VION®
Building your enterprise solutions

vion.com

The Path to Zero-Trust: Protecting Data at the Source

Traditional file storage systems continue to be exploited by malware infected clients and malicious insiders. Although the industry has progressed steadily in creating better security, the biggest area of weakness has been protecting data at the source. Most cyber solutions protect perimeter defenses, but data is most vulnerable in its primary storage systems and online archives, whether it's in the cloud, at the edge, or in the data center. Now data is everywhere and it's hard to tell where it's moving. Historically, we've relied on perimeter security, thinking it's enough, but insider threats have changed that. With the growth curve of data, most organizations will be in a zettabyte volume in the next decade. For government organizations, this vulnerable data can be a matter of national security that requires a different approach.

Why Protecting Data at the Source is a Game Changer

Consider how a bank is set up to protect its money. There are a series of defenses starting outside the building, on-site security guards and many layers of personnel that have varying levels of access to the funds. As you get closer to the money the security increases steadily – hence why banks have sophisticated vaults. Protecting data should be no different. A perimeter-only strategy doesn't work for a bank and it won't work in the data center either - particularly because insider threats represent 34% of data breaches. Only by creating a chokepoint in front of the data, can we ensure complete visibility and control over every application and user accessing the data.

The New Data "Vault": A Zero-Trust CyberConverged™ System

Because storage has emerged as the weakest link in the system, a zero-trust architecture provides greater visibility to prevent breaches. Zero-trust changes the traditional model so that individuals only have access to the data he/she needs, keeping classifications by segment with frequent verifications. This new model puts controls in the hands of data owners versus system administrators. The system admin has a lot to surveil and typically doesn't have all the details, whereas the data manager knows who should have access, as well as who has interacted with the data or who hasn't in a project. This greater control for data managers allows them to de-escalate privileges or identify compartmentalized data in someone's personal files, which are critical to zero-trust and protecting from insider threats.

Securing unstructured data means adopting a "never trust" and "always verify" mentality, while maintaining protection and accessibility of that data. The RackTop BrickStor Security Platform is a true CyberConverged solution run

on HPE's servers and enterprise storage to accomplish this without impeding the mission. As part of the HPE Secure Compute Lifecycle, HPE Gen10 Servers provide advanced security features such as silicon root of trust from HPE along with FIPS, CNSA, and NIST compliance. HPE Gen10 Servers combined with RackTop can 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 data from being held hostage, stolen, or compromised. The platform empowers organizations by protecting data where it resides without the cost, complexity, and security vulnerabilities of traditional bolt-on software solutions.

A dynamic defense is the only way to meet the new adversaries. While cybersecurity has traditionally been network focused, this CyberConverged solution is data-focused using dynamic controls versus a fixed strategy that is NIST RMF and HIPAA compliant, providing active defense and policy enforcement against unusual data access.

Getting on the Path to Zero-Trust

As organizations analyze their existing infrastructures and security measures, there is a specific set of criteria to consider as the foundation for a true zero-trust infrastructure.

Zero-trust action list:

- Audit user interaction
- Audit admin interaction
- Encrypt data with keys controlled by the organization
- Determine normal user patterns by user type
- Continuously monitor the log and audit data
- Immediately investigate and ask end-user about anomalous behavior

The right system can make this action list easier to manage, with greater visibility and control – deployed in an organization's enclave or virtually in the cloud. Leverage ViON's 40 years of experience delivering complex solutions for enterprise data centers and the RackTop CyberConverged system on HPE's secure servers to level up your organization's security profile.

ViON®
Building your enterprise solutions

Hewlett Packard Enterprise

RACKTOP

About ViON Corporation

ViON Corporation is a value-added reseller with over 40 years' experience designing and delivering enterprise infrastructure solutions for public and private sector. The company's portfolio includes hyperconverged infrastructure, data management and back-up and recovery solutions to enable secure, scalable infrastructures that support multicloud, AI and advanced analytics. ViON also offers professional and managed services to provide expert support and consultation at every step. A veteran-owned company, ViON is based in Herndon, Virginia. (**vion.com**).

About HPE

Hewlett Packard Enterprise (NYSE: HPE) is the global edge-to-cloud company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open and intelligent technology solutions delivered as a service – spanning Compute, Storage, Software, Intelligent Edge, High Performance Computing and Mission Critical Solutions – with a consistent experience across all clouds and edges, designed to help customers develop new business models, engage in new ways, and increase operational performance. For more information, visit: www.hpe.com.

About RackTop

RackTop Systems is the pioneer of CyberConverged™ data security, a new market that fuses data storage with advanced security and compliance into a single platform. Engineered by U.S. Intelligence Community veterans, RackTop's BrickStor Security Platform is architected following a Zero Trust security model that protects data from ransomware, detects insider threats, and facilitates meeting complex data privacy and regulatory compliance requirements. BrickStor SP is a zero-impact, drop-in replacement for existing network attached storage (NAS) systems, which eliminates the cost, complexity, and added vulnerabilities of bolting on disparate security suites to legacy storage. The security platform also features an embedded transparent data mover, which can leverage third party cloud systems to tier archive data without sacrificing security or impacting customer experience. Headquartered in Fulton, Md., RackTop was founded in 2010 by cyber experts who have been solving the most complex data and security problems for more than two decades. RackTop's technology has been deployed at numerous organizations in a variety of industries worldwide, including government/DoD/public sector, media/advertising and entertainment, financial services, health care, higher education and life sciences.