Red River

DELL Technologies TITANIUM PARTNER

IT Modernization for Commercial & SLED Organizations

Aging hardware, cloud strategies and maintaining security in an increasingly complex environment are all top considerations for leaders driving toward IT modernization. What is the best path forward and what's at stake?

Aging On-Prem Hardware Causes Vulnerabilities & Inefficiencies

Manufacturers **recommend a hardware refresh every five years** because server hardware becomes less efficient and incurs more performance issues that drive up costs and frustrate staff. Adopting modern on-prem solutions can address these concerns.

Lower TCO
Adopting efficient server technology that minimizes TCO will make budgets stretch as far as possible.

Top-End Performance
Higher DRAM capacity offers more in-memory processing, which means a faster time for any advanced computing.

Reduced latency, faster response times, and faster data access and transfer speeds will make for a more efficient and effective workforce – without sacrificing security. Modern servers, like Dell Technologies' PowerEdge with 4th generation AMD EPYC processors, are designed with the needs of today's organizations in mind.

In 2025, public cloud security incidents reached unprecedented levels, with a 47% increase in cyberattacks per week compared to 2024, and 80% of organizations experiencing at least one cloud security incident.

Common issues include IAM misconfigurations, insecure API keys, lack of security monitoring, and insecure data backup use.

Get Full Control of Your Data

Challenge:
Intense proliferation of cloud services means it's not always identifiable where the data is actually being stored.

Solution:
Adopting modern on-prem servers for data storage ensures that the data is always fully in control.

"Cloud Smart" doesn't mean "Cloud Always."
With high-end on-prem servers, the need for public cloud is reduced if not eliminated.

A Higher Standard

The National Institute of Standards and Technology (NIST) has released new standards for cloud security known as the **NIST Cloud Computing Standards Roadmap** which includes guidance on how organizations can assess their risks and migrate to the cloud safely.

NIST standards are important for public sector SLED organizations to **protect sensitive data and comply with regulatory requirements**, but implementing these standards can also help businesses demonstrate their commitment to data security for customers and partners.

New encryption standards have been introduced to deal with the advent of (and proliferation of) new quantum computing solutions.

SLED organizations must make sure that they are working with cloud service providers who are **compliant to ensure data is properly protected**.

Best practices for a better cybersecurity posture

- Performing regular risk assessments
- Monitoring activity
- Implementing strong authentication and authorization controls
- Encrypting data
- Training Employees

Accelerate Your Digital Transformation

Built on a combination of effective technologies for management, governance and security, the Dell Technologies Data Protection Suite offers organizations a path forward when facing vulnerabilities with legacy technology and increasing data demands. Whether in a data center, a virtual environment or in the cloud, the Data Protection Suite has all the tools to protect data, optimize backup and recovery operations and modernize IT infrastructure.

Red River

DELL Technologies TITANIUM PARTNER

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, AI, cybersecurity, modern infrastructure, collaboration and cloud solutions.

Learn more at **redriver.com**.

12619