DELL Technologies

Zero Trust

A path to better cybersecurity

Take a Zero Trust journey with an experienced technology and security partner.

Organizations advancing their cybersecurity maturity are building an actionable roadmap that identifies ways to reduce their attack surface, detect and respond to cyber threats, and implement ways to recover from cyber attacks, all with Zero Trust enabling capabilities.

To address increasingly sophisticated cyber threats, Dell utilizes the built-in security capabilities in our solutions and our partners to help our customers achieve Zero Trust that aligns to our customers business objectives.

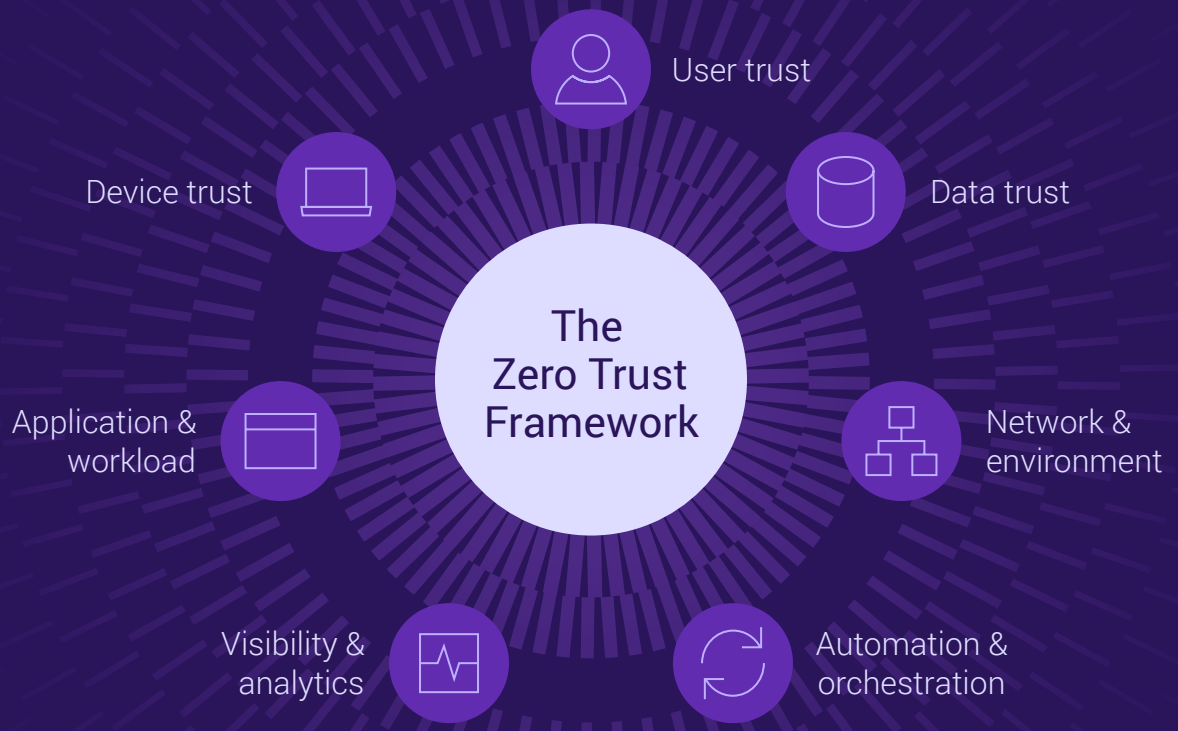
What is Zero Trust?

Imagine your network as a castle. Once the bridge is down and someone enters, they can roam freely. It's time to update the perimeter-based defense security model to the more modern, more secure, Zero Trust framework.

Zero Trust is an architectural approach to security versus a product you buy. It never trusts and always verifies legitimate business use before granting anyone or anything access to resources. This means that users and devices are not trusted by default, even if they're connected to a permissioned network and even if they were previously verified.

Never trust, always verify.

Fundamentals for a secure IT ecosystem.



The Zero Trust framework, as defined by the National Institute of Standards and Technologies (NIST), has been adopted and built into an architecture by the U.S. Department of Defense (DoD).

It includes seven interrelated pillars guiding Dell Technologies across all security domains. When combined, the pillars provide a multifaceted, integrated architecture for a comprehensive security approach that protects your organization's data and infrastructure.

Zero Trust adoption has been challenging due to the complexity of integrating diverse security capabilities and navigating fragmented options among a number of security providers.

NIST

U.S. Department *of* Defense

DELL Technologies

Advance your Zero Trust maturity.

No matter where you are on your journey, Dell has solutions to help.

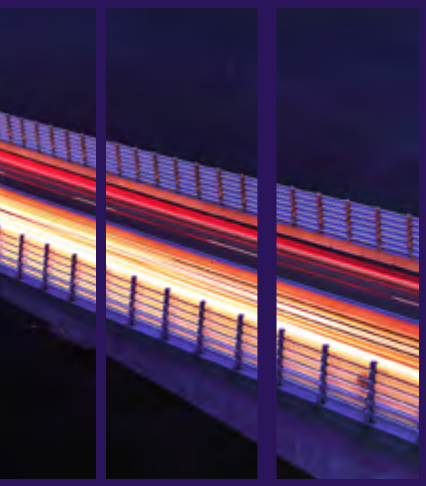
Dell Technologies brings choice and flexibility to your organization. If you're looking to advance your cybersecurity maturity, we can provide security solutions with Zero Trust capabilities to enhance your ability to harden, detect, defend and recover from malicious cyber activity.

Activate Zero Trust principles.

Enable choice and flexibility for advancing cybersecurity maturity.

Dell Technologies offers security solutions and Zero Trust capabilities to enhance your ability to harden, detect, defend and recover from malicious cyber activity. This is how:

- Built in protections that enhance automation, threat intelligence, authentication, visibility and more
- Services to develop a roadmap, integrate key technologies and manage proactively in support of Zero Trust
- Professional, managed, and security advisory services
- Extensive partner ecosystem



Dramatically simplify Zero Trust adoption.

Go all-in with a fully integrated architecture.

Because Zero Trust is an architectural approach to security, it isn't a single product and requires a carefully planned harmony of solutions. Dell is removing the Zero Trust integration burden. Here's how:

- Dell is building the first and only fully integrated Zero Trust Architecture designed, tested and validated by the US Department of Defense

DELL Technologies

Activate Zero Trust principles.

Achieve Zero Trust in a way that builds on your specific security ecosystem.

Dell helps advance cybersecurity maturity in support of Zero Trust strategies, which help reduce the attack surface, enhance detection and speed recovery from cyber threats.

Within each of the Zero Trust pillars pictured are technologies, processes and people aligned to critical areas where security and business policies are needed to protect your organization. Dell Security Services can help with:

- Security maturity, Zero Trust and risk assessments
- Strategy and roadmap development
- Managed services of key Zero Trust capabilities

DELL Technologies

Zero Trust foundations.

We provide advanced, embedded security solutions that give you an advantage on your path to Zero Trust.

Dell Data Protection

Cyber Recovery vault | PowerProtect Data Manager | CyberSense transparent snapshots | Cloud IQ | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access | Cloud IQ

Dell PowerEdge servers

Software bill of materials | Secure component verification | Silicon Root of Trust | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access | Cloud IQ

Dell storage platforms

Data isolation | Data immutability | Threat detection | Access control authentication | Data encryption | STIG hardening | HW Root of Trust | Secure boot | Digitally signed firmware | Role-based access | Secure snapshots

Dell HCI/CI

Hardware root of trust | Secure boot chain of trust | Digitally signed updates | Key management | Secure logging | Distributed virtual switches | VM isolation | Authentication & authorization | Ecosystem connectors | Continuously validated states | Software code integrity | Electronic compatibility matrix

Dell commercial PCs

BIOS/firmware security | Hardware security | Supply chain assurance | Threat management software (EDR, XDR, VDR) | Network and cloud data protection software

Dell edge solutions

HW/SW/VM attestation | Secure onboarding | Chain of trust | Secure OS/application delivery | Data rights management

Dell network switches

SmartFabric | Cloud IQ | SD-WAN | VLAN segmentation | Enterprise SONiC | Access control lists | RADIUS | TACACS+ | Cryptography | Switch hardening | Micro-segmentation | Virtual routing & forwarding

DELL Technologies

Our accelerated approach.

Fast and thorough, Project Fort Zero integrates Zero Trust throughout your organization holistically.

Project Fort Zero offers a validated method for immediate advanced maturity in Zero Trust, cutting adoption time, reducing disruptions and managing costs.

Based on our expertise and reach within the industry, the U.S. Department of Defense asked Dell Technologies to help accelerate the rate of adoption of Zero Trust. To help private and public sector organizations simplify adoption and globally scale the Zero Trust architecture, Dell is building a ecosystem and leading the integration of more than 30 leading technology and security companies. We are leading the development and global scaling of Zero Trust architecture for both private and public organizations worldwide. This is a testament to Dell's commitment to the US DoD objectives to achieve Zero Trust.

On-premises

In data centers for organizations where data security and compliance are paramount.

Remote or regional

At locations like retail stores where secure, real-time analysis of customer data can deliver a competitive advantage.

The detachable edge

In places such as airplanes or vehicles with intermittent connectivity where temporary implementation is needed for operational continuity.

DELL Technologies

We'll help you accelerate Zero Trust adoption by deploying all **152** activities put forth by the U.S. DoD for an advanced level of Zero Trust.

Execution enablers

Doctrine | Organization | Training | Material | Leadership & Education | Personnel | Facilities | Policy

Zero Trust target level

User trust	Device trust	Application & workload	Data trust	Network & environment	Automation & orchestration	Visibility & analytics
User Inventory	Device Help Tool Gap Analysis	Application/Code Identification	Data Analysis	Define Granular Control Access Rules & Policies Pt. 1	Policy inventory & Development	Scale Considerations
App Based Permission	Integrate NextGen AV Tools with C2C	Resource Authorization Pt. 1	DLP Enforcement Point Logging and Analysis	Define SDN APIs	Task Automation Analysis	Log Parsing
Rule Based Dynamic Access Pt. 1	NPE/PKI Device Under Management	Build DevSecOps Software Factory Pt. 1	DRM Enforcement Point Logging and Analysis	Define Granular Control Access Rules & Policies Pt. 2	Response Automation Analysis	Asset ID & Alert Correlation
Organizational MFA/IDP	Deny Device by Default Policy	Approved Binaries/Code	Define Data Tagging Standards	Implement SDN Programmable Infrastructure	Tool Compliance Analysis	Threat Alerting Pt.1
Implement System and Mitigate Privileged Users Pt. 1	Implement UEDM or equivalent tools	Vulnerability Management Program Pt. 1	Implement Data Tagging & Classification Tools	Datacenter Macro Segmentation	Organization Access Profile	Implement Analytics Tools
Organization Identity Life-Cycle Management	Enterprise Device Management Pt. 1	SDC Resource Authorization Pt. 1	File Activity Monitoring Pt. 1	Implement Micro Segmentation	Implement SOAR Tools	Cyber Threat Intelligence Program Pt. 1
Deny User by Default Policy	Implement EDR Tools & Integrate w/ C2C	Resource Authorization Pt. 2	Implement DRM and Protection Tools Pt. 1	Segment Flows into Control Management and Data Planes	Standardized API Calls & Schemas Pt. 1	Log Analysis
Single Authentication	Implement Asset, Vulnerability and Patch Management Tools	Build DevSecOps Software Factory Pt. 2	Implement Enforcement Points	B/C/P/S Macro Segmentation	Workflow Enrichment Pt. 1	Threat Alerting Pt. 2
Implement System and Mitigate Privileged Users Pt. 2	Enterprise IDP Pt. 1	Automate Application Security & Code Remediation Pt. 1	Interoperability Standards	Application & Device Micro Segmentation	Enterprise Security Profile Pt. 1	User/Device Baselines
Enterprise Identity Life-Cycle Management Pt. 1	Implement C2C/ Compliance Based Network Authorization Pt. 1	Vulnerability Management Program Pt. 2	Develop SDS Policy	Protect Data In Transit	Enterprise Integration & Workflow Provisioning Pt. 1	Establish User Baseline Behavior
Implement UEBA Tooling	Implement App Control & FIM Tools	Continual Validation	Manual Data Tagging Pt. 1		Implement Data Tagging & Classification ML Tools	Baseline & Profiling Pt. 1
Periodic Authentication	Managed and Limited BYOD & IOT Support	SDC Resource Authorization Pt. 2	File Activity Monitoring Pt. 2		Standardized API Calls & Schemas Pt. 2	Cyber Threat Intelligence Program Pt. 2
Enterprise PKI/IDP Pt. 1	Enterprise Device Management Pt. 2		Implement DRM and Protection Tools Pt. 2		Workflow Enrichment Pt. 2	
	Implement XDR Tools & Integrate w/ C2C Pt. 1		DLP Enforcement via Data Tags and Analytics Pt. 1			
			Integrate DAAS Access w/ SDS Policy Pt. 1			
			DRM Enforcement via Data Tags and Analytics Pt. 1			
			Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1			

Total target activities: 91

Source: DoD Zero Trust Strategy Publication, November 07, 2022

DELL Technologies

Advanced Zero Trust

User trust	Device trust	Application & workload	Data trust	Network & environment	Automation & orchestration	Visibility & analytics
Rule Based Dynamic Access Pt. 2	Enterprise IDP Pt. 2	Enrich Attributes for Resource Authorization Pt. 1	Manual Data Tagging Pt. 2	Network Asset Discovery & Optimization	Enterprise Security Profile Pt. 2	Threat Alerting Pt. 3
Enterprise Roles and Permissions Pt. 1	Implement C2C/ Compliance Based Network Authorization Pt. 2	Enrich Attributes for Resource Authorization Pt. 2	Database Activity Monitoring	Real-Time Access Decisions	Enterprise Integration & Workflow Provisioning Pt. 2	Baseline & Profiling Pt. 2
Alternative Flexible MFA Pt. 1	Entity Activity Monitoring Pt. 1	Continuous Authorization to Operate (ATO) Pt. 1	Automated Data Tagging & Support Pt. 1	Process Micro segmentation	Implement AI Automation Tool	UEBA Baseline Support Pt. 1
Real Time Approvals & JIT/JEA Analytics Pt. 1	Fully Integrate Device Security Slack w/ C2C	Automate Application Security & Code Remediation Pt. 2	DRM Enforcement via Data Tags and Analytics Pt. 2		Workflow Enrichment Pt. 3	UEBA Baseline Support Pt. 2
Enterprise Identity Life-Cycle Management Pt. 2	Enterprise PKI Pt. 1	REST API Micro-Segments	DLP Enforcement via Data Tags and Analytics Pt. 2		AI driven by Analytics decides A&O modifications	AI-enabled Network Access
User Activity Monitoring Pt. 1	Managed and Full BYOD & IOT Support Pt. 1	Continuous Authorization to Operate (ATO) Pt. 2	Integrate DAAS Access w/ SDS Policy Pt. 2		Implement Playbooks	AI-enabled Dynamic Access Control
Continuous Authentication Pt. 1	Implement XDR Tools & Integrate w/ C2C Pt. 2		Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2		Automated Workflows	
Continuous Authentication Pt. 2	Entity Activity Monitoring Pt. 2		Integrate SOS Tool and/or Integrate with DRM Tool Pt. 1			
Enterprise PKI/IDP Pt. 3	Enterprise PKI Pt. 2		Automated Data Tagging & Support Pt. 2			
Enterpriser Roles and Permissions Pt. 2	Managed and Full BYOD & IOT Support Pt. 2		Comprehensive Data Activity Monitoring			
Alternative Flexible MFA Pt. 2			DRM Enforcement via Data Tags and Analytics Pt. 3			
Real Time Approvals & JIT/JEA Analytics Pt. 2			DLP Enforcement via Data Tags and Analytics Pt. 3			
Enterprise Identity Life-Cycle Management Pt. 3			Integrate DAAS Access w/ SDS Policy Pt. 3			
User Activity Monitoring Pt. 2			Integrate SDS Tool and/or integrate with DRM Tool Pt. 2			
Enterprise PKI/IDP Pt. 2						

Total advanced activities: 61

Dell Technologies can simplify the complexity of achieving Zero Trust maturity quickly.

Source: DoD Zero Trust Strategy Publication, November 07, 2022

DELL Technologies

Meeting the needs of all organizations.

Advance your Zero Trust maturity.

Zero Trust is a defined framework and set of principles that guide how security should be approached and it can be implemented using a variety of capabilities. Whether you're all-in on Zero Trust or focused on targeted improvements, aligning to the Zero Trust principles, Dell is an experienced security partner to help you on advancing your security journey.

Chemical	Information Technology	Communications	Emergency Services
Food & Agriculture	Defense	Healthcare & Public Health	Manufacturing
Financial	Nuclear Reactors	Commercial	Government
Energy	Transportation	Water & Wastewater	Dams

DELL Technologies

DELL Technologies

An experienced technology and security partner for your organization's Zero Trust journey.

Improve cybersecurity for the long-term by implementing Zero Trust.

Dell Security Services offers:

Expert assessment of security maturity and overall risk.

Development of a Zero Trust roadmap.

Ongoing management of security activities.

DELL Technologies

Dell.com/SecuritySolutions

Request a callback

Chat with a security advisor

Call 1-800-433-2393