Fortifying Cyber Resilience: The Power of Defense-in-Depth from Pure Storage and Rubrik

Summary

Cyberattack vectors are evolving quickly and constantly. A new comprehensive reference architecture from Pure Storage and Rubrik provides a multi-layered approach that strengthens cyber resilience.

[bws_pdfprint display='pdf,print']

Renowned castle architect, Master James of Saint George, was an early advocate of defense-in-depth strategies. In the Middle Ages, he protected the realm's most valuable asset, his patron, King Edward I, by designing layered defense systems of moats, inner and outer walls, turrets, and battlements.

More than 500 years later, we're still building multi-layered defenses to protect our valuable data and keep the bad guys at bay. But unlike the Middle Ages, in the digital age, attack vectors evolve rapidly and constantly. This evolving threat landscape requires a more sophisticated, automated, cyber-resilient architecture to ensure comprehensive data security.

A Joint Reference Architecture

A modern cyber-resilient strategy delivers multiple layers of security, such as anomaly detection, encryption, immutable snapshots, and even SLAs, to protect against malicious attacks. By creating layered defenses, organizations can ensure that even if one security layer is compromised, others remain intact, thereby enhancing overall resilience and reducing the risk of costly data breaches.

That's why Pure Storage and Rubrik have collaborated to create a comprehensive reference architecture that addresses the critical challenges of data security and cyber resilience. Here are some of the key features and benefits of our multi-layered approach:
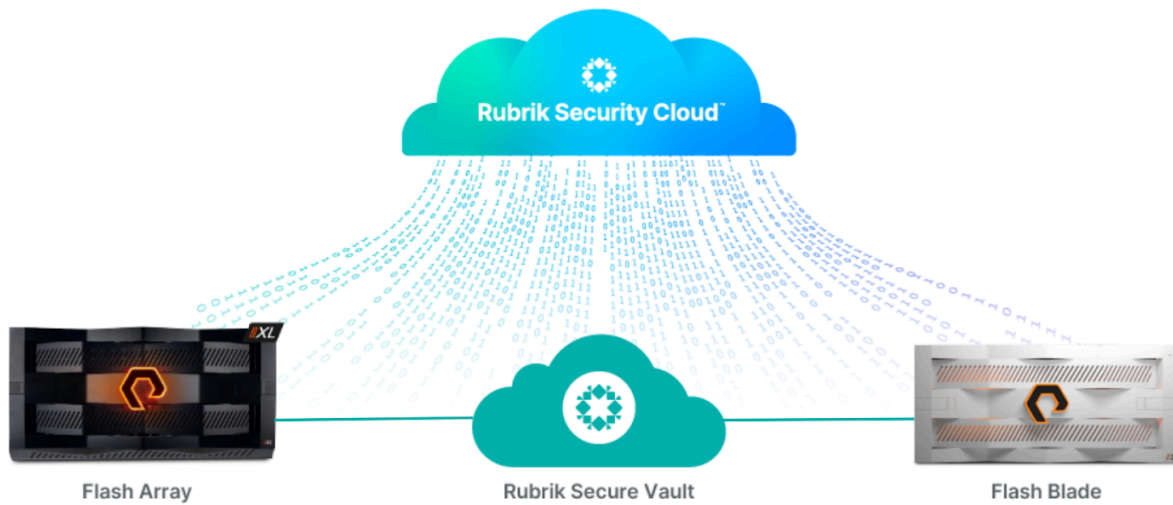
Figure 1: Reference architecture for Rubrik and Pure Storage solutions.

SafeMode-protected Snapshots: Pure Storage® SafeMode™ is our first layer of defense, preventing data from being altered or deleted. These immutable, indelible snapshots provide privileged user attack protection for recovery points with RPO as low as one hour.

Pure Storage vSphere Client Plugin: Pure Storage's plugin for vSphere supports easy storage provisioning and management via Storage Policy Based Management (SPBM), provides orchestration for recovering VMs from SafeMode-protected snapshots, and can even manage replication of those snapshots to provide DR testing and orchestrated failover.

Centralized Security Posture Analysis: Pure1® provides complete visibility and insights across all production workloads, ensuring that all data is protected

with best practices.

Anomaly Detection: Pure Storage's AI-driven fleet-wide monitoring also detects anomalous behavior and trends, quickly pinpointing compromised data sets and identifying healthy recovery points from your snapshots. Rubrik adds to the defenses with machine learning to detect deletions, modifications, and encryptions, determining the scope of cyberattacks for optimal ransomware investigation.

Threat Monitoring: Rubrik automatically identifies indicators of compromise within backups using an up-to-date feed of threat intelligence and performs incremental catalog analysis when new recovery points are introduced.

Threat Hunting: Rubrik analyzes the history of data for indicators of compromise (IOCs) to identify the initial point, scope, and time of infection, adding the ability to hunt for zero-day attacks.

Data Security Posture Management (DSPM): Rubrik's DSPM helps customers proactively reduce the risk of data exposures and exfiltration across on-premises, cloud, and SaaS environments.

Sensitive Data Monitoring: Rubrik helps customers manage exfiltration risk by discovering sensitive data types and their locations, leveraging its web-scale architecture for performance analysis on new recovery points.

User Intelligence: Integration with Microsoft Active Directory and Rubrik's Sensitive Data Monitoring allows customers to identify critical data exposure and reduce unqualified access.

Ransomware Response Team: Rubik's skilled Ransomware Response Team assists customers in responding to and recovering from ransomware attacks.

Ransomware Warranty: Rubrik offers a $10 million ransomware recovery warranty for Enterprise Edition customers adhering to best practices.

Cyber Recovery and Resilience SLAs: With an Evergreen//One™ subscription, Pure Storage guarantees a clean recovery array shipped within 24 hours, including a full recovery plan, data transfer rate, and bundled professional services.

A Castle with Layers Endures

This partnership between Pure Storage and Rubrik ensures your data remains protected through advanced automation, enabling quick and efficient backup and recovery. Our collaboration strengthens cyber resilience by offering robust tools for deep visibility into data sensitivity and potential threats. These tools are designed to detect anomalies and other indicators of compromise, empowering businesses to identify and respond to security risks before they escalate.

Together, Pure Storage and Rubrik deliver a comprehensive solution that secures data and ensures it can be swiftly restored in the event of an attack, giving customers the confidence to navigate today's ever-evolving cyber threats.

Learn more about our partnership and our new cyber-resilience reference architecture.

Hacker's Guide to Ransomware Mitigation and Recovery

[Read the Guide](#)

Ebook

A Hacker's Guide to Ransomware Mitigation and Recovery

By Hector Xavier Monsegur and Andy Stone

PURESTORAGE®

WRITTEN BY:

[Brian Ferrar](#)

Data Defenders

Learn more about our partnership with Rubrik.

Find Out More