

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.

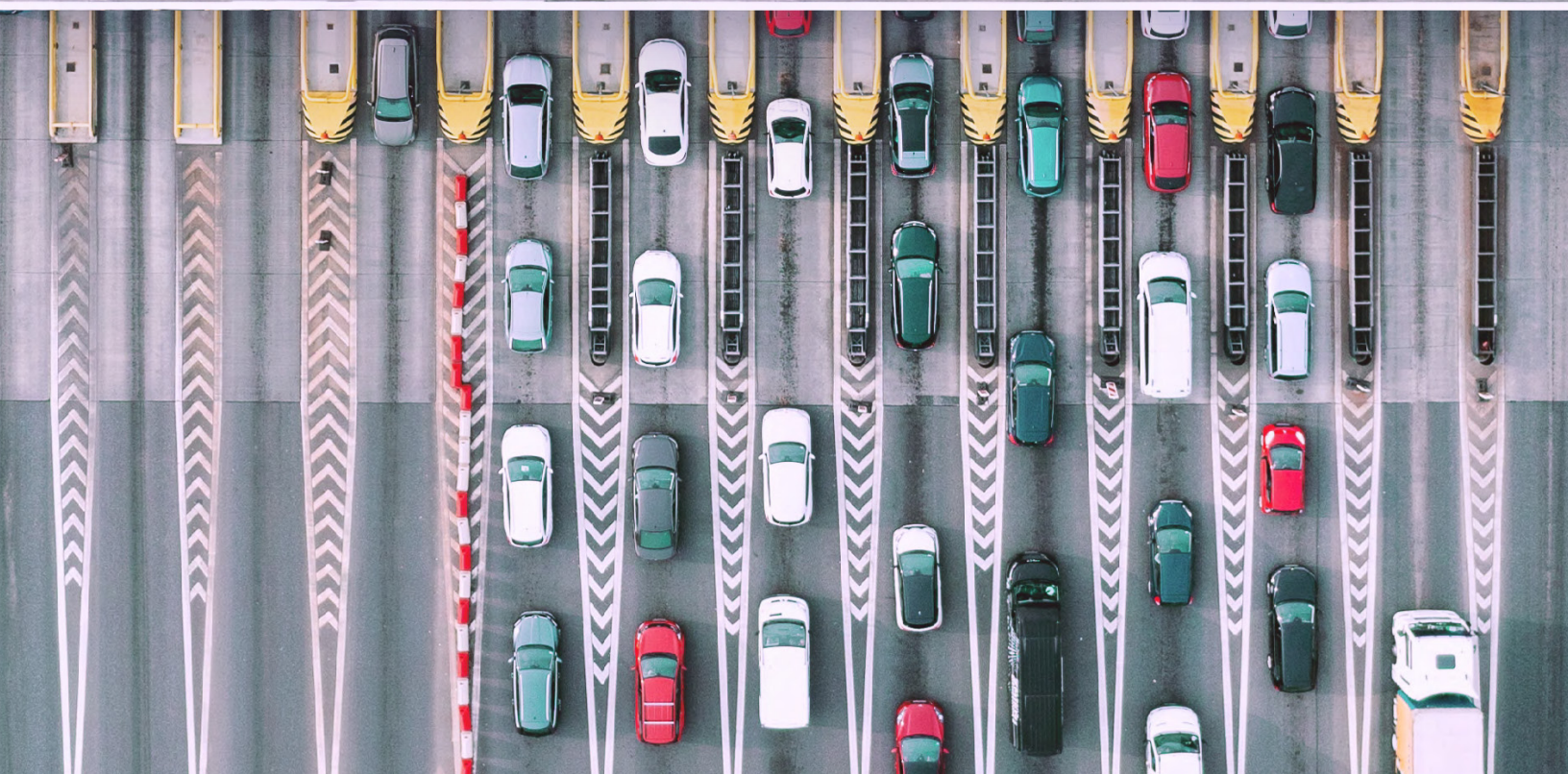
To address increasingly sophisticated cyber threats, Dell utilizes the built-in security capabilities in our solutions and our partners to help our customers achieve zero trust that aligns to our customers business objectives.



What is zero trust?

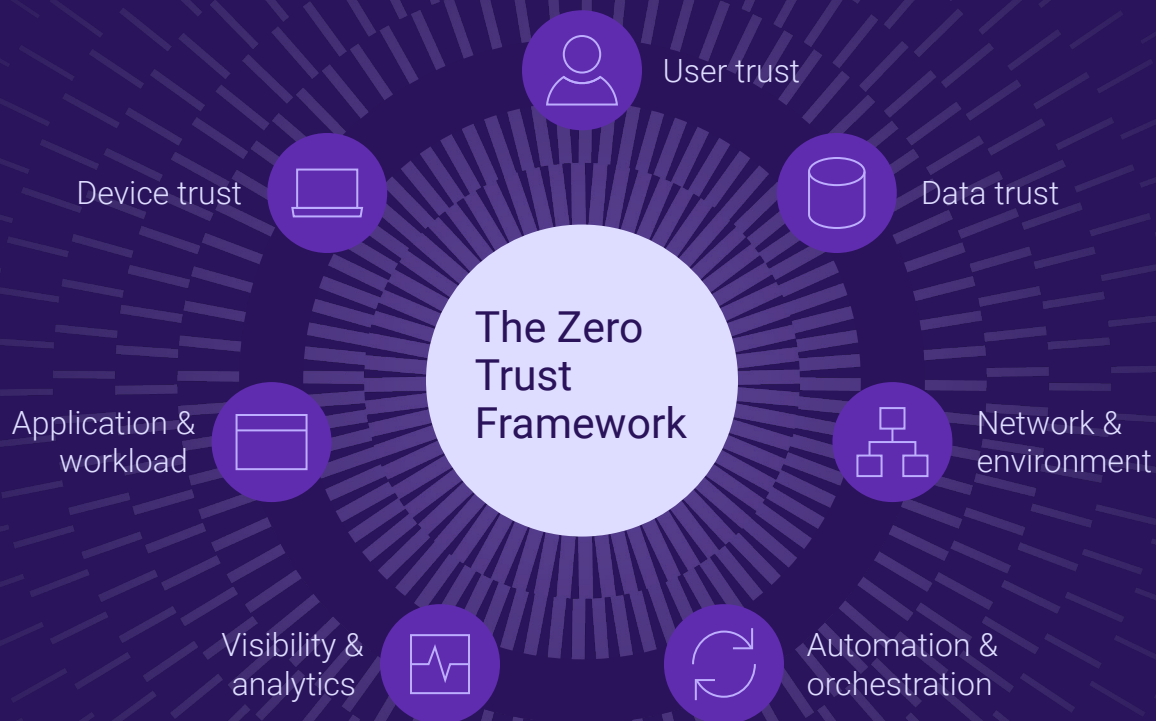
Imagine your network as a castle. Once the bridge is down and someone enters, they can roam freely. It's time to update the perimeter-based defense security model to the more modern, more secure, zero trust framework.

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 permitted 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).

NIST



U.S. Department of Defense

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.

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

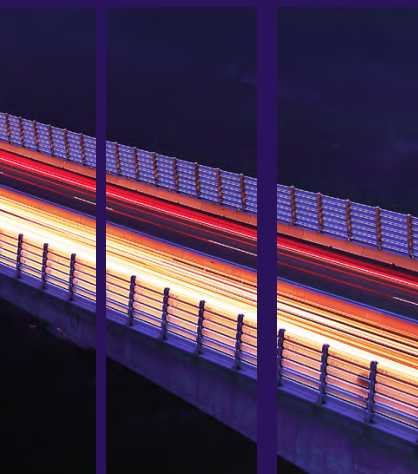


Dramatically simplify zero trust adoption.

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



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



Zero trust foundations.

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



Dell Cyber Resilience

PowerProtect Data Domain | Cyber Recovery vault | CyberSense | PowerProtect Data Manager | Transparent Snapshots | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access | AI Ops | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access



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 | AI Ops



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



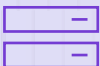
Dell commercial PCs

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

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


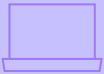





In places such as airplanes or vehicles with intermittent connectivity where temporary implementation is needed for operational continuity.

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 App Based Permission Rule Based Dynamic Access Pt. 1 Organizational MFA/IDP Implement System and Mitigate Privileged Users Pt. 1 Organization Identity Life-Cycle Management Deny User by Default Policy Single Authentication Implement System and Mitigate Privileged Users Pt. 2 Enterprise Identity Life-Cycle Management Pt. 1 Implement UEBA Tooling Periodic Authentication Enterprise PKI/IDP Pt. 1	Device Help Tool Gap Analysis Integrate NextGen AV Tools with C2C NPE/PKI Device Under Management Deny Device by Default Policy Implement UEDM or equivalent tools Enterprise Device Management Pt. 1 Implement EDR Tools & Integrate w/ C2C Implement Asset, Vulnerability and Patch Management Tools Enterprise IDP Pt. 1 Implement C2C/ Compliance Based Network Authorization Pt. 1 Implement App Control & FIM Tools Managed and Limited BYOD & IOT Support Enterprise Device Management Pt. 2 Implement XDR Tools & Integrate w/ C2C Pt. 1	Application/Code Identification Resource Authorization Pt. 1 Build DevSecOps Software Factory Pt. 1 Approved Binaries/Code Vulnerability Management Program Pt. 1 SDC Resource Authorization Pt. 1 Resource Authorization Pt. 2 Build DevSecOps Software Factory Pt. 2 Automate Application Security & Code Remediation Pt. 1 Vulnerability Management Program Pt. 2 Continual Validation SDC Resource Authorization Pt. 2	Data Analysis DLP Enforcement Point Logging and Analysis DRM Enforcement Point Logging and Analysis Define Data Tagging Standards Implement Data Tagging & Classification Tools File Activity Monitoring Pt. 1 Implement DRM and Protection Tools Pt. 1 Implement Enforcement Points Interoperability Standards Develop SDS Policy Manual Data Tagging Pt. 1 File Activity Monitoring Pt. 2 Implement DRM and Protection Tools Pt. 2 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	Define Granular Control Access Rules & Policies Pt. 1 Define SDN APIs Define Granular Control Access Rules & Policies Pt. 2 Implement SDN Programmable Infrastructure Datacenter Macro Segmentation Implement Micro Segmentation Segment Flows into Control Management and Data Planes B/C/P/S Macro Segmentation Application & Device Micro Segmentation Protect Data In Transit	Policy inventory & Development Task Automation Analysis Response Automation Analysis Tool Compliance Analysis Organization Access Profile Implement SOAR Tools Standardized API Calls & Schemas Pt. 1 Workflow Enrichment Pt. 1 Enterprise Security Profile Pt. 1 Enterprise Integration & Workflow Provisioning Pt. 1 Implement Data Tagging & Classification ML Tools Standardized API Calls & Schemas Pt. 2 Workflow Enrichment Pt. 2	Scale Considerations Log Parsing Asset ID & Alert Correlation Threat Alerting Pt.1 Implement Analytics Tools Cyber Threat Intelligence Program Pt. 1 Log Analysis Threat Alerting Pt. 2 User/Device Baselines Establish User Baseline Behavior Baseline & Profiling Pt. 1 Cyber Threat Intelligence Program Pt. 2
Total target						91

activities:

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

Copyright © Dell Inc. or its subsidiaries. All Rights Reserved.

Advanced zero trust

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

61 Total advanced activities:

Dell Technologies can simplify the complexity of achieving zero trust maturity quickly.

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
ServicesFood &
Agriculture

Defense

Healthcare &
Public Health

Manufacturing

Financial

Nuclear
Reactors

Commercial

Government

Energy

Transportation

Water &
Wastewater

Dams



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.com/SecuritySolutions

[Request a callback](#)

[Chat with a security advisor](#)

Call 1-800-433-2393