

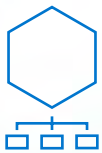
TRUST

Dell Trusted Infrastructure

Secure your organization for the modern era.

IT runs wherever the business takes it, and data is created and accessed everywhere, far from the centralized data centers of the past. Physical, virtual and software-defined systems, multicloud environments, edge devices and as-a-service delivery define IT infrastructure in the modern era — and this is changing everything we know about cybersecurity and cyber resiliency.

A trusted infrastructure operates everywhere providing maximum flexibility and business agility without compromising security. A trusted infrastructure is modern, resilient and intelligent, supporting a Zero Trust architecture or however you choose to secure and preserve your organization's most vital digital assets.



Modern

A modern infrastructure is no longer limited to on-premises data centers but is highly distributed or delivered as-a-Service and includes edge devices as well as multicloud environments to enable modern organizations.



Resilient


To be resilient, you must ensure your organization can withstand and recover your data and operations from a cyber attack. Proactive monitoring and identification of cyber threats provide confidence that your data, systems and operations are protected.



Intelligent

Intelligent infrastructure incorporates advancements like automation, machine learning and AI to enable you to scale your security posture and policies with consistency across your entire IT infrastructure.

How our secure supply chain strengthens Dell Trusted Infrastructure.



Supply chain attacks are widespread and impactful. They exploit the natural seams between organizations and abuse relationships — targeting organizations in a way that drives compromise deep into the technology stack to undermine development and administrative tools, code-signing and device firmware. Dell takes a holistic approach to protect our supply chain and deliver IT solutions and services that customers can trust. Our strategy of “defense-in-depth” and “defense-in-breadth” involves multiple layers of controls to mitigate threats that could be introduced into the supply chain. These controls, along with effective risk management, help establish our supply chain security.

Resilience

Reliable manufacturing and sourcing flexibility you can trust. Dell’s global footprint and supplier relationships are vital to the resilience of our supply chain. Our focus on continuous security improvement integrates business continuity, crisis management and disaster recovery programs across our operations. Through these strategic programs, we take proactive steps to identify and mitigate risk,

including performing frequent and ongoing business impact analysis and testing. This focus on developing resilience enables us to take a coordinated approach to assess risk and make critical decisions with complex supply chain threats. We also maintain resilience and continuity of supply plans for essential operations and supplier locations and actively consider alternate locations as a part of our sourcing strategy.

Security

We take a multifaceted approach to secure supply chain information, personnel and physical spaces. Every Dell infrastructure product and solution is conceived, designed, prototyped, implemented, produced, deployed, maintained and validated with security as a priority.

Integrity

Through trusted relationships and high standards of responsibility and integrity for ourselves and across our supply chain network, we ensure our products are genuine, unaltered and perform to specifications.

Quality

Our quality assurance reduces vulnerabilities that may limit functionality, lead to failure or provide situations that create exploitation.

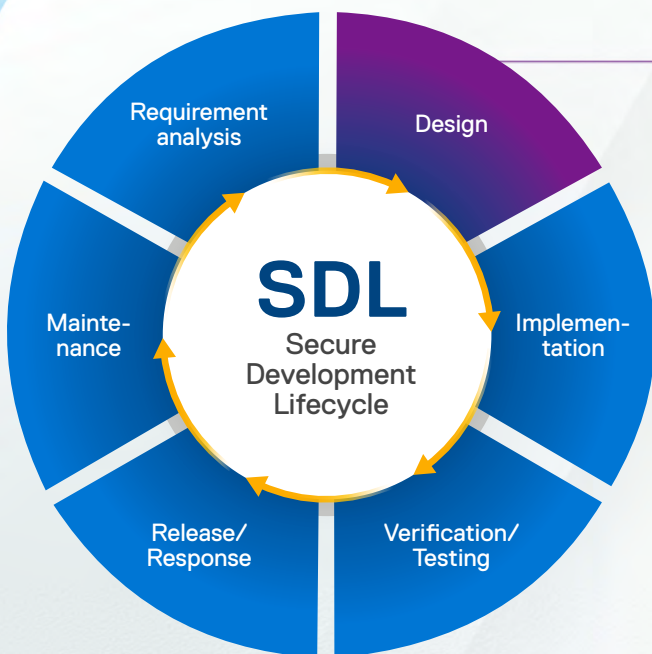
Learn more about
Dell’s Secure Supply Chain 

Fortifying Dell Trusted Infrastructure with a secure development lifecycle.

With the accelerating deployment of technology into every facet of our professional and personal lives, the traditional approach to software security isn't working. For decades, developers have been trained to test features and performance vulnerabilities at the end of the development cycle, which left flaws that continue to be exploited by

cyber criminals. To address these shortcomings, Dell integrates security testing at every stage of the software development process. We include tools and processes that encourage collaboration between developers, security specialists, and operation teams to build software that is both efficient and secure.

At Dell, we ensure intrinsic security is built into our Secure Development Lifecycle (SDL).



When engineers design new features and functionality, they follow strict procedures that prevent vulnerabilities, even within third-party components.

During product design, engineering teams create threat assessments and a model to determine the threat surface and where to focus testing after the code is developed.

Once they have created and refined the code, they follow a rigorous testing process of the source code to assure that it has been designed safely.

Risk assessments are conducted using special tools to scan for security vulnerabilities and, when finalized, verify that the threat model was accurate.

Software in our integration and delivery pipeline leverages SDL automation when building, testing and deploying applications, ensuring that security is integrated within each phase.

When needed, a team of expert ethical hackers is directed to undertake penetration testing — depending on the outcome of the threat assessment and model.

To learn about all the stages in our Secure Development Lifecycle, please visit the [Dell Security and Trust Center](#).

Dell Trusted Infrastructure

A modern, resilient, and intelligent technology foundation of secure IT solutions and services.

Like everything we do, Dell Trusted Infrastructure is designed, developed and delivered with security top of mind. Our Secure Development Lifecycle and supply chain ensures that our infrastructure solutions and services are secured from sourcing components through manufacturing and transit.



Protect data and systems

Whether at the edge, on-premises or across multiple cloud providers, you can combat cyber threats to critical systems, applications and data — all from a single provider. No one does security alone. With Dell Trusted Infrastructure, you have a holistic security presence that provides secure communications and persistent event monitoring across our entire IT ecosystem of storage, servers, hyperconverged, networking and data protection solutions.



Enhance cyber resiliency

Plan, prepare and practice recovery to lessen the impact of cyberattacks and resume operations rapidly with confidence. Dell Trusted Infrastructure provides intelligent workflows and software-defined solutions so you can quickly recover critical systems, applications and data. You can align incident response and recovery to business processes to achieve greater operational continuity as you follow Zero Trust principles or other strategies to secure your organization and assets.



Overcome security complexity

Modernize security operations and confidently build or expand your Zero Trust architecture in the face of increasing complexity. Dell Trusted Infrastructure provides proactive monitoring, machine learning and predictive analytics that simplifies operations and takes the guesswork out of what's a valid threat and what's not. See telemetry and alerts all in one place. No more jumping from tool to tool searching for the data you need to understand what's happening across systems and locations.

Dell Storage

Have peace of mind that your data is secure, protected and available.



Learn more about
Dell Storage

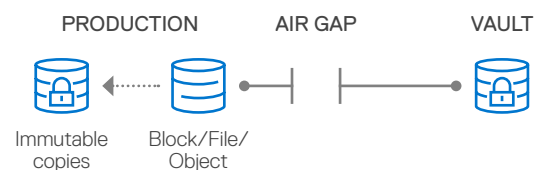


86% of organizations victimized by a successful ransomware attack in the last 12 months failed to recover all data after paying a ransom.¹

Is it possible to have secure storage solutions along with comprehensive threat detection and response? Yes, it is. Our storage solutions are designed with threat intelligence and cyber resiliency built-in to safeguard your valuable data from cyberattacks.

Data Isolation

Boost your cyber resiliency with network separation of business-critical data to protect against ransomware and automate failover and recovery.



Intelligent detection

Monitor storage and data access to identify suspicious activity and minimize exposure.

- AI-powered tools detect patterns in data access that indicate a compromise
- Security alerts are integrated with upstream security platforms with API-based automation
- Centralized storage and continuous cybersecurity monitoring provide early detection

Rapid recovery

Provide flexible, granular data recovery and application failover.

- Secure data with policy-driven automation, for space-efficient snapshot creation, access and retention
- Ensure business continuity with instant recovery in the event data is corrupted or deleted

Dell Servers

Meet today's threat landscape with a Cyber Resilient Architecture that provides evolving security controls, features and solutions.



Learn more about
Dell Servers



USD 4.82 million, the average cost of a critical infrastructure data breach.²

Server security is fundamental to an overall security strategy. Dell servers are architected to be cyber resilient, with a security-first approach that informs every phase of the product lifecycle, including evolving security controls and features to meet an ever-changing threat landscape.

Protect your server investments and valuable data. Dell provides you with capabilities that detect anomalies, breaches and unauthorized operations while also enabling recovery from unintended or malicious events.

Our PowerEdge servers come with built-in cybersecurity

capabilities, such as self-encrypting drives, end-to-end boot verification and anchoring security with a silicon-based Root of Trust. We also ensure a secure supply chain for our server components, so when your system arrives, you can validate if it has been tampered with or is secure "as built."



Secure
Supply Chain



Secure
Server Lifecycle



'Root of Trust' and End-to-End
Verified Boot Resilience

Dell Networking

Protect your infrastructure with networking capabilities that strengthen security from core to edge to cloud.



Learn more about
Dell Networking



67% of environments had ten or more devices running Server Message Block (SMB) version 1, the protocol exploited in major attacks including WannaCry and NotPetya.³

Dell Networking combines multiple layers of security at the edge and in the network, in hardware and software including a set of rules and configurations designed to protect integrity, confidentiality and accessibility of network assets.

Each network security layer implements policies and controls, including network segmentation, centralized management,

automation and scalability. When implemented through open standards, software-defined networking simplifies network design, operation and helps bring about other security trends, such as Zero Trust network access and increased cloud adoption.



Centralized
Management



Network
Segmentation



Automation
and Scalability

Dell Hyperconverged Infrastructure

Fortify applications at every layer of the stack including virtual and container environments to detect unusual data access patterns and suspicious behavior.



Learn more about
Dell Hyperconverged
Infrastructure



USD 3.05 million, the average cost savings associated with fully deployed security AI and automation.⁴

Not all Hyperconverged Infrastructure solutions are equal. With Dell, you have an agile infrastructure with full stack integrity and comprehensive lifecycle management to drive operational efficiencies and reduce risks. Dell HCI's Product Development includes security that is integrated through the product life cycle. Product features are designed with security

in mind, our concepts and designs are thoroughly analyzed to assess the potential security impact. Furthermore, we design these features so that Dell HCI solutions can be easily integrated with existing security infrastructures to meet your security objectives and compliance requirements.

AI-Powered Threat Detection

Gain insights for more informed cluster resource use and health monitoring.

Simplified, Powerful and Innovative

Built on our next-generation PowerEdge servers to deliver cloud-like agility, scalability and simplified IT management with intrinsic security and data protection.

Software Lifecycle Management

Software updates can fix issues that improve performance and patch security vulnerabilities, but we go beyond traditional approaches to avoid exposure by building intrinsic security into our coding practices.

Dell Data Protection

Protect data across core, edge and multicloud environments with solutions that best fit your infrastructure and IT needs.

Learn more about
Dell Data Protection



45% of breaches occurred in the cloud.⁵

Simplify and automate operations at scale with industry-proven, modern, intelligent data

protection. Using a full suite of integrated offerings and management tools, you can isolate critical data, identify suspicious activity and accelerate automated data recovery. With Dell data protection, you can quickly resume business as usual.

PowerProtect Cyber Recovery

A secure cyber vault for on-premises, multicloud and VMware.

Isolated

Protect data with an operational air gap on-premises and automated data isolation in multi-clouds.

Immutable

Preserve data integrity with security and controls that protect against destruction, deletion and alteration.

Intelligent

Machine Learning and analytics assure the recovery of good data and offer insights into attack vectors.

PowerProtect Appliances

Target, integrated and software defined to enable IT transformation.

Efficient

Industry-leading deduplication optimized for any environment and available directly from cloud marketplaces.

Open

Broad eco-system support for backup applications with advanced DD Boost integration support.

Secure

Data invulnerability architecture ensures data is stored and restored correctly.

PowerProtect Data Manager

Next generation software platform for proven and modern cloud data protection.

Resilient

Ensure your data and applications are protected and available when you need them.

Flexible

Protect existing and modern workloads, including applications, file systems, NAS, virtual machines and Kubernetes containers.

Insightful

Gain valuable insight into your data with cloud-based monitoring and analytics for continuous health tracking, notification and recommendations.

Dell CloudIQ

Gain insight into your infrastructure with proactive cybersecurity assessments and fast remediation.



Learn more about
Dell CloudIQ



99% of security misconfigurations go unnoticed.⁶

Keeping system administration access points within your infrastructure locked down is the foundation

Be more responsive with proactive security notifications right within the application administrators use to manage infrastructure health, capacity and performance. Monitoring and predictive analytics combine human and machine intelligence to deliver insights that ensure your IT infrastructure meets business demands.

for securing the data and systems that run your business. But manual methods for checking multiple security configurations in every system are impractical in today's highly distributed and complex IT environment.

Because your environment is becoming more complex, not less, Dell eases your burden by providing management solutions that continuously look at your security policies based on the NIST 800-53 r5 and NIST 800 – 209 standards and Dell best practices. In addition, we provide an automated assessment of current security settings as well as automated risk notifications with recommendations for remediation.



Security policies
based on NIST CSF



Automated
assessment



Remediation risk notifications
and recommendations

Trust in technology has never been more essential than in today's modern era.

At Dell Technologies, we understand that you need to focus on business, not ensuring that every chip in every server in every rack in every data center and cloud provider in your global IT environment is safe and secure. It's why we build security into everything we design. **Wherever you are on your security transformation journey, we can help.**

1 Assess

Do a thorough and honest assessment of your cybersecurity and resiliency readiness. Or reach out to our professional security services team for assistance.

[Take our online cyber resiliency assessment.](#)

2 Explore

Request a follow-up to explore the advanced solutions, services and intrinsic security innovations we can provide to help address any security gaps you found in your assessment.

[Request a call back.](#)

3 Plan

Security is a critical area where it pays to get out in front of both predictable and unexpected events. Work with Dell security experts to build a strategy for enhancing cyber resiliency.

[Chat with a business advisor.](#)

4 Accelerate

Modernize your cybersecurity posture to build your resiliency and confidence. It's time to accelerate both your security and digital transformations into a competitive advantage.

[Call 1-800-433-2393](#)

DELLTechnologies

Dell Trusted Infrastructure

Cyber attacks never sleep, but you can have peace of mind that your journey to IT transformation is secure.

[Learn how.](#)

¹ [ESG Research on Cyber Resilience & Ransomware - 2021](#)

² [Cost of a Data Breach Report 2022, Ponemon Institute and IBM Security](#)

³ [Extrahop Security Advisory – 2021](#)

⁴ [Cost of a Data Breach Report 2022, Ponemon Institute and IBM Security](#)

⁵ [Cost of a Data Breach Report 2022, Ponemon Institute and IBM Security](#)

⁶ [Cloud-Native: The Infrastructure-as-a-Service Adoption and Risk](#)