SEAGATE | RACKTOP

Solution Brief
DATA STORAGE WITH SECURITY

Defend your data with Seagate and RackTop

Seagate and RackTop have partnered to provide a turnkey solution to manage and actively defend your data against insider threats, ransomware, and cyberattacks.

Challenge Summary

Cyber attacks—including organizational data breaches and data theft—have increased each year, and traditional storage solutions don't include any active protections for unstructured data.

Benefits Summary

- A turnkey storage solution with a data-centric, zero trust architecture.
- Data-storage protection.
- Improved business operations.
- Strong defense against insider threats, ransomware, and cyberattacks.

For true cyber protection, organizations need a cyberstorage solution that can actively defend against data theft and ransomware before they occur—Seagate® systems with RackTop BrickStor SP software provides this solution.

Unstructured data—typically accounting for 80% to 90% of an organization's data—is often stored on file shares and network-attached storage (NAS) lacking data security capabilities that protect against breaches and insider threats. In addition, unstructured data grows at a rate of 55% to 65% every year, and keeping this data secure from hackers and malicious insiders is a major challenge.

Organizations are becoming increasingly aware of their vulnerability to ransomware attacks due to the aggressive growth in highly visible and operationally disruptive assaults. Because modern ransomware attacks now include data theft—which often leads to extortion—it's critical to detect any data breach at its earliest stage to stop it before major damage is done. Regulatory controls and rising cyber insurance premiums are forcing organizations to accelerate the adoption of advanced security technology to protect data assets. Considering the lasting negative financial and reputational impacts of a data breach, organizations need to act now to protect their data, reputation, and bottom line. Cyberstorage, a new class of unstructured data storage with active security protections designed to stop modern threats, is an effective answer to this complex problem.

Challenge/Problem

Cyber attacks, including data breaches, are increasing each year, leading to rising insurance premiums, regulatory requirements, and damage to organizational reputations. Traditional cybersecurity approaches—even zero trust architectures without a data-centric approach—leave the organization's most valuable asset, data, unprotected. Organizations need a solution that actively defends their data against insider threats, ransomware, and cyber attacks.

Top challenges

- Rising cyber insurance premiums
- Regulatory compliance requirements
- Risk of damaged reputation

Adversaries are able to bypass perimeter security, endpoint monitoring, and zero trust networks via phishing, supply chain vulnerabilities, misconfiguration, and other security gaps within most IT infrastructures—both on premises and in the cloud. Modern organizations need a security solution that protects the data as close as possible to the data's source. The challenge for IT organizations has become more difficult with distributed IT and workforce teams.

Organizations must assume they're going to be attacked. And in the event of an attack, they should have a plan in place that allows them to continue operations.

Solution Approach

The most effective way to protect data is through storage. To implement a data-centric, zero trust security architecture, organizations must adopt NAS and file share solutions that can evaluate trust for each file operation and keep up with the speed of business. In fact, the right solution will improve business operations by providing a strong defense against insider threats, ransomware, and cyberattacks, as well as enabling resilience should one of these scenarios occur.

In Hype Cycle™ for Storage and Data Protection Technologies, 2022, Gartner® reports that "by 2025, 60% of all enterprises will require storage products to have integrated ransomware defense mechanisms, up from 10% in 2021."

The Seagate Solution

Seagate and RackTop have partnered to combine Seagate systems, enclosures and drives with RackTop's revolutionary BrickStor Security Platform (SP). This turnkey solution offers a data-centric, zero trust architecture and includes Seagate's enterprise storage systems and leading Seagate Exos® X drives with Seagate Secure™ SEDs (self-encrypting drives) that provide FIPS-validated encryption for data at rest.

RackTop uses Exos X mass storage systems and Exos E expansion storage for scalability and reliability. Seagate provides industry-leading enclosures, hard drives, and solid state drives to meet any enterprise workload or use case.

Seagate Exos X SAN systems combine Seagate's industry leading ADAPT data protection controller using our 6th generation VelosCT.

Partner Solution

RackTop's BrickStor SP software-defined NAS architecture provides high-performance SMB and NFS file sharing with embedded security and compliance features. BrickStor SP's active defense features allow it to analyze file operations in real time and instantly block malicious users and applications from accessing more data. Meanwhile, the good users and systems can continue to function and access data, creating cyber resiliency for the organization.

BrickStor SP lets organizations see what data is being accessed, by who and when, with user behavior auditing and analytics features. This information is valuable for data management, risk management, and data security. Many organizations lack this information today and are unable to make informed decisions or quickly investigate the implications of a cyber incident.

Total Solution

The Seagate/RackTop cyber resilient solution uses active defense capabilities to isolate and contain an attack by blocking the offending clients from accessing further data while allowing legitimate users to operate as usual. A fully integrated incident workflow engine incorporates user behavior analytics to pinpoint affected files and instantly report them to administrators, security operations centers, and third-party applications. Paired with always-on immutable data protection, incidents are intelligently assessed to enable one-click automatic selecting of the appropriate files to remediate and recover, optimizing an organization's ability to return to service quickly.

Features & Benefits

- **Active Defense:** protect unstructured data through inline, real-time assessors that scan for malicious and abnormal file activity.
- **Agentless User Behavior Auditing & Analytics:** get visibility and governance into how users and applications access data, without deploying agents.
- **Immutable Snapshots:** instantly restore an individual file or entire data set.
- **Ransomware Protection:** enable cyber defense and resiliency via embedded data protection policies, user behavior auditing, and analysis capabilities.
- **Integrated Compliance Reports:** quickly and easily demonstrate security and regulation compliance via generated reports.
- **Data-at-Rest Encryption:** leverage key management and self-encrypting drives while maintaining high performance.
- **Data-Centric, Zero Trust Architecture:** evaluate trust for each file operation in real time.

Conclusion

Cyber attacks are on the rise, and the best way to protect an organization's critical data is by putting protections as close to the data as possible—where it's stored. New regulatory frameworks are forcing organizations to adopt a zero trust architecture because traditional security models and existing security investments aren't effective enough to stave off the rise in data breaches.

Organizations can adopt a data-centric, zero trust architecture seamlessly, while meeting the requirements of the Cybersecurity Executive Order and the CISA zero trust maturity model without having to change workflows or user behaviors. By adopting the Seagate/RackTop solution, organizations will immediately gain cyberstorage capabilities as a last line of defense to protect unstructured data, enable cyber resiliency, and align with new and emerging compliance requirements.

Ready to Learn More?

Talk to an expert **www.seagate.com**

SEAGATE