



Rubrik Security Cloud – Private

Data Sovereignty and Cyber Resilience for Regulated Industries

Regulators demand that sensitive data stays within defined borders. Your adversaries want to make sure you can never recover it. RSC-P lets you satisfy both without compromise.

THE CHALLENGE

Regulated industries are caught between two accelerating forces: cyber threats that specifically target recovery infrastructure, and compliance frameworks that restrict where data can live and who can touch it.

Data Residency Is No Longer Enough

Demonstrating that data sits within national borders is table stakes. Today, regulators demand exclusive organizational control over data, metadata, and the operational systems that manage it. Hyperscaler sovereign offerings frequently maintain governance ties to foreign parent companies, exposing organizations to extraterritorial legal demands even when data physically resides in-country. GDPR, DORA, NIS2, HIPAA, and sector-specific frameworks are increasingly prescriptive about jurisdiction, access, and control.

Attackers Go for Recovery First

Nation-state actors and ransomware groups have learned that destroying backup infrastructure is more effective than destroying production data. If you cannot recover, the leverage is infinite. Organizations need immutable, air-gapped recovery systems to access immutable and clean copies when primary infrastructure is fully compromised.

Legacy Platforms Create Risk, Not Reduce It

General-purpose operating systems, hypervisor dependencies, and fragmented management tools and control planes expand the attack surface with every new deployment. Identity infrastructure, the backbone of access control and business continuity, is left outside most recovery plans entirely.

THE SOLUTION

RSC-P brings cloud-inspired cyber resilience entirely within your security perimeter: no external cloud connections required, no third-party jurisdictional exposure, no compromise on isolation.

- **Dark Site:** R7K hardware appliance, fully within your security perimeter. Zero external dependencies after registration.
- **VM Form Factor:** Virtual deployment on your existing vSphere/ESXi infrastructure. No new hardware. Ideal for cost-sensitive environments.
- **Sovereign Cloud:** Virtual deployment in your own cloud tenant or subscription, under your jurisdictional control.
- **Hybrid:** On-premises and sovereign cloud managed from a single unified control plane.

Both the physical and virtual form factors run the same software stack with no external internet dependency after registration.

CORE VALUE PROPOSITION



Uncompromised Data Sovereignty and Compliance

Deploy Zero Trust Data Security entirely within your borders, eliminating dependencies on foreign-owned cloud infrastructure and the legal and geopolitical risks they carry. Your auditors get what they need. Your adversaries get nothing.



Definitive, Immutable Resilience

Immutable backups and a logical air-gap ensure a clean recovery copy is always available, even if attackers reach the hypervisor layer. Immutable backups on the R7K CDM cluster cannot be encrypted, deleted, or tampered with, even if attackers compromise your hypervisor. The system operates fully air-gapped after initial registration. No internet connection required. Your recovery works when everything else does not.



Strategic Autonomy

One platform replaces fragmented legacy tools without surrendering control to a single vendor or hyperscaler. Encryption keys stay under your control via KMIP-compliant key management, backed by FIPS 140-3 validated cryptography. You own your recovery. No exceptions.

ADDITIONAL CAPABILITIES

Compliance-Ready Data Residency

All data, metadata, and control plane operations remain within defined geographic or organizational boundaries, with no external cloud dependencies for advanced functionality.

Protect Petabyte-Scale Unstructured Data

NAS Cloud Direct protects massive file stores at line speed with a custom-built NFS/SMB client, multi-threaded parallel scanning, and a globally scalable metadata index. Eliminate the visibility gaps that leave your largest data stores exposed.

Recover Identity First

When Active Directory or Entra ID is compromised, everything downstream stops. Identity Recovery restores critical identity infrastructure independently of compromised systems, so access controls and business continuity are rebuilt before downstream applications come back online.

Consistent Control Across Every Site

One console manages protection policies, backup status, and compliance reporting across distributed and isolated environments, without breaking isolation requirements.

RUBRIK IS SECURITY & COMPLIANCE CERTIFIED



CONCLUSION

Compliance and resilience are not a trade-off. RSC-P delivers both: inside your borders, under your control, at the scale your organization requires.

[Request a demo briefing](#) with a Rubrik specialist.



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is the Security and AI Operations Company, delivering one platform built at the intersection of data, identity, and AI. The platform enables agentic cyber resilience and trusted AI operations for enterprises worldwide, built to recover before disruption strikes and stay a step ahead, so security is never the reason ambition stalls. For more information, please visit www.rubrik.com and follow Rubrik on LinkedIn and X.

brf-rsc-private-for-regulated-industries / 20260930

KEY CAPABILITIES



Advanced Threat Detection

ML-powered anomaly detection establishes baseline activity patterns and identifies deviations that may indicate ransomware or insider threats, using a two-phase analysis examining metadata changes and entropy scans, all without external connections.



Threat Monitoring

Always-on, continuous scanning of backup data for indicators of compromise using Rubrik threat intelligence feeds including YARA rules and file hashes. Set it once. It automatically ingests new threat intelligence and scans new snapshots without manual intervention.



Turbo Threat Hunting

On-demand scanning across thousands of backups in seconds. Security teams submit suspect hash values and RSC-P rapidly identifies all affected snapshots using pre-built hash catalogs, enabling fast scoping and confident identification of clean recovery points during active incidents.



NAS Cloud Direct

Protects petabyte-scale unstructured data at line speed with a custom-built NFS/SMB client, multi-threaded parallel scanning, and a globally scalable metadata index supporting billions of entries.



Identity Recovery

Orchestrate recovery of complex Active Directory Forest and Entra ID deployments. Granular object-level recovery, attribute comparison, and domain controller recovery all supported. Test and validate workflows before an incident occurs.



Orchestrated Application Recovery

Define recovery plans including boot order, resource mapping, and post-recovery scripts. Test procedures without impacting production systems. Recover complex, multi-application environments in minutes, not days.



Data Classification and Sensitive Data Discovery

Discover and classify sensitive information across the protected environment to support regulatory compliance, data governance, and residency mandates.



Air-Gapped Operation

No internet connectivity required for day-to-day operation after registration. Supports fully disconnected environments and organizations that prohibit external telemetry by default.