



ZERO TRUST WITH RACKTOP BRICKSTOR SP SECURE NAS

HPE Complete products

RackTop BrickStor SP

The RackTop BrickStor Security Platform (SP) is a software-defined NAS embedded with security, compliance, and encryption services engineered specifically to eliminate the threat of ransomware attacks, stop data breaches, and simply address complex data compliance requirements. Built by veterans of the Department of Defense Intelligence Community with expertise in offensive cyber and data security, RackTop BrickStor replaces legacy insecure platforms. The platform solves today's most challenging security and compliance issues without bolting on multiple third-party applications.

HPE Complete benefits:

- Single HPE purchase order—One-stop shop for both HPE and third-party branded products
- Build with confidence—HPE Complete Assured validation of compatibility and interoperability
- Customer experience—Simplified solution deployment with custom HPE and third-party developed integration guides and tools
- HPE Complete Assured—HPE Complete Assured testing validates reliability and interoperability of partner products with HPE storage and server solutions, and helps ensure solution concurrency over time; customers can rest easy knowing the combined solutions work well together now and into the future

HPE and RackTop deliver advanced cyber protections fused into a scalable storage platform for end-to-end zero-trust architecture.



SOFTWARE-DEFINED SECURE NAS

Data breaches, ransomware, and insider threats are all too common in today's digital landscape. Legacy security strategies and storage solutions leave data prone to cyberattacks. To help eliminate these risks, HPE and RackTop offer a software-defined secure NAS solution with built-in data management and increased security, while achieving uncompromised performance and a simplified user experience. Features like HPE's secure server platforms and RackTop's strict security compliance enable organizations to defend against insider threats and stop any cyberattack before it is too late.

WHAT IS ZERO TRUST?

With traditional perimeter security approaches, a security breach can result in unchecked access to internal systems and data. Because internal users, systems, and services are often trusted within the network, downloaded malware and other nefarious entities can easily gain unfettered access to your most valuable data.

A zero-trust architecture is one that does not automatically assume that any entity can be trusted. All users, systems, and services must be verified before providing access, whether they are inside or outside the security perimeter.

Solution brief

RackTop and HPE

BrickStor secures unstructured data at its source so that it can't be seized, maliciously encrypted, or exploited. Paired with HPE's world-class secure and versatile hardware, for the first time, customers can achieve end-to-end infrastructure security from a single vendor without gaps or loosely coupled bolt-on applications. HPE customer solutions center offers customer demonstrations upon request. Call your HPE sales representative to learn more.

As part of the HPE Secure Compute Lifecycle, HPE Gen10 Servers provide advanced security features such as Silicon Root of Trust along with FIPS, CNSA, and NIST compliance. HPE Gen10 Servers combined with RackTop provide a unified zero-trust platform for simplified storage, management, security, and compliance of all file data both on-premises and in the cloud. The architecture prevents your data from being held hostage, stolen, or compromised. RackTop simplifies the most complex regulatory compliance without additional complexity or costly bolt-on software packages. As a result, IT operations are simplified by consolidating multiple file servers and their associated security, governance, and compliance technologies into a simple-to-manage solution.

**100% ENCRYPTED,
100% OF THE TIME.**



TABLE 1. Basic building blocks

Product	SKU
1x HPE ProLiant DL360 Gen10 Management Server	2x HPE SKU P19765-B21
2x HPE ProLiant DL380 Gen10 All-Flash NAS Head Server	HPE SKU P19717-B21
2x HPE D3710 Enclosure	HPE SKU Q1J10A

UNCOMPROMISING DATA SECURITY FOR UNSTRUCTURED DATA

RackTop is built by Department of Defense Intelligence Community veterans and designed it from the ground up to protect your valuable unstructured data. All data is encrypted twice, at both the physical and logical layers, with little to no performance impact. Using RackTop, data is 100% encrypted, 100% of the time.

RackTop collects and indexes vast amounts of data about each file, whether the data is local, in snapshots, or replicated to other systems. Analysis engines transform that data into intelligence. This is used to reduce risk and exposure, meet regulatory compliance, and spot impossible-to-find security issues without any human intervention. User behavior and interactions are analyzed to build a fingerprint for what normal operation looks like. This enables RackTop to identify and stop anomalous user behavior, with orders of magnitude faster than network-based tools.

While data remains secured, performance of the HPE and RackTop solution leverages the power of HPE Gen10 Server technology, using up to 1 TB of RAM for data caching. Unlike competitors, HPE and RackTop's advanced data protection and security features can be achieved without compromising performance, simplicity of management, or overall user experience.

TABLE 2. Regulatory compliance

Category	Compliance
Privacy	FIPS 140-2, CMMC, GDPR, HIPAA, HITRUST
Financial	SOX/J-SOX, NYDFS
Security	PCI-DSS, FERC-CIP, NIST, FEDRAMP

Make the right purchase decision.
Contact our presales specialists.



Chat



Email



Call



Get updates

**Hewlett Packard
Enterprise**

LEARN MORE AT

[hpe.com/us/en/storage/
hpe-complete.html](https://hpe.com/us/en/storage/hpe-complete.html)

© Copyright 2020 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50002184ENW, August 2020