Red River

DELL Technologies
TITANIUM PARTNER

The Benefits of IT Modernization for Commercial & SLED Organizations

Updating IT infrastructure and server deployments can make any organization more efficient and cost-effective. Private businesses are increasingly adopting remote and hybrid workforces, which makes them more attractive places to work for many employees. With a need for updated hardware, modern on-prem solutions from Dell Technologies provide an effective approach to address these concerns.

While adopting cloud solutions is one path to address the issue, it must be paired with modernizing on-prem hardware as well. Cutting-edge server technology can reduce total cost of ownership (TCO) and increase speed and efficiency—all while keeping key data secure.

Aging On-Prem Hardware Causes Vulnerabilities and Inefficiencies

Most equipment manufacturers recommend a hardware refresh cycle every five years. After this time, server hardware becomes less efficient and may encounter increasingly common performance issues. This can drive up costs, make task completion slower and frustrate the workers who staff these organizations. What's more, in a world increasingly defined by our awareness of climate change and a need to reduce energy consumption and one's carbon footprint, "higher energy costs for lower performance" is an equation that shouldn't make sense to anyone.

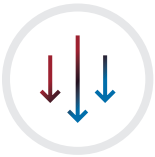
With a clear need for updated hardware, it only makes sense to adopt modern on-prem solutions to maximally address these concerns.

Modern servers, like Dell Technologies' PowerEdge with 4th generation AMD EPYC processors, are designed with the needs of today's business in mind.

Top-end Performance

At the end of the day, speed is everything. Modern servers, like Dell Technologies' PowerEdge with 4th generation AMD EPYC processors, are designed with the needs of today's business in mind. Higher core count means more computing power, which can power more virtual machines for a remote workforce. Higher DRAM capacity offers more in-memory processing, which means a faster time for any advanced computing to see results.

Similarly, increased I/O capacity for GPU acceleration offers better ROI for GPU investment and faster calculation. These enterprise-grade features will boost efficiency in organizations, which often need to process a staggering amount of data. Reduced latency, faster response times, and faster data access and transfer speeds will make for a more efficient and effective workforce – without sacrificing security.



Lower TCO

This advanced performance doesn't have to come at an exorbitant price. Organizations are often limited by budgetary concerns, so keeping TCO down is key to making this hardware attractive for adoption in a hardware refresh.

When choosing new server hardware, it should be a priority to reduce the number of servers required to run traditional applications and workloads. This lowers licensing costs and power consumption, which together reduce the drain on the organization's budget. For instance, AMD EPYC processors, like those found in the latest server technology, double the number of cores with the same space and power envelope as older servers.

Organizations often have to make their budgets stretch as far as possible, and adopting efficient server technology that minimizes TCO will do just that, saving hundreds of thousands of dollars compared to legacy solutions.

The Current State of the Cloud

The average organization now uses over 1,200 cloud services—and growing. Organizations begin with major solutions and then integrate and extend those solutions. But each of these cloud solutions may present a vulnerability. Now that organizations are moving to the cloud, they are finding themselves meeting another challenge—the challenge of scaling and securing a system of exponential complexity.

Do You Trust Your Secured Data in the Cloud?

When it comes to secured data, many organizations are still somewhat skeptical about the cloud. Private enterprises are similar—many are now using hybrid solutions rather than entirely cloud-based solutions to benefit from the cloud without leaving the entirety of their system exposed.

New ecosystems operate within multi-cloud platforms, hyper-converged architecture and edge computing services. By combining the best of all these worlds, organizations can manage their security solutions from end to end—from multi-cloud platforms to mobile device management.

The newest hardware, like Dell Technologies' PowerEdge servers, offers some advanced security features not found in public cloud solutions.

On-prem servers will always have an edge over public cloud technology when it comes to keeping critical data secure. The newest hardware, like Dell Technologies' PowerEdge servers, offers some advanced security features not found in public cloud solutions:

- Secure root-of-trust technology monitors BIOS software and ensures it is booted without corruption.
- Secure memory encryption makes it possible to encrypt the contents of main memory with only a change in BIOS settings.
- Secure encrypted virtualization (SEV) helps protect confidentiality by encrypting each virtual machine with a unique key that is known only to the processor.
- Technologies help to maintain data encryption wherever it exists across the vast Federal eco system.

Growing Challenges with IT Modernization

As the number of cloud services grows, so too does the challenge of keeping track of all the security solutions and ensuring they are properly managed. Configuration creep, permissions creep and third-party tools can all present potential operational hazards.

It's understood that these new technologies are constantly accelerating, and that some element of risk is inherent with any major change in infrastructure. Organizations must be especially cautious when modernizing their IT—while still taking advantage of the benefits that modern IT can provide.

To some extent, cloud solutions address this issue head-on. Providing additional resources and state-of-the-art, next-generation technologies, cloud solutions and edge computing processes may both increase the organization's performance and its security. But these solutions still have to be configured and maintained by expert security specialists; otherwise, it becomes too easy for the organization to become vulnerable over time.

New Standards for Cloud Security

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

Furthermore, new encryption standards have been introduced to deal with the advent of (and proliferation of) new quantum computing solutions. To ensure that their data is properly protected, organizations must make sure that are working with cloud service providers who are compliant with these standards.

Cryptography and Quantum Computing

Quantum computing could radically change what we consider secure. New cryptographic standards are a requirement because now, brute forcing previously unbreakable encryption could become possible. As this technology could advance exponentially, it also behooves every organization to increase its security exponentially—to future-proof it.

Quantum computing isn't just a threat today, but one that reaches into the past.

Quantum computing isn't just a threat today, but one that reaches into the past. If encryption standards are lax today, data could be stolen today and cracked in 10 years. That could have exceptional impact on organizations. Consider the personally identifiable information of citizens being released in 10 years; this information would still be relevant, and the breaches would still be costly.

Quantum computing and other next-generation solutions such as hyperautomation and edge computing services will bring together a new world of even more advanced technologies. Organizations will be able to use these systems to intelligently automate systems, reduce workload and increase efficiency.

Cloud Smart Doesn't Mean Cloud Always

After the intense proliferation of cloud services, concerns about the right approach to cloud adoption have emerged, especially around identifying where data is actually being stored. What happens when important organizational data is stored on servers outside the country?

Adopting modern on-prem servers for data storage ensures that the data is always fully in control by the organization that uses it.

Adopting modern on-prem servers for data storage ensures that the data is always fully in control by the organization that uses it. "Cloud Smart" doesn't mean "Cloud Always." With high-end on-prem servers, the need for public cloud is reduced, if not eliminated.

But with IoT threats, the "Cloud Smart" philosophy becomes even more of a challenge to tackle. What happens when employees have Wi-Fi connected devices that are also connected to cloud servers across the world? Famously, athletic trackers were once used to identify military bases through their Wi-Fi-enabled GPS. This is something easily replicated through social media sharing apps.

Zero Trust policies, enhanced perimeter security and machine learning algorithms must all be used to better engage in and improve in security best practices.

Data Protection, On-Prem or in the Cloud

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. This collection of solutions gives IT an advantage in oversight and governance, automated policy management and the flexibility of containers to protect the assets and applications that matter most to an organization. It leverages cost-effective object storage and offers the ability to back up data and applications to the cloud as needed, helping organizations shift to more modern and scalable IT environment.

Achieving Cybersecurity Maturity: Zero Trust and the CMMC

Zero Trust is important for any state, local and education organization or commercial business handling sensitive data.

In Q1 2025, the Cybersecurity Maturity Model Certification (CMMC) will go into effect for government contractors handling sensitive data. But CMMC compliance is built on a Zero Trust cybersecurity approach. Zero Trust is important for any state, local and education organization or commercial business handling sensitive data.

Zero Trust cybersecurity challenges the traditional perimeter-based security model. Under Zero Trust, systems require a continuous verification of user identity and device integrity, granting minimal access privileges based on specific needs. This approach minimizes the risk of insider threats and unauthorized access.

Organizations can leverage Zero Trust principles to achieve their goals by implementing continuous verification, enforcing least privilege access, micro-segmenting networks, encrypting data, maintaining asset inventories, and providing user training. These principles enhance access control, data protection, monitoring, and incident response, aligning with the CMMC's stringent security requirements, ultimately ensuring robust cybersecurity and compliance.

What Organizations Can Do to Prepare

Organizations must take steps to improve their security, beginning with a comprehensive approach to security that includes not just technology, but also people and processes.

Best practices for a better cybersecurity posture include:

Performing regular risk assessments
Organizations should assess their risks on a regular basis and have a plan in place to mitigate them.

Implementing strong authentication and authorization controls
These controls will help to ensure that only authorized users have access to sensitive data. If possible, organizations should switch to a Zero Trust-only authorization system.

Encrypting data
Data should be encrypted both at rest and in transit.

Monitoring activity
Organizations should monitor activity on their networks and look for any anomalous behavior.

Organizations should monitor activity on their networks and look for any anomalous behavior.

Training employees
Employees should be trained on cybersecurity best practices and policies.

Keeping up with the latest news
Organizations should stay up-to-date on the latest cybersecurity news and trends.

Invest in Technology that Prioritizes Security

As organizations modernize, every investment is pivotal in creating a path for growth with a secure profile. Dell Technologies' PowerEdge servers harness cryptographic verification, system lockdown and robust boot and firmware safeguards—anchored by a silicon Root of Trust. PowerEdge security technologies help fortify IT defenses, instilling confidence while helping accelerate the adoption of a Zero Trust security strategy.

*Dell Technologies PowerEdge R760 Server pictured

To properly protect data, organizations first need to have visibility into all of their systems—including those in the cloud.

Taking the Next Steps to Secure Data

To properly protect data, organizations first need to have visibility into all of their systems—including those in the cloud. They also need to have the ability to detect and respond to incidents quickly. And they need to have a plan in place for how to recover from an outage or attack.

A Security Operations Center (SOC) can help organizations more effectively manage their security posture by providing 24/7 monitoring, detection and response capabilities. Understandably, however, many entities don't have the time to manage their security from the ground up—they need a qualified security partner.

Accelerate Your Digital Transformation

Be ready for whatever comes next with help from Red River and Dell Technologies. Digital transformation is imperative for all organizations. And while many are moving in that direction, a recent study shows that 89% of organizations feel like they're lagging. Organizations that want to drive innovation must operate at the cutting edge of technology.

Dell Technologies and Red River are 100% committed to your mission. Whether you're providing critical services, innovating for the next generation or securing your community, we bring the right technology, targeted expertise, and far-reaching vision to help guide your journey. Whether you're optimizing your existing infrastructure or exploring emerging technologies — 5G, AI, data management, on-demand or as a service — in the cloud or at the edge, we have the technology expertise, end-to-end solutions, world-class services and relentless spirit to help prepare for today's top-of-mind issues and tomorrow's unknowns.

Dell Technologies' family of PowerEdge servers are designed to address the most challenging workloads, working autonomously and collaboratively across all its IT environments. Paired with Dell Technologies' OpenManage integrated IT management system, PowerEdge servers include powerful automation and reporting features to help users focus on the most important tasks for the business.

Red River

DELL Technologies
TITANIUM PARTNER

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.

12625