DELL Technologies

intel®

PowerEdge - Cyber Resilient Infrastructure for a Zero Trust world

Combat threats with an in-depth security stance that begins with Dell PowerEdge servers, powered by Intel® Xeon® Scalable processors.

Get Started

Table of Contents

Click on the icons or chapter titles below to navigate to specific sections. Use the arrow buttons at the top to navigate page by page. Use the home button in the top-left corner to return to the start.

Part 1: The cybersecurity landscape

Evolving threats

Cyberthreats and attacks are becoming more nefarious and widespread, and they're predicted to accelerate. In 2020, Cybersecurity Ventures predicted global cybercrime costs would grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015.[1] As data is accessed across devices, on-premises and in the cloud, high-impact data breaches continue to mount. To maintain a more secure environment, businesses must be more comprehensive in their approach.

Digital transformation was the top story in the 2000s and has only accelerated in the 2020s as organizations scramble to adapt to new and rapidly changing business environments. With increased adoption of the software-defined data center (SDDC), organizations have become more dependent on servers as the foundation for business functions. This means server security should be foundational to your overall enterprise defense strategy, guarding against threats right down to the firmware layer.

Ransomware attacks are expected to cost the world **$265 billion by 2031.**[3]

Cybersecurity challenges

Cyberthreats are coming at your business from all directions. The traditional players include hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and corporate spies, but increasingly you must also be wary of insider threats.

Today's news stories focus on the increased velocity, sophistication, effectiveness and financial impact of cyberattacks. For example, 2021 saw 50% more cyberattacks per week on corporate networks compared to 2020.[2] And while ransomware cost the world $20 billion in 2021, that number is expected to rise to $265 billion by 2031.[3]

[1] CyberCrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, November 13, 2020

[2] DARKReading, Businesses Suffered 50% More Cyberattack Attempts per Week in 2021, January 11, 2022.

[3] Cloudwards, Ransomware Statistics, Trends, and Facts for 2022 and Beyond, March 22, 2022.

Common attacks include:

Malware — This includes any malicious software such as spyware, adware or viruses that can harm your server's performance or security.

Ransomware — Ransomware is a form of malicious software or malware that, when downloaded to a server, can block access to data and files on the device until a ransom is paid.

Phish attacks, or phishing — Phishing is the act of fraudulently contacting multiple individuals or companies in an attempt to obtain unauthorized access to sensitive and/or personal information.

Supply chain — These are situations where hackers are increasingly looking to exploit weaknesses in the supply chain or third-party vendors as organizations like yours improve security.
A 2020 cyberattack on a major IT management firm, went unnoticed for months, allowing it to infect its clients with malicious code.

40%
of cyberattacks are aimed at the supply chain.[4]

[4] Accenture, Securing the Supply Chain, 2020

Compliance and regulatory pressure

As global threats increase, there is continued regulatory pressure to define best practice guidance for securing not only government and critical infrastructures but also the private sector. It's significant because, in the United States, almost 90% of critical infrastructure, like healthcare, energy, finance, transportation, telecom and utilities is held by the private sector.[5]

In May 2021 and January 2022, the United States issued White House Executive Orders that outlined a framework for protecting the nation's infrastructure and provided detailed guidance around Zero Trust architecture. The United States is not alone in its will to act. International governments are developing regulatory guidance in response to cyberthreats, and private institutions are creating policies and mandates to mitigate advanced persistent threats. These requirements extend beyond just federal agencies to critical infrastructure and other vertical markets.

As governments seek to curb or minimize cyberattacks, organizations should also expect more guidance and mandates such as:

- **Multifactor Authentication (MFA)** — MFA, also known as two-factor authentication (2FA),[6] protects data from being accessed by an unauthorized third party. It is a security technology that requires a user to be verified to gain access by using two or more independent credentials. Industries including "finance, healthcare, defense, law enforcement, and the federal government already require two-factor authentication to access systems, networks, websites, and physical building locations."[7]
- **Data-at-rest encryption** — Self-encrypting drives with enterprise class key management

[5] The White House, Press Briefing: Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure, July 28, 2021.
[6] NIST, Back to Basics: What's multi-factor authentication - and why should I care?, June 16, 2016.
[7] Okta, Which Industries Require Two-Factor Authentication?, accessed June 2022.

Cybersecurity landscape | Industry best practices | NIST framework support | Zero-trust model | Your company success

What's at stake?

Cyberattacks can be devastating to an organization. Depending on how widespread the attack is and the damage caused, recovery time can be substantial. It takes, on average, 22 days to recover from a ransomware attack.[8] Challenges organizations may encounter:

- Downtime to try to uncover what happened and then recover any lost data
- Permanent loss of internal and customer data, compromising long-term prospects
- Paying of fines and retrofits to ensure you comply with all rules and regulations
- Bad publicity and loss of business in the immediate aftermath of a cyberattack
- Loss of reputation in the long term as customers are reluctant to continue doing business with companies that have been attacked

It takes, on average,
22 days
to recover from a ransomware attack.[8]

Some organizations are so focused on growing the business that they may overlook appropriate security provisions to protect and sustain the business. Yet, a breach can rapidly change your organization's ability to perform. Combine this with the fact that infrastructure, workloads and data usage are becoming more complex, the result is that maintaining a secure IT infrastructure and operations has become significantly more complicated.

While digital transformation creates unlimited opportunities, the challenges of building an agile, modern IT environment while sustaining the confidence of your customers and stakeholders remain. If you can't stay ahead of growing security threats, the damage could be catastrophic. A lesson to note is that 64% of Americans would blame an enterprise over the hacker for losing their personal data in an attack.[9] Furthermore, 84% of consumers confirmed that they are more loyal to companies they perceive as having strong security controls.[10]

[8] Statista, Length of impact after a ransomware attack Q1 2020- Q3 2021, November 2021.

[9] Forbes, 50 Stats Showing Why Companies Need To Prioritize Consumer Privacy, June 22, 2020.

[10] SalesForce Research Report, State of the Connected Customer: Third Edition, June 2019.

Resources

Cyber Resilient Architecture infographic

Cyber Resilient Architecture video

Cyber Resilient Security in Dell PowerEdge Servers technical paper

Part 2: Industry best practices

Zero Trust

is a security strategy that requires explicit validation before granting access to data or devices.

Zero Trust is a response to the complexity of modern IT environments, including cloud and hybrid cloud — cloud-based assets that are not located within your organization's network boundary. Also compounding the complexity problem are the recent surge in remote users, millions of bring-your-own-devices (BYOD) and other government regulations.

Zero Trust is a set of guiding principles for workflow, system design and operations. Effective security approaches have evolved from a static, coarse-grained set of perimeters to something much more fluid in nature — where no trust is granted to assets or user accounts based solely on their physical or network location or asset ownership.

In other words, a Zero Trust approach evaluates and validates many points in the IT environment before granting permissions. The critical element of Zero Trust is the verification of assets within the enterprise before providing access — and continued verification prior to process execution or lateral movement within the network.

Regulatory pressure has ramped up significantly since successful ransomware attacks have hit federal entities, critical infrastructure and private sector. An example of this is the White House Executive Order issued on May 12, 2021. Since then, much documentation has been created laying out details for security implementation and new regulations. As regulatory guidance continues to evolve, organizations are finding solutions for security have become imperative rather than optional. Zero Trust requirements which started with SP800-207 with the DoD continued to be defined in conjunction with the White House executive order and in cooperation with CISA and OMB. We are finding international governments are following suit with more stringent requirements across the globe.[11]

Resources

Zero Trust infographic

[11] NIST, Zero Trust Architecture, August 10, 2020.

Part 3: Beginning with a secure foundation

The Dell philosophy for security lies in our cyber resiliency.

Building effective cyber resiliency starts with a vision of protecting your organizations from malicious actors throughout the equipment lifecycle. In alignment with the NIST Cybersecurity framework, Dell uses a security development lifecycle (SDL) (NIST SP800-160) approach to creating products and solutions that encompass security needs from design, manufacturing, supply chain and management to decommissioning.

- Server firmware is designed to obstruct, oppose and counter malicious code injection during all phases of the product development lifecycle.
- Secure coding practices are applied at each stage of firmware development.
- Threat modeling and penetration testing coverage takes place during the design process.

Safeguarding your data and intellectual property requires a layered approach. In Dell PowerEdge servers, security features are designed with overlapping layers intentionally, so if one mechanism is compromised, another layer is present to thwart the attack. This "defense in depth" approach provides improved resilience and is at the heart of our cyber-resilient architecture.

PowerEdge servers are powered by Intel Xeon Scalable processors that deliver advanced security capabilities, including Intel SGX, which helps protect data and application code in real time from the edge to the data center and multi-tenant public cloud. This enables enhanced collaboration (for example for federated learning in AI) using shared data — without compromising privacy. Intel Crypto Acceleration increases the performance of encryption-intensive workloads including SSL web serving, 5G infrastructure, and VPN/firewalls and reduces the performance impact of pervasive encryption.

This architecture builds on a PowerEdge security legacy with enhanced capabilities that effectively protect your infrastructure by reliably detecting threats and rapidly recovering from cyberattacks. It's an approach that aligns with key components of the NIST Framework (NIST SP 800-193).

Silicon root of trust

PowerEdge servers use an immutable, silicon-based root of trust to cryptographically attest to the integrity of BIOS and Integrated Dell Remote Access Controller (iDRAC) firmware. This root of trust is based on one-time programmable, read-only public keys that protect against malware tampering. One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. The root of trust provides a trusted anchor for boot operations. Complementary to this, the BIOS boot process leverages Intel Boot Guard technology, which verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in the silicon by Dell Technologies in the factory.

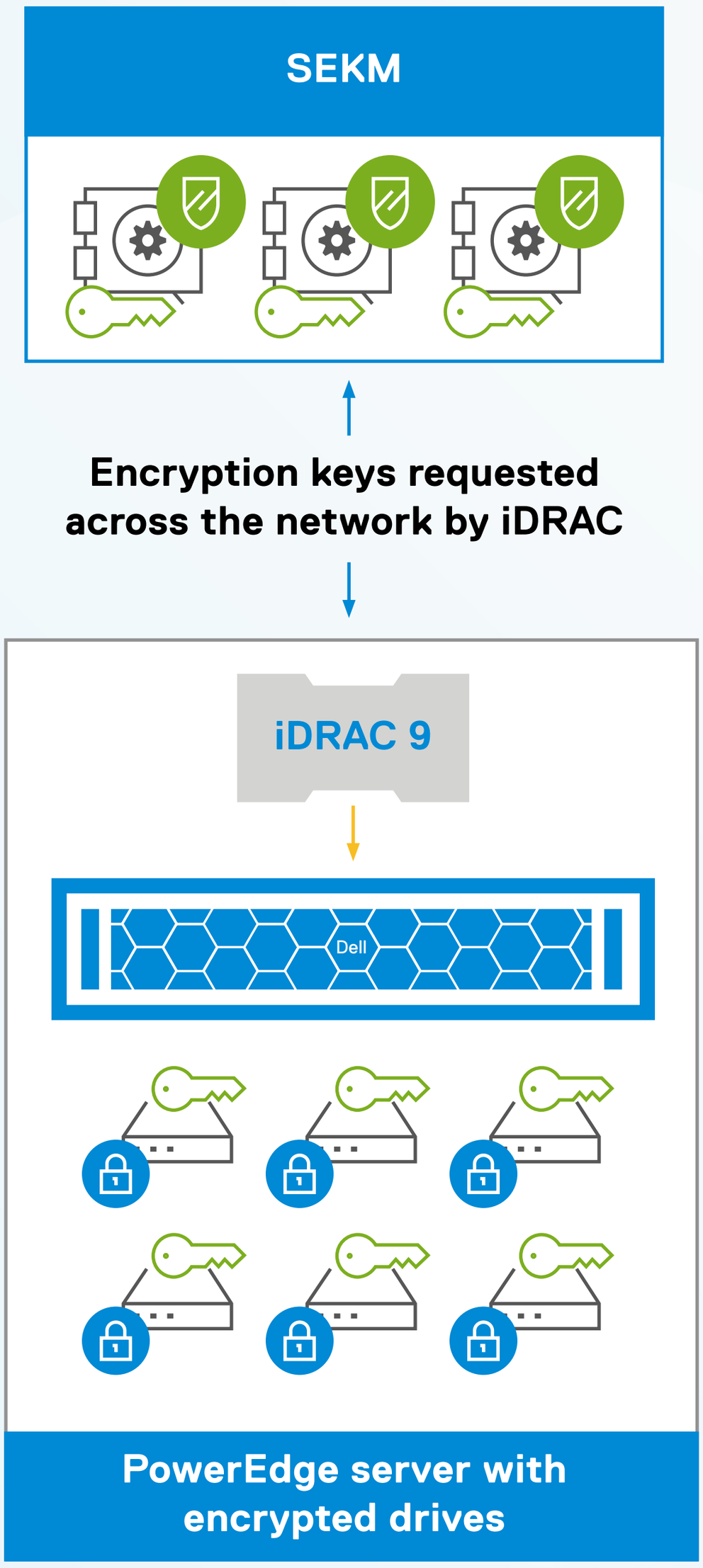
Identity and access management

Identity and access management (IAM) is a critical area particularly for protection against ransomware attacks with controls such as MFA to enable least privilege and a Zero Trust oriented approach to security. IAM is designed to ensure that only the right people can access the appropriate IT assets and data and control the scope of access.

Advanced data protection

Data protection involves safeguarding your business data, whether it is in use, in transit or at rest, typically through encryption. PowerEdge servers offer a wide array of secure storage options for your data.

External key management is a best practice where keys are stored away from drives and hosting server. Secure enterprise key manager (SEKM) allows PowerEdge customers to manage keys centrally for SEDs in PowerEdge servers and scales with storage capacity expansion. Local key management (LKM) is also available for environments where central access may be difficult or security requirements are less stringent.



Example of SEKM implementation

Resources

Data Protection infographic

SEKM webpage

SEKM video

Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers technical paper

SEKM infographic

Cyber Resilient Architecture video

Dell Security Development Lifecycle

Dell Technologies deliberately creates security controls code for every phase in the server lifecycle, from gathering of requirements to server maintenance. This includes code developed to obstruct, oppose and counter injection.

Cybersecurity landscape

Industry best practices

NIST framework support

Zero-trust model

Your company success

Verified supply chain assurance

The Dell Technologies comprehensive approach to supply chain assurance includes foundational provisions like physical personnel and cybersecurity controls. Dell Technologies also enhances component integrity assurance with its secured component verification (SCV) offering. SCV allows customers to cryptographically verify that the components set in the factory match what was delivered to them.

Security

provides the confidentiality, integrity and availability of information that describes the IT supply chain, or traverses the IT supply chain, as well as information about the parties participating in the IT supply chain.

Integrity

ensures IT products or services in the IT supply chain are genuine and unaltered and will perform according to acquirer specifications and without additional unwanted functionality.

Quality

reduces vulnerabilities that may limit the intended function of a component, lead to component failure or provide opportunities for exploitation.

Resilience

ensures that IT supply chain will provide required IT products and services despite disruptions.

Resources

Secured Component Verification video

Secured Component Verification tech note

Secured Component Verification tech talk

NCC Group: Secured Component Verification Security Assessment supply chain technical paper

Benefits of cyber-resilient products

- Maximum uptime for staff productivity
- Preservation of business reputation
- Customer trust
- Compliance to avoid costly fines and retrofits
- Freedom to innovate without distraction

Part 4: Using cyber resilience to meet Zero Trust requirements

The Dell Technologies Zero Trust approach has been refined to align with the U.S. Department of Defense (DoD) standards.
We accelerate your Zero Trust adoption through extensive cyber-resilient capabilities and a seven-pillar approach that allows users to verify at every point in the IT environment before permissions are granted.

Pillar 1: Device trust

Our silicon-based hardware root of trust provides a level of security across the entire server lifecycle from design to decommissioning. Our secure supply chain includes multiple layers of controls, like component verification, to help ensure that our servers and software have not been tampered with or maliciously modified. SCV features cryptographically signed inventory certificates across the entire PowerEdge server portfolio, including secure self-verification, so you experience peace of mind about the integrity of your hardware during transit to your data center.

Pillar 2: User trust

With iDRAC, IT administrators can securely deploy, update and monitor PowerEdge servers locally or remotely. To enhance security, iDRAC offers MFA using RSA SecureID also with integrations via Active Directory, LDAP integration with single sign-on (SSO) and with role-based access control and auditing.

Pillar 3: Transport and session trust

The PowerEdge BMC (iDRAC) has a dedicated network module, and secure shell (SSH) / transport layer security (TLS) options work to encrypt and authenticate the data that passes between your server(s) and the browser running your iDRAC web user Interface. The iDRAC enables remote management and monitors the system for critical events using sensors on the system board. Alerts and log events are sent when parameters exceed their present thresholds.

Pillar 4: Software trust

We perform proactive verification, validation and security testing throughout the software lifecycle to safeguard our software and reduce the likelihood of malware or coding vulnerabilities being inserted into it. End-to-end verified boot includes signed BIOS and firmware images, which ensure that unauthorized code won't run on a PowerEdge server. Other cyber-resilient features include automated drift detection, secure UEFI boot capabilities and recovery for BIOS and operating systems.

Pillar 5: Data trust

SEKM works in conjunction with self-encrypting drives for hardware-based encryption along with scalable central key management to help you deploy and monitor encryption keys, including remote locations and even in the cloud. This provides protection against unauthorized access to lost or stolen drives or systems. This hardware encryption can be combined with software encryption such as VMware® vSAN™ encryption on VxRail.

Confidential Compute enables protection of data-in-use at the CPU and memory and includes technologies from Intel (SGX, TME). Intel SGX provides application or function-level isolation to minimize trust perimeter.

Combining data-at-rest encryption, scalable key management and confidential compute can deliver the levels of protection needed to counter today's evolving threats.

Pillar 6: Visibility and analytics

The ability to observe what is occurring in your environment is critical. Firmware drift detection, for instance, provides real-time insights into firmware health status including any unauthorized changes. If changes are detected the system can be rolled back to a known secure state. In addition, change events can be tracked via automated logging and alerts, which will support audit and analysis for assessing overall system health.

Pillar 7: Automation and orchestration

OpenManage Enterprise is a systems management and monitoring application that provides a comprehensive view of PowerEdge servers, internal storage and other components. It includes drift detection to find changes from a user-defined configuration template, creates alerts and logs to track system status, and enables remediation for misconfigurations based on pre-setup policies. OpenManage includes firmware rollback, centralized updates, automatic secure sockets layer (SSL) certificate renewal and automated deployments for consistent security configuration.

Resources

[OpenManage Secure Enterprise Key Manager](#) solution brief

[Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing](#) base models

[Zero Trust](#) infographic

[Zero Trust](#) Video

Cybersecurity landscape | Industry best practices | NIST framework support | Zero-trust model | Your company success

Part 5: Positioning your company for success with Dell Technologies and Intel

The increase in sophistication and the expanding attack surface of threats demand a modernized approach to cyber resiliency. Our response is to support you in building a Zero Trust architecture with a range of tools and technologies. Our approach to security enables more granular controls starting with access and authorization and extending to data and system resiliency while delivering a superior user experience.

With Dell Technologies and Intel as your partners, you'll get:

- Proven cyber resiliency where security is built-in, not bolted on
- Simplicity in balancing your business objectives and productivity with security and privacy
- A suite of hardware and software designed to protect your IT infrastructure while providing you with confidence, control and scale for your security posture
- Ongoing vigilance to maintain a strong security posture using rapid response to common vulnerabilities and exploits

Resources

Security solutions webpage

Business Resiliency Services

Managed Detection and Response

Learn more about cyber-resilient PowerEdge servers, visit Dell.com/Servers.

Subscribe to our popular Dell Technologies Power of Technology podcast and catch up on the latest episodes on security and cyber resiliency.

DELL Technologies

intel

Published in the USA 09/22 ebook

Cybersecurity landscape

Industry best practices

NIST framework support

Zero-trust model

Your company success