Hewlett Packard Enterprise | RACKTOP

Technical white paper

HPE COMPLETE: RACKTOP SYSTEMS TECHNICAL OVERVIEW

CONTENTS

THE CHALLENGE

In today's data-driven society, unstructured data accounts for a growing portion of an organization's assets. Most of this data is not easily searchable, nor is it organized in a predefined manner.

In data-driven organizations, the challenge of protecting data often becomes cumbersome and unstructured because data access cannot be managed linearly. Data is everywhere. To overcome this challenge, organizations have adopted cybersecurity models that build a hard exterior around their networks, yet the resulting trusted interior is where most threats now originate. In the traditional model of taking a linear approach, for example, placing all data behind a firewall, a significant gap grows between the data and its protections. These gaps can persist and open an organization up to insider threats, or well-meaning employees can unwittingly introduce ransomware or other cyberthreats into the infrastructure.

This is where RackTop Systems comes in. Instead of following the traditional model, RackTop follows a data-centric zero trust model where data is protected at every step of its lifecycle, from the core to the edge. This model offers insight into all organizational data assets, their current state, and the patterns of interaction that users have with them. RackTop eliminates the need for implicit trust and evaluates trust on each file operation without sacrificing the user experience or application performance.

HIGH-LEVEL OVERVIEW

RackTop Systems pioneered CyberConverged data security, with the BrickStor Security Platform, a product that fuses data storage with advanced security and compliance into a single platform. RackTop is a high-performance software-defined Cyberstorage solution with embedded security, compliance, and encryption. The platform empowers organizations by protecting data where it resides without the cost, complexity, and security vulnerabilities of traditional bolt-on software solutions. BrickStor SP can be deployed in various configurations from the edge to the core to the cloud. Organizations can even leverage existing storage capacity and convert it into secure Network Attached Storage (NAS) and file share capacity.

Distinguishing features of RackTop

RackTop's benefits include, but are not limited to the following:

- Data-centric zero trust architecture with active defense provides built-in ransomware detection, protection, and remediation
- Memory-based storage architecture delivers data security and compliance through a high-performance user experience
- User behavior auditing (UBA) and analysis enables rapid threat detection and response along with a better understanding of system user activity
- Data protection policies guarantee and enable simplified data backup and recovery with user self-service
- Hybrid cloud architectures with Transparent Data Movement (TDM)
- Integrated compliance reports simplify and accelerate system accreditation and regulatory audit processes
- FIPS AES-256 encryption at the data set or volume level provides encryption for data at rest
- TDM, snapshot replication, SMB 3.1.1, and NFS with krb5p all provide encryption for data in transit
- Native features include thin provisioning, inline compression, deduplication, unlimited snapshots, clones, zero silent data corruption, and data self-healing
- Software-defined storage available on HPE Enterprise class hardware or customer based virtual environments
- Hybrid storage integrating RAM, SSDs, and HDDs to deliver the maximum performance at the lowest cost
- Reduced total cost of ownership when compared to other storage solutions that bolt-on security
- Public API to enable programmatic workflows and security responses
- Secure and compliant by default and design

ANALYZING THE RACKTOP SECURITY PLATFORM

RackTop is a unified NAS with flexible configuration and deployment options. BrickStor SP can be deployed in front of enterprise block storage or as a virtual machine on your favorite hypervisor, HCI, dHCI, or cloud. HPE server configurations have been designed to provide the optimal level of performance and cost. In SAN gateway mode two DL380 servers can be used in an active-active configuration with Fibre Channel or iSCSI connectivity to HPE Alletra 9000, HPE Alletra 6000, HPE Nimble Storage, HPE 3PAR, HPE Primera, and HPE XP or other block storage. And, for smaller deployments or less performance intensive deployments organizations can deploy a virtual machine edition of the BrickStor SP. Replace Windows and Linux® file servers with a hardened purpose-built solution that will actively defend your data against any threat. Both versions use the same software and are completely interoperable.

RackTop provides robust data protection at both the micro and macro levels, ensuring data integrity and protecting against silent data corruption, while also protecting data from hardware failures. RackTop's embedded data protection capabilities provide always-on, full end-to-end control of data movement, and visibility of the blocks so that full and integrated end-to-end checksumming can be performed. The filesystem checksums are a more advanced type of hierarchical checksum that identify media deterioration known as bit rot, as well as other types of data corruption across the I/O path and repair it before it results in data loss. RackTop supports the following RAID implementations: mirrored, triple mirrored, single parity RAID, double parity RAID, triple parity RAID, and striped (no RAID).

RackTop primarily focuses on file protocols to store and serve unstructured data. The platform supports block protocols for cases like iSCSI boot where a file protocol cannot be used. Each system supports both block and file-based protocols and there is no limitation to the number of shares or volumes presented. RackTop natively supports the following protocols:

- CIFS/SMB 2/3/3.1.1
- NFS 3/4/4.1/4.2
- iSCSI

From a network perspective, each RackTop instance can support multiple Ethernet interfaces, including 1GbE, 10GbE, 25GbE, 40GbE, or 100GbE. Systems can be configured with all-flash or all HDD pools, or a hybrid system with both drive types available.

User Behavior Auditing and Analysis

RackTop's UBA and analysis capability is the perfect defense against cyberattacks and insider threats. UBA provides a real-time stream of user activity that captures their identity, source IP address, and protocol. Administrators can analyze user behavior activity within the myRack Manager user interface or automatically forward it to an RFC 5424-compliant SIEM, such as Splunk or an anomaly detection engine. myRack Manager provides a feature-rich data visualization interface, which displays top users, hot files, and activity outside of normal business hours. It can also easily help determine who moved or deleted a file, a common problem for many IT organizations today. Administrators can use the UBA stream to orchestrate automatic responses to suspicious and malicious activity to stop bad actors before it is too late.

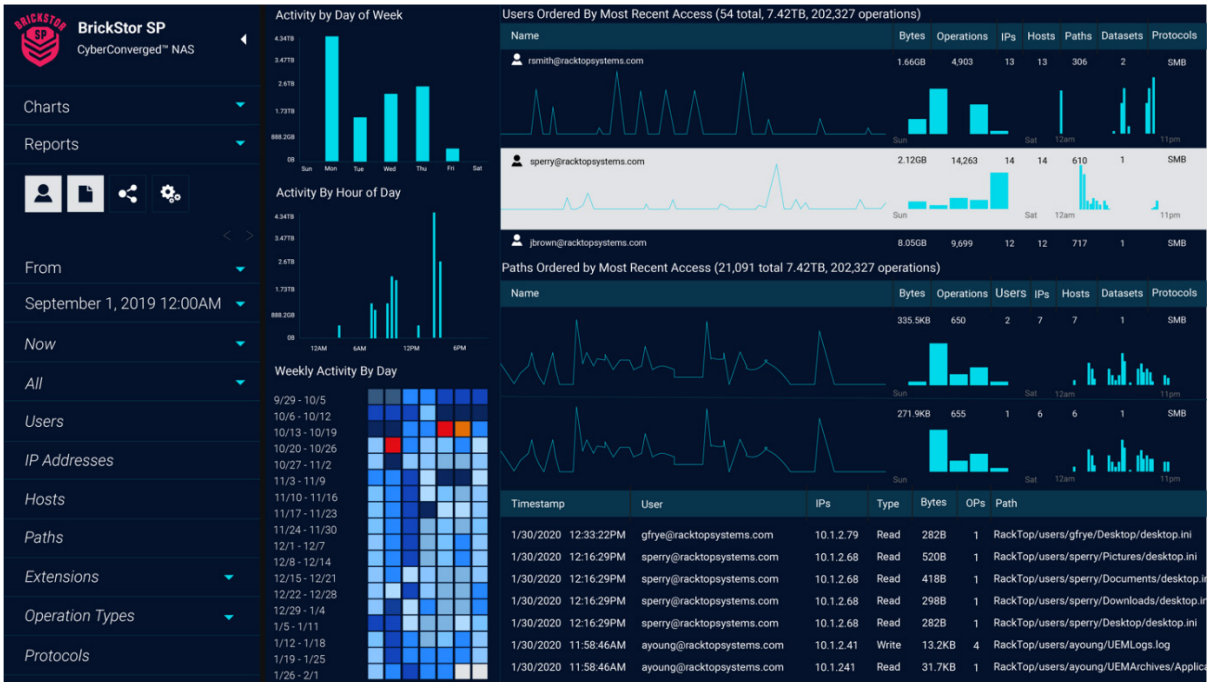

FIGURE 1. UBA in myRack Manager

Active Defense

RackTop is the first solution to implement a data-centric zero trust architecture with active defense and policy enforcement against unusual data access, ransomware, insider threats, and excessive file access. The active defense features of the BrickStor SP can immediately alert security and infrastructure teams about suspicious behavior as well as block the suspicious user accounts and IP addresses from accessing further data. And when it comes to ransomware, the BrickStor SP creates a cyber resilient architecture that stops and contains the ransomware attack, automatically generates an incident report, and allows other non-offending users and applications to access data and continue to deliver critical services. The built-in incident management features make it easy to determine the source of the attack and immediately restore files that were affected from immutable snapshots and return the system to service quickly.

Transparent Data Movement

TDM allows the movement of data from a BrickStor SP to other storage including non-RackTop Systems that support NFS or S3. With TDM, a file's metadata stays on the primary tier while the file is compressed and encrypted before it is pushed to a remote tier. This allows for infrequently accessed or archived data to be moved to a lower-cost storage class without changing the user's workflow. To the user the data is on the network share where they stored it.

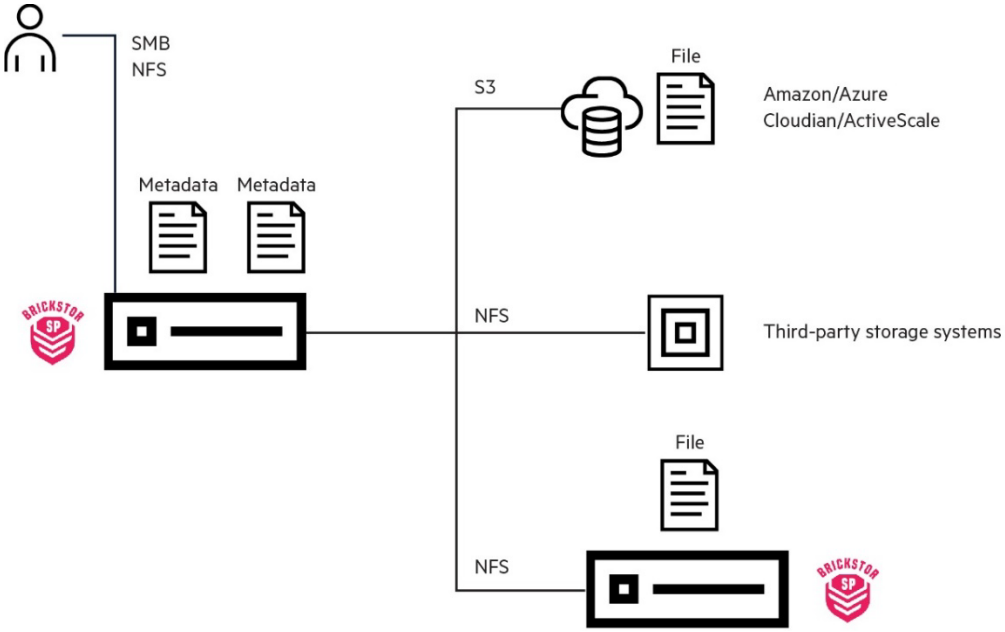

FIGURE 2. RackTop's TDM process

Unified Global Management

RackTop's unified global management system, also known as myRack, allows global command and control of all RackTop appliances through a single user interface. This unified approach simplifies data management and enables administrators and managers to provision and modify storage rapidly. The myRack appliance explorer user interface allows users to search for files across any RackTop, and forecasts data growth. myRack provides administrators with single-click executable suggestions for resolving capacity contention or shortages. It is a powerful interface that simplifies storage administration and provides managers with a detailed understanding of return on investment and projected storage needs by department, application, or location.

Frictionless storage provisioning

RackTop is an intelligent software-defined storage solution that enables admins to provision storage rapidly, optimizing systems for each workload or application. Administrators provision storage by selecting the appropriate use case, such as file shares, streaming media, archives, e-discovery, server virtual machines, and so on. Once provisioned, the storage self-configures and provides the maximum performance, appropriate data protection, and the most efficient system utilization.

Compression

Inline real-time compression is provided at the data set level with the system offering the choice of multiple compression algorithms.

Deduplication

RackTop supports inline block-level deduplication for further data reduction in all-flash environments for highly duplicative data.

Thin provisioning

RackTop supports thin provisioning to provide maximum flexibility and growth in environments where growth per data set may be hard to predict. Thin provisioning provides an efficient way to provision usable space with physical capacity oversubscription. RackTop data visualization allows the administrator to see at a glance how much space is logically and physically consumed by a data set.

INTEGRATED DATA BACKUP AND DISASTER RECOVERY CAPABILITIES

RackTop's zero footprint snapshots and advanced data replication provide customers with exemplary off-site backup, business continuity, and disaster recovery capabilities. RackTop can replicate data to cloud locations or to other RackTop instances, based on the data protection level and recovery point objective organizations need to meet their SLAs.

Data protection policies

Data protection policies define the frequency of snapshots, the retention period, and the location and priority at which each data set is replicated. Users define storage profiles or custom data protection policies, based on specific business data protection priorities, that automatically activate when storage is provisioned. User-configurable through the myRack Manager interface, RackTop makes it easy to ensure critical data is protected without having to purchase additional licensing or backup software.

Copy data management: Snapshots

RackTop's copy-on-write file system enables the instantaneous creation of snapshots and clones. At creation, no additional space is required for snapshots. RackTop does not limit the number of snapshots the user can create or retain per system and does not require pre-reserved capacity. This approach along with our ability to index files inside snapshots enables the rapid restoration of a version of an individual file or virtual machine from within a snapshot. Entire snapshots can be cloned to become operational for disaster recovery, backups, or testing purposes. Snapshots are a critical part of RackTop's windowless backup and near-zero recovery time objective, which enables true enterprise disaster recovery and business continuity.

Windows users can restore previous version of files from previous versions of Windows Explorer. Users can select and restore to the version of the file captured from any snapshot. Similar capabilities exist for NFS using command-line utilities. Administrators may use myRack Manager to restore any file, data set, or virtual machine to any location.

RackTop's unlimited cloning capability enables the instantaneous creation of zero-footprint clones and acts as a preemptive, performance-increasing, and deduplication capability. Clones leverage the same core blocks of data as their parent snapshots, which improves performance and caching, since RackTop caches the most frequently and most recently used blocks of data in DRAM. Clones provide an effective method for running tests or upgrades against a point-in-time instance of a database or virtual machine to validate patches and upgrades.

Replication

RackTop's replication technologies are WAN-optimized and can securely transmit snapshots between systems. RackTop's block-level replication only transmits the changed blocks between snapshots to expedite transmission and reduce bandwidth usage. RackTop's block-level replication has dynamic WAN bandwidth throttling, prioritization based on data set, and the ability to pause and resume replication. Replication will restart at a checkpoint if interrupted before completing the replication of an entire snapshot. Replication can occur within systems or between multiple storage appliances. RackTop also supports file-level replication to other NAS platforms, as well as S3-compliant object storage.

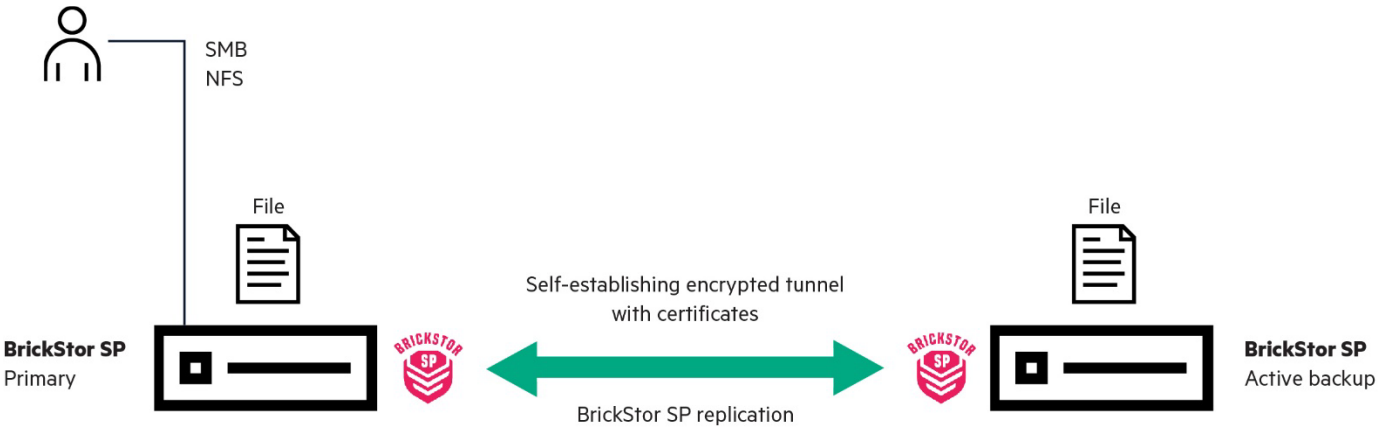

FIGURE 3. RackTop replication process

Administrative Audit and Change Control

RackTop logs and audits user and administrator activity, providing a list of administrator actions performed through the API and myRack Manager. The audit log includes the administrator's user ID, an optional commit message, and full details of the action. The commit message makes it easy to provide traceability of the actions performed to approved tickets or change requests. The audit log can be exported for compliance or archive.

Access control

RackTop integrates with LDAP and Active Directory for simplified access control management. RackTop provides features to review access and manage least privileged access easily from myRack Manager. This eliminates the need for complex and costly privileged access management (PAM) tools that require extensive training and administrator support. In addition to discretionary access control, RackTop supports NFS 4.2 context security labels to provide support for mandatory access control. With SELinux and context security labels, RackTop is a high-performing and scalable shared storage solution for multilevel security (MLS) implementations. MLS implementations allow a single storage solution to provide data across multiple domains at different classification levels. This is a critical capability for securing data while enabling cross-domain collaboration.

Encryption

RackTop can encrypt all data in transit and at rest. When enabled, two levels of data at rest encryption are available. The first is file system level encryption which is available on all RackTop Systems. The second, is self-encrypting hard drive encryption (SED) available on systems with SED drives. SED drives are FIPS 140-2 compliant, and both levels encrypt with the AES-256 cipher. RackTop protects data in transit through protocols such as NFS with krb5p, SMB 3.1.1, and with built-in transfer technology TDM and snapshot replication. The system can serve encrypted data to users and applications or replicate data securely to a remote RackTop instance without decrypting it to provide extra protection. RackTop automatically rotates encryption keys to meet key rotation compliance requirements. Key rotation does not require the system to decrypt and re-encrypt the data.

RackTop includes a key management service that manages all the keys for data sets. The enterprise key manager can be configured to store keys locally on removable media such as a USB key or retrieve keys from an external enterprise key manager over KMIP.

If encryption is enabled on a data set, the system requests a key from the key management service upon creation. RackTop encrypts data before it is written to disk using the AES-NI instruction set. Data in RAM is not encrypted, which enables high-performance, low-latency I/O without risk. However, all data written to non-volatile media is encrypted.

Metadata intelligence services

RackTop efficiently analyzes data as it changes to provide improved storage services, security, and compliance. The system analyzes metadata to allow for rapid search, workflow actions, and reporting about the data stored on the system. For example, a user can quickly find and restore a file on the system because of the index. Additionally, an organization can provide the provenance of a file by showing the hash has been consistent and who has accessed the file for security and compliance reasons. This information can also feed other systems to provide increased security based upon threat intelligence related to known malicious files. When a malicious file is discovered, the system can quarantine it immediately.

Key management

RackTop's key orchestration service manages encryption key material as well as maintenance functions such as automatic key rotation, periodic key verification, key activity auditing, and reporting. The key management daemon can store keys in a secure local database, on a removable disk, or connect to a KMIP-compliant enterprise key manager. The key orchestration architecture allows customers to use their key material to provide the highest-level trust in key material as is often required by government agencies and financial institutions.

RackTop provides complete transparency to the user about what is encrypted, key verification, key rotation dates, and more through built-in reporting. The policy engine enables admins to set a key rotation policy that will allow RackTop to request new keys on a defined schedule to automatically rotate keys in accordance with organizational policies.

THE CYBERSTORAGE ADVANTAGE

Traditional Storage

The traditional approach to storage requires bolt-on security solutions which inevitably lead to multi-vendor solutions to overcome the security deficiencies within storage systems. This approach creates complexity in deploying, managing, and updating systems. Having multiple vendors can result in shifting blame during critical moments of downtime instead of a focus on resolution. Having a single support team results in quicker issue resolution.

Upgrades become more complex as the number of vendors increases. Multiple change windows become a requirement, resulting in multiple scheduled downtimes. Lack of native cybersecurity integration results in greater difficulty testing upgrades, as upgrades from one vendor can break other vendor's solutions. This complex testing becomes the responsibility of the customer, rather than the vendors.

Storage performance suffers as multiple vendors scan the storage, using up valuable IOPS required by operational applications. Cache is also rapidly polluted by having multiple vendors read and scan for changes and backups.

Licensing varies from vendor to vendor resulting in CAPEX for some and OPEX for others. This results in a much higher total cost of ownership, making it difficult to realize a positive return on investment.

Cyberstorage

RackTop Systems' Cyberstorage solution removes the burden of typical multi-vendor solutions with a single, easy-to-use convergence of storage and cybersecurity on one platform that is far easier and faster to implement and manage. Having a single integrated solution results in a significantly lower total cost of ownership.

RackTop is embedded with military-grade security, using multiple levels of encryption, and built-in key management. These features in combination with user behavior analysis and proactive remediation result in a solution that is actively protecting your data.

Integrated compliance reports (NIST, SOX, HIPAA, MPAA, FINRA, SEC, and CMMC) make it easy to demonstrate continuous compliance with all relevant data security controls and compliance regimes. RackTop includes compliance reporting and auditing capabilities, along with multiple levels of encryption and active defense against ransomware, insider threats and cyberattacks.

Zero trust: Tying it All Together

RackTop Systems' Cyberstorage approach follows zero trust concepts, offering strong protections as close to the data as possible. The BrickStor security platform's built-in approach combines data storage, security, and compliance into a nimble security platform for the data-driven era. The platform is purpose-built to close the gap between organizational data and its protection.

LEARN MORE AT

hpe.com/us/en/storage/hpe-complete.html

a50002672ENW, Rev. 3

Hewlett Packard Enterprise