

CyberConverged[™] Data Security

The CyberConverged Difference

Increased cyber threats and complex data compliance regulations are changing the way you run your business. CyberConverged data security combines data storage, compliance, and security into an easy to use integrated solution designed to meet these complex challenges head on. It is the most efficient and effective means to protect unstructured file data from insider threats, malware, and cyber attacks. In this modern IT era, it is the only way to effectively store data at scale while preventing it from being unknowingly altered, stolen, or destroyed.

Top 5 Advantages of CyberConverged Data Security

1. Reduce Management Complexity and Administration

CyberConvergence enables IT staff to eliminate mistakes that could lead to data loss, system vulnerabilities, or non-compliance with laws and regulations. A CyberConverged solution eliminates the burden of managing heterogeneous software and improves overall effectiveness by reducing configuration complexity.

2. Eliminate Critical Attack Vectors

Using bolt-on software for security and compliance creates gaps and seams that can be exploited with minimal detection. Software that is external to traditional data storage systems requires fully privileged system account to remotely perform its functions, exposing all data within centralized systems to sophisticated attacks, which can steal data silently.

3. Detect and Stop Threats in Their Tracks

With a CyberConverged architecture, organizations can take a proactive approach to data security and stop access to data based upon suspicious behavior before it is too late. Traditional architectures send alerts to an already busy Security Operations Center (SOC) requiring human investigation, while the CyberConverged approach has enough machine intelligence to not only alert the SOC, but also take action on its own.

4. Improve User Experience and Application Performance

A CyberConverged architecture embeds security and compliance features into the architecture in a way that doesn't diminish the cost of performance. Internal compliance features, such as data scans, don't require costly IOPS or pollute the data storage cache with administrative data, allowing data systems to meet security and compliance needs without impacting operational workloads.

5. Reduce Total Cost of Ownership

CyberConverged Data Security reduces the number of disparate products an IT admin must learn and manage. A CyberConverged architecture automates routine tasks and enforces configurations through policies that are set once and enforced continuously. This ultimately enables user self-service and workflow automation that are both secure and compliant, while increasing overall organizational efficiency and agility.

Book a meeting with one of our experts to discuss the immediate benefits of moving to a CyberConverged architecture.



How Do I Move To a CyberConverged™ Architecture?

Fortunately moving to a CyberConverged data storage solution is actually easier, faster, and more cost effective than moving to some other new storage with bolt on compliance and data security software. RackTop's CyberConverged data storage platform BrickStor SP supports all the major file protocols making it the perfect drop-in replacement for your existing data storage. Migrating data is simple with BrickStor SP's built in migration features. And because BrickStor SP includes many security and compliance features, you can begin to eliminate costly software license renewals which you will no longer require. Additionally, the upgrades are always easy since the upgrade for storage, security and compliance capabilities comes in a single image and all are upgraded together to prevent version incompatibility or the typical challenges associated with upgrading a integrated solution of bolt-on security software.