

WHITE PAPER

Rubrik and Pure Storage Cyber Resilience Stack

Cyber recovery with near-zero RTO

Contents

- Executive overview** 3
- Audience** 3
- Data security and cyber resilience challenges** 3
- The missing pieces** 4
 - Solution overview 4
 - New integration: cyber resilience visibility 5
- Solution components** 6
 - Unified block and file storage 6
 - Data security 7
 - Archival location 8
- Deployment recommendations** 8
 - Pure Storage FlashArray 8
 - Rubrik Security Cloud 9
- The benefits** 10
 - Keeping data secure and available 10
 - Stay protected with automation 11
 - Efficient backup and recovery 11
 - Enable cyber resilience 13
- Summary** 14
- Learn more** 14



Executive overview

This document explores the challenges of modern data security and describes a joint solution between Rubrik and Pure Storage® that addresses these issues. As cyber threats grow in sophistication and data footprints increase, many organizations face challenges securing, managing, and recovering their data. Rubrik and Pure Storage have combined their advanced data security, data protection, and cyber-resilient storage technologies to create a comprehensive, layered solution ensuring cyber resilience. This solution simplifies protection at scale with a Zero Trust architecture, automated discovery, threat detection and remediation, and policy-driven workflows, integrating best-in-class data security, rapid recovery capabilities, and long-term data retention.

A newly introduced cyber resilience visibility integration further strengthens this stack by blending the speed of Pure Storage indelible SafeMode™ Snapshots with the intelligent threat analytics of Rubrik Security Cloud, enabling quick and clean cyber recovery of large data sets directly on the array. Rubrik and Pure Storage empower organizations to protect their critical data and ensure business continuity in the face of evolving cyber threats. This document helps IT decision-makers understand how the combined offerings meet the growing demands for secure, scalable, and resilient data infrastructure.

Audience

This document is intended for IT decision-makers, security professionals, and business leaders responsible for ensuring their organization's data security, availability, and resilience, including chief information officers (CIOs), chief information security officers (CISOs), IT directors, data protection officers, system architects, and administrators. The content is particularly relevant to those facing the challenges of safeguarding critical data against cyber threats, managing large-scale data growth, and ensuring rapid recovery in case of a breach or system failure. Organizations focusing on enhancing their cybersecurity posture and seeking a reliable, scalable solution for data protection and storage will benefit from understanding how the combined offerings of Rubrik and Pure Storage can deliver an effective, layered defense to achieve cyber resilience.

Data security and cyber resilience challenges

Organizations today face unprecedented challenges in data security and cyber resilience. Cyber threats are intensifying, with the average data breach cost in the [US soaring to \\$9.36M](#). Yet, [70% of organizations fail to store backups offsite or secure them as immutable](#), making them vulnerable to sophisticated attacks. Alarming, attackers target backups in [96% of cyber incidents and achieve partial success in 74%](#) of cases, often rendering all copies of data unusable. As everything becomes digitized, data availability is increasingly critical to business survival.

Attackers frequently operate within the network perimeter and remain undetected until the damage is done, resulting in extended downtime, lost revenue, and significant recovery costs. The resulting repercussions may include compliance failures, regulatory fines, irreparable damage to brand and reputation, and lawsuits from affected stakeholders. The exponential growth of data compounds these challenges, with 40% of organizations needing compliance policies for backups, and manual intervention often introduces errors. The risk escalates as data footprints expand, with [66% of IT and security leaders reporting that data growth outpaces their ability to secure it](#).

Recovery efforts are further complicated by unpredictable and inconsistent performance over time, increasing the complexity of data recovery. The lack of visibility into data, including what is stored and where, impedes comprehensive threat detection. The absence of robust forensic capabilities makes it difficult to identify infected systems and prevent reinfection. Despite many security tools, the sheer volume of attacks and the rise of zero-day threats render prevention insufficient. A lack of visibility into data sensitivity and user access further exacerbates the risks.

In this volatile environment, organizations must prioritize cyber resilience, ensuring data security, availability, and quick recovery capabilities to safeguard against threats and maintain business continuity.



The missing pieces

Despite the growing sophistication of cyber threats, many organizations still need critical components to ensure comprehensive cyber resilience. Keeping the data secure and available for cyber recovery remains a required capability as businesses struggle to secure their data with air-gapped, immutable, and access-controlled backups. Organizations are only fully protected with a defense-in-depth strategy that protects data, defends itself from threats, and eliminates single points of failure.

Simplifying protection at scale via automation is another gap that organizations face. The sheer volume of data growth requires automated discovery and policy-driven workflows to enforce security at scale, yet many rely on manual processes, introducing risk. A subscription-based model ensures solutions evolve and improve over time, while the ability to scale as needed prevents wasteful overprovisioning. Operational simplicity is crucial, with Zero Trust security at the core of any scalable, secure data environment. Moreover, a validated architecture with Rubrik and Pure Storage allows organizations to create a minimum viable business recovery environment, ensuring that even during a cyberattack, recovery can be achieved with minimal downtime.

To truly enable cyber resilience, organizations must secure their data and gain visibility into their sensitive data and user access. Many struggle to assess their data's security posture, understand the nature of the threats they face, and evaluate the health of their data catalog. These insights are necessary, as recovery timelines will remain long and uncertain without them. The ability to identify and contain attacks quickly, coupled with optimized flash performance at scale, can significantly reduce recovery times, allowing organizations to recover from cyber incidents faster and more effectively.

Solution overview

The joint solution provided by Rubrik and Pure Storage takes data security to the next level by strategically combining the power of Rubrik with Pure Storage. The result is a holistic cyber resilience foundation that aligns perfectly with the original 3-2-1 and updated 3-2-1-1-0 rules for data protection. This widely recognized best practice advises that organizations maintain three copies of their data stored on two different media types—one copy offsite, one copy offline or immutable, and zero errors within the backup data. Rubrik and Pure Storage address this with a seamless, scalable architecture that protects data at every level.

Pure Storage FlashArray™ provides primary storage with industry-leading performance and reliability. FlashArray has the advanced ability to instantly create and restore immutable snapshots to support ultra-low recovery point objectives (RPOs) and recovery time objectives (RTOs), ensuring business-critical data can be rapidly recovered during an attack. With SafeMode-enabled immutable and indelible snapshots, these primary storage snapshots are protected against tampering or deletion by malicious actors, preserving data integrity even if administrator credentials become compromised.

Rubrik Secure Vault extends Pure Storage FlashArray data protection capabilities by providing a secondary backup copy, ensuring two copies of data are stored on different media types. Built on Zero Trust principles that assume a breach will occur, Rubrik Secure Vault creates an immutable copy of production data using a proprietary append-only file system, which prevents any changes or modifications from the moment the data is backed up. This secure vault delivers ultra-low RPOs and RTOs with short-term retention, allowing quick recovery if primary data copies are compromised or lost.

Supporting compliance, monthly and annual backups are moved from Rubrik Secure Vault to Pure Storage FlashBlade® for long-term retention and offsite data protection. Whether maintaining compliance or keeping critical data protected for extended periods, this architecture ensures data is safeguarded on an offsite copy, aligning with the “offsite and offline or immutable copy” principles of the 3-2-1-1-0 rule.



Layered into this comprehensive solution is Rubrik Security Cloud, which adds a powerful dimension of advanced data security and intelligence. Rubrik Security Cloud provides continuous data security posture monitoring, offering detailed insights into where sensitive data is located and the protection status of all data across the hybrid-cloud environment. Its robust threat monitoring and hunting capabilities allow for identifying suspicious activity and potential cyber threats, proactively defending against ransomware, malware, and other attacks. Threat hunting also allows for analyzing backup snapshots, providing critical insights against zero-day vulnerabilities that help avoid malware reinfection during recovery. The platform also delivers actionable user intelligence, helping organizations understand who has access to what data and respond to abnormal behavior patterns that could indicate security breaches.

New integration: cyber resilience visibility

Rubrik and Pure Storage have expanded their existing cyber resilience stack with the new cyber resilience visibility integration, which combines the speed of Pure Storage indelible SafeMode Snapshots with the intelligence of Rubrik data threat analytics. This empowers customers to identify and respond to threats, providing the fastest RTO possible and ensuring data is safe for operations, preventing reinfection.

This integration provides the following benefits:

- **Threat pinpointing:** Identify threats directly within Rubrik backups of virtual machine (VM) workloads running on Pure Storage.
- **Comprehensive threat identification:** Detect and identify threats, anomalies, and quarantined recovery points in Pure Storage production data and snapshots.
- **Proactive remediation and recovery:** Proactively remediate and intelligently recover your data.
- **Near-zero RTO:** Achieve near-zero RTOs, with capabilities like hundreds of terabytes recovered in seconds.
- **Guaranteed clean recovery:** The solution uniquely combines Pure Storage SafeMode Snapshots with Rubrik ransomware detection to help customers identify and recover only verified clean data.

Here's how Rubrik and Pure Storage, working together, deliver a clean recovery:

- **Proactive threat hunting:** Rubrik protects your VMware workloads running on Pure Storage FlashArray, indexing and hashing all data. Rubrik continuously scans these hash indexes for indicators of compromise (IOCs), entropy, and anomalies (like encryption), providing deep file inspection to uncover threats early.
- **Automated threat tagging:** When Rubrik detects a threat or anomaly, it automatically labels the infected data.
- **Unified visibility in Pure1®:** Pure1 workflow automation then queries the Rubrik Security Cloud for any identified threats, anomalies, or quarantined backups, correlating them with the Pure Storage FlashArray volumes and snapshots on which they reside.
- **Actionable intelligence:** Pure1 workflow automation then tags the specific Pure Storage volumes and snapshots identified by Rubrik as containing threats. This provides your security teams with immediate, clear insight into compromised data, allowing you to bypass guesswork.



When ransomware or another type of disaster strikes, orchestrated application recovery enables fast, automated recovery across on-premises, cloud, or hybrid environments. This automated recovery workflow ensures applications are brought back online swiftly and accurately, minimizing downtime and mitigating the operational impact of a cyberattack. The integration of Rubrik Security Cloud enhances the joint Rubrik and Pure Storage solution by providing an all-encompassing security framework that protects data and enables intelligent monitoring, fast recovery, and proactive defense strategies.

By combining best-in-class primary storage, data security, and long-term retention with Rubrik Security Cloud's advanced security posture and intelligence capabilities, this joint solution offers a holistic approach to cyber resilience. It empowers businesses with the tools to defend against modern cyber threats while ensuring continuity and recovery at scale.

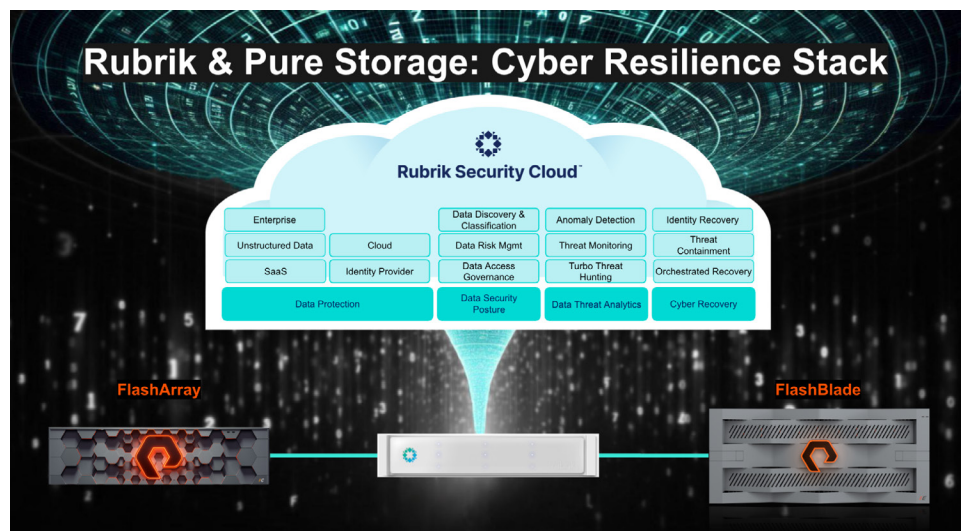


FIGURE 1 Solution overview and logical diagram

Solution components

We've emphasized that achieving true cyber resilience requires a multi-layered defense strategy. Now, let's dive into the critical components of the Rubrik and Pure Storage-validated architecture for superior cyber resilience. Robust, layered protection is powered by the seamless integration of cutting-edge solutions from Rubrik and Pure Storage, working together to deliver maximum security and peace of mind.

Unified block and file storage

For this validated architecture, the Pure Storage FlashArray family of unified block and file storage arrays provides unmatched performance, Zero Trust security, durability, and scalability, serving as the first layer of defense against cyberattacks.

The FlashArray family of all-flash storage arrays offers customers many options to support performance and capacity requirements.

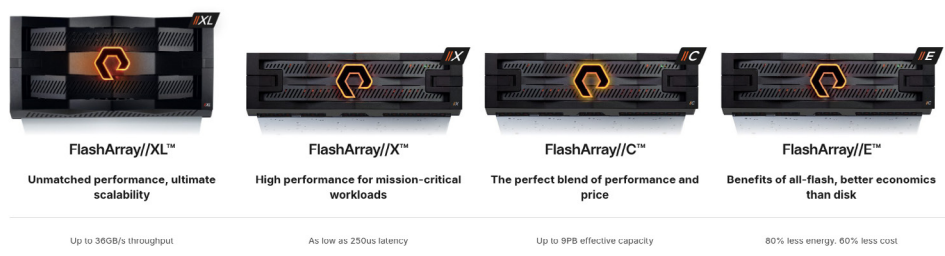


FIGURE 2 FlashArray family of all-flash storage arrays



Data security

Rubrik Security Cloud and Rubrik Secure Vault deliver complete cyber resilience for data stored on the Pure Storage FlashArray. As a crucial second layer of protection, Rubrik Secure Vault creates an immutable, onsite backup, ensuring rapid recovery during data loss or a cyberattack. The Rubrik Secure Vault r7000 series offers flexible starting configurations, enabling seamless scalability to accommodate data growth and evolving security demands.



FIGURE 3 Rubrik Secure Vault r7000 starting configurations

Note: In addition to Rubrik’s r7000 product line, Rubrik Secure Vault can be deployed on various third-party hardware options.

The Rubrik Security Cloud Enterprise Edition license provides a centralized management platform for all Rubrik Secure Vault deployments. Beyond centralized control, it allows organizations to fully leverage Rubrik’s comprehensive suite of data security solutions, addressing compliance and data protection needs across their environments. Rubrik Security Cloud’s core strengths include a native Zero Trust architecture with immutable, air-gapped backups; strict access controls; built-in encryption; multi-factor authentication (MFA); and role-based access management. It also features integrated threat detection with continuous scanning for ransomware activity and anomalies, providing real-time visibility and proactive risk mitigation through anomaly detection, threat monitoring (for IOCs), and threat hunting (to prevent malware reinfection and identify zero-day attacks).

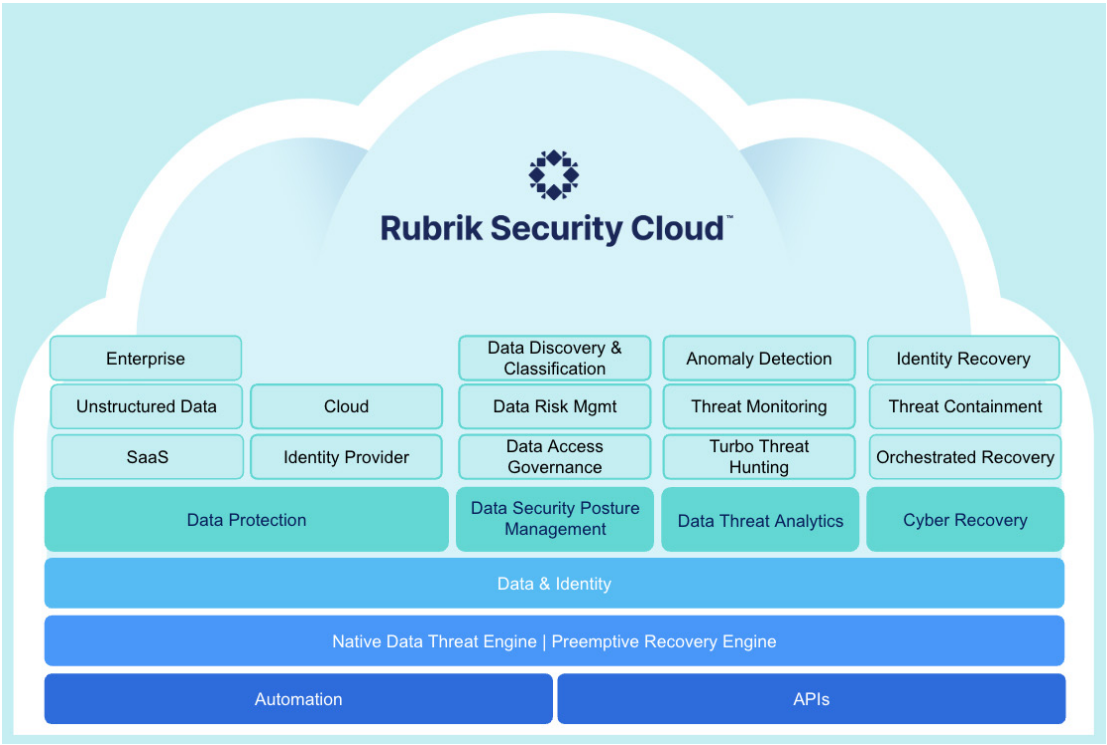


FIGURE 4 Rubrik Security Cloud features

Archival location

The Pure Storage FlashBlade product line offers a range of configuration options for archival and long-term retention. It delivers massive scale-out and immutable, secure, cost-effective storage designed for petabyte-scale recovery, even for data stored over extended periods.

Both the performance-optimized FlashBlade//S™ and the economical-at-scale FlashBlade//E™ can be leveraged for the archival location, offering flexibility based on customer needs.

For guidance on architecting and properly sizing these components, contact your Rubrik and Pure Storage sales representatives.

Deployment recommendations

Now that we've reviewed the required and supported components, let's examine the recommended Rubrik and Pure Storage configuration and protection policies. While this is not an exhaustive list or a complete deployment guide, it serves as a reference for critical Pure Storage Protection Groups and Rubrik SLA Domain policies.

Pure Storage FlashArray

Auto-on SafeMode on Pure Storage FlashArray automatically protects all your data from accidental or malicious threats by default, with no additional effort required. This establishes the initial layer of defense for your primary data infrastructure. We recommend adjusting the default policy as follows to create hourly recovery points.

1. Adjust the **pgroup-auto** protection group snapshot schedule to create snapshots every hour and retain them for three days, then retain four snapshots from each day for an additional five days. Note that specific workloads may benefit from more or less aggressive frequency and retention. This is intended as a general guideline for the majority of environments.
2. Verify that the SafeMode Retention Lock feature is set to ratcheted. Auto-on SafeMode automatically does this for you, as shown in Figure 5.

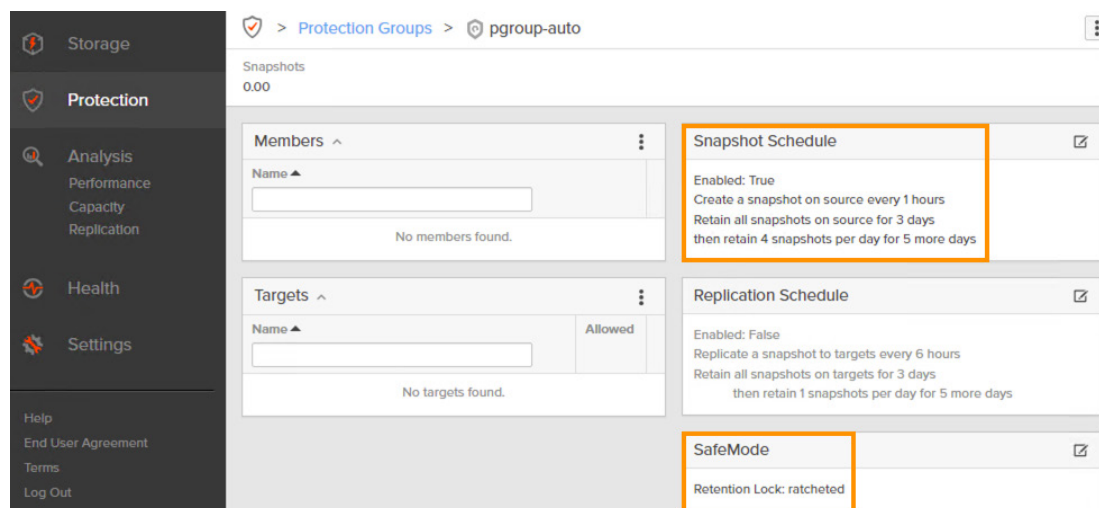


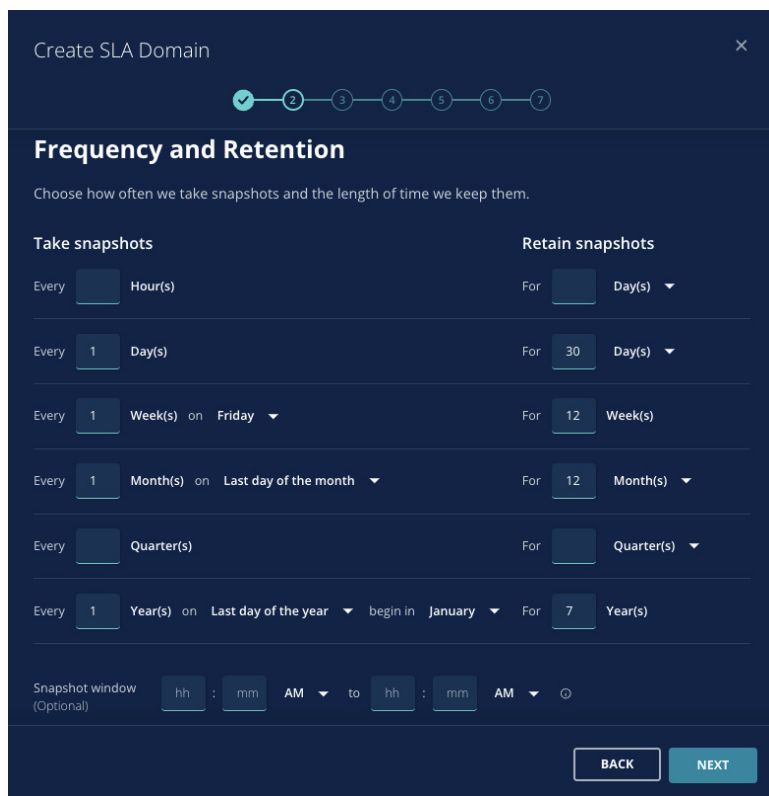
FIGURE 5 Pure Storage FlashArray snapshot policy configuration with Auto-on SafeMode

Rubrik Security Cloud

Define your data protection SLA Domains to create Rubrik snapshots as follows (shown in Figure 6).

- Every **1** Day(s)—retain For **30** Day(s)
- Every **1** Week(s)—retain For **12** Week(s)
- Every **1** Month(s)—retain For **12** Month(s)
- Every **1** Year(s)—retain For **7** Years (depending on business internal policies/regulatory requirements)

Although your business and regulatory needs may vary, the key is to ensure overlapping recovery points on the Pure Storage FlashArray, Rubrik Secure Vault, and Pure Storage FlashBlade in case of a data loss event.



Create SLA Domain

Frequency and Retention

Choose how often we take snapshots and the length of time we keep them.

Take snapshots	Retain snapshots
Every Hour(s)	For Day(s)
Every Day(s)	For Day(s)
Every Week(s) on	For Week(s)
Every Month(s) on	For Month(s)
Every Quarter(s)	For Quarter(s)
Every Year(s) on begin in	For Year(s)

Snapshot window (Optional) : AM to : AM

BACK NEXT

FIGURE 6 SLA Domain configuration

Now, enable archiving and ensure you have defined the Pure Storage FlashBlade as the archive location.

1. Archive backups after 30 days to Pure Storage FlashBlade. Some of the weekly and all monthly and yearly backups created by Rubrik will reside in the Pure Storage FlashBlade archive. The overlap of RPOs creates a layered approach to protecting the data, with three times daily RPOs living on both FlashArray and Rubrik Secure Vault.
2. Optionally, enable Instant Archive on the Rubrik SLA to copy all backups in Rubrik to the Pure Storage FlashBlade immediately after backup completion, providing lower RPOs with the immutable archive copy. Archiving to Pure Storage FlashBlade allows administrators to recover the entirety of the catalog from the archive in the unlikely event that both the FlashArray and Rubrik Secure Vault are destroyed or compromised.

Note: The use of Instant Archive does result in additional storage consumption on the archive/long-term retention target (Pure Storage FlashBlade), as recovery points that would typically only reside on Rubrik are also located in the archive.

The benefits

Combining three best-in-class solutions from Rubrik and Pure Storage allows organizations to build a defense-in-depth strategy for their intellectual property. These three tiers provide critical features and functionality that improve an organization's cyber resilience. When deployed according to best practices, they create a solution that helps mitigate risk to data by providing the best chance for a fast recovery. Understanding each feature and its role in securing the data is a critical first step in establishing a cyber-resilient foundation across hybrid-cloud environments.

Keeping data secure and available

As organizations strive to fortify their data security at every level, Pure Storage and Rubrik offer powerful, complementary features that enhance recovery success. Together, they deliver a robust defense system designed to tackle the unavoidable challenges of data protection. By equipping administrators with diverse tools and options, Pure Storage and Rubrik ensure that data remains secure and accessible whenever needed.

- **FlashArray immutable snapshots:** Pure Storage FlashArray offers natively immutable copies of all production data stored immediately adjacent to production workloads. These snapshots provide a first line of defense and can be configured as frequently as every five minutes.
- **SafeMode governance:** Full privileged user attack protection for all copies of data on the Pure Storage platform means that bad actors cannot modify, encrypt, or delete snapshots from the Pure Storage FlashArray.
- **Fleet-wide security and data protection visibility:** Pure Storage and Rubrik offer complete analysis across all production workloads for AI-driven insights into data protection posture and recommendations.
- **Immutable file system:** Rubrik Secure Vault leverages a proprietary append-only file system that does not allow changes or modifications from the first backup. It runs atop a hardened Linux operating system with no shell access, forming the bedrock of Rubrik's Zero Trust architecture.
- **Air gap:** Rubrik's backups do not need Network File System (NFS) or Server Message Block (SMB) network protocols, which are common attack vectors for bad actors, making it difficult for them to find customer data.
- **Access controls:** Rubrik's granular role-based access controls (RBAC); mandatory, natively enforced MFA; and time-based, one-time passwords (TOTP) prevent unauthorized access to the platform, which is the most common method of compromise faced by organizations today.
- **Intelligent data lock:** Rubrik's intelligent recycle bin holds data longer when anomalous activity is detected to prevent bad actors from deleting data, providing another failsafe against malicious or accidental deletion.
- **Retention lock with Network Time Protocol (NTP) protection:** Rubrik QAuth Retention Lock establishes rules to prevent malicious changes to retention policies from prematurely aging or deleting data and disrupting recovery operations. NTP protection keeps bad actors from tampering with NTP to prematurely age data during its security life cycle.
- **End-to-end encryption:** Rubrik's encryption in flight and at rest adds a layer of security against physical breaches and man-in-the-middle attacks.
- **Data Security Command Center (DSCC):** Rubrik's DSCC identifies security gaps, quantifies data risk, and creates actionable recommendations to improve data security posture.
- **Object Lock immutability on Pure Storage FlashBlade:** Rubrik and Pure Storage FlashBlade integrate to create indelible copies in the archive, preventing bad actors from altering or deleting protected data while also leveraging the bucket to secure a recoverable copy of Rubrik's backup catalog.



Stay protected with automation

Pure Storage and Rubrik have partnered to develop cutting-edge data management solutions that scale with their customers' evolving needs. This strategic partnership leverages Pure Storage data architecture expertise with Rubrik's innovative web-scale data security technology to create a robust, adaptable foundation for cyber resilience that scales alongside the data footprint. Together, they empower businesses to manage, analyze, and optimize their data more efficiently, ensuring seamless growth and a competitive edge in an increasingly data-driven world. The following features automate and simplify data protection so that every additional byte is as safe and secure as its predecessors.

- **Default protection groups:** Auto-on SafeMode automatically protects new Pure Storage FlashArray workloads with indelible snapshots, automating the configuration of newly created workloads and helping establish the first line of defense in this joint solution.
- **vSphere plug-in for FlashArray:** The Pure Storage vSphere plug-in enables automatic protection for production VMware workloads through storage policy-based management.
- **Automated discovery:** Rubrik automatically discovers data as it is created across physical systems—operating systems, VMs, databases, file systems, and containers—ensuring that all data is automatically protected according to data governance policies as soon as it is generated.
- **Automated policies:** From backup frequency and retention to replication and archival, replace hundreds or thousands of backup jobs with just a few policies with Rubrik. These automated policies can be assigned to the infrastructure itself to auto-protect new workloads, minimizing the risk of an overlooked workload as the environment scales. Rubrik SLA Domains incorporate frequency, retention, archive, and replication requirements without needing separate jobs to establish the 3-2-1 methodology.

Efficient backup and recovery

Legacy architectures and data protection products were designed for a time when data volumes were smaller and less complex, making them ill-suited for today's expansive and dynamic data environments. As businesses generate and rely on vast amounts of data, these outdated systems struggle to keep pace, leaving companies vulnerable and unable to protect their critical information effectively. Recognizing this gap, Pure Storage and Rubrik have partnered to develop innovative features and product offerings that are purpose-built to scale with modern data footprints, providing the robust security and adaptability that today's businesses demand.

- **vSphere plug-in for FlashArray:** The Pure Storage vSphere plug-in provides full VM recovery from array snapshots from the vSphere client, allowing end users to recover from array-based snapshots in seconds.
- **Massively scalable and performant platforms:** Pure Storage and Rubrik scale to meet the needs of the most demanding enterprises, with performance-optimized recovery to support the lowest possible RTO.
- **VMware snapshots:** Pure Storage and Rubrik leverage the incremental-forever vSphere vStorage API – Data Protection (VADP)-based VM backups, allowing for faster backups and incremental recovery. Now, even the trickiest workloads can enjoy incremental-forever VADP-integrated snapshots via API-based snapshot integration.
- **I/O stun prevention:** Pure Storage array snapshots minimize VMware snapshot lifespan to seconds, preventing I/O stun.
- **Rapid recovery:** With the cyber resilience stack by Rubrik and Pure Storage, customers can recover petabytes of data within hours. The new cyber resilience visibility integration further accelerates this by enabling near-zero RTOs, allowing the restoration of hundreds of terabytes in seconds by leveraging Rubrik's ability to identify recovery-ready Pure Storage snapshots.



- **Flexible retention:** Pure Storage and Rubrik provide local, remote retention and cloud archiving to meet regulatory requirements, reduce costs, and provide optimal recovery performance.
- **Cyber recovery:** Access critical applications within a clean room infrastructure through Rubrik Cyber Recovery, an integrated workflow that allows administrators to analyze troubled workloads before promoting them to production. This is enhanced by the new cyber resilience visibility integration's ability to identify threats directly within Rubrik backups of VM workloads running on Pure Storage and within Pure Storage production data and snapshots, ensuring a guaranteed clean recovery.
- **Flash-speed backups:** Rapid backups minimize the impact on production. The Pure Storage primary storage flash arsenal allows Rubrik to protect terabytes of data rapidly thanks to minimal read latency. FlashBlade archive allows organizations to automate the data life cycle quickly and efficiently without sacrificing recovery speed.
- **Hyperconverged platform:** Rubrik's unique architecture reduces complexity and hardware with a scale-out architecture that provides the fastest results. Adding nodes to Rubrik Secure Vault increases capacity and performance.
- **Incremental forever:** Rubrik leverages change region tracking to reduce local storage requirements and dramatically improve backup times. In addition, Rubrik automatically creates synthetic full backups to minimize the long recovery times commonly associated with incremental-forever technologies.
- **Application consistency:** Rubrik creates recovery points while an application is in a consistent state, enabling graceful application recovery.
- **Parallel streaming:** Rubrik's rapid data ingestion reduces backup times and provides scalability for even the largest enterprises, and the ability to stream from FlashArray dramatically improves performance to help achieve the lowest possible RPOs.
- **Flash archive economics:** The Pure Storage FlashBlade platform provides a cost-effective archive solution with long-term retention options, driving down costs without sacrificing performance and security.

Enable cyber resilience

Cyber resilience relies on a company's ability to defend against threats and recover quickly from them. Central to this is visibility into the sensitivity of the data, knowing who has access to it, and the ability to monitor the data for signs of infection or compromise. Without these insights, businesses are left vulnerable to breaches and data loss. To address these challenges, Pure Storage and Rubrik have partnered to create advanced layers of protection that enhance visibility and control. Their joint solution highlights potential vulnerabilities, ensuring businesses can confidently safeguard their critical assets.

- **Centralized security posture analysis:** Pure1 provides complete visibility and insights across all production workloads to ensure that all data is protected with best practices. Pure1 leverages advanced automation and AI-driven analytics to simplify storage management, optimize performance, and provide proactive health monitoring, predictive support, and intelligent capacity planning.
- **Anomaly detection:** Pure Storage provides AI-driven, fleet-wide monitoring for anomalous behavior and trends to help quickly pinpoint compromised data sets and find healthy recovery points from protected SafeMode Snapshots. Rubrik's anomaly detection determines the scope of cyberattacks by using machine learning to detect deletions, modifications, and encryptions for optimal ransomware investigation.
- **Threat monitoring:** Rubrik detects security threats early by automatically identifying IOCs within backups using an up-to-date feed of threat intelligence. This proactive analysis provides various options for threat feeds, including Mandiant, and performs incremental catalog analysis when new recovery points or YARA rules are introduced.
- **Threat hunting:** Prevent malware reinfection by analyzing the history of data for IOCs to identify the initial point, scope, and time of infection. Threat hunting adds the ability to hunt for zero-day attacks, acting as an on-demand analyzer for IOCs while leveraging the web-scale horsepower of the Rubrik cluster.
- **Data security posture management:** With Rubrik's data security posture management, customers can proactively reduce the risk of data exposures and exfiltration across on-premises, cloud, and software-as-a-service (SaaS) environments.
- **Sensitive data monitoring:** Rubrik customers can reduce sensitive data exposure and manage exfiltration risk by discovering what types of sensitive data they have and where they live. This asynchronous process leverages Rubrik's web-scale architecture to perform analysis on new recovery points, scaling the performance of the analysis alongside the data footprint.
- **User intelligence:** Thanks to Microsoft Active Directory integration and sensitive data monitoring, Rubrik customers can identify critical data exposure to reduce unqualified access.
- **Ransomware warranty:** Rubrik provides a \$10 million [ransomware recovery warranty](#) for Enterprise Edition customers who adhere to best practices.
- **Ransomware response team:** Support from the Rubrik Ransomware Response Team, skilled at responding to and recovering from ransomware attacks, is free to existing customers with a support contract. The team has guided hundreds of customers through successful recoveries from cyberattacks.
- **Cyber recovery and resilience SLAs:** With an Evergreen//One™ subscription, Pure Storage guarantees a clean recovery array shipped to you within 24 hours, which includes a full recovery plan, data transfer rate, and bundled professional services to get your business back as soon as possible.
- **Proactive remediation:** The new cyber recover visibility integration empowers you to remediate and intelligently recover your data, preventing reinfection preemptively.
- **Enhanced security analytics:** Leverage Pure Storage performance to accelerate security analytics tools (like log management), ensuring the resilience of even archived data.
- **Critical storage resilience:** Benefit from the inherent availability and data resilience of Pure Storage for critical workloads, providing a multi-layered, defense-in-depth strategy for your data, apps, and infrastructure.



Summary

Pure Storage and Rubrik partnered to address the critical challenges of keeping data secure and accessible in an increasingly complex digital landscape. Their collaboration and reference architecture ensure that data remains protected through advanced automation, allowing customers to back up and recover their information quickly and efficiently. By automating these processes, businesses minimize downtime, reduce the risk of data loss, and maintain the availability of their critical data assets without the need for constant manual intervention.

Beyond backup and recovery, this partnership strengthens cyber resilience by offering robust tools that provide deep visibility into data sensitivity and potential threats. These tools are designed to detect anomalies and other IOCs, empowering businesses to identify and respond to security risks before they escalate.

The new cyber resilience visibility integration further enhances this by empowering customers to pinpoint threats, achieve near-zero RTOs, and ensure guaranteed clean recovery by combining Pure Storage SafeMode Snapshots with Rubrik ransomware detection and threat analytics. 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

- [Learn about Pure Storage and Rubrik integration solutions.](#)
- Explore [Pure Storage cyber resilience.](#)