WHITE PAPER

Cyberstorage Eliminates Security Gaps in Government IT Infrastructure

Introduction

Leading security analysts have concluded that traditional cybersecurity solutions that only monitor the network, endpoints, and application interfaces aren't sufficient to protect data against the modern threat landscape that includes insiders, nation states, and malware gangs. Government organizations such as CISA have identified the need for a data-centric zero trust architecture with protections around the data itself. Adversaries want to steal the data, not the network.

Network security has been and continues to be the greatest focus of cybersecurity, but it is just not comprehensive enough. That's why we continue to see the theft of classified and unclassified data. Data-centric zero trust security will prove to be the most effective and secure method for protecting the DoD's most valuable assets – data.
RackTop's BrickStor Security Platform (SP) defends data in real-time to actively stop insider threats and ransomware attacks.

Actively Defend Data with Cyberstorage

Data theft, manipulation, and loss are the leading challenges facing the government, particularly when sensitive intelligence and personal information are at stake. The multiple levels of secure and non-secure data across the broad footprint of government agencies, military sites, and contractor facilities create complex and vulnerable environments. While procedure, controls, and perimeter security systems help defend against external threats, the most critical infrastructure – the systems storing data – are vulnerable to assailants. RackTop is the first to fuse data storage with advanced security and compliance into a single CyberConverged™ platform built to protect data and comply with the latest NIST publications.

In the Hype Cycle™ for Storage and Data Protection Technologies, 2023[1], Gartner® recognizes the need for prioritizing active protection and security by integrating cyberstorage into data storage systems as an additional layer of protection to backup and disaster recovery. Gartner defines the emerging market, "Cyberstorage offers an active defense of the storage systems and their data against cyberattacks through prevention, early detection and blocking of attacks, and aids in recovery through analytics and storage-specific recovery capabilities." It is important because, "Ransomware attacks are increasingly common and disruptive, requiring the adoption of cybersecurity tools for active defense and recovery. Although numerous solutions are available for endpoint protection, object, file system and block storage systems provide inadequate protection from malicious downloads, deletion, destruction, or encryption of data. Cyberstorage provides active defense and recovery against cyberattacks on storage systems and their data."

RackTop is a leading and innovative provider of data storage solutions that actively defend against ransomware and insider threats. RackTop's BrickStor SP is the only unified solution on the market today that delivers all Cyberstorage capabilities in a single product. With the release of BrickStor SP, RackTop is the first to implement a data-centric zero trust architecture. BrickStor SP's modern data security features includes data at rest encryption, with end-to-end protection, that's suitable for

[1] GARTNER and HYPE CYCLE are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner, Hype Cycle for Storage and Data Protection Technologies, 2023, Julia Palmer, 13 July 2023

protecting classified information. BrickStor SP uses open standards and can be implemented in any modern IT environment. Its modern user interface makes it simple to implement and maintain by IT generalists.

The architecture of BrickStor SP places critical protections close to the data in order to uniquely identify, protect, detect, respond, and recover from advanced persistent threats (APTs). Unlike traditional network and perimeter-based security tools, BrickStor SP accounts for, and defends against, insider threats. BrickStor SP has the capability to share data securely using common file and block protocols (SMB, NFS, iSCSI). It also includes data protection capabilities that orchestrate data versioning, replication, retention, and disposition. RackTop's BrickStor SP eliminates complexity and disparate tools, resulting in a unified, simple to manage and secure data protection solution.

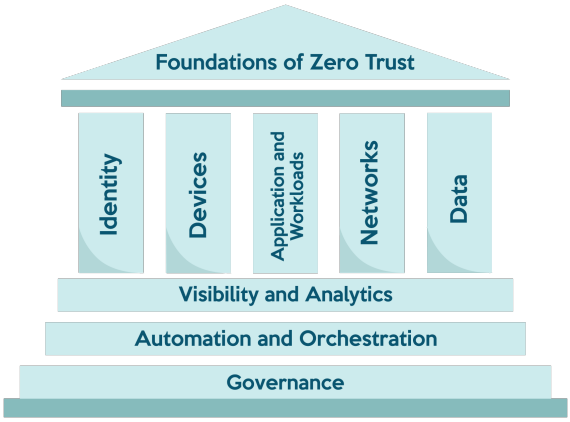
Why RackTop

RackTop's vision is to enable every organization to protect their valuable data as if it were a national secret. RackTop has decades of experience working in national security and recognizes the inadequate protections provided by traditional file and data storage solutions. These solutions hold an organization's most valuable assets but lack sufficient integrated data security protections. RackTop saw a need and created a product that can be easily maintained while it protects data against the most sophisticated adversaries including nation states and malicious insiders. RackTop has leveraged decades of experience in national security to provide a solution that addresses the distinct needs and challenges of the federal government.

FEATURES

Data-Centric Zero Trust

NIST defines zero trust as moving from an implicit trust model based on a user's position within the network to a dynamic trust model where each transaction with an enterprise resource is evaluated for trust. Files and unstructured data are an organization's most indispensable assets. Counterintuitively, however, they are often an under protected enterprise resource. BrickStor SP can evaluate trust for each file operation at the speed of any mission without negatively affecting user experience or application performance. Out of the box, BrickStor SP satisfies *all* the requirements of the data pillar for the CISA zero trust maturity model.



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.

Active Defense

RackTop is the first storage solution to implement a data-centric zero trust architecture with active defense and policy enforcement against ransomware, insider threats, and unusual or excessive file access. The active defense features of BrickStor SP immediately alert security and infrastructure teams about suspicious behavior and block those user accounts and IP addresses from accessing further data. BrickStor SP's cyber resilient architecture stops and contains a ransomware attack in

real-time while simultaneously allowing non-offending users and applications to continue to access the data and deliver critical services. Built-in incident management and automatically generated incident reports make it easy to determine the source of an attack, immediately restore affected files from immutable snapshots, and quickly resume normal operations.

BrickStor SP proactively protects unstructured data through inline real-time assessors that are looking for malicious and abnormal file activity perpetrated by a user or application. BrickStor SP's active defense features are extensive and can tie into an organization's security ecosystem through webhooks and email alerts. In addition to detecting abnormal access and employing a zero trust evaluation model for file operations, BrickStor SP can enforce policy and stop an attack in real-time before it is too late.

By default, BrickStor SP has assessors to detect:

- Excessive File Access (reads, writes, and deletes per dataset)
- Unusual File Access (access by a privileged account, for example)
- Ransomware
- Destructive Malware

Organizations can add custom rules and incident responses based on their organizational needs. Active defense makes the BrickStor SP another high-fidelity security sensor within an organization's infrastructure. It can eliminate blind spots and detect attackers, internal or external, that sidestep endpoints by exploiting devices that do not have endpoint monitoring. BrickStor SP does not rely on agents, can audit all file access activity, and will alert relevant security teams and applications for accelerated response.

Simplified Secure Architecture

BrickStor SP is designed by default to be secure and compliant yet operationally structured with IT generalists in mind. It eliminates the need for subject matter experts by relying on policy-based configurations and system automation.

Highly Scalable

The platform can scale from just a few terabytes to multiple petabytes per node. A single BrickStor can service thousands of users and virtual machines, and multiple BrickStor appliances across data centers can be managed through a single pane of glass user interface.

Policy Engine

BrickStor SP has a policy driven architecture that ensures consistent and compliant behaviors on the system including data security, data encryption, data protection, data retention, and data replication. The platform automatically applies settings based on use case and associated data protection policies, which set the frequency and retention period of snapshots. Replication can also be configured as a policy to replicate snapshots efficiently with replication windows, priority, and bandwidth throttling from one instance to others.

Agentless User Behavior Auditing and Analysis

BrickStor provides complete visibility and governance into how users and applications are accessing data without the need to deploy any agents on the client or endpoints. The BrickStor user behavior audit log can be stored locally, or forwarded and streamed to external log repositories, which allows for easy integration with Security Incident Event Managers (SIEMs) like Elastic Search, Splunk, HPE ArcSight, and IBM QRadar. These integrations allow for user activity, file activity, and key orchestration events to be reviewed and executed upon as part of cyber response operations. Audit functions coupled with workflow allow users to have a platform to monitor and execute response plans that include removing user access to data and data exposure. BrickStor's integrated analysis tools allow for detailed threat hunting and discovery with a fidelity and granularity that was not previously possible or available to security analysts. This built-in tool is paramount for active defense against insider threats and enterprise monitoring.

Data Backup and Disaster Recovery

Every BrickStor includes always-on ransomware protection and zero footprint snapshots to enable users and administrators to revert to previous versions of files, folders, and virtual machines instantly. These snapshots can be replicated asynchronously to other BrickStors for complete disaster recovery and Continuity of Operations (COOP). BrickStor's replication capability is WAN efficient and can systematically replicate over high latency low bandwidth connections.

Ransomware Protection

The embedded data protection policies and user behavior auditing and analysis capabilities provide cyber defense and resiliency against ransomware so that an organization *never* has to pay a ransom. Should a ransomware attack successfully encrypt some files on the platform, administrators can immediately see which account(s) have the ransomware and are infecting the environment. Immediately, administrators can deny those account's access to data to stifle malware spread and reinfection. Because the data protection features of BrickStor keep data in an immutable format, the infected files can be restored in seconds to a previous, unmaligned version.

Encryption

BrickStor SP has a built-in key manager or can work with a KMIP compliant external key manager. BrickStor SP can manage FIPS Self-Encrypting Drives to provide inline data at rest encryption without sacrificing performance. It also supports dataset level encryption so that each folder has its own unique encryption key. This offers double encryption for data and the ability to securely clean up data spillage without having to erase or destroy the entire system. BrickStor SP also supports the latest file protocols to provide encryption for data in flight between the client and BrickStor SP as well as between multiple BrickStors for replication. In an instant, BrickStor SP can cryptographically erase drives in the field to protect data from getting into the wrong hands.

Privileged Access Management

A major issue facing government organizations is ensuring that only those people with a need to know have access to data. BrickStor SP makes it easy for data owners to review access policies to ensure users no longer involved in a project are removed and sensitive data is not over exposed. Furthermore, BrickStor SP alerts the security team when administrator or privileged access credentials are used to access files. This enables unusual activity to be scrutinized, thwarting common insider threat tactics, Advanced Persistent Threats (APT), and many others.

Integrated Compliance Reports

BrickStor includes compliance reports that enable organizations to quickly demonstrate they are meeting the controls of cybersecurity and regulatory frameworks such as NIST 800-53. There are 25 categories of compliance reports including, but not limited to: data encryption, key management, privileged access management, administrator auditing, user behavior auditing, and data retention. Upcoming features make it easy to map applicable NIST controls and show when even a portion of a system is not compliant with the relevant control, while also providing a remediation action.

Meet the Requirements of the new Cyber Security Executive Order

BrickStor SP makes it easy to comply with the Cybersecurity Executive Order 14028 which requires all federal agencies to implement a data-centric zero trust architecture. The order calls for organizations to improve detection of cybersecurity incidents on federal government networks. Poor logging hampers an organization's ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact. BrickStor SP's user behavior auditing and active defense provide immediate capabilities to ensure 100% visibility into what is happening and what happened within an environment.

Logical Segmentation – Enclave Elimination

Organizations that want to eliminate physical system segmentation and silos to enable centralized monitoring and dynamic resource allocation can overcome previous security challenges with the advanced access control features built into BrickStor SP's operating system. BrickStor SP includes granular access control capabilities to restrict access down to the individual file

level. BrickStor SP includes discretionary access control across all client platforms, which are the most common access control scenarios, and sufficient for government security accreditation of multiple enclaves within the same security domain. Additionally, BrickStor SP supports host-based access control on top of discretionary access control. With SE Linux and NFS 4.2, BrickStor SP can enable mandatory access control through the support of context security labels. With this architecture, a single BrickStor SP system can be accredited for access from multiple security domains and enclaves.

Application Areas

BrickStor hybrid or all flash storage can handle large files, small files, random IO, and streaming IO on the same system. Common use cases in the private and public sector include:

- Organizational file shares
- Full motion video recording and playback
- DevOps
- Virtualized environment requiring ultra-fast storage
- Online archive
- Intelligence production chain (sensor to policymaker)
- Secure enclaves, MLS
- Computer forensics
- High performance computing (HPC)
- Medical image analysis and research
- SecOps
- Secure virtual desktop infrastructure (VDI)
- Analysis and simulation

Flexible Form Factors for Deployment

BrickStor SP software can be deployed in various form factors from the tactical edge, to the core, or to the cloud. It's an enabling technology that can protect data in flight and at rest. Deployments are available on ruggedized platforms and special form factors to meet underwater, surface, land, and airborne requirements.

BrickStor SP is a software defined NAS that can be deployed on bare metal, or as a virtual machine in the cloud or on any major hypervisor. For physical platforms, BrickStor SP can be deployed in hybrid or all flash configurations to meet performance requirements. The solution is also available to deploy in a rugged Pelican rolling case with over 150TB of all flash FIPS/TAA self-encrypting drives to meet airline carry-on size requirements.

Conclusion

RackTop has identified and solved a critical vulnerability of even the most secure data networks. BrickStor SP solves many common data loss problems and is simple to use and manage with no impact on application performance and mission operations. BrickStor SP offers best-in-class capabilities including data management, data at rest encryption, and key management. The solution solves the challenges of protecting sensitive intelligence and personal identifiable information, and securely manages multiple levels of classified data on a single system. BrickStor SP enables organizations to install Cyberstorage software and gain immediate security benefits without having to re-engineer existing applications or hire additional resources.