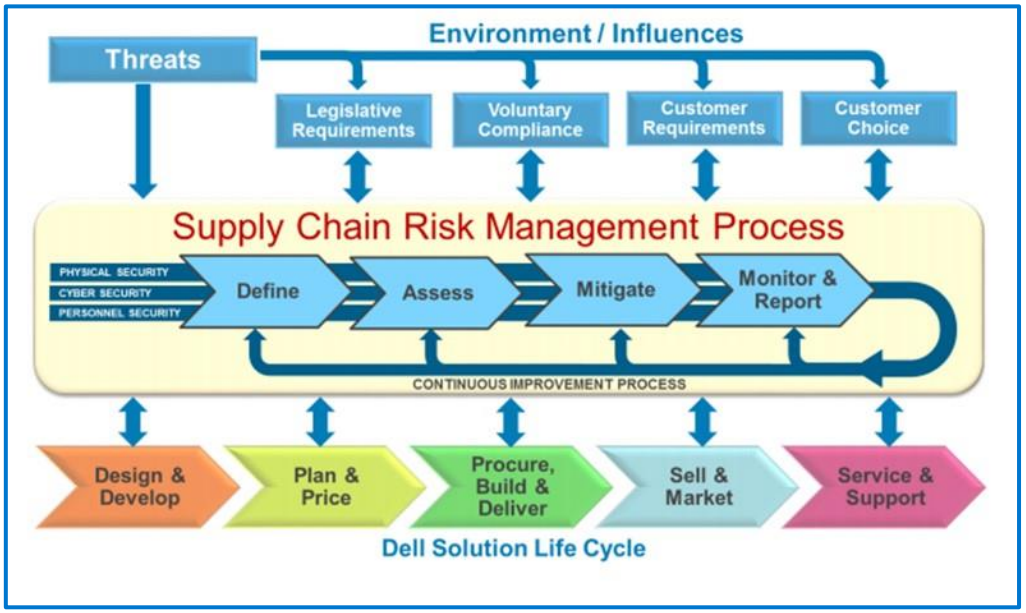

Figure 2 Managing the supply chain for Dell Technologies products

The process includes these safeguards by Dell Technologies for the supply chain:

1. Supplier governance by Dell
   a. Audits
   b. Global Inventory Control Policy
   c. Measure suppliers' security practices against industry best practices for physical security and for mitigating counterfeit components, tainted software and firmware, and intellectual property theft
   d. Quarterly Reviews

2. Supply Chain Security

   a. Physical (factory/manufacturing) – factories where Dell products are built must meet specified Transported Asset Protection Association (TAPA) facility security requirements. Dell also maintains certification with the United States Customs and Border Patrol's Customs-Trade Partnership Against Terrorist (C-TPAT).

   b. Personnel – Dell policy requires employees throughout the supply chain, including those at contract suppliers, to go through a pre-employment suitability screening process.

   c. Information – Dell collects and uses sensitive information about products, solutions, customers, suppliers and partners throughout the supply chain lifecycle. Dell uses numerous measures to guard this sensitive information against exposure and exploitation.

3. Supply Chain Integrity

   Dell has developed baseline specifications that are securely preserved and later used as a reference to verify that no unauthorized modifications have been made to hardware or software. The goal is to ensure that the products received by customers are the products customers expected and will operate as intended.

   For hardware, this includes processes to minimize the opportunity for counterfeit components to infiltrate our supply chain. For software, Industry software engineering best practices include security throughout the development process for any code, including operating systems, applications, firmware, and device drivers. Dell reduces opportunities for the exploitation of software security flaws by incorporating Secure Development Lifecycle (SDL) measures throughout the development process. These measures are tightly aligned with Software Assurance Forum for Excellence in Code (SAFECode) guidelines and ISO 27034.

4. Stronger together

   Dell participates in supply chain risk management activities with trusted industry groups and public/private partnerships. Dell has been actively engaged in the Open Group Trusted Technology Forum (O-TTPF), the Software and Supply Chain Assurance Forum, SAFECode, the Supply Chain Risk Leadership Council, the Internet Security Alliance, and the IT Sector Coordinating Council. Dell is also an active member of the Government Information Data Exchange Program (GIDEP). Dell has participated in the development of numerous standards and best-practice guidelines related to supply chain integrity including the Open Group Trusted Technology Provider Standard (O-TTPS) which is also recognized as ISO 20243, SAFECode, ISO 27036, and National Institute of Science and Supply Chain Assurance v4.0 | Dell Inc., 2018 6 Technology (NIST) Interagency Report (IR) 7622, NIST Special Publication (SP) 800-161, NIST SP800-53, and the NIST Cybersecurity Framework. To address customer concerns about product tampering and supply chain assurance, Dell continues to monitor and influence the development and potential impact of legislation, regulations, voluntary standards, and contract language

For more details on Dell supply chain security please refer to this white paper:
https://i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf?newtab=true

In Conclusion

Security must be designed within the architecture of the server to effectively withstand sophisticated cyber-crime: phishing attacks that harvest credentials, advanced persistent threats (taking control of firmware), data exfiltration (stealing data). Yet it's not just the server features that need to support customer security – it is also necessary to provide protection against the possibility of corruption in manufacturing and within the server supply chain. These layers of security must be considered as critical criteria for user decisions on integrating technical equipment into their environments.

As Dell EMC designs products, it will always be to protect, protect, and protect customer data and assets – and in consideration of worst-case scenarios, ensure that users of Dell EMC solutions can recover quickly, and resume production with as little disruption as possible. With these goals, Dell EMC is constantly evaluating new ways within each security layer to protect customers.

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news