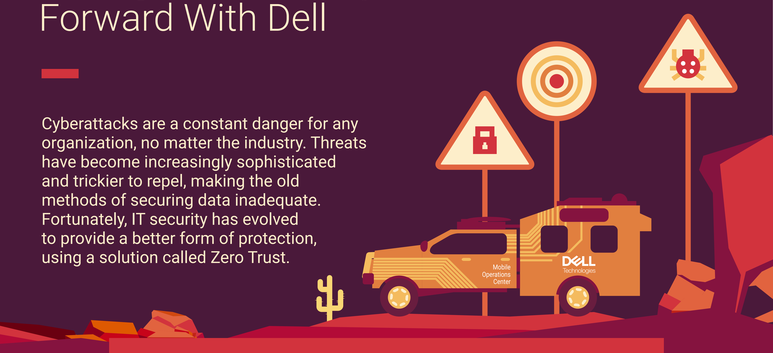
DELL Technologies

Driving Data Security Forward With Dell

Cyberattacks are a constant danger for any organization, no matter the industry. Threats have become increasingly sophisticated and trickier to repel, making the old methods of securing data inadequate. Fortunately, IT security has evolved to provide a better form of protection, using a solution called Zero Trust.



Zero Trust means exactly that: trusting nothing. Explicitly preventing any activity that is not known and authorized significantly strengthens the overall security posture. When implemented fully and correctly, Zero Trust secures your data by:

- Blocking unauthorized access
- Reducing operational risk
- Limiting the scope of damage
- Minimizing entry points
- Restricting movement if a hacker does breach the system
- Protecting against compromised technology
- Improving effectiveness of response

Dell's 5G-connected, Zero Trust-protected Mobile Operations Center showcases how the company is replicating the U.S. Department of Defense-approved Zero Trust architecture. Dell's Project Fort Zero will provide an end-to-end, validated Zero Trust solution to help organizations minimize the risk of cyberattacks.

The Mobile Operations Center and Dell's Zero Trust Center of Excellence use the seven pillars of Zero Trust—established by the U.S. Department of Defense— to help customers accelerate their adoption of Zero Trust.

77%

of information technology decision makers (ITDMs) haven't yet explored or built a Zero Trust architecture.[1]

The Seven Pillars of Zero Trust

1. User

Constantly authenticate, access, and monitor user activity patterns.

2. Device

Understand the health and status of every device to inform risk decisions.

3. Network and Environment

Segment, isolate and control the network environment.

4. Data

Ensure transparency and visibility, secured with enterprise infrastructure, applications, end-to-end encryption, and data tagging.

5. Applications and Workload

Secure everything, from applications to virtual machines.

6. Orchestration and Automation

Automate your security response using defined processes and protocols.

7. Visibility and Analytics

Analyze behaviors, events and actions to improve response time, detection, and enable real-time access decisions.

By covering each of these seven areas with a thorough and effective security solution, the Zero Trust approach makes sure risk is lowered and damage reduced. Zero Trust is not a new concept, but organizations can still struggle to implement it, opting for ad-hoc approaches rather than setting DoD validated Zero Trust as an end goal.

With Dell's security solutions and a Zero Trust approach can pave the way to secure your organization against cyber threats, and make it better protected, resilient–and ready to drive innovation.

Learn more at Dell.com/SecuritySolutions

Sources: 1. The Innovation Index, Dell Technologies, February 2023, www.dell.com/innovationindex