




Red River

DELLTechnologies

FEDERAL TITANIUM PARTNER

2022 DATA STORAGE TRENDS



2022 brings with it an extraordinary amount of data. It's believed that the world is now producing and consuming close to 100 zettabytes of data every year. How are government agencies managing this data? How can companies glean actionable insights from the data they have – and secure and protect the data that they need?

Increased levels of regulatory compliance, the need to integrate and combine data and the proliferation of cloud-based solutions are all giving rise to converged and hyperconverged infrastructure (HCI), new data storage philosophies and new data security technologies.



DATA FABRIC WITHIN THE MULTI-CLOUD ENVIRONMENT

Today, it's important to understand the data fabric within a multi-cloud environment. As systems continue to move to the cloud, it's usually done in a disorganized fashion. Cost goes up, security is weakened and access controls aren't appropriately transferred. Ultimately, this can lead to repatriation: bringing systems back on-premises.

Hybrid cloud solutions have given rise to both complex on-premises and multi-cloud architecture. But again, understanding the data fabric is essential. For federal entities, often they aren't allowed to deploy fully on the cloud. They need to have protected, on-premises solutions.

Major issues with data include:

- **The cost of data storage.** Companies are increasingly moving toward cloud systems, as they only need to pay for the resources they use. Many companies are also creating tiered solutions through which the data that they need is rendered instantly accessible and the data that is archived can be moved to physical media or alternative locations.
- **The time it takes to process the data.** Cloud services leverage extensive resources to process exceptionally large data sets. Companies are also moving toward technologies like machine learning (AI) to process these data sets with fewer resources.
- **The risk of data breaches.** The more data there is, the more exposed the organization is. Companies have to maintain and secure their active data and their data archives. The company's attack surface will constantly be growing as the data increases.

These issues will only grow in volume and impact as the data itself grows. Trends presently are changing between converged architecture and hyperconverged. As organizations undergo their cloud journey, the many are considering moving from a multi-tier solution to hyperconverged infrastructure.

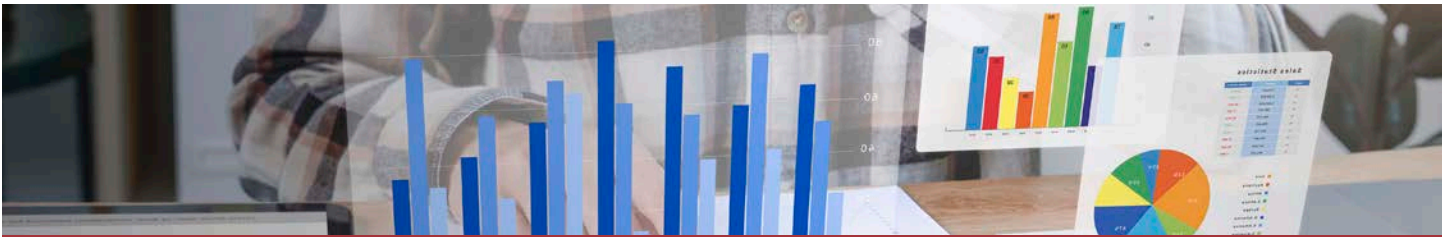
COST AND DATA MANAGEMENT

Organizations are quickly finding that their existing data management solutions are surprisingly costly. When organizations are inclined to preserve and protect all their data, even on the cloud, the costs swiftly rise. Unmetered and unchecked, many organizations are consuming far greater levels of resources than they truly need to.

These rising costs come down to a few critical issues:

- **Protecting personally identifiable information (PII).** Personally identifiable information demands higher levels of security and maturation than other data. This is especially true if an organization has to follow additional guidelines, such as HIPAA compliance. Organizations protecting PII, confidential information and intellectual property must invest more in their security systems. If they are running a multi-cloud or hybrid architecture that is poorly integrated, this can lead to multiple security solutions being paid for, managed, and monitored simultaneously.
- **Controlling access on a granular level.** Organizations need to control access more fiercely under a hybrid or cloud-based model, as the attack surface is both greater and more exposed. Many organizations are switching to Zero Trust models of security, but this also means that the organization must manage and audit its access protocols with greater levels of control. If the organization isn't willing to outsource its security, this can lead to time-consuming work for an internal IT department.
- **Racking up compute cycles.** Data stored and accessed on the cloud will ultimately cost the organization money. If the organization isn't filtering and managing its data, these costs can quickly become unwieldy. At this to the fact that Microsoft Azure and AWS cloud computing costs can be confusing or even unintelligible to those who aren't experts within the system, and it leads to budgets going off the rails quite quickly.
- **Delineating between on-prem and cloud data tiers.** Organizations need to do a certain level of management between their on-prem and cloud data tiers. On-prem, organizations need to keep their most vital and confidential data. On the cloud, organizations need to keep the data that must be most accessible to employees. Unfortunately, this also means that a lot more time must be spent on managing data on both an administrative and IT level. Without the right support and automation, this can lead to confusion and cost.

These issues can be largely addressed through better system management. But organizations themselves often don't have the time to manage their own data — especially maintenance tasks such as moving data from quick access, cloud solutions to on-prem, archival solutions.



REPORTING ANALYTICS AND DATA STORAGE THROUGH AI AND ML

Why are organizations keeping such tremendously large volumes of data? For the most part, it's for analytics and analysis. Organizations need to dig deep into the data that they have, accessing it frequently, which further boosts compute cycles and costs.

Huge data sets pumped through systems, such as AI and machine learning systems, consume significant resources. Companies aren't just keeping large volumes of data, but they're also finding that they need to keep this data accessible. And this also means that much of their data cannot be moved to lower tiers; they need to be ready and active.

In 2022, companies are finding themselves:

- **Collecting far more data.** Not only is this data value to the company, but it's a virtual necessity within highly competitive, data-driven markets. Today, companies use data to manage their logistics, their customer retention and their employee productivity.
- **Analyzing far more data.** Ten years ago, organizations found themselves collecting large volumes of data but unable to properly analyze the bulk of it. Today, analysis is occurring on both a broader and deeper scale.
- **Gleaning actionable insights.** Importantly, companies find that the data that they collect and organize is clearly generating revenue — it has become essential to their functions even if it can become a cost sink.

All of this is being achieved through artificial intelligence and machine learning technology. AI/ML technology is becoming advanced enough to glean truly actionable insights from seemingly disparate sets of data.

At the same time, even though this data is useful, it also must be managed. Organizations are finally seeing the true benefits of big data and machine learning solutions, but it can come at a hefty cost. Consider that as more organizations make use of this data, it becomes necessary to leverage this data to remain competitive. Thus, organizations need to have a firm data management strategy.



THE RACE FOR FASTER ON-PREMISES SOLUTIONS

A move toward hybrid architecture has another side effect: organizations are moving toward faster on-premises solutions. As government agencies cannot adopt full cloud technology, they must still ensure that their organization's on-premises solutions can meet their data needs.

In 2022, on-premises data trends include:

- **PCIe Gen 4/5 data storage controllers and flash SSDs.** PCIe Gen 4 has twice as much bandwidth as Gen 3, while Gen 5 has twice as much bandwidth as Gen 4. Meanwhile, flash SSDs are becoming far more stable and reliable.
- **Data processing units.** Data processing units offload some of the critical activities of data management and storage, much like GPUs are able to offload the critical activities relative to graphical processing.
- **High-bandwidth NICs and higher performance storage controllers.** AMD, Intel and ARM are all producing higher performance utilities, which can then be used to improve the organization's on-premises infrastructure.

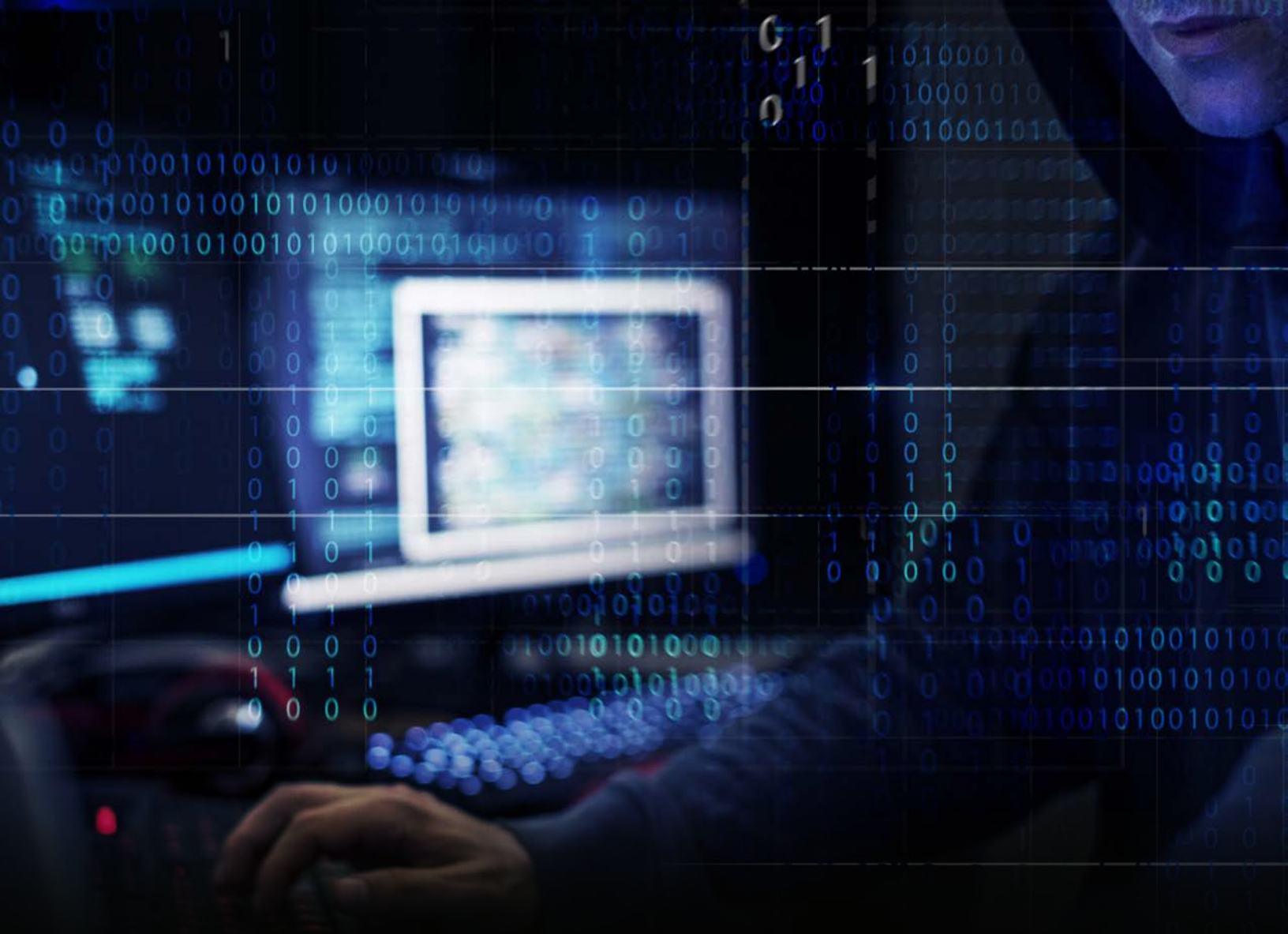
Organizations are also looking to future-proof themselves for their data needs. They aren't investing in technologies that can suit them today or even a year from now, but rather technologies that will still be upgradeable and improvable in five years.



5G AND IOT DATA ON THE RISE

The ripple effect of 5G and IoT data is just now being seen and will likely become even more significant late in 2022. 5G data facilitates IoT connectivity and sensors; IoT devices can connect with faster speeds and greater levels of fidelity. This is increasing the use of IoT devices, which is further increasing the data that organizations are likely to store and maintain.

As IoT devices are adopted, they create other data intrusion and data management concerns. Not only will organizations have to manage these extraordinarily large data sets that are coming from an increasingly large data fabric, but they will also need to secure their IoT devices and themselves. Zero trust policies can only go so far in ensuring that IoT devices remain active and not compromised and that the data collected from IoT devices is useful and accurate.

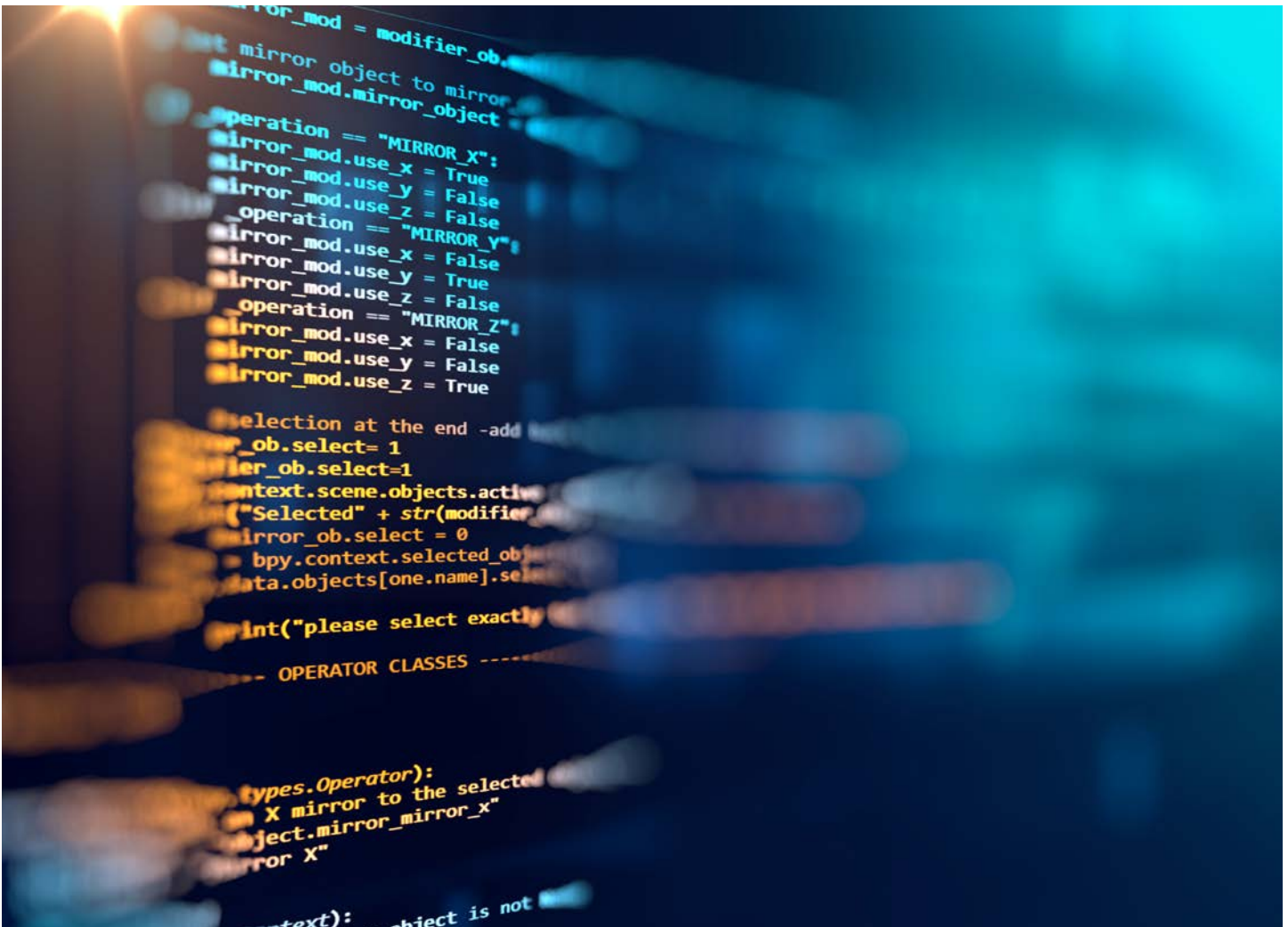


RANSOMWARE AND BLACKMAIL CONTINUES

While largely a security concern, ransomware and blackmail remain critical concerns within the realm of storage. Ransomware has continued to be a major issue for most businesses, while blackmail has also become an emerging threat for high-profile entities.

Companies will need to be increasingly mindful of how well their data fabric can be secured and whether it can be secured with the resources they have. For this reason (among others), companies are now investing in managed services providers and outsourcing their security.

Though ransomware has been the reality for many organizations for the past decade, recently many malicious attackers have become emboldened. Government agencies have been hit, there have been high-profile attacks and billions of dollars of revenue has been lost.



UNSTRUCTURED DATA MANAGEMENT AND NOSQL

How do you create a database of a thousand different documents? How do you search, manage and protect files that have radically different sizes and types? Organizations are increasingly finding themselves in need of unstructured data management tools such as NoSQL databases.

It's not only that modern companies and other entities are collecting large volumes of data — it's that these pieces of data are often entirely disparate. Unstructured data requires special tools to simply manage, which leads to a heightened importance of applications, NoSQL databases and data lakes.

Organizations are going to see a vast increase in the number of data lakes. Companies stream multiple sources of data into a single, consolidated platform, which is then used to analyze that data on equal footing. Some of these systems are ETL systems which import and manage the data directly. Other systems are meta systems which instead analyze the data but do not modify or transport it.



DATA SOVEREIGNTY A RISING CONCERN

Geopolitical instability and the complexities of the modern world has led to a rise in the data sovereignty movement. As organizations become increasingly unaware of where their data is actually being kept in the physical realm, regulatory standards and issues of compliance become more difficult to meet. Data sovereignty is important for many organizations. but it is absolutely essential for federal agencies and contractors hoping to meet FedRAMP or CMMC compliance.

Global regulations are increasingly being put into place for the purposes of consumer privacy, sanctions are being escalated in various regions, and customers are becoming more aware of how their data is being used and (potentially) misused. Companies must become more aware of where their data is physically located and how that ultimately impacts their security and compliance.



MOVING FORWARD INTO 2022

The amount of data the average organization maintains is constantly increasing. When it comes to cloud technologies and hybrid solutions, this creates an ever-growing problem for internal data management and data security. Organizations are now responsible for tremendously large volumes of data spread across multiple, tiered systems. They must find ways to keep this data accessible while still managing their costs and productivity.

2022's data management and data security trends show organizations continuing to move to cloud solutions and hybrid solutions. For federal entities, it's impossible to move to a single cloud solution — so multi-cloud solutions and hybrid cloud solutions are used. For organizations protecting confidential information, PII or intellectual property, the need for on-premises solutions is inescapable.

Still, organizations need to find better ways to manage data across these large and disparate systems. This is leading to better integrated technologies such as hyperconverged infrastructures. By consolidating data within a single entity, organizations can better manage their data security and their costs.



Red River

DELLTechnologies
FEDERAL TITANIUM PARTNER

ACCELERATE YOUR AGENCY'S 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. This is also true at the federal level. Government agencies, like yours, are relied upon to lead. You must operate at the cutting edge of technology if you want to drive innovation and encourage citizen confidence.

To this end, the partnership of the Dell Technologies federal team and Red River is 100% committed to your mission. Whether you're providing critical citizen services, innovating for the next generation, or securing the nation, we bring the right technology, a secure supply chain, 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 your agency for today's top-of-mind issues and tomorrow's unknowns.

When it comes to storage, Dell PowerScale, the world's most flexible scale-out NAS solution, is designed to be flexible and reliable at any scale. Regardless of the kind of data, where it lives, or how big it gets, your data lake always stays simple to manage, simple to grow, simple to protect, and simple enough to handle the most demanding workloads of today and tomorrow.



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 data center, security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.