

Cyber Resilient Security in Dell PowerEdge Servers

October 2023

H19738.1

White Paper

Abstract

This white paper highlights the Dell PowerEdge Cyber Resilient Architecture and describes the server life cycle for implementing zero-trust principles for your infrastructure. Dell PowerEdge security controls provide a comprehensive security solution that ensures resiliency while enforcing a zero-trust posture.

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2023 Dell Inc. or its subsidiaries. Published in the USA October 2023 H19738.1.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary	5
Overview	5
Revisions.....	5
We value your feedback	5
Introduction	6
Digital infrastructure complexity	6
Sophistication and complexity of threats	6
Regulatory landscape and internal mandates	6
Zero Trust strategy for the modern world	6
Core principles of Zero Trust	7
Seven pillars of Zero Trust.....	8
The Dell advantage	9
Security journey across the server life cycle	10
First stage – Choosing the server	10
Challenges	10
PowerEdge solutions.....	10
Dell Secure Development Lifecycle	11
Compliance advantage.....	11
Rapid response to new vulnerabilities	12
Bug Bounty Program.....	12
Solutions covering threat vectors for every layer of the server.....	13
Second stage – Supply chain security	14
Challenges	14
PowerEdge solutions.....	14
End-to-end supply chain assurance	14
Secured Component Verification.....	16
Software Bill of Materials.....	16
Third stage – Efficient deployment and configuration at-scale	17
Challenges	17
PowerEdge solution.....	17
System integrity.....	17
Hardware security	20
Protecting data at rest	21
Protecting Data in Flight.....	23
Protecting data in use	26
Identity Access Management	28
Capabilities and automation for efficient at-scale deployment	30

Fourth Stage – Security management and monitoring	31
Challenges	31
PowerEdge Solutions	31
Visibility, logging, and alerts	31
SELinux framework	33
Real-time detection – BIOS Live scan	33
Silicon-based Root of Trust	34
Automated and manual recovery	36
Updating	38
Restoring server configuration after hardware servicing	38
CloudIQ.....	39
Managed detection and response services	39
Fifth stage – Secure decommissioning and repurposing	40
Challenge	40
PowerEdge solutions.....	40
Secure Erase	41
Secure erase – physical disk.....	41
Data sanitization and destruction services.....	42
Summary	42
References	44
Dell Technologies documentation	44

Executive summary

Overview

The Dell Technologies approach to security is intrinsic in nature – it is built-in, not bolted-on later, and it is integrated into every step of Dell’s Secure Development Lifecycle. We continuously strive to evolve our Dell PowerEdge security controls, features, and solutions to meet the ever-changing threat landscape and to help customers accelerate Zero Trust adoption.

Securing your infrastructure is not a one-time investment, but a mindset and overall approach. This white paper uses this journey perspective to describe the PowerEdge advantages across the server life cycle. In each of the life cycle phases, from deployment through maintenance to decommissioning, we highlight how Dell’s PowerEdge Cyber Resilient Architecture security features work together to provide both resiliency and a zero-trust approach. The Dell Remote Access Controller (iDRAC9) enables many of these features.

We continue to anchor security with a Silicon-based Root-of-Trust (RoT). Since the previous PowerEdge cyber resilient security whitepaper, many new features have been added that span from access control to data encryption to supply chain assurance. All features make extensive use of intelligence and automation to help you stay ahead of the threat curve, and to enable the scaling demanded by ever-expanding use models. Dell’s Cyber Resilient Architecture, enhanced over many years, is the foundation for the critical elements of a Zero Trust environment.

Revisions

Date	Part number/ revision	Description
November 2022	H19738	Initial release
October 2023	H19738.1	Updated to include the 16 th generation of PowerEdge servers

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

Authors: Deepak Rangaraj, Kim Kinahan

Contributors: Marshal Savage

Note: For links to other documentation for this topic, the [Dell Technologies Info Hub for PowerEdge](#).

Introduction

Digital infrastructure complexity

Modern IT environments have changed drastically in the past few years with servers being deployed in various use cases such as on-premises, multicloud, Edge, Telco, and so on. The server platforms are becoming more complex with an ever-increasing number of components that require firmware for configuration and management. We are generating data at a speed and volume higher than ever and this data is often generated and stored at numerous locations distributed geographically. This increasing complexity necessitates effective management of security controls to mitigate the expansion of the attack surface.

Sophistication and complexity of threats

The Dell Technologies Digital Transformation Index found that data privacy and cybersecurity concerns are the leading barriers to digital transformation¹. The complexity, sophistication, and frequency of cyberattacks are increasing, and the damage caused by attacks is becoming more costly. Complicating matters further, today's threat actors are taking advantage of technological advancements, such as AI and a lower cost of entry. Malicious actors are continuously searching for vulnerabilities to exploit. With the assistance of advanced AI systems, they can carry out nefarious activities at an unprecedented scale and manipulate systems in innovative and harmful ways beyond human capabilities. Global damages related to cybercrime are predicted to reach \$10.5 trillion by 2025.²

Regulatory landscape and internal mandates

As global threats increase, governments worldwide are developing regulatory guidance in response to cyber threats. As a result, private institutions are creating stronger policies and mandates to mitigate advanced persistent threats. Also, there are more mandates for security requirements that are needed to work with the government. These requirements impact suppliers, vendors, and any organization that partners with the government. In addition, regulations are carrying over to the critical infrastructure sectors, such as healthcare, transport, and finance. Outside of government regulations, many customers want to harden their infrastructure and are developing their own internal mandates or security policies.

Zero Trust strategy for the modern world

The increasing infrastructure complexity and threat landscape are driving a critical need to secure not only infrastructure hardware, but also the firmware and the supply chain itself. When applying a Zero Trust strategy, customers focus on business controls, the control plane, and applications and data. However, there is a critical need to secure what is below these items, including infrastructure hardware and firmware, supply chain for the infrastructure, and design and processes used to build the infrastructure. Zero Trust principles must be applied to all these aspects for more comprehensive cyber resilience.

Dell Technologies has security built into our industry-leading servers, storage, HCI, and data protection appliances to help protect data wherever it is stored, managed, or used. As a foundation for securing our PowerEdge server products, they are foremost cyber resilient – capable of anticipating, withstanding, and recovering from cyber threats.

¹ Dell Technologies 2020 Digital Transformation Index

² www.cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Simultaneously, the process of designing PowerEdge security controls and tools incorporates Zero Trust principles. By anticipating how customers want to use these capabilities while they are setting up their Zero Trust deployments, we have adapted our approach. We made it easier to work with us no matter where customers are on their journey towards Zero Trust adoption.

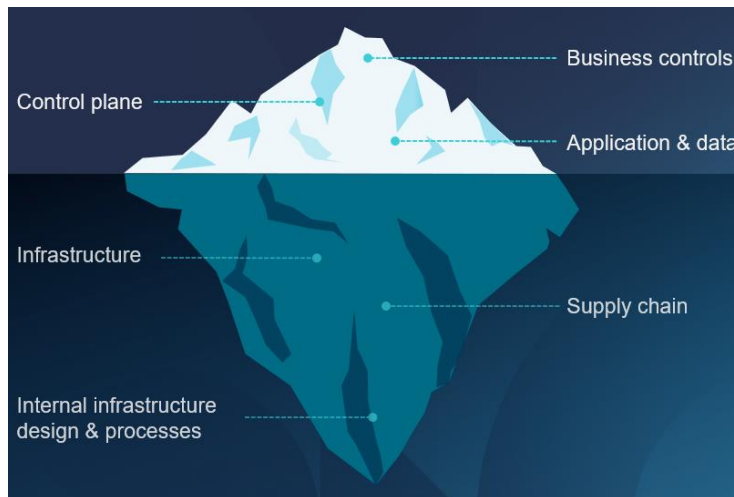


Figure 1. Infrastructure security and Zero Trust

The Dell infrastructure security approach is integral to Dell products and accelerates Zero Trust adoption because it is:

- Designed and built using Zero Trust principles
- Provides Zero Trust capabilities and features
- Provides common, consistent behavior

Core principles of Zero Trust

The tenets of Zero Trust architecture are built on a set of principles that presume that the *network is always vulnerable to compromise* and sets out to safeguard access to critical data and resources. Unlike trust-then-verify frameworks, a zero-trust approach eliminates implicit trust. Every user, device, and application must be continuously *authenticated and explicitly authorized* based on a range of factors such as identity, device status, location, and behavior.

Identity plays a crucial role in Zero Trust. Identification pertains not only to people but to applications, communication paths, network devices, and the data itself. When an IT asset is identified, authenticated, and explicitly authorized, the principle of *least privilege* is applied. This approach ensures that only authorized entities are given a minimum level of access required to perform their specific task. The data-centric security model constantly limits access while also looking for anomalous or malicious activity. The Zero Trust approach reduces the granularity of validation at key intersections for verified trust, optimizing least privilege without impacting workload efficiency. The goal is to deter attacks and reject them at point of entry. However, if a breach occurs, the amount of damage is minimized, along with an enhanced ability to detect and remediate immediately.

Adopting the Zero Trust mindset and using Zero Trust principles enables systems administrators to control how users, processes, and devices engage with data. These

principles can prevent the abuse of compromised user credentials, remote exploitation, insider threats, and even mitigate the effects of malicious supply chain activity.

Seven pillars of Zero Trust

The Zero Trust model, defined by the National Institute of Standards and Technology (NIST)³, identifies seven interrelated pillars that work together to provide a comprehensive and holistic approach to infrastructure and data security. Each pillar represents a specific functional or key focus area for implementation of Zero Trust security controls. When combined, these seven pillars provide a multifaceted, layered, and integrated security framework.

Dell's Zero Trust approach integrates a broad set of security controls and automation capabilities for the management of the infrastructure and the applications running on it. The following table highlights Dell's capabilities across the seven pillars as outlined by NIST:

Table 1. Dell Zero Trust approach across the seven pillars

Zero Trust pillar	NIST description ³	PowerEdge highlights
User	<p>User identification, authentication, and access control:</p> <ul style="list-style-type: none"> • Only validated and authorized users can access data and resources. • The principle of <i>least privilege</i> is applied where users are granted the minimum level of access required to perform their specific tasks. 	<ul style="list-style-type: none"> • Identity and Access Management • Multi-Factor Authentication—RSA Secure ID • Active Directory or LDAP integration with single sign-on (SSO) support • Role-based access control and auditing
Device	<p>Monitoring and enforcement of device health, compliance, and device posture assessment:</p> <ul style="list-style-type: none"> • Monitoring - looking for anomalies and suspicious read/write activity. • Health – confirming the latest version of the firmware. • All devices are identified, inventoried, authorized, authenticated, and updated. 	<ul style="list-style-type: none"> • Silicon Root-of-Trust (ROT) with complementary Intel Boot Guard and AMD Platform Secure Boot (AMD PSB) • Secure supply chain with Secured Component Verification (SCV) • Chassis locks and intrusion detection • Dynamic USB port enable/disable • Trusted Platform Module (TPM) • Device attestation with SPDM (Security Protocol Data Model from DMTF)
Data	<p>Ensure data transparency and visibility by using enterprise infrastructure, applications, standards, solid end-to-end encryption, and data tagging.</p>	<p>Data-at-rest protection:</p> <ul style="list-style-type: none"> • Drive encryption with local (LKM) or Secure Enterprise Key Management (SEKM) with direct-attached NVMe drive support • Baseboard Management Controller (BMC)-based Local Key Management (iLKM) <p>Data-in-use protection:</p>

³ National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture

Zero Trust pillar	NIST description ³	PowerEdge highlights
		<ul style="list-style-type: none"> Confidential compute—Intel SGX, Intel MKTME, AMD Secure Memory Encryption (SME) AMD SME, AMD Secure Encrypted Virtualization (SEV) SEV, AMD persistent memory encryption
Application and Workload	Secure applications and workloads, and protect containers and VMs.	<ul style="list-style-type: none"> Secure Development Lifecycle Cryptographically signed BIOS and firmware updates Secure end-to-end boot and Unified Extensible Firmware Interface (UEFI) boot capabilities Drift detection Rapid Response and mitigations for CVEs
Network and Environment	Encrypt, monitor, and analyze network. Logically and physically segment, isolate, and control the network and the environment (on-premises and off-premises) using granular access and policy restrictions.	<ul style="list-style-type: none"> Dedicated BMC (iDRAC) network module SSH/TLS communication options TLS 1.3 support DPU/SmartNIC
Visibility and Analytics	Monitor activities and behaviors across the infrastructure (user, device, data, network, and application) to identify patterns and anomalies. Use analytics to detect and respond to security threats.	<ul style="list-style-type: none"> Persistent event logging and auditing Real-time and boot time firmware scanning Security alerts CloudIQ
Automation and Orchestration	Automate manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale.	<ul style="list-style-type: none"> OpenManage Enterprise drift detection Firmware rollback Automatic BIOS and operating system recovery Centralized updates Automatic SSL certificate renewal

The Dell advantage

Security is in our DNA, and we are committed to making our products secure by design and secure by default. PowerEdge servers are built using Zero Trust principles internally and have capabilities that enable customers to set up a Zero Trust IT environment and operations. Our products also strive to provide common and consistent behavior and controls across our portfolio.

PowerEdge servers with iDRAC9 have an integrated immutable silicon-based platform Root-of-Trust (RoT) that is used to establish a verified chain of trust that extends throughout the server life cycle, from deployment through maintenance to decommissioning. This RoT combined with security controls and comprehensive management tools provides robust layers of security across the PowerEdge hardware and firmware.

First stage – Choosing the server

These PowerEdge capabilities not only ensure cyber resiliency to protect, detect, and recover from attacks, they also maintain a locked-down posture for a Zero Trust approach of least privilege. Least privilege ensures that users and devices are only given access to what they need to perform their tasks. Our goal is to make Zero Trust a reality for our customers and accelerate its speed of adoption.

Security journey across the server life cycle

Implementing security across your infrastructure requires a series of ongoing efforts and measures to protect underlying systems, networks, and resources. Transitioning to a mature security model is not a one-time investment and cannot be accomplished overnight. It is an ongoing journey and approach of implementing stringent security policies. As your Zero Trust implementation matures over time, enhanced visibility and extensive controls allow you to keep pace with the threat landscape. We have organized this journey into five stages.

- **Stage 1: Choosing the server**—Customers want assurance that security is a top priority and is built into every aspect of design.
- **Stage 2: Ensuring supply chain security**—Customers face the real risk of malicious offenders replacing original components with counterfeits, implants, or malware.
- **Stage 3: Efficient deployment and configuration at scale**—How a server is deployed has a direct impact on its performance, stability, and security. Proper planning and configuration are essential to ensure that the server is set up correctly and that all necessary components are in place.
- **Stage 4: Security management and monitoring**— Because attacks happen quickly, faster than a human can detect, customers must proactively monitor their environment to take quick action. The lack of skills and training can also exacerbate the problem.
- **Stage 5: Secure repurposing and decommissioning**—Data security is a key consideration when the server is repurposed or retired. IT best-practices recommend removing all data from the server to ensure that confidential information is not inadvertently shared or compromised.

First stage – Choosing the server

Challenges

Customers want to be confident that their server is secure in its entirety and does not introduce any vulnerabilities into their environment. They want assurances from server vendors addressing every aspect of design, the entire supply chain, including hardware, software, and firmware. This level of assurance differentiates on-premises infrastructure when compared to cloud service providers who might only offer a black box infrastructure, leaving customers uncertain about the security of the underlying components of their cloud-based system.

PowerEdge solutions

The first step of the Zero Trust journey with Dell Technologies starts before you receive your PowerEdge server. Intrinsic security practices are incorporated into hardware product design and software or firmware code development. These practices include processes and policies that ensure security features are implemented at the time of product inception and continue throughout the development cycle. In essence, security is

'built' in. To perform this practice effectively, our engineers are required to take mandatory security training before handling the code. Security champions are assigned to each development team to drive a security culture in the organization.

Dell Secure Development Lifecycle

Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development. The Secure Development Lifecycle (SDL) model is used to make security an integral part of the overall server design process. Some key aspects of this process include:

- Features that are conceived, designed, prototyped, implemented, set into production, deployed, and maintained with security as a key priority
- Server firmware that is designed to obstruct, oppose, and counter the injection of malicious code during all phases of the product development life cycle:
 - Threat modeling and penetration testing provide coverage during the design process.
 - Secure coding practices are applied at each stage of firmware development.
- For critical technologies, external audits that 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 2. Dell Secure Development Lifecycle

Compliance advantage

Dell Technologies has received the certifications that are needed to comply with major United States Federal and other global governmental requirements as well as industry standards such as from NIST, as described in the following table:

Table 2. Certification descriptions

Certification	Description
Common Criteria	Certain configurations of PowerEdge Servers include components with common criteria certifications. (For example, iDRAC and TPM)
FIPS 140	Certain configurations of PowerEdge Servers include FIPS 140-certified cryptographic modules (For example, TPM, iDRAC9, Chassis Management Controller (CMC), Self-Encrypting Drives (SEDs), and SSDs)
IPv6	<ul style="list-style-type: none">• PowerEdge Servers are fully USGv6r1 and IPv6 Ready Logo-compliant and certified with IPv6-only capabilities while running operating systems such as Red Hat Enterprise Linux 8.4 and the applicable versions of Windows 2019 or Windows 2022 Server.• Dell PowerEdge iDRAC9 (with 5.1x firmware) is USGv6r1 and IPv6 Ready Logo-compliant and certified with IPv6-only capabilities.

Rapid response to new vulnerabilities

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.

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

- The products that are affected
- Remediation steps
- If needed, availability of updates to address the CVEs

Bug Bounty Program

Dell Technologies recognizes the value of the security research community to broaden visibility into potential vulnerabilities and threats and welcomes the opportunity to collaborate with community members who share this common goal.

Dell's Bug Bounty Program applies to security vulnerabilities identified in Dell-branded or currently supported products.

Solutions covering threat vectors for every layer of the server

There are many threat vectors in today's changing landscape. The following tables summarize the Dell approach to managing critical threats in each of the server layers.

Table 3. Dell solution for common server platform layer threat vectors

Server platform layers		
Security layer	Threat vector	Dell solution
Physical server	Server/component tampering or theft of component	<ul style="list-style-type: none"> Secured Component Verification (SCV) Chassis Intrusion Detection Secure Enterprise Key Management Intel TME SPDM
Firmware and software	<ul style="list-style-type: none"> Firmware corruption Malware injection 	<ul style="list-style-type: none"> Silicon-based Root-of-Trust Intel Boot Guard AMD Secure Root-of-Trust UEFI Secure Boot Customization Cryptographically signed and validated firmware
	Software	<ul style="list-style-type: none"> CVE reporting Patching as required
Attestation trust features	Server identity spoofing	<ul style="list-style-type: none"> TPM Intel TXT Chain of trust 802.1x features SPDM
Server management	<ul style="list-style-type: none"> Rogue configuration and updates Unauthorized open-port attacks 	<ul style="list-style-type: none"> iDRAC9 Remote attestation

Table 4. Dell solution for common server environment layer threat vectors

Server environment layers		
Security layer	Threat vector	Dell Technologies solution
Data	Data breach	<ul style="list-style-type: none"> • Self-Encrypting Drives (SED) – FIPS or Opal/TCG • Secure Enterprise Key Management ISE-only (Instant Secure Erase) drives • Secure User Authentication
Supply Chain Integrity	<ul style="list-style-type: none"> • Counterfeit components • Malware threats 	<ul style="list-style-type: none"> • ISO9001 certification for all global server manufacturing sites • Secured Component Verification • Proof of possession • Software Bill of Materials (SBOM) • Security measures implemented as part of the Secure Development Lifecycle
Supply Chain Security	<ul style="list-style-type: none"> • Physical security in manufacturing sites • Theft and tempering during transport 	<ul style="list-style-type: none"> • Transported Asset Protection Association (TAPA) facility security requirements • Customs-Trade Partnership Against Terrorism (C-TPAT) • Secured Component Verification

Second stage – Supply chain security

Challenges

Modern server platforms are becoming more complex with hundreds of components that require firmware for configuration and management. As a result, the server supply chain is also becoming increasingly complex with hundreds of third-party vendors supplying components as well as the use of open-source software. This complex supply chain contributes to an increase in the attack surface available for threat actors if not managed properly. Customers face the risk of vulnerabilities and threats being introduced into their environments if the supply chain integrity is not assured. The two main aspects of supply chain integrity include:

- **Maintaining hardware integrity**—Ensuring that there is no product tampering or the insertion of counterfeit components or malicious implants before the product is shipped to customers.
- **Maintaining software integrity**—Ensuring that no malware is inserted in firmware or device drivers before shipping the product to customers and preventing code with known vulnerabilities from being introduced into the environment.

PowerEdge solutions

End-to-end supply chain assurance

Dell Technologies employs a multifaceted approach to protect its supply chain and delivers solutions that customers can trust in an increased threat environment. Our supply chain security consists of prevention and detection controls that protect physical assets, inventory, information, intellectual property, and people. These security measures provide

supply chain assurance and ensure integrity by reducing opportunities for the malicious or negligent introduction of malware and counterfeit components into the supply chain.

Dell supply chain controls span supplier selection, sourcing, production processes, and governance through auditing and testing. When 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 might have entered the supply chain.

Additionally, Dell Technologies maintains ISO 9001 certification for all global manufacturing sites. Strict adherence to these processes and controls helps minimize the risk of counterfeit components being embedded among the Dell products or malware being inserted into firmware or device drivers. As part of SDL, Dell Technologies has several long-standing, key practices that establish and maintain security in manufacturing facilities and logistical networks.

Facilities used to design, build, customize, or fulfill Dell products must demonstrate compliance with several internationally recognized physical security standards such as those defined by the Transported Asset Protection Association (TAPA), American Society for Industrial Security (ASIS), International Standards Organization (ISO), and the Business Alliance for Secure Commerce (BASC).

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 Technologies audits suppliers and facilities, addressing various factors, including the use of digital closed-circuit TV cameras, access control systems, intrusion detection, and guard service protocols. Other controls are applied to protect Dell cargo during the shipping and logistics process, including tamper-evident packaging, cargo locks and seals, and threat intelligence monitoring of key freight lanes. Internet of Things (IoT) tracking devices are also deployed on select shipments to enable real-time telemetry data monitoring to escalate any security noncompliance events observed during transit.

Dell Technologies also maintains certifications in multiple secure trade and commerce programs such as Tier 3 status with the United States Customs and Border Protection's Customs Trade Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP), Singapore's Secure Trade Partnership, and Authorized Economic Operator (AEO) status in several other nations. These programs are internationally recognized by member states of the World Customs Organization and demonstrate "best in class" supply chain security standards in the private sector. These programs focus on supplier accountability, security management policies, counter smuggling, trafficking controls, and tamper prevention – all intended to secure trade across international borders.

Second stage – Supply chain security

Supply chain integrity ensures that customers' products are safely delivered and when received, operate as intended. An important feature of supply chain integrity is the development of hardware and software baseline specifications that are preserved securely and later used as a reference to verify that no unauthorized modifications have been made.

Secured Component Verification

Dell Technologies' Secured Component Verification (SCV) for PowerEdge is a supply chain assurance offering that verifies that the server received by a customer matches the configuration that was shipped from the factory. The factory generates a certificate that contains unique component IDs for a specific server. This certificate is stored in a cryptographically secure vault in iDRAC. On receiving the server, the customer runs the SCV application on the host to generate an inventory of the current system, including unique component IDs, and then validates it against the golden factory inventory in the SCV certificate stored in iDRAC.

The SCV application generates a report that identifies any component mismatches from what was installed in the factory. It also verifies the certificate and Chain of Trust along with the Proof of Possession of the SCV Private key for iDRAC. The current implementation supports direct ship customers and does not include Value Added Reseller (VAR) or Part Replacement scenarios.

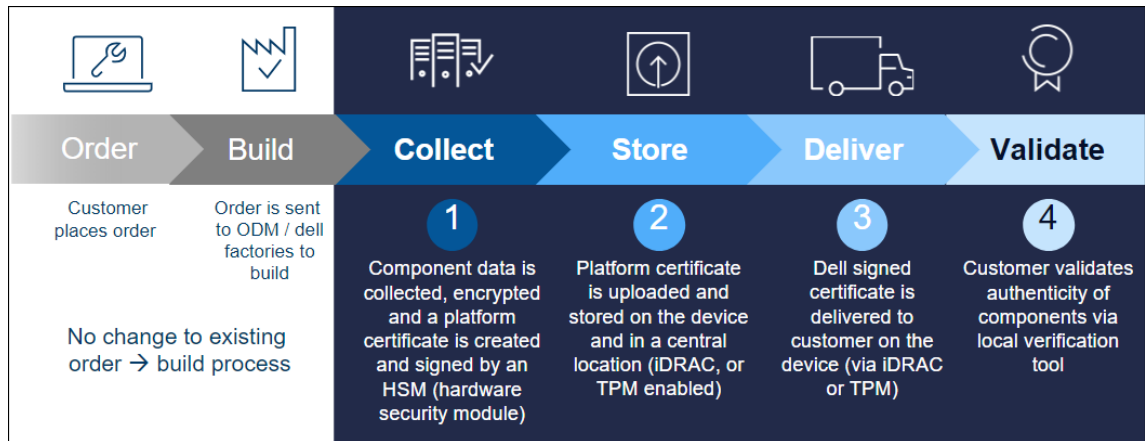


Figure 3. Dell Secured Component Verification

Software Bill of Materials

As part of Dell's software supply chain security controls, NIST standards, and in alignment with the President's Executive Order (EO) 14028, a Software Bill of Materials (SBOM) is available for a limited number of products across our portfolio. Dell SBOM data adheres to the Software Package Data Exchange (SPDX) standard and is provided in JSON format. SBOM data provides software supply chain transparency and can be used in vulnerability scanning and asset tracking tools on the customer side.

SBOM enables customers to gain a clearer understanding of the software components, versions, licenses, and any open-source software used on the platform. It can facilitate faster detection of known security vulnerabilities in the software components, ultimately enhancing security.

Third stage – Efficient deployment and configuration at-scale

Challenges

Cyber resilient configuration and deployment of the servers is a critical step in the server life cycle. Any mistakes or oversights during this process can result in poor server performance, downtime, or even security breaches. The right set of controls and gates must be in place to ensure system and data integrity throughout the server operation. This configuration and deployment must be performed for hundreds or thousands of servers while ensuring consistency and minimizing any manual errors.

PowerEdge solution

System integrity

Ensuring system integrity is foundational for securing the server and establishing a lockdown posture for Zero Trust operations. This integrity starts with ensuring that server hardware and components are genuine, and from a trusted and authorized source. Then, the firmware and software must be verified to ensure that a bad actor has not tampered with them. For PowerEdge, this process of ensuring system integrity starts with a silicon-based platform RoT. This RoT anchors the other security controls on the server platform and establishes a chain of trust for cryptographic verification of hardware and software components on the server.

RoT as the anchor for 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 operating system or updating firmware.

All PowerEdge servers have an immutable, silicon-based RoT burnt into them from the factory. The RoT has one-time programmable, read-only public keys that can be used for cryptographic verification and attestation of integrity.

The BIOS boot process uses Intel Boot Guard technology or AMD PSB technology that cryptographically verifies the BIOS code to be loaded. A verification failure results in a server shutdown and the Lifecycle Controller Log includes a notification. The IT administrator can then initiate the BIOS recovery. If Boot Guard validates successfully, a chain of trust procedure validates the remaining BIOS modules until control is handed off to the operating system or hypervisor.

In addition to Boot Guard's verification mechanism, iDRAC9 4.10.10.10 or higher provides a RoT mechanism to verify the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time, on demand, or at user-scheduled intervals.

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 operating system 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 RoT to meet recommendations in NIST SP 800-147B (*BIOS Protection Guidelines for Servers*) and NIST SP 800-155 (*BIOS Integrity Measurement Guidelines*).

Security Protocol Data Model for component attestation

The Distributed Management Task Force (DMTF), of which Dell Technologies is a leading member, defines the Security Protocol Data Model (SPDM). SPDM defines a consistent, open-standard method of communicating in the server to gather information about server components. This component information is protected by encrypting it and using authenticated key exchange to integrity-protect all communications between components. iDRAC SPDM implementation provides visibility into the PERC12 and certain NIC components. As part of the hardware inventory, iDRAC verifies the authenticity and integrity of PERC12 and NIC devices by cryptographically verifying the identity, firmware, and configuration.

TPM Support

PowerEdge servers support two versions of TPM:

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

TPM can be used to perform public key cryptographic functions, compute cryptographic hash functions, generate, manage, and securely store keys, and perform attestation. Intel's Trusted Execution Technology (TXT) functionality and Microsoft's Platform Assurance feature in Windows Server 2016 is also supported. TPM can also be used to enable the BitLocker hard drive encryption feature in Windows Server 2012, Windows Server 2016, and Windows Server 2022.

Attestation and remote attestation solutions can use TPM to take measurements at boot time of a server's hardware, hypervisor, BIOS, and operating system, and compare them in a cryptographically secure manner against "golden" or "base" measurements. These measurements are commonly stored outside the TPM on a remote attestation server solution. The TPM PCR measurements stored in the TPM are recalculated on every boot. If they are not identical, the server system might have been compromised and system administrators can disable and disconnect the server either locally or remotely.

Servers can be ordered with or without TPM, but for many operating systems and other security provisions, it is becoming a standard. TPM is enabled through a BIOS option. It is a Plug-In Module solution; the planar has a connector for this plug-in module.

UEFI Secure boot for firmware

PowerEdge servers also support industry-standard UEFI Secure Boot that checks the cryptographic signatures of UEFI drivers and other code loaded before the operating system is running. Secure Boot represents an industry-wide standard for security in the preboot 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, the 14th, 15th, and 16th generations of PowerEdge servers offer the unique flexibility of using a customized boot loader certificate. This certificate is primarily a feature for administrators of Linux environments that want to sign their own operating system boot loaders instead of relying on the default signing certificate provided by Microsoft's UEFI Certificate Authority (CA). Custom certificates can be uploaded by using the preferred

iDRAC API to authenticate the customer's specific operating system boot loader. The NSA cites this PowerEdge UEFI customization method for mitigating Grub 2 vulnerabilities in servers.⁴ PowerEdge supports complete customization of Secure Boot, including removal of all industry-standard certificates provided by Microsoft, VMware, or the UEFI CA.

Intel Boot Guard and AMD PSB

Intel Boot Guard and AMD PSB are host processor features that provide strong firmware integrity guarantees, by preventing firmware that is not authorized by the Dell OEM from running on the system. By enabling these features as additional defense-in-depth measures, certain classes of physical attacks are mitigated, such as flash memory replacement or reprogramming, and Time-of-Check-Time-of-Use (TOCTOU) race conditions. All combined, the RoT features in the system make compromise of the trusted computing base (TCB) difficult.

iDRAC/BMC

The Integrated Dell Remote Access Controller (iDRAC) is a Baseboard Management Controller (BMC) that is integrated in Dell PowerEdge servers. iDRAC provides secure and remote server access for many common management functions; administrators can deploy, manage, monitor, update, troubleshoot, and remediate Dell servers from any location without the use of agents and out of band.

iDRAC offers industry-leading security features that adhere to and are certified against well-known NIST standards, Common Criteria, and FIPS 140-2. It is through iDRAC9 that the end user can configure security features to maximize the security posture of the system.

iDRAC credential vault

The iDRAC service processor provides a secure storage memory that protects 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 memory protects against physical attacks where the attacker desolders the chip to gain access to the data.

SELinux framework

SELinux operates at the core kernel level on iDRAC and does not require user input or configuration. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to enrolled customers. In future iDRAC releases, these logs will be available in the Lifecycle Controller Logs.

Factory-generated default passwords

By default, all 14th, 15th, and 16th generations of PowerEdge servers ship with a unique, factory-generated iDRAC password to provide additional security. This password is on the pull-out Service Tag on the front of the chassis, next to the server asset label. If you choose this default option, use this password to log in to iDRAC for the first time, rather than using a universal default password. For security purposes, Dell Technologies strongly recommends changing the default password.

⁴ [CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF \(defense.gov\)](#)

Hardware security

Hardware security is an integral part of any comprehensive security solution. Some customers want to limit access to external ports, such as USB. Generally, a server chassis does not need to be opened after it has been put into production. At a minimum, customers always want to track and log any such activities. The overall goal is to discourage and limit any physical intrusion.

Chassis intrusion detection and 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.

Dynamic USB port management

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.

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 you to attach a standard Micro-AB USB cable to this port and the other end of the cable (Type A) to a laptop. A standard web browser can then access the iDRAC UI for extensive debugging and management of the server. If the iDRAC Enterprise license is installed, you can access the operating system desktop using the iDRAC's Virtual Console.

Because you use iDRAC credentials for logging in, iDRAC Direct works as a secure crash cart with the additional advantage of extensive hardware management and service diagnostics. This method is 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).

iDRAC Connection View with Geolocation

Connection View enables iDRAC to report the external switches and ports connected to Server I/O.

It is a feature on select networking devices and requires the Link Layer Discovery Protocol (LLDP) to be enabled on connected switches.

Some of the benefits of Connection View enable you to:

- 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
- Avoid tracing cables in the server room hot aisles
- Retrieve information for all connections by accessing the UI or by using RACADM commands

Beyond the obvious time and monetary savings, Connection View provides an additional benefit – real-time geolocation of a physical server or VM. Using iDRAC Connection View, administrators can pinpoint a server to see to which switch and port the server is connected. This information helps secure servers from being connected to networks and devices that do not comply with corporate security guidelines or best practices.

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

Protecting data at rest

Data at rest protection ensures that sensitive data that resides in storage is protected from unauthorized access through encryption and external key management.

Dell Technologies provides:

- Software-based encryption (for example, virtual devices)
- Enterprise key management (for example, SED devices and key management)
- Hardware drive encryption (for example, SED devices)

Whether it is due to internal policies or external compliance, securing data continues to be a high priority for organizations of all sizes.

The 14th, 15th, and 16th generations of PowerEdge servers offer several storage drive options for securing data, as shown in the following figure:

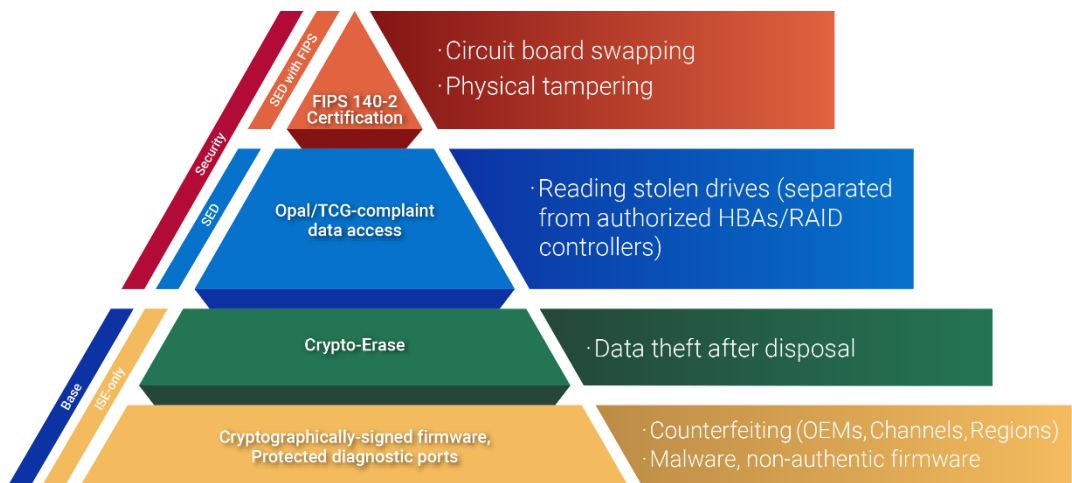


Figure 1. Storage drive options

The options start with drives that support Instant Secure Erase (ISE), a new technology to erase user data instantly and securely. The 14th, 15th, and 16th generations of PowerEdge servers offer ISE-capable drives as a default. This white paper describes ISE in more detail later as part of the System Erase feature description.

Third stage – Efficient deployment and configuration at-scale

The next higher security option is Self-Encrypting Drives (SEDs), which offer locking protection that binds the storage drive to the server and RAID card used. This method protects against so-called “smash and grab” theft of drives and the subsequent loss of sensitive user data. When thieves try to use the drive, they do not know the required locking key passphrase and are thwarted from accessing the encrypted drive data. Customers can protect against theft of the entire server by using Secured Enterprise Key Manager (SEKM), which is described in the following section.

NIST FIPS 140-2 certified SEDs offer the highest level of protection. Testing laboratories have accredited drives conforming to this standard. Tamper-resistant stickers are applied to the drive. Dell SED drives have FIPS 140-2 certification by default.

Secured Enterprise Key Manager

OpenManage Secured Enterprise Key Manager (SEKM) delivers a central key management solution to manage data at rest across the organization. It enables you to use an external Key Management Server (KMS) to manage keys that iDRAC can use to lock and unlock storage devices on a PowerEdge server. Using embedded code that is activated with a special license, iDRAC requests that the KMS creates a key for each storage controller, which iDRAC fetches and provides to the storage controller on every host boot so that the storage controller can unlock the SEDs.

The advantages of SEKM over Local Key Management (LKM) include:

- Protection against “Theft of a server” because the keys are not stored on the server and are stored externally and retrieved by connected PowerEdge server nodes (using iDRAC)
- Centralized and scalable key management for encrypted devices with high availability
- Support for the industry-standard Key Management Interoperability Protocol (KMIP), which enables the use of other KMIP-compatible devices
- Protection of data at rest when drives or the entire server are compromised
- On-drive encryption performance scales with drive count

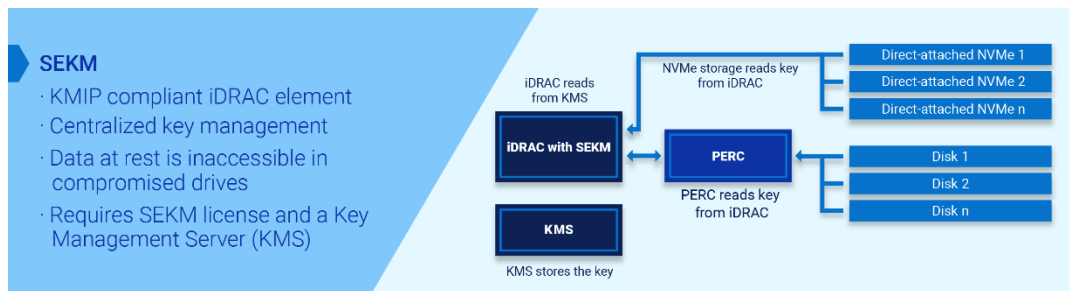


Figure 2. Secure Enterprise Key Manager (SEKM)

Local Key Management

PowerEdge servers provide the ability to secure SED drives connected to a PERC controller using Local Key Management (LKM).

To ensure user data protection if a drive is stolen, the SED must be locked with a separate key so that it does not decrypt user data unless that key is provided. This key is

referred to as the Key Encryption Key (KEK). The KEK is stored in the PERC, not on an external server.

Set a keyId/passphrase on the PERC controller to which the SED is connected. Then, the PERC controller generates a KEK using the passphrase and uses it to lock the SED. When the drive is powered on, it comes up as a locked SED and encrypts or decrypts user data only when the PERC provides the KEK to unlock it. If a locked drive is stolen, an attacker cannot provide the KEK, and the user data is protected.

The following figure shows the LKM solution:

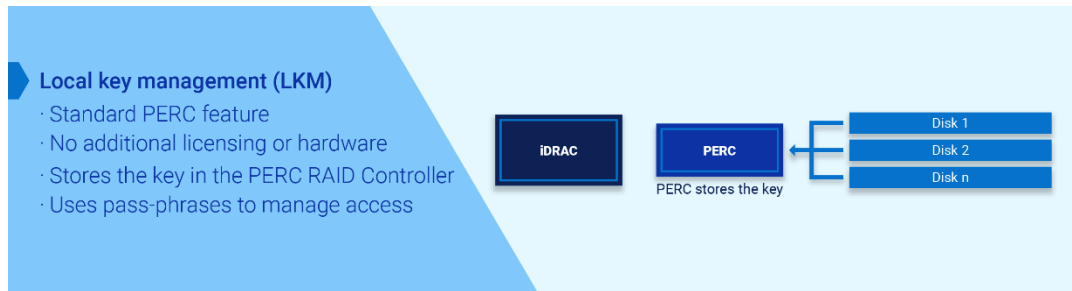


Figure 3. Local Key Management (LKM)

iLKM

For direct attach NVMe configurations where a PERC RAID controller is not available, iDRAC can be used as the key manager. This solution called OpenManage iLKM, is iDRAC-based and enables key exchange locally. iDRAC acts as a key manager and generates authentication keys that can then be used to secure storage devices. You can transition from iDRAC-based iLKM to iDRAC-based SEKM to upgrade to external key management.

The following figure shows the iLKM solution:

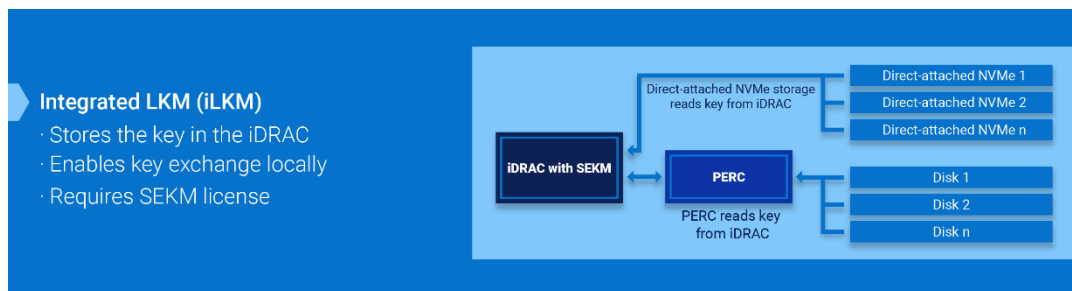


Figure 4. Integrated Local Key Management (iLKM)

Protecting Data in Flight

Data-in-flight protection ensures that data is protected from unauthorized disclosure or interception as it travels across networks or between systems. Sensitive data can be intercepted, stolen, or modified in transit, leading to data breaches, loss of intellectual property, and other security risks.

Distributed and cloud environments where data is constantly moving between systems and across networks, protecting your data through encryption and access controls are important components for data-in-flight protection in a Zero Trust environment.

TLS 1.3

The iDRAC web server uses a TLS/SSL certificate to establish and maintain secure communications with remote clients. Web browsers and command-line utilities, such as RACADM and WS-Man, use this TLS/SSL certificate for server authentication and establishing an encrypted connection.

There are several options available to secure the network connection using a TLS/SSL certificate. iDRAC's web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Whichever method you choose, when iDRAC is configured and the TLS/SSL certificate is installed on the management stations, TLS/SSL-enabled clients can access iDRAC securely and without certificate warnings.

SSH

iDRAC provides user control over the cryptographic settings for the SSH daemon such that you can determine the ideal settings for your environment. The control given to you is not a relaxation of the settings. Instead, the feature enables you to modify the value set for each option to achieve a narrower and stringent cryptographic policy. That is, you can only remove values from the options but cannot add any values other than those values that have been defined and allowed in the default value-set.

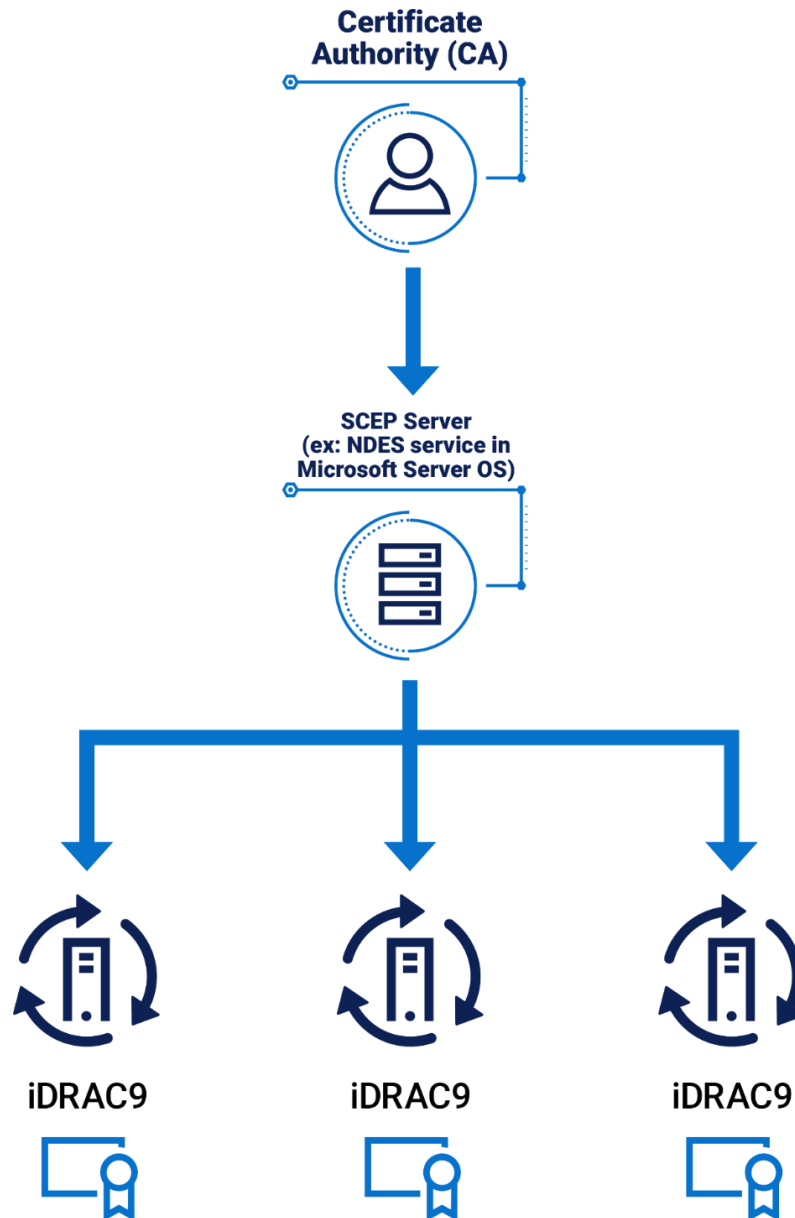
The cryptographic policies are configured using the following options:

- Ciphers — Ciphers
- Host-Key-Algorithms — HostKeyAlgorithms
- Key-Exchange Algorithms — KeyExchangeAlgorithms
- MACs — MACs

Typically, the values for each of these options are set to prudent settings that reflect the best security practices that cater to a wide variety of environments. As such, the iDRAC default settings for these options are the same as those options assigned by the SSH package open-source community. These settings can be configured using the RACADM command-line interface. See the *iDRAC RACADM CLI User's Guide*.

Automatic certificate renewal

iDRAC9 v4.0 and later has added a client for Simple Certificate Enrollment Protocol (SCEP) support and requires a Datacenter License. SCEP is a protocol standard used for managing certificates for large numbers of network devices using an automatic enrollment process. iDRAC can now integrate with SCEP-compatible servers such as the Microsoft ServerNDES service to maintain SSL/TLS Certificates automatically. This feature can be used to enroll and refresh a soon-to-be-expired web server certificate. You can use Server Configuration Profile to set the certificates on a one-to-one basis in the iDRAC UI. Also, you can provide scripts using tools such as RACADM.

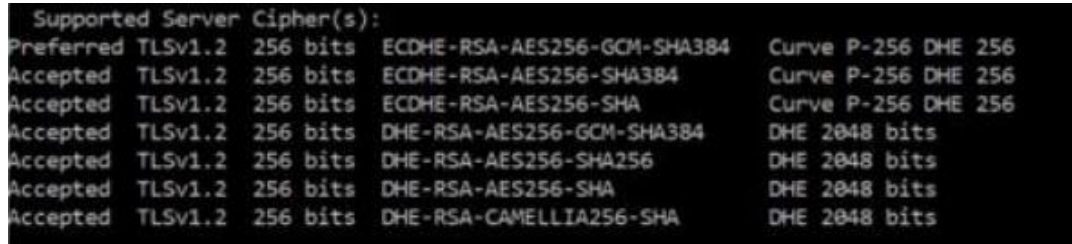


iDRAC Cipher Select

The Cipher Suite Selection can be used to limit the ciphers that the web browser can use to communicate with iDRAC. Also, it can determine the security of the connection. These settings can be configured through the iDRAC web interface, RACADM, and Redfish. This functionality is available across several iDRAC releases – iDRAC7, iDRAC8 (2.60.60.60 and higher), and the current iDRAC9 (3.30.30.30 and higher).

Commercial National Security Algorithm (CNSA) support

The supported ciphers available in iDRAC9 with TLS1.3 Bit and 256 Bit Encryption are shown in the following figure. The ciphers available are inclusive of the ciphers in the CNSA-approved set.



```
Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
```

Tips for securing iDRAC connection

The most secure network connection is the iDRAC's Dedicated NIC because it can be connected to a network that is physically separated from the production network. This method physically separates the iDRAC management traffic from the production network traffic.

If use of the iDRAC's Dedicated NIC is not feasible, iDRAC can be run in Shared LOM mode with a VLAN enabled. However, the iDRAC's management traffic is sent across the same connection as the production network. Alternatively, if the use of a VLAN is not possible while in Shared LOM mode, access to iDRAC must be secured using strong passwords and other security measures.

For further information, see the [iDRAC Security Configuration Guide](#).

IEEE.802.1x

The network standard IEEE 802.1x has been enabled on PowerEdge servers. This network protocol provides port-based network authentication. Devices requesting access to the LAN or WLAN must be authenticated and validated before authorization for access.

Domain isolation

The 14th, 15th, and 16th generations of PowerEdge servers provide additional security by using domain isolation, an important feature for multitenant hosting environments. To secure the server's hardware configuration, hosting providers might want to block any reconfiguration by tenants. Domain isolation is a configuration option that ensures that management applications in the host operating system have no access to the out-of-band iDRAC or to Intel chipset functions, such as Management Engine (ME) or Innovation Engine (IE).

Protecting data in use

Protecting application data that is being used in memory has become increasingly important. Whether data in use is a machine learning dataset or relates to keeping a secret in memory such as in multitenant environments, data in-use can be vulnerable to

threat vectors that can intrude on the contents of memory or the access bus. Data in use protection is necessary to secure computations that are increasingly operating on large datasets in memory. Additionally, code running on the data must be trusted and tamper-free. There must be facilities to separate trusted and nontrusted code execution environments for data in use.

New developments in CPU technology for confidential computing allow secure enclaves to protect application data at the hardware layer, enabling a more comprehensive data protection strategy. Starting with the 15th generation of server offerings, Dell Technologies enables these CPU technologies, including Intel SGX/TME and AMD SEV/SME.

AMD confidential compute features

AMD introduced Secure Encrypted Virtualization (SEV) with the first generation of AMD EPYC processors. It encrypts full system memory and individual virtual machine (VM) memory isolating the VM memory from the hypervisor. With each generation of AMD EPYC processors, AMD has enhanced SEV with additional features to safeguard privacy and integrity by encrypting each VM with one of up to 509 unique encryption keys known only to the processor. The keys are used to encrypt memory using 128-bit AES encryption engines in the memory controller. The hypervisor manages the keys in the memory controller with the help of AMD's Secure processor. The key AMD SEV technologies that are part of the Infinity Guard technology solution suite from AMD that address different use cases, deployments, and threat models include:

- AMD's SME technology refers to using a single key to encrypt system memory.
- AMD SEV uses one key per VM to isolate guests and the hypervisor from one another.
- AMD SEV-ES encrypts all CPU register contents when a VM stops running to prevent leakage of information from CPU registers to the hypervisor.
- AMD SEV-SNP adds strong memory integrity protection to help prevent hypervisor-based attacks like data replay, memory remapping, and so on.

Intel confidential computing features

Starting with the 3rd Generation Intel Xeon platform, Intel introduced several key security innovations. Total Memory Encryption (TME) is available to ensure memory accessed from the CPU is encrypted. By encrypting all memory, existing software applications run unmodified while simultaneously providing greater protection for system memory.

Intel TME helps ensure that all memory accessed from the Intel CPU is encrypted, including customer credentials, encryption keys, and other intellectual property or personal information about the external memory bus. Intel developed this feature to provide greater protection for system memory against hardware attacks, such as removing and reading the dual inline memory module (DIMM) after spraying it with liquid nitrogen or installing purpose-built attack hardware. Using the NIST storage encryption standard, AES XTS, an encryption key is generated using a hardened random number generator in the processor without exposure to software. This method allows existing software to run unmodified while better protecting memory.

Identity Access Management

Identity and Access Management (IAM) is a set of security controls to manage digital identities and provide authentication and authorization by controlling the requestor's access to information and resources, at the right level, and at the right time to limit unauthorized access. IAM frameworks provide advantages over simple passwords, such as:

- **Enhanced security**—Includes various tools such as single sign-on (SSO) services, multifactor authentication (MFA), and privileged access management for stronger security and to avoid risks from vulnerable passwords. IAM plays a critical role in protecting organizations against phishing and social engineering attacks by implementing strong authentication, access control, monitoring, and user education. It helps organizations reduce their attack surface and respond effectively to threats.
- **Reduction of compromised passwords**—Deters credential theft from phishing, social engineering, and brute-force attacks by using MFA and additional security layers.
- **Granular access control**— Enables fine-grained control over user access permissions by using role-based access control (RBAC) and attribute-based access control (ABAC) to ensure that users only have access to necessary resources and data.
- **Centralized management**—Controls user accounts and access policies, which provides easier management of users as they join, move within, or leave the organization.
- **Auditing and logging**—Monitors user activities to identify and remediate suspicious access attempts.
- **Scalability**—Adapts to the need for a growing number of users and resources
- **Regulatory compliance**—Adheres to regulatory requirements to avoid legal consequences.
- **User experience**—Provides SSO services and password management to enable users to access multiple applications and services by using one set of credentials.
- **Adaptive authentication**—Applies additional security measures by assessing risk factors.
- **Emergency access and recovery**—Grants temporary emergency access for critical situations while maintain security controls.
- **Integration**—Integrates with various systems, applications, and cloud services for seamless access management across the entire IT ecosystem.

As a broad IT issue spanning technological and regulatory requirements, IAM is a strategic business imperative for all organizations to enhance security and resiliency. Zero Trust Architecture (ZTA) has emerged as the standard choice for securing all levels of infrastructure and is a foundational part of ZTA. The unofficial mantra of Zero Trust is “never trust, always verify” and if you cannot verify then you cannot trust. IAM provides that verification.

The foundation to a strong cybersecurity framework and the adoption and implementation of Zero Trust principles is identity. Identification of not only people but of applications, communication paths, network devices, and the data itself. If an organization does not have a strong Identity Credentialing and Access Management (ICAM) practice, then the underlying security practices are at risk. An effective identity and access solution must include necessary tools and controls that can capture and store user login details, facilitate the assignment and revocation of user access credentials, and oversee the central enterprise database of user roles, levels, and access privileges. At a minimum, access must only be allowed to facilitate the necessary functions that the organization has defined. As an example, users must only have access and permission to data, applications, and services to do what is defined in their job. Practices and tools must be implemented to ensure that this role is maintained and that even in that role, a user must be monitored to ensure that they are not doing anything that violates the organization's goals for data utilization.

MFA – Smartcards (CAC/PIV)

MFA for Smartcards (CAC/PIV) is a general-purpose certificate authentication that includes Common Access Card (CAC) and Personal Identification Verification (PIV) cards. Certificate authentication uses the client identity certificate to authenticate the user. It is used primarily in government or organizations that work with the federal industry.

MFA – RSA SecurID

RSA SecurID is another means of authenticating a user on a system. As another two-factor authentication, iDRAC9 supports RSA SecurID with the Datacenter license and starting with firmware 4.40.00.00 and later, as another two-factor authentication.

Directory integration for authorization

For centralized user and domain management, iDRAC supports integration into privileged management tools such as Lightweight Directory Access Protocol (LDAP) and Active Directory. Using a directory service provides a central location for easier user inventory management and assigning user account access controls and settings.

You can use LDAP to authenticate users and groups in iDRAC. To configure the LDAP directory service, you can use the objects in the `cfgLdap` and `cfgLdapRoleGroup` groups with the `config` command. You can also use the objects in the `iDRAC.LDAP` and `iDRAC.LDAPRole` groups with the `set` command 12.

For Active Directory integration, you can configure LDAP over SSL (LDAPS) on iDRAC to communicate with Active Directory domain controllers. After a valid certificate is installed on the domain controller and the connection to the DC using SSL over port 636 is verified, you can use the directory service integration test on iDRAC/OME to communicate with the domain controller.

SSO

iDRAC supports SSO, which provides the ability to share validated credentials and identifications across multiple domains without having to rechallenge or reauthenticate the user. SSO enables an authenticated operating system administrator to directly access the iDRAC web interface without requiring login using separate iDRAC administrator credentials. iDRAC supports the following SSO protocols:

- **OpenID connect** is an open standard and is a decentralized authentication protocol that is typically used for machine-to-machine-like RestAPIs.

- Open-standards **Security Assertion Markup Language (SAML)** is typically used for UI SSO.

Role-based access controls

Role-based access control (RBAC) is the most popularly used form of access control. Permissions are grouped in roles and are typically assigned to a group. Assigning authorization capabilities to users and groups is managed in Active Directory.

You can set up user accounts with specific privileges (role-based authority to manage your system using iDRAC and maintain system security). By default, iDRAC is configured with a local administrator account. The default iDRAC username and password are provided with the system badge. As an administrator, you can set up user accounts to allow other users to access iDRAC. For more information, see the documentation for the server.

You can set up local users or use directory services such as Microsoft Active Directory or LDAP to set up user accounts. Using a directory service provides a central location for managing authorized user accounts.

iDRAC supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read-only, or none. The role defines the maximum privileges available.

Time-based access controls

Time-based access control is another valuable tool for enhancing security and managing access to sensitive data, facilities, or systems in a tightly controlled and monitored environment. For instance, if a technician needs physical access to the USB port on the server, the iDRAC administrator can enable/disable specific access times for USB port access.

Scope-based access control

Scope-based access control provides more granular control than user- and role-based access control. It allows the administrator to apply a policy with a set of permissions that are evaluated when an entity tries to access the resource. For instance, access can be restricted, based on resource location, IP address range, and so on.

Capabilities and automation for efficient at-scale deployment

Zero-touch automation with iDRAC – Server configuration profiles

Zero Touch provisioning is available with iDRAC Enterprise or Datacenter licenses. Zero Touch provisioning automates all hardware configuration, certificate installation, repository firmware updates, and operating system deployment. The IT Admin can preconfigure security settings and ensure uniform server images. Zero Touch provisioning is available through the iDRAC Server Configuration Profile feature and with OpenManage Enterprise.

CloudIQ

CloudIQ monitors the health and cybersecurity of your enterprise-wide servers and predicts their performance so that you can proactively address issues before they impact your business.

CloudIQ offers a simple and intuitive solution to collect firmware details from PowerEdge servers including BIOS, iDRAC, NICs, PERC, drives, and supported peripherals. A recent

feature from both OpenManage Enterprise and CloudIQ identifies BIOS and firmware that requires an update. CloudIQ can report the current installed version, compare it to the latest Dell release available, and schedule updates. This information is collected from each server using the agent-free iDRAC, consolidated by OpenManage Enterprise, and then transferred to CloudIQ to be processed. This powerful feature includes user rights integrated in both OpenManage Enterprise and CloudIQ to allow only authorized users to run these commands. Also, CloudIQ can consolidate multiple OpenManage Enterprise instances into one server fleet management view.

Fourth Stage – Security management and monitoring

Challenges

You cannot defend what you cannot see. Attacks happen quickly, faster than a human can detect and respond. Protecting your critical assets in real-time within a dynamic and complex threat environment is a challenge. Lack of skills and resources exacerbates the problem. As IT administrators face ongoing challenges in their environments, more easily managing the infrastructure—through more automation, fewer task steps, and more intuitive interactions—is key to administration productivity.

It is critical that your business remains resilient and unaffected by adverse outcomes. The business must stay nimble to be aware, respond, and recover:

- Observability and transparency enable effective security event awareness and timely remediation.
- Lack of skills and resources increases problems. Monitor activity across infrastructure (user, device, data, network, and application) to identify patterns and anomalies. Analytics can be used to detect and respond to security threats.
- Automation is important.
- Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve models that improve detection and reaction time in making real-time access decisions. Simplification is foundational and fundamental to a resilient infrastructure.

PowerEdge Solutions

The Dell management portfolio simplifies administrator tasks. It improves security and health monitoring to scale security confidently by using automation and intelligence. Monitoring and logging are a key part of a zero-trust implementation.

Visibility, logging, and alerts

It is critical to have a detection capability that provides complete visibility into the configuration, health status, and change events in a server system. This visibility must also detect malicious or other changes to BIOS, firmware, and option ROMs in the boot and operating system runtime process. Proactive polling must be coupled with the ability to send alerts for any events in 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.

Dell OpenManage Enterprise enables users to set up alert policies once and then automatically assign them for future alerts. Also, OpenManage Enterprise can apply a template to many servers at once. The OpenManage Enterprise solution ultimately saves time and effort by automating actions based on alerts after administrators have created a policy.

Telemetry

Beginning with iDRAC9 v4.00.00.00 firmware and a Datacenter license, IT managers can integrate advanced server hardware operation telemetry into their existing analytics solutions. Telemetry is provided as granular, timeseries data that is streamed or pushed. The advanced agent-free architecture in iDRAC9 provides over 180 data metrics that are related to server and peripheral operations. Metrics are precisely timestamped and internally buffered to allow highly efficient data stream collection and processing with minimal network loading. This comprehensive telemetry can be fed into analytics tools to predict failure events, optimize server operations, and enhance cyber resiliency. The iDRAC9 Telemetry Streaming collects and streams live system data from one or more PowerEdge servers to a centralized collector.

iDRAC Lifecycle Logs

The Lifecycle Logs are a collection of events that occur in a server over time. They provide a description of events with timestamps, severity, user ID or source, and recommended actions. This technical information helps with security tracking and other hardware alerts.

The various types of information that is recorded in the Lifecycle Controller Log (LCL) include:

- 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

Alerts

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

iDRAC supports several types of alerts such as:

- Email or IPMI alert
- SNMP trap
- Operating system and Remote System logs
- Redfish event

Alerts are categorized by severity – Critical, Warning, or Informational. The 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**—For example, upgrades or downgrade

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

TLS for Remote Syslog

The iDRAC Remote Syslog feature allows you to write the RAC log and the System Event Log (SEL) remotely to an external syslog server. You can read all logs from the entire server farm from a central log. The Remote Syslog protocol does not require user authentication. For the logs to be entered in the Remote Syslog server, ensure that there is proper network connectivity between iDRAC and the Remote Syslog server and that the Remote Syslog server is running on the same network as iDRAC.

The iDRAC's web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Redfish scripts can perform automated certificate uploads. When a link has been established between the two servers, TLS encryption and SSL decryption enable secure data transport.

SELinux framework

SELinux operates at the core kernel level on iDRAC and does not require user input or configuration. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to customers enrolled in this new feature. In future releases of iDRAC, these logs will be available in the Lifecycle Controller Logs.

Real-time detection – BIOS Live scan

BIOS live scanning verifies the integrity and authenticity of the BIOS image in the primary ROM when the host is powered on. BIOS live scanning is not in the POST process. This feature is available only with the iDRAC9 4.10.10.10 (supported AMD platforms) and iDRAC9 4.40.20.00 (supported Intel platforms) Datacenter licenses. You must have administrator privileges or operator privileges with the “Execute Debug Commands” debug privilege to perform this operation.

Fourth Stage – Security management and monitoring

You can initiate BIOS image scanning either on demand or by scheduling the scan through the iDRAC UI, RACADM, and Redfish interfaces. The BIOS live scan feature is available starting with 15th generation of PowerEdge servers with AMD “Rome”-based processors or Intel “Ice Lake”-based processors.

Boot time and run time BIOS scanning

A critical aspect of server security is ensuring that the boot process is verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an operating system 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 RoT to meet the following recommendations:

- NIST SP 800-147B, BIOS Protection Guidelines for Servers
- NIST SP 800-155, BIOS Integrity Measurement Guidelines

On the Dell PowerEdge servers with iDRAC9, iDRAC first boots with chain of trust authentication, and then verifies BIOS integrity. iDRAC assumes the role of hardware-based root of trust. For AMD platforms, iDRAC accesses the primary BIOS ROM through SPI and the AMD fusion controller hub (FCH), and performs the RoT process. For Intel platforms, iDRAC accesses the primary BIOS ROM through SPI and the Intel Platform Controller Hub (PCH), and performs the RoT process.

iDRAC9 directly accesses the BIOS primary ROM to perform a RoT operation on the processor on both the security block and the host Initial Boot Block.

Silicon-based Root of Trust

PowerEdge servers use an immutable, silicon-based RoT to attest to the integrity of BIOS and iDRAC9 firmware cryptographically. This RoT is based on one-time programmable, read-only public keys that provide protection against malware tampering. The BIOS boot process uses Intel Boot Guard technology or AMD Platform Secure Boot technology. This technology verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in silicon by Dell Technologies in the factory. A verification failure results in a server shutdown and user notification in the Lifecycle Controller Log. The user can initiate the BIOS recovery process. If Boot Guard validates successfully, the other BIOS modules are validated by using a chain of trust procedure. Then, control is given to the operating system or hypervisor. In addition to Boot Guard, iDRAC9 4.10.10.10 or later provides a RoT mechanism that verifies the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time, on demand, or at user-scheduled intervals.

For the chain of trust, each BIOS module contains a hash of the next module in the chain. The key modules in the BIOS include:

- Technical support and resources ID 483
- Initial Boot Block (IBB)
- Security (SEC)
- Pre-EFI Initialization (PEI)
- Memory Reference Code (MRC) o Driver Execution Environment (DXE)

- **Boot Device Selection (BDS)**

If Intel Boot Guard authenticates the IBB module, the IBB module validates the SEC and PEI modules before handing control to it. The SEC and PEI modules then validate the PEI and MRC modules, which further validates the DXE and BDS modules. Next, control is handed over to UEFI Secure Boot. Similarly, for PowerEdge AMD EPYC-based servers, AMD Secure Root of Trust technology ensures that servers boot only from trusted firmware images. AMD Secure Run Technology encrypts the main memory, keeping it private from malicious intruders accessing the hardware. There are no required application modifications to use this feature, and the security processor never exposes the encryption keys outside of the processor. iDRAC takes on the role of hardware-based security technology and accesses the primary BIOS ROM through SPI. iDRAC, along with the AMD fusion controller hub (FCH) performs the RoT process.

Under the following conditions, iDRAC9 recovers the BIOS:

- BIOS integrity check failed
- BIOS self-check failed

Note: Use the RACADM command to recover the BIOS setup.

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

System lockdown

iDRAC9 offers a feature that ‘locks down’ the server hardware and firmware configuration and requires an Enterprise or Datacenter license. You can enable this mode by using the UI, the RACADM CLI, or the Server Configuration Profile. Users with administrative privileges can set System Lockdown mode, which prevents users with lesser privileges from changing the server. The IT administrator can enable or disable this feature. 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 data center when using Dell tools and agents and protect against malicious attacks against embedded firmware when using Dell Update Packages. Lockdown mode can be enabled dynamically, without requiring a system reboot. iDRAC9 v4.40 introduced enhancements where in addition to the current System Lockdown which only controls the updates using Dell Update Package (DUP), this lockdown functionality is extended to select NICs.

Note: Enhanced Lockdown for NICs only includes firmware lockdown to prevent firmware updates.

Configuration (x-UEFI) lockdown is not supported. When the customer sets the system in lockdown mode by enabling or setting attributes from any of the supported interfaces, iDRAC will take additional actions depending on the system configuration. These actions depend on the third-party devices detected as part of the iDRAC discovery process.

Drift detection

By enforcing standardized configurations and adopting a “zero tolerance” policy for any changes, organizations can reduce the potential for exploitation. Dell OpenManage

Fourth Stage – Security management and monitoring

Enterprise Console allows you to define your own server configuration baselines and then monitor the drift of your 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 Enterprise 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 window while servers reboot to make the production environment compliant again. This staged process enables you to deploy configuration changes to production without any server downtime during nonmaintenance hours. It increases the server availability without compromising the serviceability or security.

Chassis intrusion detection

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 Logs after power is supplied.

Automated and manual recovery

BIOS and operating system recovery

The 14th, 15th, and 16th generations of PowerEdge servers include two types of recovery: BIOS Recovery and Rapid Operating System (OS) Recovery. These features enable rapid recovery from corrupted BIOS or operating system images. In both cases, a special storage area is hidden from run-time software (BIOS, operating system, device firmware, and so on). These storage areas contain pristine images that can be used as alternatives to the compromised primary software.

Rapid Operating System (OS) Recovery enables rapid recovery from a corrupted operating system image (or an operating system image suspected of malicious tampering). The recovery media can be accessed using an internal SD card, SATA ports, M.2 drives, or internal USB. The selected device can be exposed to the boot list and the operating system to install the recovery image. It can then be disabled and hidden from the boot list and operating system. In the hidden state, the BIOS disables the device so that the operating system cannot access it. If there is a corrupted operating system image, the recovery location can then be enabled for the boot process. These settings can be accessed through BIOS or the iDRAC interface.

In extreme cases, if the BIOS is corrupted (either by a malicious attack, a power loss during the update process, or any other unforeseen event), it is important to provide a way to recover the 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.

- BIOS itself initiates automatic BIOS recovery.
- Users using the RACADM CLI command can initiate on-demand BIOS recovery.

FW rollback

We recommend that you update the firmware 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 roll back 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 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 for iDRAC and CMC
- Lifecycle Controller UI
- 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 UI, you can roll back the firmware using the iDRAC web interface. You can perform firmware rollback for multiple devices with one system reboot.

On 14th, 15th, and 16th generations of PowerEdge servers that have a single iDRAC and Lifecycle Controller firmware, rolling back the iDRAC firmware also rolls back the Lifecycle Controller firmware.

Firmware rollback protection

If the firmware has a known vulnerability which would expose your server to attack, the BIOS itself can prevent downgrade to a previous version. The firmware release notes state that you cannot rollback when performing an update.

Full Power Cycle

In a Full Power Cycle, the server and all 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 removing the AC power cable, waiting for 30 seconds, and then putting the cable back. This method poses a challenge when working with a remote system. A feature in the 14th, 15th, and 16th generations of PowerEdge servers enables you to perform an effective full power cycle from the iDRAC Service Module (iSM), iDRAC UI, BIOS, or a script. A full power cycle takes effect at the next power cycle.

The 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.

Updating

Dell Technologies provides a rich set of tools to make it easier to keep your server's firmware and BIOS up-to-date and update quickly. Ensuring firmware is up to date is a vital task to keep production servers secure and operating efficiently. Tracking and implementing these updates can be burdensome for administrators. iDRAC9 provides automatic updates with the ability to schedule firmware updates as wanted.

Many companies schedule monthly maintenance windows to handle operating system, application, and firmware updates. With OpenManage Enterprise, systems administrators can stage firmware updates for the next time the system is rebooted or for a scheduled deployment. This method ensures that nobody must be physically present to run the updates.

PowerEdge provides patches to security vulnerabilities with Dell security advisories. The advisories provide timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities.

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)

Parts replacement

iDRAC automatically saves the firmware image and configuration settings for NIC cards, RAID controllers, and Power Supply Units (PSUs). If there is 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.

Easy Restore (for motherboard replacement)

Easy Restore is an integrated storage component that maintains critical configuration information. The Easy Restore feature allows you to restore your system's service tag, all licenses, UEFI configuration, system configuration settings (BIOS, iDRAC and NIC), and the OEM ID (Personality Module) after replacing the system board. All data is backed up to a backup flash device automatically. If the BIOS detects a new system board and the service tag in the backup flash device, the BIOS prompts you to restore the backup information. You can still choose to perform the full system backup with iDRAC8 as you do with iDRAC6 and iDRAC7. This solution backs up and restores the actual firmware

versions in addition to the hardware settings. Easy Restore does not copy the firmware drivers due to size limitations.

CloudIQ

Misconfigurations of infrastructure systems can open your organization to cyber intrusion and are a leading threat to data security. The CloudIQ cybersecurity feature proactively monitors infrastructure security configurations for Dell PowerStore and PowerMax storage systems and PowerEdge servers, and notifies users of security risks. A risk level is assigned to each system, placing the system into one of four categories, depending on the number and severity of the issues: Normal, Low, Medium, or High.

By using CloudIQ Cybersecurity policy templates, users can quickly set up security configuration evaluation tests and assign them to large numbers of systems with just a few clicks. Once assigned, the test plan is evaluated against each associated system, and the system administrator is notified in minutes of any unwanted configuration settings.

When a security risk is found, remediation instructions are provided to help you address the issue quickly. CloudIQ evaluates outgoing Dell Security Advisories (DSAs) and intelligently notifies users when those advisories are applicable to their specific Dell system models with specific system software and firmware versions. This notification eliminates the need for users to investigate if a Security Advisory applies to their systems and allows them to focus on remediation immediately.

Managed detection and response services

Dell Technologies Managed Detection and Response services is a cloud-based offering that helps organizations quickly and significantly improve their security posture—while reducing the burden on IT. This fully managed, end-to-end, 24/7 service monitors, detects, investigates, and responds to threats across the entire IT environment.

Designed for organizations with 50 endpoints or more, this unique service uses two key capabilities:

- The power of the open Secureworks Taegis XDR security analytics software, built on more than 20 years of SecOps expertise including real-world threat intelligence and research, and experience detecting and responding to advanced threats
- The expertise of Dell Technologies security analysts, gained through years of experience helping organizations worldwide to better protect their business

[Dell Technologies Managed Detection and Response](#) provides around-the-clock access to security experts. They provide end-to-end visibility and protection from endpoint to cloud, covering every aspect of advanced threat detection and response supported by Taegis XDR's database of 52,000 unique threat indicators that are managed and updated daily. Taegis XDR also ingests data from existing security solutions to use any previous security investments.

Dell Technologies security analysts assist with initial setup, monitoring, detection, remediation, and response—all for one predictable price. They work closely with your IT team to understand the environment. They provide advice about improvements to the security posture and help you set up and deploy the Taegis XDR software agent to endpoints. Then, using the Taegis XDR application, they monitor and review alerts 24/7.

Fifth stage – Secure decommissioning and repurposing

If an alert merits investigation, analysts determine and perform the appropriate response. If a threat is malicious or requires your action, you are informed and, if necessary, provided with step-by-step instructions. As part of the service, Dell Technologies also provides up to 40 hours per quarter of [remote remediation assistance](#), such as helping with troubleshooting, issue resolution, software deployments, patch and asset assessment, and configuration of IT environments.

If there is a security incident, Dell Technologies initiates the process to get your business up and running and provides up to 40 hours of remote incident response assistance a year.

Fifth stage – Secure decommissioning and repurposing

Challenge

Data security is a key consideration throughout the life cycle of a server, including when the server is repurposed or retired. Many servers are repurposed as they are transitioned from workload to workload, or as they change ownership from one organization to another. All servers are retired when they reach the end of their useful life. When such transitions occur, IT best practices recommend removing all data from the server to ensure that confidential information is not inadvertently shared.

PowerEdge solutions

Beyond best practices, in many cases government regulations about privacy rights also necessitate complete data elimination when IT resources are transitioned. Data erasure is a key capability encompassed in the Dell Secure Development Lifecycle (SDL). The SDL and secure server management tools ensure that PowerEdge servers are secure at every stage in the server life cycle, from server conception, design and manufacturing, to operation and decommissioning.

At this final stage (decommissioning/retirement), or when a server is repurposed due to change of workload or ownership, a capability starting with the PowerEdge 14th generation of servers, can simplify data erase.

System Erase, with iDRAC9 and the 14th, 15th, and 16th generations of PowerEdge servers, simplifies the process of erasing server storage devices and server nonvolatile stores such as caches and logs. To meet varying Systems Administrator needs for interactive and programmable operations, the following methods can perform System Erase:

- Lifecycle Controller UI
- WS-Man API
- RACADM CLI

Using one of these methods, an administrator can selectively reset a PowerEdge server to its original state (factory settings), removing data from internal server nonvolatile stores and from storage devices within the server.

System Erase can discover server-attached storage including hard disk drives (HDDs), SEDs, ISE, and nonvolatile memory drives (NVMe). Data stored on ISE, SED, and NVMe devices can be made inaccessible using cryptographic erase while devices such as non-ISE SATA HDDs can be erased using data overwrite.

Secure Erase

Through the life cycle controller, customers can repurpose or retire a system. All drives now shipping on PowerEdge systems can be securely erased. On an older platform that might not have encryption-capable drives, there is a “standard disks (overwrite data)” option. Unrecoverable processes generate warning messages. The server is powered off after a retire or repurpose operation. You can view the Lifecycle Logs in iDRAC to confirm that the operation was successful.

At the end of a system life cycle, it can either be retired or repurposed. For either scenario, System Erase removes sensitive data and settings from the server. Secure Erase wipes storage devices and server nonvolatile stores such as caches and logs so that no confidential information unintentionally leaks. It is a utility in Lifecycle Controller (F10) that erases logs, configuration data, storage data, and cache.

The System Erase feature can erase the following devices, configuration settings, and applications:

- iDRAC is reset to default settings, erasing all data and settings.
- Lifecycle Controller (F10) data is cleared.
- BIOS and NVRAM are reset to default settings.
- Embedded diagnostics and operating system driver packs are cleared.
- iDRAC Service Module (iSM) are cleared.
- SupportAssist Collection reports are cleared.

The following components can also be erased:

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

Note: vFlash not available on 15th generation of PowerEdge servers or later.

System Erase cryptographically disposes of data on the following components:

- Self-Encrypting Drives (SED)
- ISE drives
- NVM devices such as Intel Apache Pass and NVDIMMs

Secure erase – physical disk

Reset the drive to the factory settings. All data on the SSD is permanently removed and cannot be recovered. To sanitize the drive, the mapping table is deleted and all blocks to which data has been written are erased. Not all SSDs support the sanitize feature.

Overwrite erase

Overwrite-erase is a software-based method that overwrites data with zeros and ones. Data overwrite can erase non-ISE SATA hard drives.

Summary

Crypto erase

ISE destroys the internal encryption key that is used in the 14th, 15th, and 16th generations of PowerEdge drives and renders the user data unrecoverable. Used on self-encrypting drives, the encryption key is erased. The data remains on the drive but is inaccessible without the key. ISE is a recognized method of data erasure on storage drives as seen in NIST Special Publication 800-88 “Guidelines for Media Sanitization.”

Advantages of the new ISE feature with System Erase include:

- **Speed**—ISE is faster than data overwriting techniques like DoD 5220.22-M (seconds compare with hours)
- **Effectiveness**—ISE renders all the data on the drive, including reserved blocks, unreadable.
- **Better TCO**—Storage devices can be reused instead of being physically destroyed.

The following methods can perform System Erase procedure:

- Lifecycle Controller interface (F10)
- RACADM CLI
- Redfish

Data sanitization and destruction services

Data continues to grow and drive strategic advantage. Meanwhile, national security issues and data privacy regulations are escalating. As organizations navigate technology changes, they are further challenged with data security and compliance.

The end of the product life cycle is an aspect of data security that is increasingly important. Data Sanitization for Enterprise is a software-based method of securely overwriting data to render it unrecoverable. The various options include:

- **Data Sanitization for Enterprise Onsite**—An option for customers looking to refresh or redeploy assets. This service performs sanitization at the business’ location, securing data while assets remain in the environment.
- **Data Sanitization for Enterprise Offsite with Asset Resale and Recycle**—A service that removes assets from the business’ environment, sanitizes them at a secure location, and evaluates them for resale or reuse. The customer is compensated if value is found. If no value is found, assets are recycled according to local regulatory guidelines.

Data Destruction for Enterprise—A process that renders data inaccessible through the process of physical shredding. It is available for all Dell infrastructure solutions and similar third-party non-Dell branded assets. This process does not require systems to be operational.

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 must be built into server hardware design, not added on later.

Dell Technologies has been a leader in using silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. The 14th, 15th, and 16th generations of PowerEdge product lines feature 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 and overall data center security. It includes features like silicon-based Root-of-Trust, digitally signed firmware, and automatic BIOS recovery.
- Secure Boot, which checks the cryptographic signatures of UEFI drivers and other code loaded before the operating system runs.
- 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.
- Dynamic System Lockdown, a capability unique to PowerEdge servers, helps secure any system configuration and firmware from malicious or unintended changes while alerting users to any attempted system changes.
- Enterprise Key Management delivers a central key management solution to manage data-at-rest across the organization.
- System Erase, which allows users to easily retire or repurpose their 14th, 15th, and 16th generations of PowerEdge servers by securely and quickly wiping data from storage drives and other embedded nonvolatile memory.
- Supply Chain Security provides supply chain assurance by ensuring there is no product tampering or counterfeit components before shipping products to the customers.

The 14th, 15th, and 16th generations of PowerEdge servers, with their industry-leading security, form a trusted foundation for IT transformation on which customers can securely run their IT operations and workloads, and accelerate to Zero Trust adoption. Dell Technologies stops at nothing to help our customers build their breakthrough deployments. Our modern security approach ensures that an organization's environment is secure and resilient so that customers can focus on their core competencies, introduce their innovations, and advance human progress.

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- [iDRAC9 Security Configuration Guide](#)
- [Dell EMC Secured Component Verification Reference Guide for Servers](#)
- [Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing Base models](#)
- [iDRAC9 System Lockdown: Preventing Unintended Server Changes](#)
- [Next Generation Dell PowerEdge Servers: Transition to Modern UEFI](#)
- [Dell EMC PowerEdge UEFI Secure Boot Customization: Reduce Attack Surface with Complete Control of Certificates](#)
- [Dell Technologies Supply Chain Security: Secured Component Verification for PowerEdge](#)
- [Dell PowerEdge: iDRAC Automatic Certificate Enrollment](#)
- [Improved iDRAC9 Security using TLS 1.3 over HTTPS on Dell PowerEdge Servers](#)
- [A Partnership of Trust: Dell Supply Chain Security](#)
- [PowerEdge Advantages in your Zero Trust Journey – Video](#)
- [AMD on PE - Extending Data Protection to Data in Use - Video](#)
- [AMD on PE – Extended Boot Protection - Video](#)
- [Zero Trust Architecture - Video](#)
- [Cyber Resilient Architecture - Video](#)
- [Secured Component Verification - Video](#)
- [SEKM – Video](#)
- [IPv6 – Direct from Development](#)
- [iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers -Direct from Development](#)
- [Transform Datacenter Analytics with iDRAC9 Telemetry Streaming](#)
- [Configure iDRAC to use Active Directory Authentication \(dell.com\)](#)
- [Securing 14th Generation Dell EMC PowerEdge Servers with System Erase \(Direct from Development\) Security in Server Design](#)
- [\(Direct from Development\) Cyber-Resiliency Starts At The Chipset And Bios](#)
- [Factory Generated Default Password for iDRAC9 for Dell EMC 14th Generation \(14G\) PowerEdge Servers](#)

- [Dell EMC iDRAC Response to Common Vulnerabilities and Exposures \(CVE\) CVE-2017- 1000251 “BlueBorne”](#)
- [\(Video\) Secure Boot Configuration And Certificatemanagement Using RACADM- Video](#)
- [Secure Boot Management on Dell EMC PowerEdge Servers](#)
- [Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers](#)
- [Rapid Operating System Recovery](#)
- [Managing iDRAC9 Event Alerts on 14th generation \(14G\) Dell EMC PowerEdge Servers](#)
- [UEFI Secure Boot Customization](#)
- [iDRAC Overview](#)
- [OpenManage Console Overview](#)
- [OpenManage Mobile Overview](#)
- [Motherboard Replacement](#)