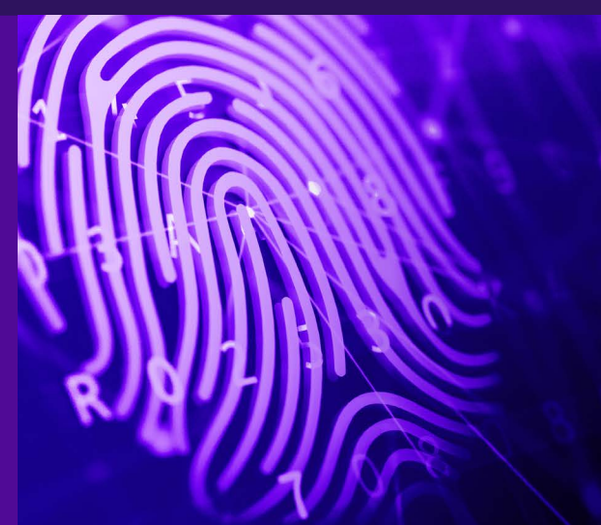
DELL Technologies

5 Recommendations to Address Your Zero Trust Needs



1	2	3	4	5
Plan for the paradigm shift to never trust, always verify	**Determine your desired path**	**The organization drives the zero trust environment, not the other way around**	**Focus on the data**	**Implement never trust, always verify throughout the IT ecosystem**
Determine the acceptable tradeoff between risk mitigation and business impact	Incremental security enhancement	Build controls around the business needs	Ensure that all network, device, and user activity is continually logged	Zero trust activities like multi-factor authentication and identity management must be applied universally to avoid critical gaps
Consider cost, the impact to operations and stakeholders, and compliance and regulatory requirements	Hyperscalers	Document processes, roles, responsibilities, and data classifications	Utilize AI and ML to analyze data and identify anomalies that could indicate threats	Include third party physical and digital supply chains in the zero trust framework
Evolve from perimeter-based security to a micro-segmented, data centric model	Dedicated environment	User experience remains critical	Keep in mind that protecting data and applications is a zero trust architecture's key role	
Leverage outside help if needed	Identity is the new perimeter	Security enhancements like zero trust can't come at the expense of usability		
		Organizational goals such as growth and innovation remain paramount		

Zero trust is widely considered to be the best practice for security architecture.

Data shows that most organizations have begun considering or are in the process of implementing zero trust[1]. While the shift to zero trust is a big one, there are some practical considerations that will help guide the journey.

Dell Technologies subject matter experts Tracy Emmersen, Director of Solution Adoption for Project Fort Zero, and Justin Vogt, Principal Security Engineer, shared their recommendations and insights with Ash Lakshmanan, Security Services Product Manager. Their key suggestions are summarized below, or you can watch their entire conversation at dell.com/cybersecuritymonth.

> "When we look at zero trust from a holistic standpoint, when we take a step back, it really is all about the data."
>
> ***Tracy Emmersen***
> *Director of Solution Adoption for Project Fort Zero, Dell Technologies*

Plan for the (big) paradigm shift to never trust, always verify

At its most fundamental, moving towards a zero trust environment represents a major shift from historical security models to one that is based on the principles of never trust, always verify, and least privilege access. "We need to look at our security posture differently than how we have in the past, getting away from traditional perimeter-based network security solutions and more towards a micro-segmented, data-centric architecture," Emmersen notes.

Determine your desired path

Emmersen explained three distinct paths to achieving the benefits of zero trust:

- **Incremental:** An iterative approach that brings key zero trust principles to the current environment
- **Hyperscaler:** Leveraging the zero trust features of the major cloud providers
- **Dedicated, fully compliant environment:** Private, on-premise environment built from the ground up, strictly adherent to zero trust standards

In addition to these three paths, virtualized, small- and medium-sized businesses can also take an approach termed, Identity is the New Perimeter. This methodology focuses on identity and access management and leverages SaaS tools to achieve zero trust-based protection. A critical component of this method is implementing multi-factor authentication (MFA) everywhere, illustrating the impact of this one zero trust capability.

The hyperscaler and identity approaches are typically lower in cost, while the incremental and dedicated environments require greater investment.

The organization drives the zero trust adoption, not the other way around

At its most fundamental, a zero trust architecture is designed to administer and secure an organization's workflows, user roles and related privileges, devices, data, applications and networks. The first part of an implementation requires robust documentation of these aspects, and then the control plane and infrastructure are designed to enforce the policies that govern them.

If the zero trust environment inhibits or significantly alters business operations to the detriment of the organization, whatever enhanced security achieved likely isn't worth it. As Vogt points out, "If [security]… gets in the way of the core mission of the organization…we're really no better than the adversaries that we're seeking to disrupt. We just provided our own denial of service."

Focus on the data

As Emmersen notes, "When we look at zero trust from a holistic standpoint, when we take a step back, it really is all about the data." Protecting the organization's data is one of the most valuable benefits of a shift to zero trust, and principles like continual verification and segmentation protect data and applications by to preventing threats from moving laterally within the network.

Logging and continuous monitoring are critical components of zero trust, and that data and telemetry is analyzed to identify anomalies that might indicate a risk or threat. For example, a change in data usage patterns can identify potential exfiltration or a ransomware attack.

1. From a Dell commissioned study by the Enterprise Strategy Group, "Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust," November, 2023

DELL Technologies

Given the massive amount of data generated by logging all activity, modern analysis tools must use AI and machine learning to be effective.

Never trust, always verify must apply throughout

While much of the focus on data, applications, users and devices is internal, the scrutiny inherent to a zero trust architecture must apply throughout the IT life cycle. Failing to do so could leave critical security gaps.

The supply chain is a good example, and Vogt suggests asking important questions about third-party hardware and software:

- "Who else had access to it?
- What is it made of?
- What else is running below the surface?
- How can we take these principles of not trusting [and] having some kind of verification process and some sort of least privilege posture to the technology that we're consuming? Even if it's upstream in the technology supply chain?"

Moving towards a zero trust architecture or implementing its principles represents the current best practice to advance cybersecurity maturity. Several paths represent different tradeoffs between cost, risk and the level of security enhancement. The first step should be to determine the organization's unique position and let that guide the technology decisions.

Learn how to address some of today's top cybersecurity challenges at **dell.com/cybersecuritymonth**

DELL Technologies