



Dell Technologies Delivers Zero Trust, Cybersecurity Solutions to Protect Multicloud and Edge Environments

October 4, 2022

Zero Trust Center of Excellence, and new cybersecurity offerings and services help deliver greater resilience for modern security

ROUND ROCK, Texas, Oct. 4, 2022 /PRNewswire/ --



News summary

- Zero Trust Center of Excellence provides a cybersecurity blueprint for customers to test their environments on a U.S. Department of Defense-approved architecture before broad deployment
- New Dell cybersecurity services, endpoint and cyber protection solutions help customers build cyber resilience
- Dell aims to simplify Zero Trust cybersecurity adoption by streamlining integration across IT environments

Full story

Dell Technologies (NYSE:DELL) will open a Zero Trust Center of Excellence in collaboration with CyberPoint International and the Maryland Innovation Security Institute (MISI) in Spring 2023 at DreamPort, the U.S. Cyber Command's premier cybersecurity innovation facility. Dell also unveils new cybersecurity services that allow organizations to assess their Zero Trust and cyber resilience maturity, endpoint security solutions to support hybrid work, and ransomware protection for object storage data.

Zero Trust is a cybersecurity model that shifts how organizations approach security from relying solely on perimeter defenses to a proactive strategy that only allows known good activity across ecosystems and data pipelines. It allows organizations to better align their cybersecurity strategy across the data center, clouds and at the edge. Dell aims to serve as a catalyst for customers to achieve Zero Trust outcomes by making the design and integration of this architecture easier.

"In a multicloud world, an organization's cybersecurity strategy must transcend its infrastructure and extend to its applications and data," said John Roesse, global chief technology officer, Dell Technologies. "We believe a Zero Trust strategy is the best path forward. Dell has the proven IT and security foundation, technology integration experience, and extensive global partner ecosystem to help simplify customers' cybersecurity transformations."

Center of Excellence to speed Zero Trust adoption

Together with MISI, CyberPoint International and a team of industry small, women-owned and veteran-owned businesses, Dell will power the Zero Trust Center of Excellence at DreamPort to provide organizations with a secure data center to validate Zero Trust use cases. The Center of Excellence will use the [Department of Defense Zero Trust Reference Architecture](#) as its foundation for organizations to test configurations before deployment in their own environments. By orchestrating across an extensive ecosystem, Dell will deliver a repeatable blueprint of the architecture, providing a quicker path to adoption, and easing the integration and orchestration burden for customers.

"We believe our critical collaboration with Dell Technologies at the DreamPort Center of Excellence will drive rapid innovation and integration of Zero Trust solutions to help the U.S. government and commercial enterprises defend increasingly complex and ongoing cyber threats," said Horace Jones, president, CyberPoint International.

Cybersecurity services to align with Zero Trust and reduce risk

To help organizations align to Zero Trust principles and achieve cyber resiliency, **Dell Cybersecurity Advisory Services** provide organizations a roadmap to Zero Trust that builds on their existing cybersecurity assets. These services find and address security gaps, determine advanced technologies customers should implement, and help them learn how to enable continuous vigilance and governance for long-term cyber resiliency. By working with Dell, organizations have the tools and actionable insights they need to better secure their data and IT environments.

To minimize attack surfaces and better protect organizations, Dell offers a new **Vulnerability Management** service with Dell experts who regularly scan customer environments for vulnerabilities, provide a full picture of exposures and help prioritize patching efforts.

Commercial PC cybersecurity offerings support hybrid work

With breaches happening above and below the operating system, secure devices are foundational to a Zero Trust-ready organization. Dell continues to enhance its portfolio with new offerings that help customers prevent, detect and respond to threats wherever they occur, and allow greater control of the IT environment:

- **Hardware protections for the industry's most secure commercial PCs:**¹ To address growing supply chain threats, customers can now opt for Dell to disable PC ports prior to shipment, which helps prevent BIOS settings tampering. Dell is also expanding availability of tamper-evident seals to Asia-Pacific, Europe, the Middle East and Africa to offer more physical security measures during shipment.

- **Firmware protections to detect growing threats:** Organizations can detect potential tampering of a PC's BIOS with the new integration of telemetry between Microsoft Intune, as part of Microsoft Endpoint Manager, and Splunk consoles. Within the Microsoft Endpoint Manager admin center, IT administrators can secure, control and configure Dell PCs, including BIOS configuration and password management. These capabilities, which Dell is first to market with, will be available in a future release of Intune, helping ensure user productivity while reducing IT complexity.
- **Advanced software protections:** New capabilities from Dell speed threat detection and remediation. Additionally, a new data loss prevention offering helps protect sensitive data from unauthorized downloads onto external USB storage devices, providing greater visibility and policy control on this behavior.

Enhanced cyber protection and recovery for object storage

To address the growth of object storage data, such as videos and photographs, it is critical to take advantage of the latest cyber protection solutions to isolate data, intelligently detect threats and enable fast data recovery.

The **Dell ECS Enterprise Object Storage** platform expands cyber protection capabilities to help secure object data to an isolated cyber vault residing locally or in a remote environment. Accessible through the AWS S3 protocol, critical applications and backup servers can continue to access the isolated copy while supporting legal compliance in the event of a cyberattack compromising the primary and secondary data copy. Together with AI-powered threat detection and immutability, the new solution provides organizations a rapid path to data recovery from ransomware and other malicious attacks.

Additional resources

- Connect with Dell via [LinkedIn](#) and [Twitter](#)

About Dell Technologies

[Dell Technologies](#) (NYSE:DELL) helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies and Dell are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

¹ Based on Dell analysis, September 2022.

 View original content to download multimedia: <https://www.prnewswire.com/news-releases/dell-technologies-delivers-zero-trust-cybersecurity-solutions-to-protect-multicloud-and-edge-environments-301639623.html>

SOURCE Dell Technologies

Media Relations: Media.Relations@Dell.com