The Data Security Forecast for Federal Agencies Managing Classified Data

Securing federal information is no easy task. But with the right approach and solutions, agency leaders can successfully secure crucial data.

Hybrid multi-cloud environments are the next step for many government IT leaders. Within a hybrid multi-cloud setting, IT leadership can leverage data wherever it resides, whether that be at the edge or the core. For citizens, this means a more responsive government. But for agencies, leveraging technology and modernizing existing legacy systems isn't without its challenges.

Despite the widespread support from the federal workforce, government organizations face a complex and rapidly evolving digital landscape. Online malevolent threat actors have been honing their craft for decades. With the promise of quantum computing on the horizon, many are turning toward data exfiltration with hopes of uncovering top secret information.

On an abstract level, containing data breaches may seem like a low priority. Data exfiltration often doesn't receive the same headline attention that spyware or ransomware receive. But one needs only to look at recent events in Ukraine to understand the importance of data security.

As government organizations pursue digital transformation, security must be top-of-mind.

However, protecting one's data in a hybrid multi-cloud environment is easier said than done. "Data is spread across multiple locations, in different formats and software databases," explains Jason Kessler, a security solutions architect at NetApp. "Not knowing what [type of data] they have, where it resides and who has access to it is one of the biggest shortcomings."

Whether it's data visibility challenges or lengthy procurement processes, one thing is certain: The current operating environment makes it challenging for agencies to keep up with the pace of digital transformation.

> **"Not knowing what [type of data] they have, where it resides and who has access to it is one of the biggest shortcomings."**
>
> **Jason Kessler** | Security Solutions Architect, NetApp

PRODUCED BY: studio 2G SPONSORED BY: NetApp | PRESIDIO FEDERAL

CSfC Solutions for National Security

With threats to government data increasing, now is the time to onboard solutions that enable security teams to protect and defend their information.

Clear data visibility and access will be important in the coming months and years, as the government contends with combative nation-states and advanced digital adversaries. Failure to adopt data-conscious solutions, or even a data-driven approach would be to cede American superiority on a digital battlefield.

However, the federal procurement process is lengthy, and with the ever-evolving nature of technology, government organizations often end up onboarding antiquated security technologies — creating a vicious cycle which threat actors exploit as security operations centers struggle with legacy tools.

The National Security Agency's Commercial Solutions for Classified program, otherwise known as CSfC, looks to help federal agencies quickly and securely onboard new cybersecurity tools. In this sense, it operates much like FedRAMP, a program designed to help government IT leaders onboard secure cloud solutions.

> **Agencies must recognize the need to reap value from their data and begin to invest in making that happen."**
>
> **Chris Rohland** | Solutions Architect, Presidio Federal

Under this new program, agencies can select from a list of verified cybersecurity vendors and solutions, including NetApp's ONTAP data management software — one of the first enterprise-grade solutions to be added. The NetApp ONTAP framework leverages powerful machine learning and artificial intelligence to monitor, manage and protect data wherever it resides on the network.

Federal customers can harness these advances in machine learning and artificial intelligence and use them to monitor their warm or cold data. This creates significant benefits, allowing security operations centers to get a holistic view of their tiered data.

"Federal agencies are on a path toward data-driven decision-making. At the core, it's a simple idea: Use data to inform decisions rather than relying on observations or preset ideas. But turning the vast and ever-growing volumes of data available into a true strategic asset comes with a host of challenges! Ultimately, agencies must recognize the need to reap value from their data and begin to invest in making that happen," says Chris Rohland, solutions architect at Presidio Federal.

But what about data spread out across devices? Employees may save files to private laptops or accidentally share files with an external contractor. To effectively manage and secure devices, ONTAP allows security operations centers to apply file access and protocols to select files. So, if there is sensitive or classified information on the network, the platform works to defend the data from exfiltration or unauthorized access.

To prevent data exfiltration or unauthorized access, the platform allows security analysts or file owners to apply authentication-based or file-based restrictions. Authentication-based restrictions rely on the AI verifying a user's identity and permissions. File-based restrictions, allow users to define download abilities and what specific groups or individuals can access the file.

With these security measures, agencies can safely share information among partners without worrying about that partner's specific approach to network security. By selecting CSfC-approved programs that help bolster data security through authentication-based and file-based restrictions, security operations centers can add another layer to their defense-in-depth strategy.

The Future of Data Security: Next Steps for Federal Agencies

Despite improved processes and technologies, a common roadblock is gaining buy-in from senior leaders within the department. Senior leaders often hold the keys to revenue, and with dwindling budgets it can be challenging for federal data leaders to secure the resources they need for data security. To effectively drive home the importance of data security and a defense-in-depth posture, data leaders should outline the significance of data to the larger mission.

Furthermore, data leaders should point toward CSfC — explaining that such programs help agencies see a return on their investment quickly. CSfC expedites the federal procurement process, liberating federal investments and ensuring they don't get tied up for months or years.

These actions are the same ones that Mark Krzysko, principal deputy director for enterprise information for the Pentagon's Office of the Under Secretary of Defense for Acquisition and Sustainment, recommends to other government organizations. "It is essential for leadership to articulate their goals to understand their data needs. Starting with a small set of use cases and the data you already have and building out your capabilities is a great way to start; however, you need to understand the problem set before knowing what tools and technologies you need to apply," Krzysko says.

At the end of the day, outlining the benefit of data security by focusing on use cases and organizations who've made similar moves is crucial — if not to secure an agency's own data but to help build a more intelligent, data-driven organization. "Data-driven government is needed now more than ever," says Rohland. "From partners, processes and tools, the culture of data-driven decisions is at our fingertips: We just have to leverage it and help our customers do the same."