DELL Technologies

Build Your Agency’s Next Breakthrough on a Zero Trust Foundation

Never trust, always verify

Zero trust isn’t a single solution or piece of hardware. It’s a set of principles that governs the way we approach cybersecurity. The intended outcome of a zero trust model is for trusted identities to get access to the applications, systems, networks and data based on their roles and what they need to perform their jobs.

Dell Technologies is a trusted partner to our nation’s government agencies and the U.S. Department of Defense. We bring together the expertise and end-to-end intelligent solutions to help you simply, securely and responsibly innovate and collaborate to deliver data-driven breakthrough experiences for your customers and your workforce, no matter where the mission takes them.

The Dell Technologies approach to zero trust is based on integrating the seven tenets outlined in a National Institute of Standards and Technology (NIST) Special Publication 800-207 as well as the seven pillars of the Department of Defense’s zero trust reference architecture.

Applications and workloads

Device trust

- Device authentication
- Device management
- Device inventory
- Device compliance

User trust

- Multifactor authentication
- User authorization
- Conditional access

Transport and session trust

- Microsegmentation
- Transport encryption
- Session protection

Application trust

- Single sign-on
- Isolation
- Any device access

Data trust

- Data-at-rest protection
- Integrity
- Data loss prevention
- Data classification

Network and environment

Visibility and analytics

- Visibility: dashboards, logging alerts, inventory submission, data tagging, metadata
- Analytics: trend graphing, traffic reporting, data utilization reporting, etc.

Automation and orchestration

- Orchestration: policy engines, baseline configuration definitions
- Automation: automated remediation engines, conditional access mechanisms, incident response playbooks

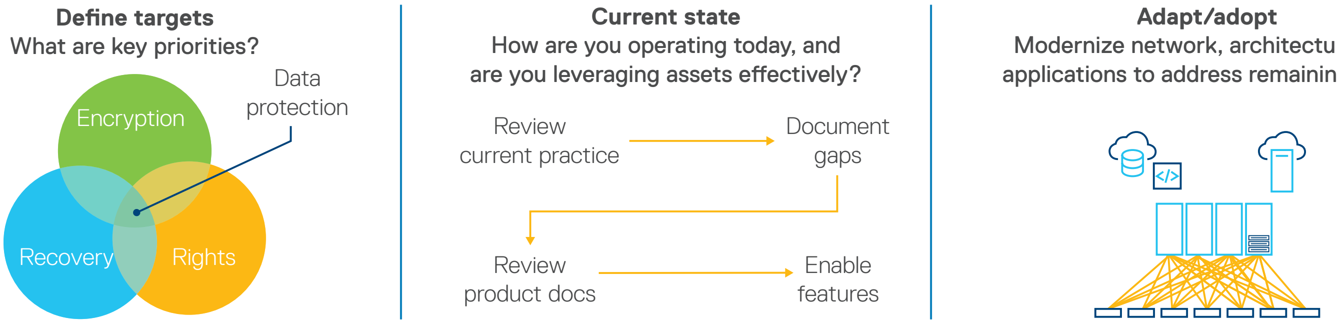
Pillar approach based off of NIST, CISA, and DoD zero trust standards.

Dell Technologies hardware as a foundation for zero trust

Dell Technologies brings a secure supply chain and built-in cyber resiliency to all of our products and solutions. We also offer a broad range of specialized security solutions to counter cyberthreats and minimize attacks that compromise sensitive data and citizen information.

Long before zero trust became an industry catchphrase, Dell Technologies products, like the next-generation PowerMax storage, employed zero trust principles. The intrinsic security capabilities of our compute and storage products map directly zero trust functions. These capabilities include PIV/CAC authentication, encryption at rest and in transit, and telemetry data for real-time monitoring. You can install as many security tools and solutions on top of servers as you want, but if the underlying hardware and firmware can't be trusted, then your security investments could potentially go to waste.

Developing a pathway



Define targets
What are key priorities?

Current state
How are you operating today, and are you leveraging assets effectively?

Adapt/adopt
Modernize network, architecture and applications to address remaining gaps.

There is no single product or process change that can address all zero trust initiatives. However, by defining your targets, understanding current operations, and adapting to new processes, you can address individual gaps with innovative zero trust architectures. Dell Cybersecurity Advisory Services can help assess where you align with recent federal mandates, and help you develop a roadmap to achieve your zero trust goals.

Drive progress with Dell Technologies

There are multiple capabilities within and spread across the zero trust pillars, and a complete solution requires products from several vendors. Dell Technologies can leverage its extensive partner ecosystem to engineer a comprehensive zero trust outcomes — like identity management, endpoint compliance, zero trust networking, and AI/ML data analytics. Our strong security foundation across our portfolio coupled with being one of the most trusted technology integrators in the world, makes Dell Technologies a great choice for assisting our customers in their zero trust journeys.

The federal civilian zero trust strategy (OMB M-22-09) and the DoD zero trust strategy are requiring government organizations to rapidly deploy this new security paradigm. Dell Technologies is working closely with Federal System Integrators and architected outcome-based zero trust solutions that are used in the U.S. government today. To further support our federal customers, Dell is building a Zero Trust Center of Excellence for testing workloads and exploring the intricacies of a zero trust environment.

For more information

Discover how Dell Technologies can modernize your infrastructure and advance your federal initiatives. Visit us at Dell.com/Federal, email DellFederalSales@federal.dell.com or call us at 855-860-9606 to learn more.

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.