rubrik

Rubrik Security Cloud – Private

Cyber Resilience for US Federal Government

When nation-state actors target federal agencies, they don't go for production systems first. They go for your identity infrastructure, your backups, and your ability to recover. RSC-P is built for exactly this threat: delivering advanced cyber resilience, including threat detection and identity recovery entirely within your agency's security boundary.

THE CHALLENGE

Federal agencies are not facing a generic cyber threat. They are facing targeted, persistent adversaries who understand that destroying the ability to recover is more powerful than destroying data itself.

The lack of visibility into potential threats increases the problem:

- **Isolated tools, blind spots everywhere.**
  Dark sites and air-gapped environments require separate control planes. The result is visibility gaps that leave agencies unable to monitor backup health, enforce consistent policies, or coordinate recovery across distributed environments.
- **Identity infrastructure is the new primary target.**
  When Active Directory or Entra ID is compromised, downstream recovery is paralyzed. Every application, access control, and authentication flow depends on identity, and most agencies have no plan to restore it independently.
- **Security and scale should not be a trade-off.**
  Legacy backup solutions force agencies to choose: stay secure and sacrifice capability, or gain functionality at the cost of isolation. That choice is no longer acceptable.

THE SOLUTION

RSC-P brings full cyber resilience inside your security perimeter: no external connections required, no compromise on isolation. Flexible deployment options make it easy for government agencies to manage recovery at scale and consolidate distributed environments:

- **Dark Site (physical):** R7K hardware appliance, fully within your security perimeter. Zero external dependencies after registration.
- **VM Form Factor (Virtual):** RSC-P on your existing vSphere/ESXi infrastructure. No new hardware. Ideal for cost-sensitive environments or customers migrating to the latest version of RSC-P.
- **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.

KEY BENEFITS

Unified Visibility Across Every Site

One console manages every workload across dark sites, air-gapped environments, and distributed locations. Enforce consistent protection policies, monitor backup status, and generate comprehensive reports without breaking isolation requirements.

Detect, Hunt, and Respond Inside the Boundary

Always-on threat monitoring scans backup data continuously for indicators of compromise. When an incident hits with a previously unknown compromise signature, Turbo Threat Hunting scans thousands of backups in seconds to identify the last clean recovery point. Both operate entirely within your security boundary.

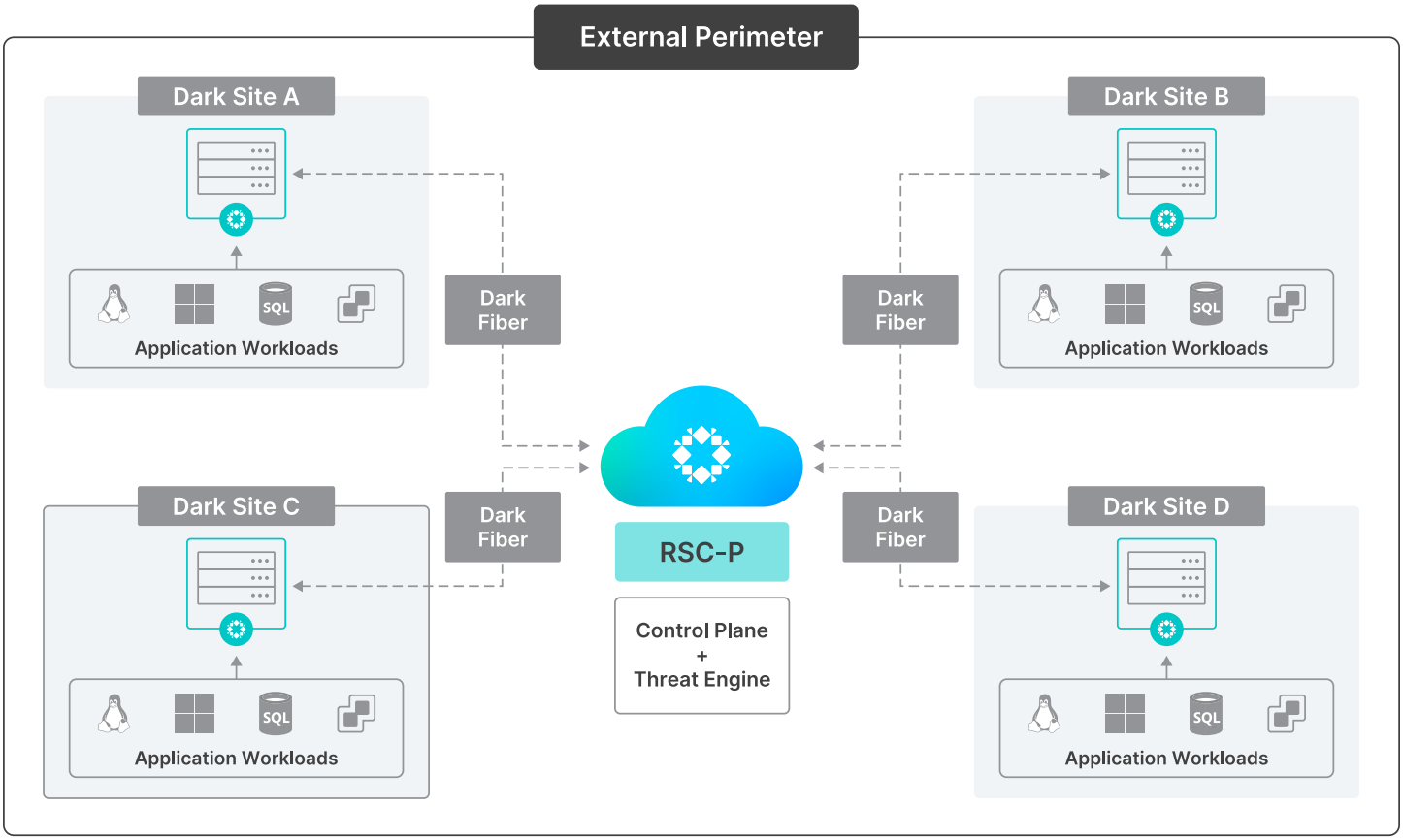
Recover Against Insider Threats

Identity Recovery orchestrates the restoration of Active Directory Forest and Entra ID independently of compromised systems. Restore critical identity infrastructure before downstream applications come back online, so recovery is sequenced correctly, not reactively.

Secure and Compliant by Design

Encryption keys stay under agency authority through Key Management Interoperability Protocol (KMIP)-integrated key managers, backed by FIPS 140-3 validated cryptography. On-demand compliance reporting gives you the documentation your auditors need, when they need it, without relying on external systems.

ARCHITECTURE



Control Plane

Runs entirely within the security perimeter, providing centralized management, policy enforcement, and monitoring across all protected workloads. Available as the R7K hardware appliance or as a VM on existing vSphere/ESXi infrastructure. Eliminates the need for separate management tools for CDM clusters or data planes across isolated environments.

Zero Trust Data Security

Immutable backups, end-to-end encryption, and role-based access control, all deployed within your security boundary. The R7K appliance delivers full hardware-layer immutability. Backups of the VM form factor can be done in an immutable storage.KMIP-managed key rotation ensures encryption keys remain under agency control at all times.

Threat Engine

ML-powered detection and classification operating entirely within your security boundary. Threat monitoring runs continuously against backup data; Turbo Threat Hunting provides on-demand, high-speed scanning across thousands of backups in seconds for active incident response.

KEY CAPABILITIES

Advanced Threat Detection

Anomaly Detection uses ML to establish baseline activity patterns and identify deviations that may indicate threats. A two-phase analysis examines metadata changes between backups and performs targeted entropy scans to assess malicious encryption, 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

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

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 Discovery and Classification

Discover and classify sensitive information across the protected environment. Customize classification rules to meet specific agency requirements and monitor sensitive data movement within security boundaries.

Air-Gapped Operation

No internet connectivity required for day-to-day operation after initial registration. All workflows meet air-gapped requirements for fully disconnected and classified environments.

RUBRIK IS SECURITY & COMPLIANCE CERTIFIED

FIPS 140-3 validated cryptography

Common Criteria EAL2+ Certified

DoDIN APL approved

CMMC 2.0 compliant

Customer Success

[Commander, Navy Installations Command] replaced fragmented backup tools with Rubrik and cut recovery times from hours to minutes, with 30-50% TCO reduction from a smaller data center footprint.

CONCLUSION

Federal agencies cannot afford to discover their recovery plan does not work during an active attack. RSC-P gives you the confidence to recover: from identity to applications to unstructured data, entirely within your security boundary.

Request a demo briefing with a Rubrik federal specialist.

rubrik

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-us-federal-government / 20260930