Enhancing Cybersecurity with RackTop BrickStor Security Platform (SP) on Scale Computing Platform

As cyber threats are evolving at an unprecedented pace, safeguarding sensitive data from live ransomware attacks, insider threats, and data breaches has become paramount for all businesses. The synergy of BrickStor Security Platform, a cutting-edge cybersecurity solution designed for cyberstorage, with Scale Computing's robust hyper converged and edge computing infrastructure, provides a powerful shield against these threats in real-time.

Traditional file servers often suffer from complex management, scalability limitations, and security gaps. Modern file systems address these issues for customer success in ways traditional providers cannot. Another continuously rising issue with file-based storage is that it is the single most attacked dataset in customer's environments. In the past, most, if not all, attacks that have been reported were targeting the NAS or unstructured data.

Other studies have determined that most customers' data consists of 60-80% unstructured data, far exceeding former estimates. With the advent of modern-day ransomware attacks this data is of utmost criticality in protecting from data leakage and malware attacks.

File services are critical to the performance of enterprise operations. Running Windows file services to meet customer requirements is ineffective, creates more management workload, and adds tremendous security inefficiencies. NAS storage has attempted to alleviate some of these various operational issues, but the security model of most enterprise NAS solutions has offered nothing to address cyber security requirements, nor do they offer any additional Zero Trust capabilities.

RackTop BrickStor Security Platform (SP) is a software-defined scale-up file storage solution designed to address many use cases. RackTop offers the essential enterprise-level file storage capabilities, such as SMB/NFS, multiprotocol access, Active Directory integration, data reduction, user/share quotas, clones, snapshots, data tiering, and replication, in addition to being the only end-to-end cyberstorage solution that can stop ransomware, insider threats, and data extortion in under a second.

BrickStor SP provides the ability to prevent data exfiltration from privileged and trusted users, as well as stopping malware at the storage processor, while ensuring production data remains online and available to all uncompromised users.

BrickStor SP can be deployed within Scale Computing HyperCore clusters, thus resulting in a solution that delivers infrastructure consolidation. When deployed as Virtual Appliance additional capacity and physical resources can be added with minimal disruption to production environments.

Key Benefits:

REAL-TIME THREAT DETECTION

BrickStor SP offers real-time threat detection capabilities, identifying and neutralizing cyber threats the moment they emerge, ensuring immediate response to potential security breaches.

BEHAVIORAL ANALYSIS AND MACHINE LEARNING

Leveraging advanced technologies such as machine learning and behavioral analysis, the platform accurately detects malicious activities and distinguishes them from legitimate user actions, reducing false positives and negatives.

AUTOMATED INCIDENT RESPONSE

The platform automates incident response procedures, allowing for swift containment and mitigation of threats without manual intervention, minimizing the impact of cyber incidents.

SEAMLESS INTEGRATION

Scale Computing Platform allows seamless integration of BrickStor SP, providing a stable and scalable infrastructure that supports the security solution's robust functionality.

FASTER TIME TO VALUE, WHERE YOU NEED IT

Scale Computing Platform brings simplicity, high availability and scalability together, for the data center, distributed enterprise, and edge computing replacing the existing infrastructure and providing high availability for running VMs in a single, easy-to-manage platform.

Stopping Live Ransomware Attacks

Ransomware attacks have become increasingly sophisticated, targeting critical data assets and paralyzing organizations. BrickStor Security Platform utilizes advanced threat detection algorithms, behavioral analysis, and machine learning to identify ransomware patterns in real-time. By promptly detecting and isolating affected files or systems, the platform prevents the encryption of data, thwarting ransomware attacks before they can cause any harm.

Mitigating Insider Threats

Insider threats pose a significant risk, as employees and authorized users have access to sensitive data. The BrickStor Security Platform employs user behavior analytics and anomaly detection to identify unusual activities that might indicate an insider threat. By continuously monitoring user behavior and access patterns, the platform can detect and mitigate malicious activities, ensuring that only authorized actions are performed within the system.

Preventing Data Breaches in Real-Time

Data breaches can have severe consequences, including reputational damage and financial losses. The BrickStor Security Platform provides real-time monitoring of data access and movement. Any unauthorized attempt to access or transfer sensitive data triggers instant alerts and automated responses, preventing data breaches before they occur. Scale Computing's robust infrastructure ensures seamless integration and high availability of the security platform, guaranteeing uninterrupted protection against breaches.

The solution between RackTop's BrickStor Security Platform and Scale Computing Platform offers comprehensive, real-time defense against live ransomware attacks, insider threats, and data breaches. By implementing this integrated solution, organizations can fortify their cybersecurity posture, protecting valuable assets and sensitive information from evolving cyber threats. Don't wait for a cyber incident to occur; secure your organization's future with the powerful combination of BrickStor SP and Scale Computing Platform. Embrace proactive cybersecurity and experience peace of mind in the face of today's digital threats.