Technical White Paper:
Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers

Dell EMC Server Solutions

January 2018

A Dell EMC Technical White Paper

Revisions

Date	Description
January 2018	Initial release

Table of contents

1 Introduction

"The world's most important resource is no longer oil, but data" according to a recent article in The Economist.[1] Organizations of every size will agree with this statement. Data has become the most important asset for many organizations. Protecting data and the underlying IT infrastructure that supports it is a paramount concern of CIOs, CISOs, and IT and datacenter managers alike. Complicating the protection of IT infrastructure is the growing complexity and volume of advanced malware. There were 357 million new malware variants in 2016 alone, an increase of 82 million in just 2 years.[2]

However, most of the cybersecurity focus today is on protecting the OS and applications from malicious attacks; less attention is sometimes given to the security of underlying server infrastructure, including hardware and firmware. Server infrastructure is key to data center security, since cyberattacks targeting firmware can be persistent and hard to detect. McAfee Labs predicts in 2017 that "advanced adversaries will continue to look for vulnerabilities in hardware and firmware that they can exploit[3]." However, according to ISACA, a non-profit IT auditing organization, over 50% of companies that do place priority on security still got infected with malware and 17 percent revealed that the incidents had a material impact.[4]

As servers become more critical in a software-defined datacenter architecture, server security becomes the foundation of overall enterprise security. Servers must emphasize security at both the hardware and firmware level by leveraging an immutable Root-of-Trust that can be used to verify subsequent operations within the server. This establishes a chain of trust that extends throughout the server lifecycle, from deployment through maintenance to decommissioning.

The 14th generation of PowerEdge servers deliver this chain of trust and combine it with comprehensive management tools to provide robust layers of security across hardware and firmware. The result is a **Cyber Resilient Architecture** that extends across every aspect of the server, including the embedded server firmware, the data stored in the system, the operating system, peripheral devices, and the management operations within it. Organizations can build a process to protect their valuable server infrastructure and the data within it, detect any anomalies, breaches, or unauthorized operations, and recover from any unintended or malicious events. This paper details the security features delivered throughout the entire lifecycle of 14th generation Dell EMC PowerEdge servers.

---

[1] https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (May 2017)
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (Internet Security Threat Report, Volume 22, April 2017)
[3] https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf (November 2016)
[4] https://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Firmware-Security-Research-Highlights-Shortcomings-Vulnerabilities.aspx (October 2016)

2 The Path to a Secure Server Infrastructure

Dell EMC PowerEdge servers have featured robust security for several generations, including the innovation of using silicon-based data security. In 14G, we have extended silicon-based security to authenticate BIOS and firmware with a cryptographic Root-of-Trust during server boot process. Dell EMC product team considered several key requirements during the design of 14th generation of PowerEdge servers in response to security threats faced in modern IT environments:

- **Protect**: Protect server during every aspect of lifecycle, including BIOS, firmware, data, and physical hardware
- **Detect**: Detect malicious cyberattacks and unapproved changes; engage IT administrators proactively
- **Recover**: Recover BIOS, firmware, and OS to a known good state; securely retire or repurpose servers

Dell EMC PowerEdge servers conform to key industry standards on cryptography and security as elaborated throughout this paper, and perform on-going tracking and management of new vulnerabilities.

Dell EMC has implemented the *Security Development Lifecycle* process with security as a key element in every aspect of development, procurement, manufacturing, shipping, and support resulting in a *Cyber Resilient Architecture* in 14G servers.

2.1 Security Development Lifecycle

Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development. This process is called the Security Development Lifecycle (SDL) model, in which security is not an afterthought but is rather an integral part of the overall server design process. This design process encompasses a view of security needs throughout the entire server lifecycle, as bulleted below and as shown in Figure 1:

- Features are conceived, designed, prototyped, implemented, set into production, deployed, and maintained, with security as a key priority
- Server firmware is designed to obstruct, oppose, and counter the injection of malicious code during all phases of the product development lifecycle
  - Threat modeling and penetration testing coverage during the design process
  - Secure coding practices are applied at each stage of firmware development
- For critical technologies, external audits supplement the internal SDL process to ensure that firmware adheres to known security best practices
- On-going testing and evaluation of new potential vulnerabilities using the latest security assessment tools

- Rapid response to critical Common Vulnerabilities and Exposures (CVEs) including recommended remediation measures if warranted.

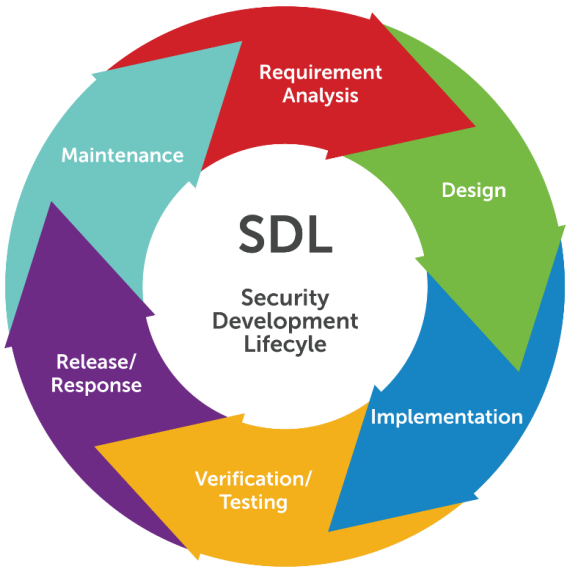


Figure 1: Security Development Lifecycle of Dell EMC

2.2 Cyber Resilient Architecture

Dell EMC 14th Generation PowerEdge servers feature an enhanced Cyber Resilient Architecture that provides a hardened server design to Protect, Detect, and Recover from cyberattacks. Some of the key aspects of this architecture are:

- Effective Protection from attacks
  - Silicon-based Root-of-Trust
  - Signed Firmware Updates
  - System Lockdown
- Reliable Detection of attacks
  - Configuration and Firmware Drift Detection
  - Persistent Event Logging
  - Secure Alerting
- Rapid Recovery with little to no business interruption
  - Automated BIOS recovery
  - Rapid OS Recovery
  - Firmware Rollback

2.3 Today's Threats

There are many threat vectors in today's changing landscape. Table 1 summarizes the Dell EMC approach to managing critical backend threats.

Table 1. How Dell EMC addresses common threat vectors

Server Platform Layers		
Security layer	**Threat vector**	**Dell EMC solution**
Physical server	Server tampering	Physical deterrents
Firmware and software	Firmware corruption, malware injection	Silicon-based Root of Trust; Intel Boot Guard; AMD Secure Root-of-Trust Cryptographically signed and validated firmware;
	Software	Patching as required
Attestation trust features	Server identity spoofing	TPM, TXT, Chain of trust
Server management	Rogue configuration and updates, unauthorized open-port attacks	iDRAC9

Server Environment Layers		
Security layer	**Threat vector**	**Dell EMC solution**
Data	Data breach	SED (Self Encrypting Drives) – FIPS or Opal/TCG ISE-only (Instant Secure Erase) drives Secure Key Management Secure User Authentication
Supply Chain Integrity	Counterfeit components Malware Threats	ISO9001 certification for all global server manufacturing sites Security measures implemented as part of Secure Development Lifecycle (SDL) process
Supply Chain Security	Physical security in Manufacturing sites Theft and tempering during transport	Transported Asset Protection Association (TAPA) facility security requirements Customs-Trade Partnership Against Terrorism (C-TPAT)

3 Protect

The “protect” function is a key component of the NIST Cybersecurity Framework and serves to guard against cybersecurity attacks. This function consists of several categories including access control, data security, maintenance, and protective technology. The key underlying philosophy is that infrastructure assets must provide robust protection against unauthorized access to resources and data as part of a comprehensive secure installation and computing environment. This includes protecting against unauthorized modifications of critical components such as BIOS and firmware. The platform meets the current recommendations in NIST SP 800-193 (“Draft Platform Firmware Resiliency Guidelines”).

The **Cyber Resilient Architecture** in PowerEdge servers offers a high level of platform protection that includes the following capabilities:

- Cryptographically-verified Trusted Booting
- User Access Security
- Signed Firmware Updates
- Encrypted Data Storage
- Physical Security
- Supply Chain Integrity and Security

3.1 Cryptographically-verified Trusted Booting

One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an OS or updating firmware. PowerEdge servers have used silicon-based security for several generations for features such as iDRAC Credential Vault, an encrypted secure memory in iDRAC for storing sensitive data. The boot process is verified using a silicon-based Root-of-Trust to meet recommendations in NIST SP 800-147B (“BIOS Protection Guidelines for Servers”) and NIST SP 800-155 (“BIOS Integrity Measurement Guidelines”).

3.1.1 Silicon-based Root-of-Trust

14th generation PowerEdge servers (both Intel or AMD-based) now use an immutable, silicon-based Root-of-Trust to cryptographically attest to the integrity of BIOS and iDRAC firmware. This Root-of-trust is based on one-time programmable, read-only public keys that provide protection against malware tampering. The BIOS boot process leverages Intel Boot Guard technology or AMD Root-of-Trust technology which verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in silicon by Dell EMC in factory. A failure to verify results in a shutdown of the server, user notification in the Lifecycle Controller Log, and the BIOS recovery process can then be initiated by the user. If Boot Guard validates successfully, the rest of the BIOS modules are validated by using a chain of trust procedure until control is handed off to the OS or hypervisor.

Let us look at the chain of trust in more detail. Each BIOS module contains a hash of the next module in the chain. The key modules in BIOS are the IBB (Initial Boot Block), SEC (Security), PEI (Pre-EFI Initialization), MRC (Memory Reference Code), DXE (Driver Execution Environment), and BDS (Boot Device Selection). If Intel Boot Guard authenticates the IBB (Initial Boot Block), then the IBB validates SEC+PEI before handing control to it. SEC+PEI then validates PEI+MRC which further validates the DXE+BDS modules. At this point, control is handed over to UEFI Secure Boot as explained in the next section.

Similarly, for Dell EMC PowerEdge servers based on AMD EPYC, AMD Secure Root-of-Trust technology ensures that servers boot only from trusted firmware images. Additionally, AMD Secure Run Technology is designed to encrypt main memory, keeping it private from malicious intruders having access to the hardware. No application modifications are needed to use this feature and the security processor never exposes the encryption keys outside of the processor.

The iDRAC boot process uses its own independent silicon-based Root-of-Trust that verifies the iDRAC firmware image. The iDRAC Root-of-Trust also provides a critical trust anchor for authenticating the signatures of Dell EMC firmware update packages (DUPs).

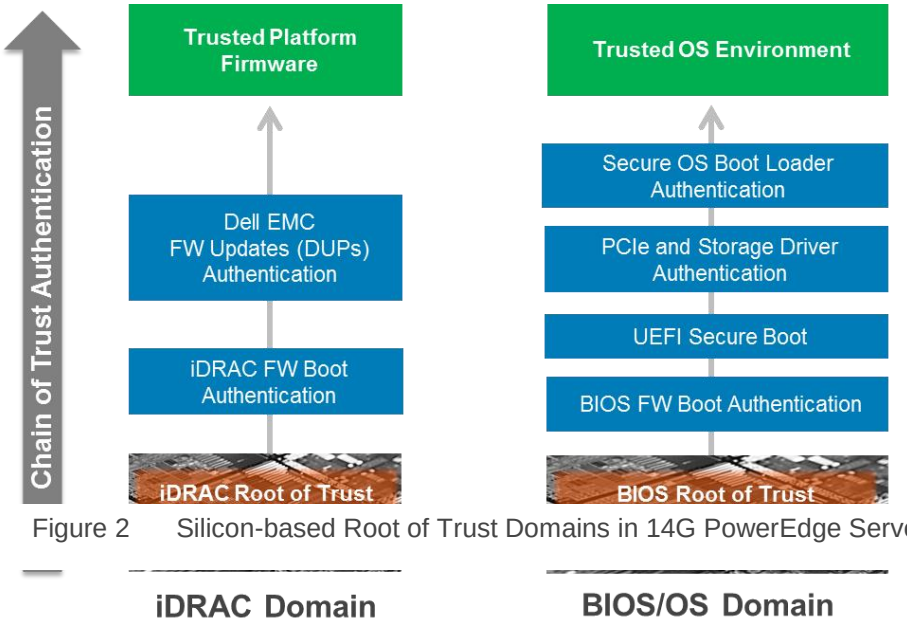


Figure 2 Silicon-based Root of Trust Domains in 14G PowerEdge Servers

3.1.2 UEFI Secure Boot Support

PowerEdge servers also support industry-standard UEFI Secure Boot which checks the cryptographic signatures of UEFI drivers and other code loaded prior to the OS running. Secure Boot represents an industry-wide standard for security in the pre-boot environment. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability.

When enabled, UEFI Secure Boot prevents unsigned (that is, untrusted) UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. You must disable Secure Boot to load unsigned device drivers.

In addition, 14th generation PowerEdge servers offer customers the unique flexibility of using a customized boot loader certificate not signed by Microsoft. This is primarily a feature for administrators of Linux environments that want to sign their own OS boot loaders. Custom certificates can be uploaded via the preferred iDRAC API to authenticate the customer's specific OS boot loader.

3.1.3 TPM Support

PowerEdge servers support three versions of TPM:

- TPM 1.2 FIPS + Common Criteria+ TCG certified (Nuvoton)
- TPM 2.0 FIPS + Common Criteria+ TCG certified (Nuvoton)
- TPM 2.0 China (NationZ)

TPM can be used perform public key cryptographic functions, compute hash functions, generate, manage, & securely store keys, and do attestation. Intel's TXT (Trusted Execution Technology) functionality and Microsoft's Platform Assurance feature in Windows Server 2016 are also supported. TPM can be used to enable the BitLocker™ hard drive encryption feature in Windows Server 2012/2016.

TPM is compatible with the remote attestation HyTrust CloudControl solution. Attestation and remote attestation solutions can use the TPM to take measurements at boot time of a server's hardware, hypervisor, BIOS, and OS, and compare them in a cryptographically secure manner against base measurements stored in the TPM. If they are not identical, the server identity may have been compromised and system administrators can disable and disconnect the server either locally or remotely.

TPM is enabled through a BIOS option. It is offered as a Plug-In Module solution, the planar has a connector for this plug-in module.

3.1.4 Security Certifications

Dell EMC has received certifications for standards such as NIST FIPS 140-2 and Common Criteria EAL-4. These are important for complying with US DoD and other governmental requirements. The following certifications have been received for PowerEdge servers:

- Server platform: Common Criteria EAL4+ certified with RHEL
- iDRAC and CMC FIPS 140-2 Level 1 certification
- FIPS 140-2 and Common Criteria certification for TPM 1.2 & 2.0
- FIPS 140-2 certification for SED storage drives

3.2 User Access Security

Ensuring proper authentication and authorization is a key requirement of any modern access control policy. The primary access interfaces for PowerEdge servers are via the APIs, CLIs, or the GUI of the embedded iDRAC. The preferred APIs and CLIs for automating server management are:

- iDRAC Restful API with Redfish
- iDRAC WS-MAN API
- RACADM CLI
- SSH CLI

Each of these provide for robust credentials like username and password security, transported over an encrypted connection, such as HTTPS, if desired. SSH authenticates a user by using a matching set of cryptographic keys (and thus eliminating the need to enter passwords that are less-secure). Older protocols, such as IPMI, are supported but are not recommended for new deployments due to the various security issues uncovered in recent years. We recommend that if you are currently using IPMI, you should evaluate and transition to iDRAC Restful API with Redfish.

TLS/SSL certificates can be uploaded to iDRAC to authenticate web browser sessions. Three options:

- **Dell EMC Self-Signed TLS/SSL Certificate** – The certificate is auto-generated and self-signed by iDRAC.
  - Advantage: No need to maintain a separate Certification Authority (see X.509/IETF PKIX std).
- **Custom Signed TLS/SSL Certificate** – The certificate is auto-generated and signed with a private key that has already been uploaded to iDRAC.
  - Advantage: Single trusted CA for all iDRACs. It's possible that your in-house CA is already trusted on your management stations.
- **CA Signed TLS/SSL Certificate** – A certificate signing request (CSR) is generated and submitted to your in-house CA or by a third party CA such as VeriSign, Thawte, and Go Daddy for signing.
  - Advantages: Can use a commercial Certification Authority (see X.509/IETF PKIX standards). Single trusted CA for all your iDRACs. If a commercial CA is used it is very likely to be already trusted on your management stations.

iDRAC9 enables integration with **Active Directory** and **LDAP** by leveraging customers' existing authentication and authorization schemas that already provide secure access to PowerEdge servers. It also supports **Role-based Access Control (RBAC)** to grant the proper level of access – Administrator, Operator, or Read Only – required to match the role of the person in server operations. It is highly recommended to use RBAC in this manner and not just grant the highest level (i.e. Administrator) to all users.

Two-factor authentication (2FA) is used more widely today because of the growing vulnerability of single-factor authentication schemes based on username and password. iDRAC9 allows use of smart cards for remote GUI access. The two factors are the physical presence of the smart card and the smart card PIN.

iDRAC9 also provides additional ways to protect against unauthorized access including **IP blocking and filtering**. IP blocking dynamically determines when excessive login failures occur from a particular IP address and blocks (or prevents) the address from logging into iDRAC9 for a preselected time span. IP filtering limits the IP address range of the clients accessing iDRAC. It compares the IP address of an incoming login to the specified range and allows iDRAC access only from a management station whose source IP address is within the range. All other login requests are denied.

3.2.1 Factory Generated Default Password

By default, all 14G PowerEdge servers ship with a unique, factory-generated iDRAC password to provide additional security. This password is generated at the factory and is located on the pull-out Information Tag located on the front of the chassis, adjacent to the server asset label. Users who choose this default option must note this password and use it to log in to iDRAC for the first time. For security purposes, Dell EMC strongly recommends changing the default password.

3.2.2 System Lockdown

iDRAC9 offers a new feature that 'locks down' the hardware and firmware configuration of a server or servers. This mode can be enabled by using the GUI, CLIs such as RACADM, or as part of the Server Configuration Profile. Users with administrative privileges can set System Lockdown mode which prevents users with lesser privileges from making changes to the server. This feature can be enabled/disabled by the IT administrator. Any changes made when System Lockdown is disabled are tracked in the Lifecycle Controller Log. By enabling lockdown mode, you can prevent configuration drift in your datacenter when using Dell EMC tools and agents, as well as protect against malicious attacks against embedded firmware when using Dell EMC Update Packages.

3.2.3 Domain Isolation

14th generation PowerEdge servers now provide additional security via **Domain Isolation**, an important feature for multi-tenant hosting environments. In order to secure the server's hardware configuration, 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, such as Management Engine (ME) or Innovation Engine (IE).

3.3 Signed Firmware Updates

PowerEdge servers have used digital signatures on firmware updates for several generations to assure that only authentic firmware is running on the server platform. We digitally sign all of our firmware packages using SHA-256 hashing with 2048-bit RSA encryption for the signature for all key server components including firmware for iDRAC, BIOS, PERC, I/O adaptors and LOMs, PSUs, storage drives, CPLD and backplane controllers. iDRAC will scan firmware updates and compare their signatures to what is expected using the silicon-based Root-of-Trust; any firmware package that fails validation is aborted and an error message is logged into the Lifecycle Log (LCL) to alert IT administrators.

Enhanced firmware authentication is embedded within many 3rd party devices which provide signature validation using their own Root-of-Trust mechanisms. This prevents the possible use of a compromised 3rd party update tool from being used to load malicious firmware into, for example, a NIC or storage drive (and bypassing the use of signed Dell EMC update packages). Many of the 3rd party PCIe and storage devices shipped with PowerEdge servers use a hardware Root-of-Trust to validate their respective firmware updates.

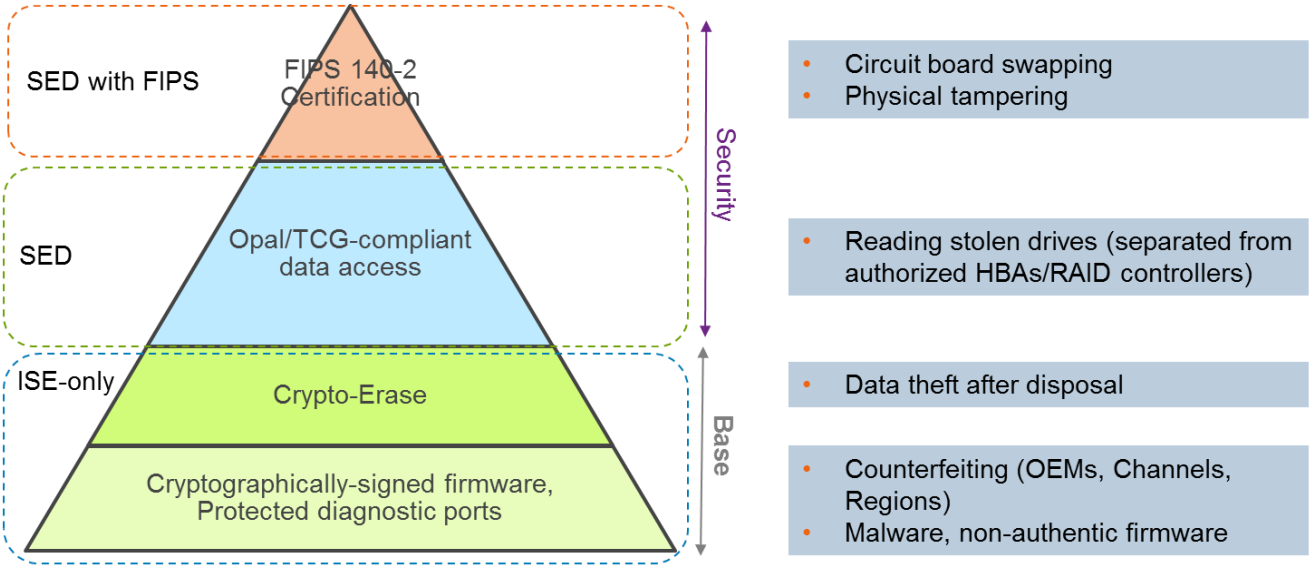
If any firmware in any device is suspected of malicious tampering, IT administrators can rollback many of the platform firmware images to a prior trusted version stored in iDRAC. We keep 2 versions of device firmware on the server – the existing production version (“N”) and a prior trusted version (“N-1”).

3.4 Encrypted Data Storage

14th generation PowerEdge servers offer several storage drive options for securing data. As shown below, the options start with drives that support Instant Secure Erase (ISE), a new technology to instantly and securely erase user data. 14G servers offers ISE-capable drives as a default. ISE is discussed in more detail later in this paper as part of the System Erase feature description.

The next higher security option is Self-Encrypting Drives (SEDs) that offer locking protection that binds the storage drive to the server and RAID card used. This protects against so-called “smash and grab” theft of drives and the subsequent loss of sensitive user data. When a thief tries to use the drive, he or she will not know the required locking key passphrase and therefore be thwarted from accessing the encrypted drive data.

The highest level or protection is offered by NIST FIPS 140-2 certified SED. Drives conforming to this standard have been accredited by testing laboratories and have tamper-resistant stickers applied to the drive. Dell EMC SED drives have FIPS 140-2 certification by default.



3.4.1 iDRAC Credential Vault

The iDRAC service processor provides a secure storage memory that protects various sensitive data such as iDRAC user credentials and private keys for self-signed SSL certificates. Another example of silicon-based security, this memory is encrypted with a unique immutable root key that is programmed into each iDRAC chip at the time of manufacture. This protects against physical attacks where the attacker de-solders the chip in an attempt to gain access to the data.

3.5 Hardware Security

Hardware security is an integral part of any comprehensive security solution. Some customers want to limit access to ports of entry, such as USB. A server chassis need not be opened in general after it has been put into production. In all cases, customers would at minimum like to track and log any such activities. The overall goal is to discourage and limit any physical intrusion.

3.5.1 Chassis Intrusion Alert

PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available. Sensors on the chassis detect when anyone opens or tampers with the chassis, even during transit. Servers that have been opened while in transit generate an entry in the iDRAC Lifecycle log after power is supplied.

3.5.2 Disable USB Ports

For more security, you can completely disable USB ports. You also have the option of disabling only the USB ports on the front. For example, USB ports can be disabled for production use and then temporarily enabled to grant access to a crash cart for debugging purposes.

3.5.3 iDRAC Direct

iDRAC Direct is a special USB port that is hardwired to the iDRAC service processor for at-the-server debugging and management from the front of the server (cold aisle). It allows a user to attach a standard Micro-AB USB cable to this port and the other end (Type A) to a laptop. A standard web browser can then access iDRAC GUI for extensive debugging and management of the server. If iDRAC Enterprise license is installed, the user can even access the OS desktop via iDRAC's Virtual Console feature.

Since normal iDRAC credentials are used for logging in, iDRAC Direct works as a secure crash cart with the additional advantage of extensive hardware management and service diagnostics. This can be an attractive option for securing physical access to the server in remote locations (host USB ports and VGA outputs can be disabled in this case).

3.5.4 iDRAC Connection View with Geolocation

A new feature for 14G is Connection View, which is the ability of iDRAC to report the external switches and ports connected to Server I/O. It is a feature on select networking devices (typically the newer, higher speed cards) and requires LLDP (Link Layer Discovery Protocol) be enabled on the switches connected.

Some of the benefits of Connection View are:

- Remotely and quickly check if server I/O modules (LOMs, NDCs, and add-in PCIe cards) are connected to the correct switches and ports
- Avoid costly remote dispatch of technicians to remediate wiring errors
- No more tracing of cables in the server room hot aisles
- Can be done via the GUI, or RACADM commands can provide information for all 14G connections

Beyond the obvious time and monetary savings, there is an additional benefit Connection View provides – providing real time geolocation of a physical server or virtual machine. Using iDRAC Connection View, admins can pinpoint a server to see exactly which switch and port the server is connected to – which helps in securing servers from being connected to networks and devices that don't comply with corporate security guidelines or best practices.

Connection View validates the location of the server indirectly by reporting the switch identities it is connected to. The switch identity helps determine the geolocation and assure that the server is not a rogue server in a non-authorized site, providing another layer of physical security. This also provides validation that an application or VM has not “crossed” country borders and is running in an approved, secure environment.

3.6 Supply Chain Integrity and Security

Supply Chain Integrity focuses on two key challenges:

(i) Maintaining Hardware Integrity: ensuring that there is no product tampering or insertion of counterfeit components before shipping product to customers

(ii) Maintaining Software Integrity: ensuring that no malware gets inserted in firmware or device drivers before shipping product to customers as well as preventing any coding vulnerabilities

Dell EMC defines supply chain security as the practice and application of prevention and detection control measures that protect physical assets, inventory, information, intellectual property, and people. These security measures also help provide supply chain assurance and integrity by reducing opportunities for the malicious or negligent introduction of malware and counterfeit components into the supply chain.

3.6.1 Hardware and Software Integrity

Dell EMC is focused on ensuring that quality control processes are in place to help minimize the opportunity for counterfeit components to infiltrate our supply chain. The controls Dell EMC has in place span supplier selection, sourcing, production processes, and governance through auditing and testing. Once a supplier has been selected, the new product introduction process verifies that all materials used during all build stages are sourced from the approved vendor list and match the bill of materials as appropriate. Material inspections during production help identify components that are mismarked, deviate from normal performance parameters, or contain an incorrect electronic identifier.

Parts are procured directly from the Original Design Manufacturer (ODM) or Original Component Manufacturer (OCM) when possible. The material inspection that occurs during the new product introduction process provides multiple opportunities to identify counterfeit or corrupted components that may have entered the supply chain.

Additionally, Dell EMC maintains ISO 9001 certification for all global manufacturing sites. Strict adherence to these processes and controls help minimize the risk of counterfeit components being embedded among the Dell EMC products, or malware getting inserted into firmware or device drivers. These measures are implemented as part of Software Development Lifecycle (SDL) process.

3.6.2 Physical Security

Dell EMC has several long-standing, key practices that establish and maintain security in manufacturing facilities and logistical networks. For example, we require certain factories where Dell EMC products are built

to meet specified Transported Asset Protection Association (TAPA) facility security requirements including the use of monitored closed circuit cameras in key areas, access controls, and continuously guarded entries and exits. Protective measures have also been put in place to guard products against theft and tampering during transport as part of an industry-leading logistics program. This program provides a continuously staffed command center to monitor select inbound and outbound shipments across the globe to ensure that shipments make it from one destination to another without disruption.

Dell EMC is also actively engaged in several voluntary supply chain security programs and initiatives. One such initiative is the Customs-Trade Partnership Against Terrorism (C-TPAT), introduced by the United States government after 9/11 to help reduce the potential for terrorism through strengthened border and supply chain security measures. As part of this initiative, the U.S. Customs and Border Protection agency asks participating members to ensure the integrity of their security practices and to communicate their security guidelines to their business partners within the supply chain. Dell EMC has been an active participant since 2002 and maintains the highest membership status.

4 Detect

It is critical to have a detection capability that provides complete visibility into the configuration, health status, and change events within a server system. This visibility must also detect malicious or other changes to BIOS, firmware, and Option ROMs within the boot and OS runtime process. Proactive polling must be coupled with the ability to send alerts for any and all events within the system. Logs must provide complete information about access and changes to the server. Most importantly, the server must extend these capabilities to all components.

4.1 Comprehensive Monitoring via iDRAC

Rather than depending upon OS agents to communicate with managed resources in a server, iDRAC employs a direct side-band path to each device. Dell EMC has leveraged industry standard protocols such as MCTP, NC-SI and NVMe-MI to communicate to peripheral devices such as PERC RAID controllers, Ethernet NICs, Fibre Channel HBAs, SAS HBAs, and NVMe drives. This architecture is the result of lengthy, multi-year partnerships with industry-leading vendors to provide agent-free device management in our PowerEdge servers. Configuration and firmware update operations also leverage the powerful UEFI and HII features that Dell EMC and our partners support.

With this capability, iDRAC can monitor the system for configuration events, intrusion events (such as chassis intrusion detection mentioned earlier in this paper), and health changes. Configuration events are tied directly to the identity of the user that initiated the change, whether it is from a GUI user, API user, or console user.

4.1.1 Lifecycle Log

Lifecycle log is a collection of events that occur in a server over a period of time. Lifecycle log provides a description of events with timestamps, severity, user ID or source, recommended actions, and other technical information that could come very handy for tracking or alert purposes.

The following are the various types of information recorded in the Lifecycle Log (LCL) are:

- Configuration Changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events

4.1.2 Alerts

iDRAC provides the capability to configure different event alerts as well as actions to be performed when a particular Lifecycle Logs event occurs. When an event is generated, it is forwarded to the configured destinations by using the selected alert type mechanisms. You can enable or disable alerts through the iDRAC web interface, RACADM, or with iDRAC settings utility.

iDRAC supports different types of alerts such as:

- Email or IPMI alert
- SNMP trap
- OS and Remote System logs
- Redfish event
- WS event

Alerts can also be categorized by severity – Critical, Warning, or Informational.

Following filters can be applied to alerts:

- System health – For Example, Temperature, Voltage, or Device errors
- Storage health – For Example, Controller errors, physical or virtual disk errors
- Configuration changes – For Example, Change in RAID configuration, PCIe card removal
- Audit logs – For Example, Password authentication failure
- Firmware/Driver – For Example, Upgrades or Downgrade

Finally, IT Administrator can set different actions for alerts – Reboot, Power Cycle, Power Off, or No action.

4.2 Drift Detection

By enforcing standardized configurations and adopting a “zero tolerance” policy for any changes, organizations can reduce the potential for exploitations. Dell EMC OpenManage Essentials Console allows customer to define their own sever configuration baseline and then monitoring the drift of their production servers from those baselines. The baseline can be built based on different criteria to fit different production enforcement, such as security and performance. OpenManage Essentials can report any deviations from the baseline and optionally repair the drift with a simple workflow to stage the changes on iDRAC out of band. The changes can then take place at the next maintenance windows while servers rebooting to make the production environment compliance again. This staged process enables customer to deploy configuration changes to production without any sever downtime during non-maintenance hours. It increase the server availability without compromise on the serviceability and security.

5 Recover

Server solutions must support recovery to a known, consistent state as a response to a variety of events:

- Newly discovered vulnerabilities
- Malicious attacks and data tampering
- Corruption of firmware due to memory failures or improper update procedures
- Replacement of server components
- Retiring or repurposing a server

Below we discuss in detail how we respond to new vulnerabilities and corruption issues, and how we recover the server to its original state if needed.

5.1 Rapid Response to New Vulnerabilities

Common Vulnerabilities and Exposures (CVEs) are newly discovered attack vectors that compromise software and hardware products. Timely responses to CVEs are critical to most companies so they can swiftly assess their exposure and take appropriate action.

CVEs can be issued in response to new vulnerabilities identified in many items including the following:

- Open source code such as OpenSSL
- Web browsers and other Internet access software
- Vendor product hardware and firmware
- Operating systems and hypervisors

Dell EMC works aggressively to quickly respond to new CVEs in our PowerEdge servers and provide customers timely information including the following:

- Which products are affected
- What remediation steps may be taken
- If needed, when updates will be available to address the CVE

5.2 BIOS and OS Recovery

Dell EMC 14th generation PowerEdge servers include two types of recovery: BIOS Recovery and Rapid Operating System (OS) Recovery. These features enable rapid recovery from corrupted BIOS or OS images. In both cases, a special storage area is hidden from run-time software (BIOS, OS, device firmware, etc.). These storage areas contain pristine images that can be used as alternatives to the compromised primary software.

Rapid OS Recovery enables rapid recovery from a corrupted OS image (or an OS image suspected of malicious tampering). The recovery media can be via internal SD card, SATA ports, M.2 drives, or internal USB. The selected device can be exposed to the boot list and the OS for the installation of the recovery image. It can then be disabled and hidden from the boot list and OS. In the hidden state, BIOS disables the device so it cannot be accessed by the OS. In the event of a corrupted OS image, the recovery location can then be enabled for boot. These settings can be accessed through BIOS or the iDRAC interface.

In extreme cases, if BIOS is corrupted (either due to a malicious attack, or due to a power loss during the update process, or due to any other unforeseen event), it is important to provide a way to recover BIOS to its original state. A backup BIOS image is stored in iDRAC so it can be used to recover the BIOS image if needed. iDRAC orchestrates the entire end-to-end recovery process.

- *Automatic BIOS recovery* is initiated by BIOS itself.
- *On-demand BIOS recovery* can be initiated by users using the RACADM CLI command.

5.3 Firmware Rollback

It is recommended to keep firmware updated to ensure you have the latest features and security updates. However, you may need to rollback an update or install an earlier version if you encounter issues after an update. If you rollback to the previous version, it is also verified against its signature.

Firmware Rollback from existing production version “N” to a previous version “N-1” is currently supported for the following firmware images:

- BIOS
- iDRAC with Lifecycle Controller
- Network Interface Card (NIC)
- PowerEdge RAID Controller (PERC)
- Power Supply Unit (PSU)
- Backplane

You can roll back the firmware to the previously installed version (“N-1”) using any of the following methods:

- iDRAC web interface
- CMC web interface
- RACADM CLI – iDRAC and CMC
- Lifecycle Controller GUI
- Lifecycle Controller-Remote Services

You can roll back the firmware for iDRAC or any device that Lifecycle Controller supports, even if the upgrade was previously performed using another interface. For example, if the firmware was upgraded using the Lifecycle Controller GUI, you can roll back the firmware using the iDRAC web interface. You can perform firmware rollback for multiple devices with one system reboot.

On the 14th generation PowerEdge servers that have a single iDRAC and Lifecycle Controller firmware, rolling back the iDRAC firmware also rolls back the Lifecycle Controller firmware.

5.4 Restoring Server Configuration after Hardware Servicing

Remediating service events is a critical part of any IT operation. The ability to meet recovery time objectives and recovery point objectives has direct implications on the security of the solution. Restoring server configuration and firmware assures that security policies for server operation are automatically met.

PowerEdge servers provide functionality that quickly restores server configuration in the following situations:

- Individual part replacement
- Motherboard replacement (full server profile backup and restore)
- Motherboard replacement (Easy Restore)

5.4.1 Parts Replacement

iDRAC automatically saves the firmware image and configuration settings for NIC cards, RAID controllers, and Power Supply Units (PSUs). In the event of a field replacement of these parts, iDRAC automatically detects the new card and restores the firmware and configuration to the replaced card. This functionality saves critical time and ensures a consistent configuration and security policy. The update occurs automatically on system reboot after replacing the supported part.

5.4.2 Easy Restore (for Motherboard Replacement)

Motherboard replacements can be time-consuming and affect productivity. iDRAC offers the ability to backup and restore a PowerEdge server’s configuration and firmware to minimize the effort needed to replace a failed motherboard.

There are two ways the PowerEdge server can backup and restore:

1. PowerEdge servers automatically backup system configuration settings (BIOS, iDRAC, NIC), Service Tag, UEFI diagnostics app and other licensed data to the flash memory.

   After you replace the motherboard on your server, Easy Restore prompts you to automatically restore this data.

2. For a more comprehensive backup, a user can back up the system configuration, including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and Network Daughter Cards (NDCs) and the configuration settings of those components. The backup operation also includes the hard disk configuration data, motherboard, and replaced parts. The backup creates a single file that you can save to a vFlash SD card or network share (CIFS, NFS, HTTP or HTTPS).

   This profile backup can be restored anytime by the user. Dell EMC recommends that you perform the backup operation for every system profile you think you might want to restore at some point.

5.5 System Erase

At the end of a system's lifecycle, it either needs to be retired or repurposed. The goal of System Erase is to erase sensitive data and settings so that no confidential information unintentionally leaks. It is a utility in Lifecycle Controller that is designed to erase logs, configuration data, storage data, cache, and any embedded apps.

The following devices, configuration settings, and apps can be erased by using the System Erase feature:

- iDRAC is reset to default
- Lifecycle Controller (LC) data
- BIOS
- Embedded diagnostics and OS driver packs
- iSM
- SupportAssist Collection reports

Additionally, the following components can also be erased:

- Hardware Cache (clear PERC NVCache)
- vFlash SD Card (initialize card)

Data on the following components are cryptographically disposed of by System Erase as described below:

- SED (Self Encrypting Drives)
- ISE-only drives (Instant Secure Erase drives)
- NVM devices (Apache Pass, NVDIMMs) – Available later in 2018

Additionally, non-ISE SATA hard drives can be erased using data overwrite.

Note that Instant Secure Erase (ISE) destroys the internal encryption key used in 14G drives thus rendering the user data unrecoverable. ISE is a recognized method of data erasure on storage drives referred to in NIST Special Publication 800-88 “Guidelines for Media Sanitization.”

Advantages of the new ISE feature with System Erase are the following:

- **Speed:** far faster than data over-writing techniques like DoD 5220.22-M (seconds versus hours)
- **Effectiveness:** ISE renders all the data on the drive, including reserved blocks, completely unreadable
- **Better TCO:** storage devices can be reused instead of being crushed or otherwise physically destroyed

System Erase can be accessed from Lifecycle GUI, WS-Man API, or RACADM CLI.

5.6 Full Power Cycle

In a Full Power Cycle, the server as well as all of its components are rebooted. It drains main and auxiliary power from the server and all components. All data in volatile memory is also erased.

A *physical* Full Power Cycle requires taking out the AC power cable, waiting for 30 seconds, and then putting the cable back. This poses a challenge when working with a remote system. A new feature in 14G servers allows you to do an effective Full Power Cycle from iSM, IDRAC GUI, BIOS, or a script. Full Power Cycle takes effect at the next power cycle.

Full Power Cycle feature eliminates the need for anyone to be physically present in the data center, thus reducing time to troubleshoot. It can eliminate, for example, any malware that is still memory-resident.

6 Summary

Data center security is paramount to business success and the security of the underlying server infrastructure is critical. Cyberattacks have the potential for extended system and business downtime, lost revenue and customers, legal damages and tarnished corporate reputation. To protect, detect, and recover from hardware-targeted cyberattacks, security needs to be built into server hardware design, not added on after the fact.

Dell EMC has been a leader in leveraging silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. The new 14G PowerEdge product line features an enhanced Cyber Resilient Architecture that uses silicon-based Root-of-Trust to further harden server security including the following features:

- **Cryptographically-verified Trusted Booting** that anchors end-to-end server safety and overall data center security. It includes features like silicon-based Root-of-Trust, digitally signed firmware and automatic BIOS recovery
- **iDRAC Credential Vault**, a secure storage space for credentials, certificates, and other sensitive data that is encrypted with a silicon-based key that is unique for every server
- **System Lockdown**, a capability unique to PowerEdge, helps secure any system configuration and firmware from malicious or unintended changes while alerting users to any attempted system changes
- **System Erase**, which allows users to easily retire or repurpose their 14th generation PowerEdge servers by securely and quickly wiping data from storage drives and other embedded non-volatile memory

In conclusion, the 14th generation PowerEdge servers, with their industry leading security, form the trusted bedrock of the modern data center upon which customers will securely run their IT operations and workloads.

A Appendix: Further Reading

Security White Papers and Collateral

- (Direct from Dev) SYSTEM ERASE ON POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242

  SECURING 14TH GENERATION DELL EMC POWEREDGE SERVERS WITH SYSTEM ERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Direct from Dev) SECURITY IN SERVER DESIGN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243

  (Direct from Dev) CYBER-RESILIENCY STARTS AT THE CHIPSET AND BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061

- FACTORY GENERATED DEFAULT IDRAC9 PASSWORD
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368

  DELL EMC IDRAC RESPONSE TO CVE-2017-1000251 “BLUEBORNE”
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605

  (Video) SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING RACADM
  https://youtu.be/mrIIN4X380c

- (Video) SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING WSMAN
  https://youtu.be/0D1Zq1CtRwg

  SECURE BOOT MANAGEMENT ON DELL EMC POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signing UEFI images for Secure Boot feature in the 14th generation and later Dell EMC PowerEdge servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255

- RAPID OPERATING SYSTEM RECOVERY
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266

PowerEdge White Papers

- iDRAC Overview
  http://www.DellTechCenter.com/iDRAC
- OpenManage Console Overview
  http://www.DellTechCenter.com/OME
- OpenManage Mobile Overview
  http://www.DellTechCenter.com/OMM
- Lifecycle Controller Part Replacement
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Motherboard Replacement
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- Managing Server Configuration by using Dell EMC OpenManage Essentials (OME)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444397