Red River

DELL Technologies
FEDERAL TITANIUM PARTNER

DATA PROTECTION IN 2022 AND BEYOND

With cyber threats on the rise, the federal government needs to take action to address high-risk information security challenges. As threats become more sophisticated, data stores larger, and technology standards evolve, agencies need to keep pace to strengthen their security posture and mitigate risk. A great place to start is by taking a look at the data protection challenges facing security professionals and the cybersecurity trends driving investments in the U.S. Federal sector.

TODAY'S CHALLENGES IN DATA PROTECTION

Why are there so many data breaches today? Why have government entities succumbed to attacks? There are a number of challenges government agencies face when it comes to data protection.

INCREASING LEVELS OF SOPHISTICATION

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. As the world becomes more digitized, so too are the methods bad actors use to commit cybercrime.

A VASTLY EXPANDED ATTACK SURFACE

The proliferation of devices, cloud services and apps has created a vast attack surface for bad actors to exploit. In fact, the average enterprise uses dozens of different cloud services. Each one of these services represents a potential point of entry for an attack.

For Federal agencies, who often handle sensitive information, there can be a deep dilemma here: Do you reduce dependency on cloud services and modern BYOD policies, which could reduce employee efficiency and reduce morale due to cumbersome requirements, in the name of achieving greater data protection?

THE GROWING IMPORTANCE OF DATA

Data is becoming increasingly important to businesses and Federal agencies. Data is more vulnerable in part because organizations are simply archiving and controlling more data. The average Federal agency may use multiple petabytes of data, all of which could contain personally identifiable information (PII) useful in cyber attacks.

This is exacerbated by the distributed nature of work in a post-COVID world, with many employees and contractors preferring to work remotely. Access to a dispersed nationwide workforce opens up the ability to hire the best people regardless of location, but can Federal agencies really trust that their data – which can be sensitive, or even classified – is secure when working with remote employees or contractors?

INEXPERIENCE IN THE CLOUD

Federal agencies are quickly moving to the cloud in an effort to improve agility and cut costs. However, many are doing so without the necessary experience or expertise. Agencies that move to the cloud and adopt new cloud technologies without the necessary knowledge to secure them will be vulnerable to attack.

INCREASINGLY FRAGMENTED INFRASTRUCTURES

Additionally, as governmental agencies adopt more cloud services, their architectures become increasingly fragmented. If an organization doesn't have a plan in place, the infrastructure becomes unwieldy. Fragmented infrastructures make it difficult to get a holistic view of the agency's data and puts them at greater risk for attack.

As a result of these challenges, Federal agencies need to invest in the latest security technologies and stay up to date on the latest threats. But frequently, that's easier said than done. The modern business – and the modern government – may be running literally dozens of clouds, latticed into a single infrastructure that's only as strong as its weakest link.

DATA PROTECTION TRENDS FOR 2022

In the next five years, data protection will continue to be a top concern for Federal agencies and contractors. But the landscape of data protection is very likely to change. Today, organizations are using the following techniques to secure their data:

- Zero-trust access
- Multi-factor authentication
- Privileged access management
- Identity and access management
- Data loss prevention
- Endpoint security

Still, for many organizations, it's a constant battle. Federal agencies and contractors need to balance their need for innovation and agility with their need for reliability and security.

Let's take a look at some of the major trends public and private organizations will see when it comes to data protection and data privacy.

1. CYBERATTACKS WILL CONTINUE TO BECOME MORE SOPHISTICATED

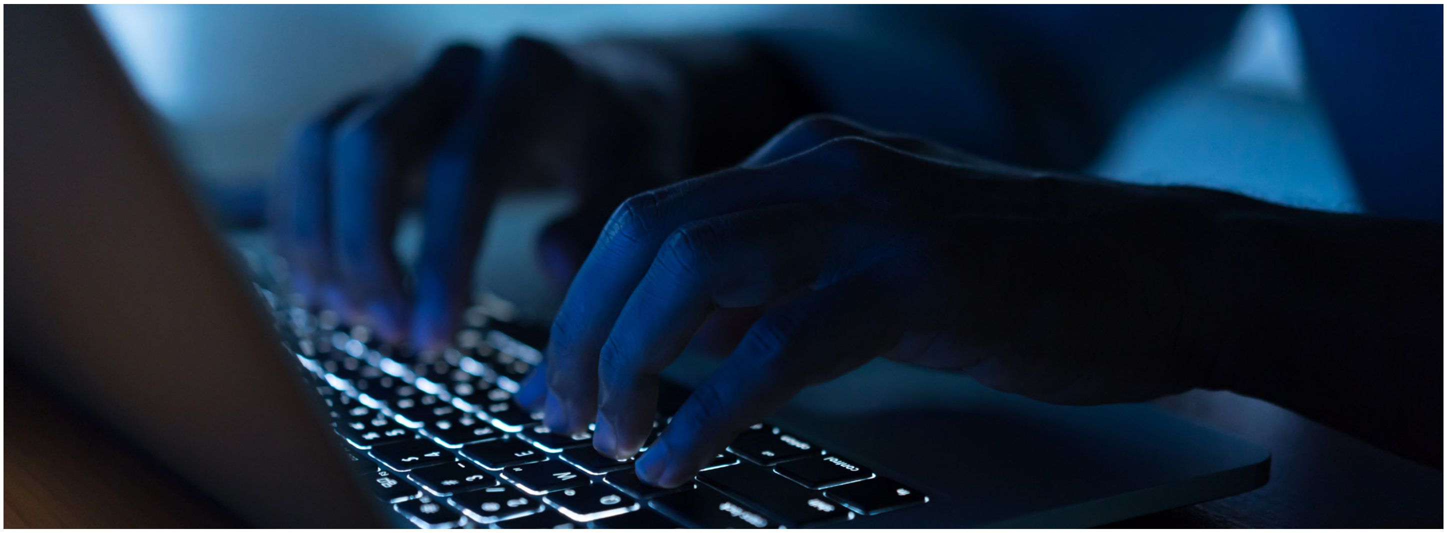
As cyberattacks become more sophisticated, agencies will need to invest in more sophisticated security measures to protect their data. This may include artificial intelligence (AI) and machine learning technologies that can identify and thwart new types of attacks.

Cyberattacks will grow in sophistication year-over-year. Just as Federal agencies now have access to cloud technologies, cybercriminals now have access to additional resources. Agencies must constantly be on the lookout for new threats and ways to protect their data.

For instance, automated and intelligent solutions can identify suspicious activity and move to isolate critical data at speeds humans could never respond to, providing an active element to data protection. For Federal agencies dealing with sensitive data, providing this active, modern protection against increasingly sophisticated cyberattacks will be key.

2. THE COST OF DATA BREACHES WILL CONTINUE TO RISE

The cost of data breaches is already in the trillions. This trend is likely to continue as the number of data records lost or stolen increases. As a result, agencies will need to invest more in data protection to avoid the homeland security, financial and reputational damage that can be caused by a breach.



3. REGULATIONS WILL BECOME MORE STRINGENT

As the cost of data breaches rises, so too will the pressure on government agencies to meet federal mandates, security frameworks and regulations.

This may impact organizations, whether associated with the Federal government or not, in unexpected ways. For example, the Cybersecurity Maturity Model Certification (CMMC) is a new set of regulations for the DoD and defense contractors. Aspiring Federal contractors that cannot meet CMMC standards will not get government business – it's that simple. Losing key government contractors could bring instability for agencies who rely on these businesses to deliver key citizen services.

4. Organizations will invest more in data protection
As the cost of data breaches rises and regulations become more stringent, Federal agencies will be forced to invest more in data protection. This may include hiring more security staff, investing in new technologies and implementing better security practices.

Of course, any organization doesn't want to infinitely invest in data security. Federal agencies will also be looking for new ways to streamline and secure their systems without increasing the burden on their employees.

5. DATA PROTECTION WILL BECOME A COMPETITIVE ADVANTAGE

Perhaps one of the most interesting things in the coming years is that data protection will become a competitive advantage. Data security and data protection is already becoming a hallmark of a solid organization. As data becomes more valuable, companies that are able to protect it will have an even clearer competitive advantage.

If the federal governmental and the contractors that serve it take data protection seriously, our country will have a competitive advantage in the global marketplace as it relates to talent, economic growth and stability and cyber warfare.

6. AGENCIES WILL MOVE TOWARD HYPERCONVERGED INFRASTRUCTURES

Hyperconverged infrastructures (HCI) are becoming more popular as they offer a simpler and more cost-effective way to manage data. HCI systems combine storage, networking and compute resources into a single appliance that can be managed from a single interface. This allows Federal agencies to reduce complexity and save on costs.

The better consolidated an organization's system is, the easier it ultimately is to protect. This is because there are fewer potential entry points for an attacker. As an additional bonus, HCI systems make it easier to deploy security measures and updates.

7. THE USE OF CLOUD SERVICES WILL CONTINUE TO GROW

Cloud computing is becoming increasingly popular as it offers a number of advantages, such as scalability and flexibility. As a result, more agencies are expected to move to the cloud. This will have a major impact on data protection, as agencies will need to ensure that their data is secure in a multi-cloud world – whether that is private, public or hybrid environments.

At the same time, cloud services also make it easier to protect systems by providing the resources necessary. Intelligent systems work more effectively on the cloud, as they aren't limited by on-premises processing. SaaS solutions will continue to leverage artificial intelligence and machine learning to provide greater levels of protection to Federal agencies.

However, many cloud solutions still fundamentally leave critical data protection elements, like backup-and-restore responsibilities, in the hands of the users. Even the most rigorous Federal agencies are vulnerable to human error. Using automated solutions let agencies use cloud services while ensuring their data is safeguarded.

8. EDGE COMPUTING WILL BECOME MORE IMPORTANT

Edge computing takes place at the edge of the network, near the data source. This allows data to be processed closer to where it is generated, which can improve performance and reduce latency. As edge computing becomes more popular, it will have a major impact on data protection as agencies will need to ensure that their data is secure at the edge of the network.

9. AGENCIES WILL BECOME MORE CONSCIOUS REGARDING THEIR DATA LOCATION

Many organizations today, whether Federal agencies or private businesses, would not be able to tell you where their data is physically located. But soon, that will be a thing of the past. Due to increasing federal regulations, it will become more important to know exactly where data is being held. This may also be influenced by increasing geopolitical tensions.

As a result, data protection will need to take into account both physical and logical data location. This means that agencies will need to have a better understanding of their data flows and where their data is stored and where their data is analyzed.

10. THE ROLE OF THE CISO WILL CONTINUE TO EVOLVE

The role of the chief information security officer (CISO) is changing as the threat landscape evolves. In the past, the CISO was responsible for managing security risks. But today, the CISO is also responsible for data protection. This change is being driven by the fact that data is becoming more valuable, and Federal agencies are starting to realize that data protection is a key mission objective.

Agencies will need to upskill their staff during a time when there is a tremendous tech shortage. It will be critical for the Federal government to ensure that every agency and department has someone driving data protection and addressing security risks.

11. INTERNET OF THINGS (IOT) DEVICES WILL BECOME MORE COMMON AND MORE DANGEROUS

As the IoT grows, so too will the number of devices that are connected to the internet. This will have a major impact on data protection as entities will need to ensure that their data is secure on all of these devices. This is part of the growing security landscape and it will have a radical impact on the risk factors and attack surface of many organizations both in the private and public sectors.

12. ORGANIZATIONS IN BOTH THE PRIVATE AND PUBLIC SECTORS WILL RELY EVEN MORE UPON EXPERT PARTNERS

As noted regarding CISOs, as data becomes more valuable, Federal agencies will need to rely even more upon expert partners to help them protect their technology infrastructure, applications and date. This may include managed service providers (MSPs), security consultants and data recovery specialists. These experts can help organizations keep their data safe from cyberattacks, comply with regulations and recover from data loss.

DATA PROTECTION IN 2022 AND BEYOND

The reality is that data protection is becoming more difficult. Organizations are holding larger volumes of data. They are being attacked from all fronts. And many are expanding their technology infrastructure and applications to the extent that they can no longer protect their attack surface. The world of data protection is moving quite fast. It's difficult, if not impossible, for many organizations to move with it.

As data becomes more valuable — and threats continue to grow — Federal agencies will need to invest more in data protection, security frameworks and data protection platforms. This may include hiring more security staff, investing in new technologies or implementing better security practices. Data protection will become a competitive advantage for companies – and countries – that are able to keep data safe from cyberattacks and those that are able to comply with evolving regulations.

ACCELERATE YOUR AGENCY'S DIGITAL TRANSFORMATION

Red River

DELL Technologies
FEDERAL TITANIUM PARTNER

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 enhancing cyber security, 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 cybersecurity, one of the most comprehensive tools for data protection is Dell PowerProtect Cyber Recovery, which automates data safeguarding and recovery in a way that preserves critical information and minimizes disruption from all-but-inevitable cyberattacks.

To protect your agency, contact Red River and learn more about our security expertise and powerful partnership with Dell.

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.