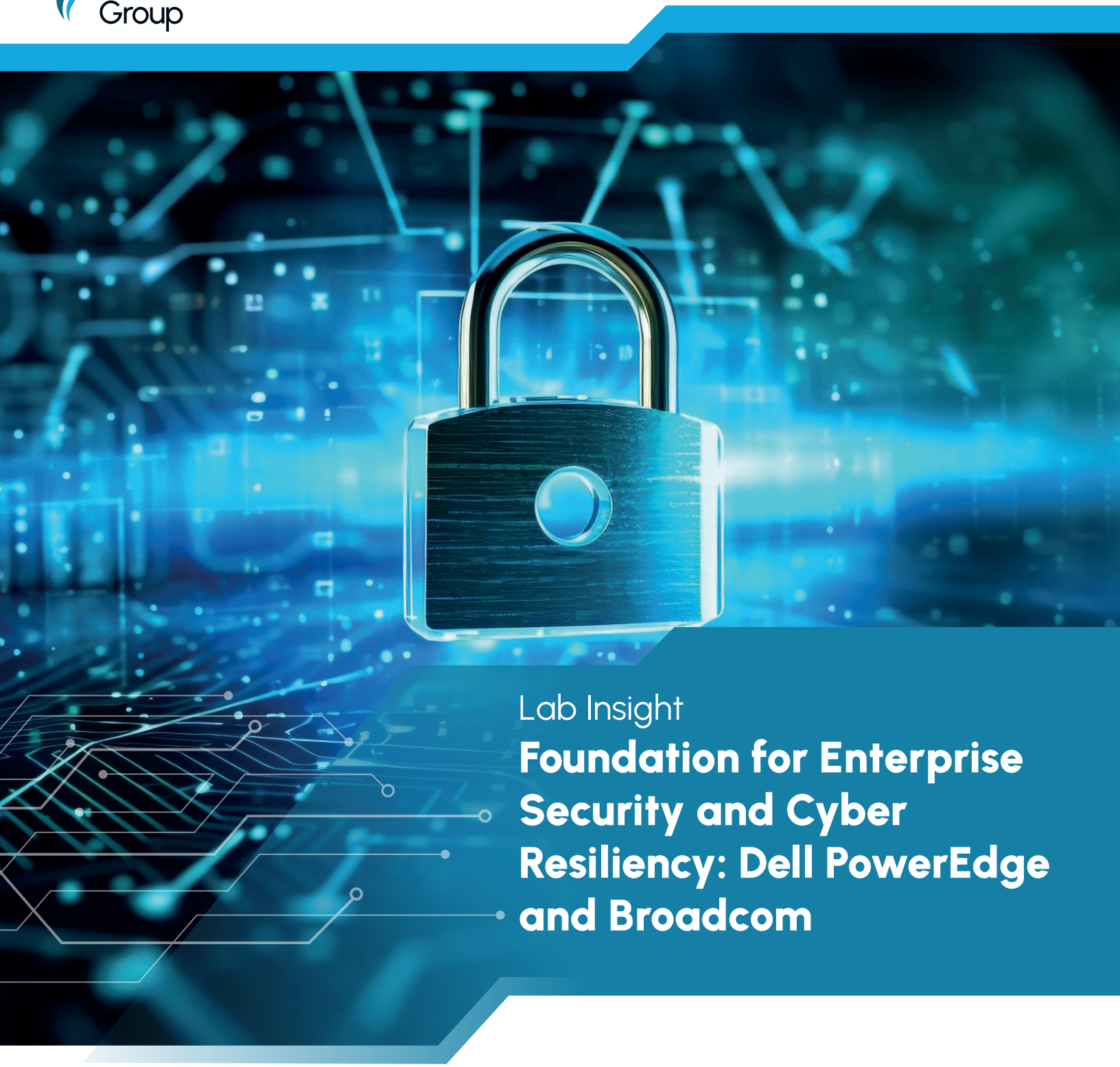
The Futurum Group



Lab Insight

Foundation for Enterprise Security and Cyber Resiliency: Dell PowerEdge and Broadcom

AUTHOR **Russ Fellows**
Head of Futurum Labs | The Futurum Group

FEBRUARY 2024

Executive Summary

There are numerous challenges companies face to establish and maintain the cybersecurity capabilities required to operate in today's complex and increasingly hostile digital world. Companies are reminded daily of the potential cost to their reputation, revenue and more for failing to maintain a competent cyber resiliency profile. Often, even a single breach can result in regulatory fines, loss of revenue and customers, and in some cases may even cause existential implications for a firm.

A Futurum Group study conducted in 2023, with more than 150 IT Security professionals from companies with 1,000 or more employees resulted in several insights. More than 80% of companies surveyed reported an increase in their cybersecurity budgets while nearly 50% are increasing their cybersecurity headcount in response to these growing threats. In terms of challenges faced, the top two items were limited budgets and high solution costs, indicating a need to improve cybersecurity without significant cost implications.

As part of The Futurum Group's ongoing research and analysis, The Futurum Group Labs has developed a cyber-resiliency framework that is designed as a holistic tool for evaluating how well a product or service offering helps a company meet their cybersecurity requirements. This framework incorporates multiple industry standards and best practices to provide a comprehensive perspective for evaluating their security requirements. The Futurum Group utilizes this framework when evaluating security aspects of products and services.

In this paper we review the important security features of Dell and Broadcom components, and how they can help companies improve their security posture and overall cyber resiliency. The Futurum Group Labs tested Dell 16th Generation PowerEdge servers with Broadcom 57508 Ethernet Network Interface Card (NIC) and PERC RAID controller cards both within our lab facilities, and remotely within Dell's lab. This analysis provides a real-world use case of managing security across a multi-site, distributed environment.

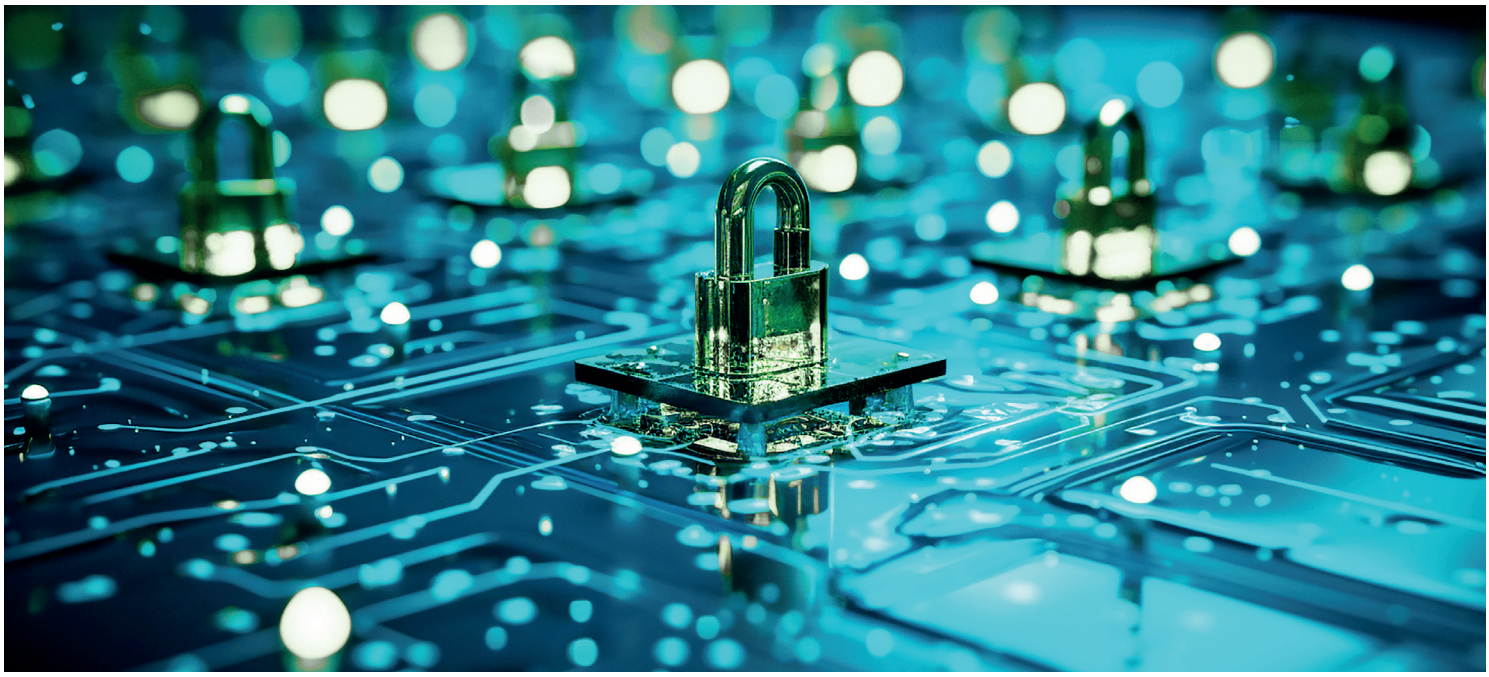
Summary of Findings

The Futurum Group Labs performed hands on testing and review of many of the security features and capabilities of Dell PowerEdge 16th Generation servers, together with Broadcom 57508 dual port 100 Gb Ethernet NIC and Broadcom SAS4116W ROC based Dell PERC 12, H965i RAID cards. Our evaluation included analyzing security best practices, along with overall system security features and capabilities.

Additionally, The Futurum Group has developed a security framework comprising areas for review across multiple areas of enterprise security. The Futurum Group's Security Framework builds upon industry best practices and multiple NIST standards and provided the basis for our evaluation process.

Against this framework, we found the Dell PowerEdge servers, together with Dell PowerEdge RAID Controller 12 (PERC) and Broadcom NICs provided an integrated security solution that met or exceeded requirements in all areas evaluated. Strengths included the following areas:

- Adherence to standards, including the NIST concepts of Identify, Protect, Detect, Respond & Recover
- Zero Trust security principles utilized by both Dell and Broadcom for all aspects of the systems
- Integrated security management via iDRAC, OME and CloudIQ provide enterprise-wide capabilities
- Dell's Secure Component Verification Process helps ensure security from order to delivery



Futurum Group's Security Framework

The Futurum Group has developed a security framework for evaluating the overall cyber resiliency rating of products operating within IT environments. This framework encompasses multiple inter-related aspects of security including ensuring that secure design methodologies are utilized during product creation.

The first area assessed is the design methodology utilized for developing products and services. Next the security features of a product are evaluated, along with the security of the manufacturing and supply chain processes. Finally, the IT security implementation of a company using the product is important. Taken together, these components provide a comprehensive tool for evaluating and analyzing the security profile of a product operating within a particular company. An overview is shown in Figure 1.

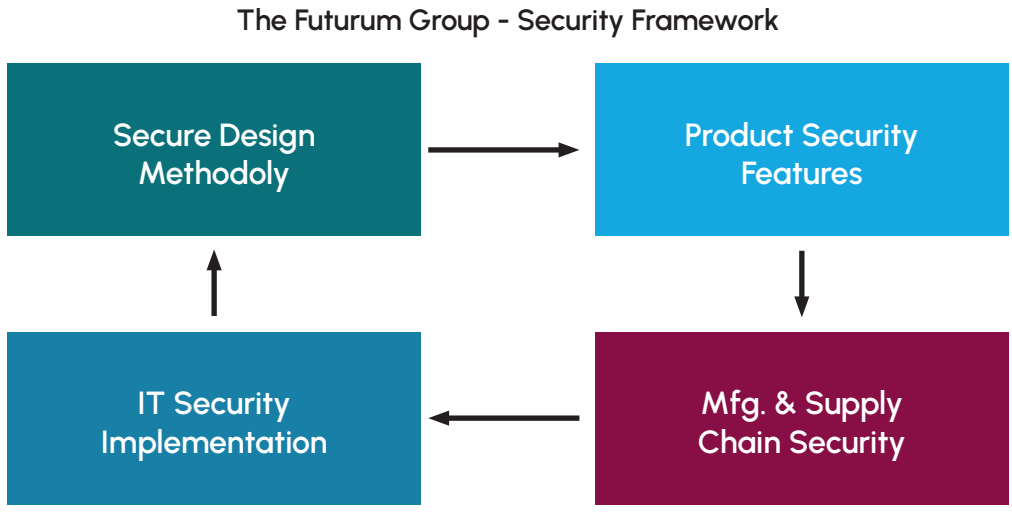


Figure 1: Security Framework Overview (Source: The Futurum Group)

It should be noted that "IT Security Implementation" was outside of the scope of work for this project. Since security responsibilities fall upon each company to utilize and implement security features appropriately.

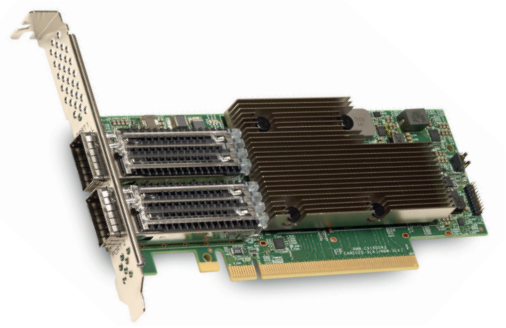
Dell Solution Overview

As a foundation for securing PowerEdge server products, intrinsic security practices are incorporated into hardware product design and software or firmware code development. These practices include the following processes to ensure security features are implemented at the time of product inception and continue throughout the development cycle. To perform this practice effectively, Dell 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 within the organization. Dell combines all components to create an integrated solution with hardware, software and services that together address security threats companies are facing.

Dell and Broadcom asked The Futurum Group Labs to evaluate Dell's servers together with Broadcom add-in cards with respect to how these products can help IT clients address security vulnerabilities and achieve the levels of cyber resiliency necessary for operations in today's challenging environment.

Specifically, The Futurum Group Labs validated the latest, 16th Generation Dell PowerEdge servers, together with Dell - Broadcom PERC 12 RAID cards and Broadcom 57508 NIC cards, along with relevant firmware and software that address security and cyber resiliency within IT environments. The Broadcom components helped provide overall end-to-end security capabilities through integration into Dell's management tools.

Dell PowerEdge 16th Generation Server



Boardcom 57508 NIC

Figure 2: *Dell PowerEdge and Broadcom NIC Products (Source: Dell and Broad-*

Dell's Security Principles for Cyber Resiliency

As companies have become increasingly sophisticated in their approach to security, it is clear that poinnit solutions are insufficient to address today's complex cybersecurity requirements. While there is naturally a focus on the hardware components themselves, an important part of the overall Dell and partner security ecosystem is the use of critical software elements that help enable security features and provide easy-to-use interfaces for IT users.

Futurum Group Comment: *Too often, security features require IT administrators to choose between usability or security. As a result, IT administrators may ignore or circumvent security best practices to improve ease of use. The management tools of the PowerEdge systems enable IT users to easily follow best practices while utilizing the comprehensive security features of Dell servers and Broadcom. This functionality helps reduce attack surfaces for malicious actors, while maintaining usability and performance.*

As described previously, The Futurum Group's Security Framework incorporates multiple best practices and industry standards, including NIST Cybersecurity Framework (CSF) which outlines five tenants:

- Identify: Ensure that an organization understands and can manage cybersecurity risk, assets, and data
- Protect: Develop and implement appropriate safeguards to ensure critical infrastructure is protected
- Detect: Quickly detect cyber events via anomaly detection and continuous monitoring
- Respond: Prepare and implement the ability to take appropriate action in response to a cyber event
- Recover: Establish the ability to maintain business resiliency and restore impacted systems

The Futurum Group Security Framework extends the NIST framework, including the following areas for assessing Dell's Cyber Resilient Architecture for security:

- User authentication and authorization using multi-factor authentication applied to users and devices (User AA and Device AA) with role-based and least privileged access controls.
- Dell PowerEdge hardware RoT creates a chain of trust from firmware to devices and supports complete customization of Secure Boot, including removal of all industry-standard certificates provided by Microsoft, VMware, or the UEFI CA.
- Using PowerEdge cyber resilient platform RoT extends to Secure Enterprise Key Management for data-at-rest protection.
- Applications and workload security to protect runtime environments, leveraging data and network security technologies including end-to-end encryption and cryptographic signatures.
- Utilize Security Protocol and Data Model (SPDM) capabilities for device attestation as part of the Zero-Trust/cyber resiliency architecture. Future capabilities include internal encrypted communication capabilities.
- Auditing and analytics for visibility and alerting of security issues using persistent event logging and real-time code and firmware scanning.
- Automation and orchestration technologies to enable automated API and CLI driven actions, along with enterprise web UI tools to provide easy-to-use global management of security alerting, reporting and automation.

Test and Validation Findings

The Futurum Group Labs Security Framework shown previously in Figure 1, was used to analyze the overall security capabilities of products or features. Our analysis examined each aspect of the Security Framework with details provided in the following four sections.

1 - Secure Design Methodology

Requirements

Confirm that security considerations begin at product inception with cybersecurity and resiliency capabilities integrated throughout product design and development.

Verify that hardware security features based on Zero Trust, such as tamper proof TPM often form the basis of software security, to deliver an integrated secure system.

Asses if the software architectures leverage hardware security and utilize the available security capabilities. Additionally, validate that threat modeling and penetration testing along with external audits and ongoing mitigation of vulnerabilities are performed.

Dell PowerEdge and Broadcom Design

Dell utilizes a secure Software Development Lifecycle (SDL) as the basis for instilling security throughout the design process. A comprehensive SDL process should ensure that any identifiable attack methods are mitigated utilizing standards-based security mechanisms to thwart these attack vectors.

As outlined previously, security starts with using a secure design methodology, with multiple considerations required to help products provide cyber resiliency:

• Security is considered for each feature
• Following industry best practices, Dell software is designed to obstruct, oppose and counter malicious attacks
• External audits of security features
• On-going evaluation of new vulnerabilities
• Rapid response to common vulnerability exposures (CVEs) with remediation

Table 1: *Dell SDL Principles*

Figure 2: *Dell SDL Model*

Additional aspects of secure design include end-to-end secure communication based upon cryptographically signing certificates used to authenticate and authorize components such as with Device-ID, 802.1x, and SPDM.

Finally, even with good design and secure implementations, vulnerabilities and breaches may still occur. Thus, it is important for products to be designed with resiliency and Zero Trust implementation, so that when penetrations do occur, their impact is limited. Dell's rapid response to critical CVEs and patching of identified components is an important aspect of mitigating threats from CVE's as they arise.

Futurum Group Comment: *Dell's rapid response to critical CVEs and patching of identified components is an important aspect of mitigating threats from CVE's as they arise. As one of the largest system vendors, Dell leverages their significant real-time monitoring via CloudIQ and other tools, to quickly respond to emerging threats and provide their customers with tools and processes to thwart attacks.*

2 – Product Security Features

Product security was an area of particular focus by The Futurum Group Labs when measuring how Dell PowerEdge servers, together with Broadcom based PERC 12 and 57508 Ethernet NICs met Futurum's Security Framework. System security requires a layered approach, with hardware security features and capabilities utilized by the firmware, that provides a secure foundation for the operating system (OS) and applications running within the OS. The hardware root of trust provides several foundational security capabilities including a secure, tamper-proof key storage location, a unique hardware encryption key, and other facilities required as part of a cryptographic framework.

Specifically, The Futurum Group Labs tested the following system components:

1. Dell PowerEdge 16th Generation systems with a Trusted Platform Module (TPM)
2. Dell PERC 12 (PowerEdge RAID Controller, 12th generation)
3. Broadcom 57508 Dual Port, 100 Gb Ethernet NIC with QSFP adapter connectivity
4. Secure BIOS management system settings, via iDRAC
5. Device identification via cryptographic framework (devices attestation uses a devices hardware RoT)

Each aspect of a system must be secured, ideally with each element utilizing industry best practices including Zero Trust principles, enabled via a silicon Root of Trust (RoT) as the foundation of physical security. Utilizing a certified RoT device that provides tamper resistance, the hardware protects the device firmware, which in turn is utilized to ensure critical software security features are verifiably operating securely. Security breach examples could include the exchange of entire PCIe cards, uploading compromised firmware or other attacks that target PCIe cards.

Delivering end-to-end security requires the entire solution integrates multiple hardware RoT devices, together with software features that leverage the underlying hardware capabilities. Dell's PowerEdge servers together with Broadcom NIC and RAID controllers provide this capability by validating each layer, from hardware to firmware and the OS using cryptographic attestation. Dell's iDRAC and other management tools leverage this integrated security environment to deliver a secure, easy to manage solution.

Futurum Group Comment: *A key aspect of the Zero Trust approach is to utilize hardware RoT devices to provide cryptographic verification to build a secure ecosystem. Using Zero Trust, each component first verifies, then trusts their counterpart based upon certified key exchanges and mutual authentication, attestation and authorization. These features are critical for the additional security mechanisms used throughout the Dell servers along with supported devices.*

As part of a standards-based approach to secure system management, a new Security Protocol and Data Model (SPDM) standard has emerged. This standard leverages Zero Trust principles and enables devices to securely verify each other (device attestation) and then establish secure communications over a variety of internal, server transport connections. Dell's 16th Generation servers, along with 12th generation PERC and Broadcom 57508 NICs now utilize SPDM, to enhance security. The SPDM standard leverages existing technologies including public key encryption, and cryptographic signing of certificates to provide device attestation between Dell's servers and Broadcom devices. In future implementations, the SPDM standard can also enable secure communication channels between devices.

Broadcom Networking

Broadcom 57508 Ethernet NIC, with speeds from 25 Gb to 200 Gb operate with Dell's security features and leverage some of the same Zero Trust principles. Broadcom's NICs also have a hardware based, silicon RoT which enable multiple additional benefits, including:

- Silicon RoT with secure key storage on servers and PCIe devices
- Secure firmware loading, updates and recovery on servers and PCIe devices
- Signed UEFI drivers, with Secure PXE boot for onboard NICs and PCIe NICs
- Device attestation (SPDM 1.2) between servers and devices, and audit logging of all devices

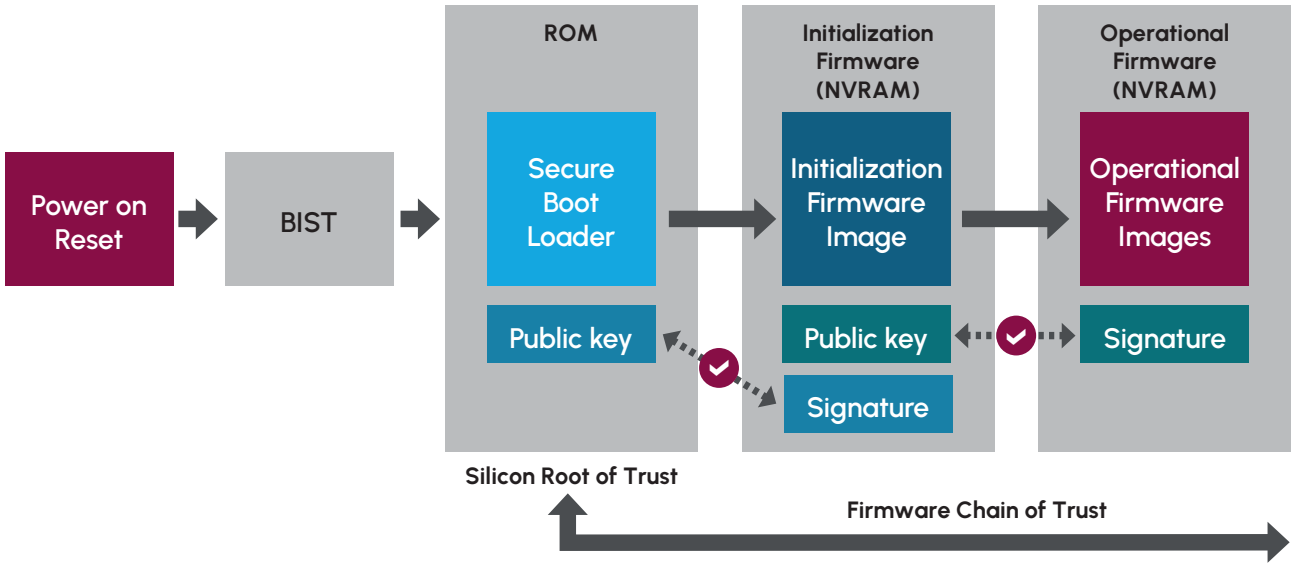


Figure 3: *Broadcom's Silicon RoT w/ Secure Firmware Loading (Source: Broadcom)*

Hardware TPM

The Futurum Group Labs verified that Dell PowerEdge's hardware security operated correctly by testing the supplied TPM version 2.0. Testing verified that all supplied features operated correctly including key generation using a true random number generator, and a secure key store. Additionally, after verifying TPM functionality, we then enabled security features including secure boot, secure lifecycle management, out of band management, and firmware updating.

Dell PowerEdge RAID Controller (PERC)

Dell's PowerEdge RAID Controllers, aka PERC 12th generation use Broadcom controller interfaces and support a variety of RAID levels and device connectivity. The PERC 12 H965i controllers tested are designed for internal and external device support and include multiple RAID levels along with SAS and NVMe connectivity.

The Dell 12th gen PERC security features include:

- Silicon based hardware RoT: Foundation for Zero Trust
- Onboard RoT builds a chain of trust by authenticating all PERC firmware prior to execution, permits only authenticated firmware upgrades
- SPDM support: Provides device attestation and secure communications
- UEFI secure boot: Helps reduce attack vectors, and root kit installations
- Secure Firmware Updates: Simplifies administrative security updates

As shown above previously in Figure 3, the process for secure booting from a Dell PERC 12 controller card is similar to securely booting via a NIC.

Dell PowerEdge 16th Generation Servers

Multiple areas of evaluation and testing were performed with the PowerEdge servers together with PERC RAID cards and Broadcom NICs. One of NIST's specifications (NIST SP 800-193) specifically addresses platform firmware resiliency. It stipulates methods for securing the BIOS, boot ROMS, along with firmware and driver signatures to verify authenticity. This guideline also outlines a method for providing a "secure boot" mechanism, whereby each component verifies subsequent components in the stack from hardware all the way to the operating system.

Secure Boot

Dell PowerEdge secure boot via Broadcom NIC, Dell PERC or local disk occurs via similar mechanisms. The secure boot process is important to ensure that a validated OS image is ultimately loaded and is used to operate the system. If an OS is altered, system security cannot be guaranteed. At a high-level, secure boot validates the UEFI drivers and boot loaders which then guarantees the authenticity and integrity of each subsequent component, firmware or software element that is loaded. This chain of trust is one of the basic elements of the Zero Trust model and basic system security. Secure boot functionality was verified with multiple devices, including secure boot of a verified OS image from Dell's PERC 12 controller, and via PXE boot using a Broadcom 100 GbE NIC card.

Authentication Access, Authorization and Auditing (IAM)

These areas include identity and access management of systems (IAM), components and users, multi-factor authentication, audit logging and alerting, and access based upon authenticated authorization. The IAM capabilities are implemented throughout Dell's management tools, including iDRAC, OME and CloudIQ.

Secure Lifecycle Management

Secure lifecycle management features were verified by first establishing a baseline, and then updating to the latest firmware and drivers via iDRAC. The secure process was verified both via the successful updates and notices, along with one image that did not update due to an invalid security certificate. The test properly identified an invalid certificate, and would not allow the firmware to be updated, which was the correct behavior. Upon obtaining a firmware image with the proper security certificate, the firmware update was successfully applied, which again was the desired security behavior.

Management, Alerting and Reporting

A critical part of Dell's cybersecurity capabilities are the management tools available. Dell's iDRAC tool continues to evolve and add capabilities for BIOS and low-level system management of PowerEdge servers and attached devices. Incorporating standards such as Redfish for secure remote manageability, enables secure programmatic API, CLI and scripting access, while also enabling secure web UI access for users preferring a graphical interface.

The Futurum Group Labs utilized and validated numerous functions and capabilities of each of Dell's enterprise management solution. iDRAC, Open Manage Enterprise and CloudIQ are designed to work together to enable a spectrum of management, alerting and reporting capabilities.

- Dell's iDRAC: system level management software pre-installed on all Dell PowerEdge servers, providing secure out-of-the box management capabilities for individual systems.

- OpenManage Enterprise (OME): Designed for IT staff to monitor and manage Dell servers within a datacenter. OME provides roll-up features to aggregate information while still providing the ability to manage individual systems, either from within OME or via linking to iDRAC.

- CloudIQ: Enables multi-site and enterprise-wide monitoring and management, with high-level management and reporting while also providing drill-down system management of some features and function.

A key part of iDRAC with OME is the integration of Broadcom components throughout, including the ability to monitor Broadcom-based PERC and NICs for firmware levels, vulnerabilities and provide updates through the secure lifecycle management capabilities.

The Dell OME management server was utilized throughout testing. Installation was straightforward and accomplished without needing to consult manuals. Downloading a preconfigured VMware image (OVA) and deploying to a VMware cluster, the OME server was operational in under 30 minutes. OME provided a way to both perform health monitoring and alerting, along with active management of desired systems. The OME interface was intuitive and provided significant fleet management features, by helping to highlight potential issues and providing the ability to resolve problems.

Futurum Group Comment: *Looking specifically at the security features of iDRAC, OME and CloudIQ, we found the health and security scoring mechanism and recommendations to be extremely effective. A significant challenge for most IT environments is prioritizing which updates are the most critical and then quickly remediating these issues. Dell's management tools enable finding and applying critical updates quickly, and is one of the most effective solutions for security we have evaluated to date.*

With CloudIQ's health scores and recommendations, it required only a few clicks to sort by the most critical issues, and then utilize the appropriate management tools to apply remediation for the vulnerabilities. Some issues may be resolved entirely from CloudIQ, with others enabled via links to OME for remediation.

Dell's CloudIQ service has continued to evolve since its storage system origins into a Dell product-wide SaaS application that effectively provides health monitoring and alerting, along with recommendations. Dell's overall management architecture provides robust security manageability, alerting and reporting capabilities that provide the critical link IT administrators require to effectively manage a secure IT environment.

3 - Manufacturing & Supply Chain Security

The concept of evaluating a product's manufacturing and supply chain for security is relatively new to many companies. Although these practices have been standard for regulated industries for years, only recently have companies began to apply supply chain security practices to products designed for commercial use. One reason is that due to increased focus on other threats, the supply chain is now seen as an area of increasing vulnerability.

One area of supply chain security that sets Dell apart from their competitors is Dell's Secured Component Verification (SCV), which is designed to help verify that the security of all components is maintained from order until it is delivered and installed at the customers location. Dell's approach to supply chain threats includes supply chain integrity with ISO certification of sites, software bill of materials and the Dell SCV process, which all help to prevent counterfeit components or malware being inserted into systems or components.

Futurum Group Comment: *Dell's approach to securing product manufacturing and supply chain is perhaps the best processes the Futurum Group Labs has evaluated. In particular, Dell's Secured Component Verification process provides unique value, enabling IT clients to quickly and easily ensure their products have not been altered or modified, including verification of both hardware and firmware components. Dell SCV is an important tool for addressing overall cybersecurity.*

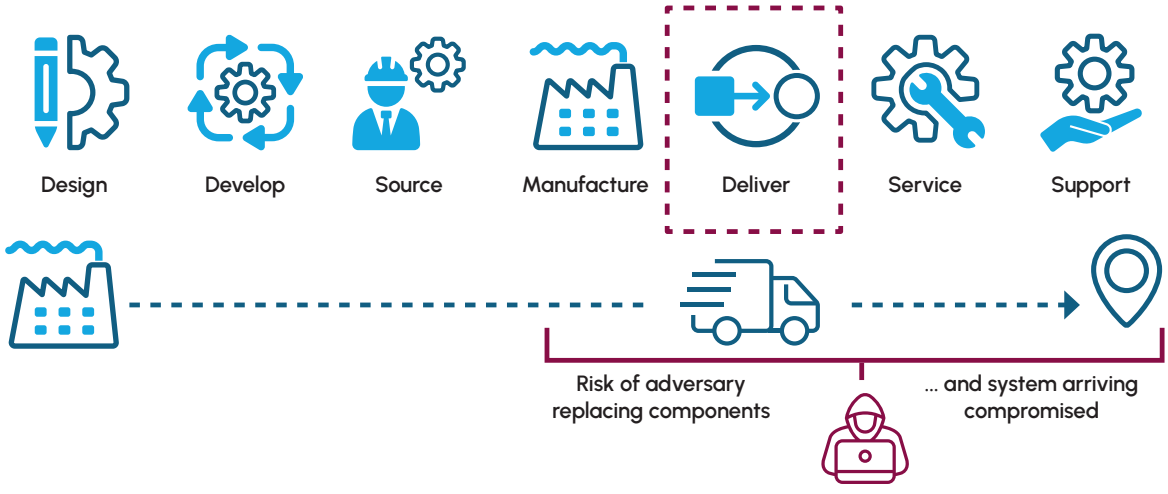


Figure 4: *Dell's Secured Component Verification Process (Source: Dell)*

The Futurum Group Labs verified that Dell's SCV can accurately report on each major system element, showing whether it is a verifiable component that was part of the original bill of materials or not. The SCV leverages the earlier security principles and technologies outlined, including Secure RoT and hardware TPM modules, cryptographic signatures for device attestation and Zero Trust principles to create a process to verify that a system has not been altered in any way.

During testing The Futurum Group Labs verified that the SCV correctly verified components that were part of the original bill of material and order, and items that were added afterwards. This capability provides a unique and easy-to-use method for IT users to attest to the authenticity and integrity of their systems.

4 - IT Security Implementation

The last major component of the Futurum Group's Security Framework is how well a company and the IT organization operates with respect to security. IT security has multiple standards, industry best practices and recommendations to help inform and guide companies towards implementations that provide the necessary security and cyber resiliency.

One guideline covering IT security is the NIST CSF [1]which includes the key phrases, Identify, Protect, Detect, Respond and Recover. The most recent update to this framework, the version 2.0 draft, adds a sixth area "Govern" to the previous list, placing more emphasis on corporate oversight and implementations.

Although important, this area falls largely outside the scope of vendors' product offerings but may be supplemented via professional services and training. As a result, The Futurum Group did not formally assess the IT Security aspects of the Futurum Group's Security Framework.

Futurum Group Comment: *The Futurum Group's Security Framework evaluates IT security through the lens of a products ease-of-use and ability to implement security best practices. In this regard, Dell enables IT security by making security best practices the default option when possible, and ensuring security features are easy-to-use. As a result of security integration between PowerEdge servers, Broadcom 57508 NICs and Dell management tools helps companies implement security best practices.*

For companies that desire security consulting to help supplement their capabilities, Dell and their partners offer a variety of security services, including cybersecurity advisory services that are designed to assess a company's security posture, and help improve internal procedures and help elevate security capabilities to attain proficiency in this area. Based upon the principles outlined previously, Dell security services include Cybersecurity Advisory Services, Recovery Services for Cyber-attacks, along with managed services for cyber-attack detection and response.

Moreover, the product design, product features, together with the secure supply chain features and security consulting services all provide sufficient tools to enable IT organizations to manage and maintain a highly secure environment that meets NIST and industry best practices for maintaining a cyber resilient posture.

(1) NIST Cybersecurity Framework, draft version 2.0, August 2023:

Final Thoughts

Security and cyber resiliency have become areas of critical focus for enterprises according to The Futurum Group's research. Additionally, conversations with IT clients often include a discussion of ransomware and cyber resiliency. Organizations that follow best practices follow the NIST or other frameworks to integrate security throughout their organization and operational procedures.

Attempting to purchase point products, or simply "add security" to existing infrastructure is challenging at best. Starting with products that are designed from the ground up with security is a key priority. According to The Futurum Group's research, a significant number of security breaches utilize compromised servers as part of their attack vector. Thus, securing servers, their networking interfaces and storage devices is an ideal area of focus for companies looking to improve their cyber resiliency.

In assessing Dell PowerEdge servers together with Broadcom add-in cards against the Futurum Group's Security Framework, we found that the systems meet or exceed requirements in all categories. There were several areas of strength noted, where PowerEdge significantly exceeded expectations. These include several security integrations between Dell's silicon RoT and Zero Trust approach, together with Broadcom NICs and PERC RAID cards own embedded RoT and Zero Trust capabilities and importantly with Dell's management tools.

Another area where PowerEdge exceeded expectations is the seamless management capabilities of iDRAC for baseboard system management, with OME for datacenter management, coupled with CloudIQ for global monitoring, alerting and reporting of multiple datacenters. The particular focus on security alerting and recommended actions of CloudIQ help IT administrators move from inaction due to an overwhelming number of issues, to action focused on the most important configuration or security issues.

Finally, Dell's SCV process significantly exceeded expectations, offering a best-in-class end-to-end process for ensuring system integrity from suppliers, manufacturing and configuration, shipping, delivery and installation. A significant area of concern for organizations is ensuring their systems do not contain malicious hardware elements that could circumvent even robust security practices. Dell's SCV provides a simple and easy way for organizations to ensure their infrastructure has not been compromised.

Taken together, Dell PowerEdge servers, with Broadcom NIC cards provide comprehensive security capabilities that provide a foundation for IT users to quickly and efficiently establish a highly secure computing environment that leverages industry best practices.

(1) NIST Cybersecurity Framework, draft version 2.0, August 2023:

Important Information About this Report

CONTRIBUTORS

Russ Fellows
Head of Futurum Labs | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION

The Futurum Group LLC | futurumgroup.com | (833) 722-5337 |