



Case Study:

How RackTop Enables a Large Federal Systems Integrator to Meet Data Security and Storage Requirements for Multiple DoD Government Programs

With one solution the organization can scale to protect classified data for hundreds of government programs

Key Risk Factors

- ▶ Challenged by complicated government compliance and approval to operate requirements
- ▶ Faced efficiency concerns related to sprawl, security controls and data classification



Situation

Our customer, a large Fortune 100 federal systems integrator (SI) supporting multiple agencies and hundreds of programs, needed a scalable and highly performant storage solution to better serve programs with classified data by being more responsive to new projects and requirements from government programs.

Because the SI provides capacity to meet the needs of a variety of sponsoring agencies, they need a secure storage solution that achieves accreditation to operate (ATO) from all sponsoring organizations. This includes meeting relevant controls from the NIST Risk Management Framework as well as the Executive Order on Improving the Nation's Cybersecurity regarding the security and protection of data and the deployment of zero trust architectures.

Provisioning IT infrastructure for a new contract start can be time-consuming and delay the billing and success of a government contract. The SI needed an efficient and cost-effective storage solution to reduce costs and sprawl. They wanted to consolidate multiple disparate storage solutions that were deployed throughout the network for a single as-a-service solution to support internal projects as well as government funded programs. The storage solution needs to handle a variety of workloads including modeling and simulation, HPC, AI/ML, archive, as well as any unforeseen workloads that arise in the future.

A key driver for this effort was maximizing efficiencies for cost, size, weight, and power while also meeting the government's stringent requirements for multilevel security which allows a single storage system to contain files for different projects and security classifications including Confidential, Secret, and Top Secret. The consolidated approach would provide attribute-based access control (ABAC) with security labels applied and stored with each file. By creating a large group of systems that would support any project or classification, the SI can provision storage on demand to whatever project or program needed it. Upon a project's conclusion, they needed to be able to securely erase the data and efficiently repurpose that capacity.

With BrickStor SP, the SI was able to meet the relevant NIST Risk Management Framework requirements for data and access control requirements as well as those in the Executive Order on Improving the Nation's Cybersecurity for a data-centric zero trust architecture, real time logging, secure supply chain, and data encryption for data at rest and in flight.

Process

After an investigation period that included several demonstrations and technical exchange meetings, the SI launched a pilot operation by deploying three small scalable systems for three core sites. RackTop's cleared engineers supported each system deployment with single day on site configurations and installations.

The pilot operation allowed the SI to test workloads while beginning the government accreditation process for the systems.


- The solution was quickly proven to meet the storage workload requirements
- Engineering and administration teams could demonstrate integrated compliance reports and documentation for approve to operate (ATO) requirements

The pilot quickly proved to be successful and garnered the full support of executive management. The project moved from a pilot phase to full operations phase. In this phase they deployed additional storage capacity at each location to approximately 20 PBs of usable capacity. Another system was deployed to a fourth site for the purposes of collecting and centralizing all the logs.

Results

The multi-site deployment of RackTop's BrickStor Security Platform provides critical services for internal SI operations and government projects. The systems are accredited and fully approved to operate and support multilevel security operations across all DoD agencies and programs. Additionally, the customer benefits from:

- Government multilevel security (MLS) accreditation for a single system to support hundreds of different government programs with classified data
- Security controls to prevent insider threats
- Artificial intelligence to detect and respond to any threats including zero days in real time
- Scalable storage for unstructured data and virtual machines supporting demanding and highly performant workloads
- Dynamically attributing storage to programs as needed regardless of the data classification type, which drives significant cost and operational savings
- An economical, space and energy efficient solution deployed across multiple data centers to support disaster recovery and continuity of operations (COOP) if one of the systems becomes unavailable
- Existing program team can manage, maintain, and upgrade the solution from a central location



BrickStor's active defense features and zero trust architecture provides constant trust evaluation to protect the organization's data from insider threats, advanced persistent threats (APTs), and other data-oriented attacks.

BrickStor's SP's crypto shredding feature enables the SI to crypto erase an individual data set containing the data of the old project to secure purge the data in accordance with NIST media sanitization standards³. This same process can be followed to clean up a data spillage event, which further reduces the SI's operational risk.

The SI can efficiently respond government contracts and immediately support missions upon contract award without needing to pre-order equipment or wait for new capacity. They can quickly allocate resources to meet the demands of any project and repurpose existing capacity. This efficient approach lowers their storage and security investment costs, which makes the company's pricing more competitive when bidding on new contracts. With BrickStor SP, the SI was able to meet the relevant NIST Risk Management Framework requirements for data and access control requirements as well as those in the Executive Order on Improving the Nation's Cybersecurity for a data-centric zero trust architecture, real time logging, secure supply chain, and data encryption for data at rest and in flight. BrickStor's active defense features and zero trust architecture provides constant trust evaluation to protect the organization's data from insider threats, advanced persistent threats (APTs), and other data-oriented attacks. The solution is future proofed because RackTop continues to develop leading edge data security features to protect against evolving adversaries and demonstrate compliance with the latest federal regulations and security requirements.

¹<https://www.nist.gov/cyberframework>

²<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

³<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>