



End to End Google Workspace Protection

Secure Data. Recover Identity. Accelerate AI.

THE STRATEGIC SHIFT: FROM PRODUCTIVITY SUITE TO ENTERPRISE OS

Google Workspace has evolved from a simple collaboration tool into the primary operating system of the modern enterprise: where strategy is built (Calendar), relationships are managed (Contacts), teams are organized (Groups), and knowledge lives (Drive, Gmail). As the primary hub for mission-critical data and the central brain for enterprise AI, this evolution demands a shift from passive compliance archiving to active operational recovery.

THE VISIBILITY GAP: MODERN THREATS TO THE WORKSPACE

Relying on native protection creates a "shared fate" vulnerability where an environment compromise, whether from a malicious admin or a hijacked identity, can wipe out your production data and your only means of recovery.

- ✗ **The 25-Day Cliff:** Native trash buffers purge data permanently after 25 to 30 days. If a mistake or breach is discovered late, the data is gone forever.
- ✗ **Metadata Destruction:** Native restores often strip folder hierarchies and sharing permissions (ACLs), turning recovery into a manual, high-friction rebuilding project.
- ✗ **Shared Fate Risks:** Native archives reside within the production tenant. If the tenant is compromised, your backups are lost alongside your live data.
- ✗ **Identity Lockout:** If a Google Super Admin or Okta account is hijacked, security teams are locked out of the recovery process entirely.
- ✗ **Autonomous AI Chaos:** AI agents move faster than humans. A misconfigured or malicious agent can corrupt thousands of files before anyone notices, requiring a precise "undo" that native tools don't provide.
- ✗ **Unprotected Workloads:** Calendar, Contacts, and Groups have no native point-in-time recovery. Once lost, these cannot be reconstructed.

INTRODUCING: RUBRIK END-TO-END GOOGLE WORKSPACE PROTECTION

Rubrik provides the first unified Cyber Resilience platform purpose-built for Google Workspace, bridging the gap between your data, the identities that control it, and the AI agents that interact with it. We don't just give you a pile of data; we give you your business back, exactly as it was.

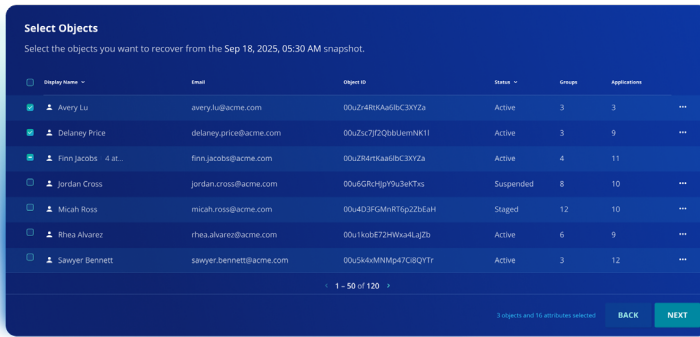
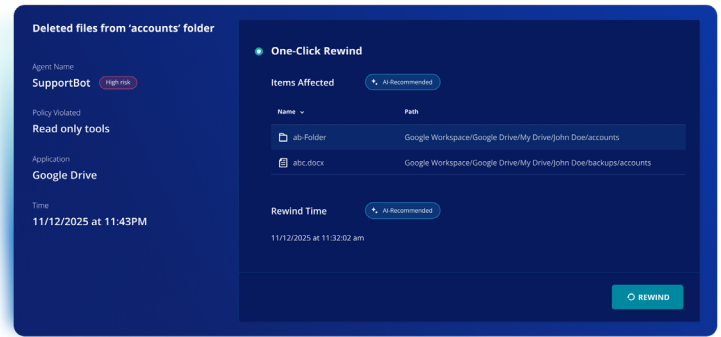
DATA RESILIENCE

Restore Your Minimum Viable Business

Pivot from passive archiving to **active operational recovery**. Rubrik replaces manual friction with automated SLAs that slash recovery times from days to minutes.

- **Full Workspace Coverage:** Immutable, air-gapped protection for Gmail, Drive, Calendar, Contacts, and Groups in a vault isolated from your primary Google tenant, covering every workload that makes your business run.
- **High-Fidelity Restoration:** Restore data in-place with 100% metadata preservation, maintaining all folder structures and complex sharing ACLs.
- **Mass Recovery:** Recover hundreds of users simultaneously, scoped by OU or application, replacing manual mailbox-by-mailbox triage with a single managed operation.
- **Prioritized Recovery:** Define restore scope by recency (last 1 to 30 days) to recover business-critical data first, ensuring mission-critical workloads are back online before broader recovery completes.
- **Self-Service Restore:** AI hallucinations corrupt files at machine speed. Empower end-users to recover Gmail and Drive data through tightly scoped permissions, reducing IT support queues without exposing global administrative rights.





IDENTITY RESILIENCE

Secure the Keys to the Kingdom

- Data security is inseparable from identity. Rubrik breaks the "shared fate" vulnerability by providing an immutable vault for your identity configurations.
- **Secure the Okta Environment:** Protect users, groups, MFA policies, and SSO settings in an immutable, air-gapped environment.
 - **Break-Glass Recovery:** Instantly restore Super Admin accounts and Okta configurations to maintain business momentum during a catastrophic identity compromise.
 - **Prevent Total Lockouts:** Ensure security teams can regain control and restore Super Admin accounts even if primary credentials are compromised or wiped.

AI RESILIENCE

Accelerate Safe AI Adoption

- Rubrik provides a critical safety net to monitor changes and undo unintended agent actions. AI hallucinations corrupt files at machine speed. Rubrik provides a critical safety net to undo unintended agent actions and empower end-users with self-service restore.
- **Monitor Agent Actions:** Automatically discover AI agents and gain full visibility into how they interact with mission-critical data.
 - **Govern Agent Behavior:** Enforce behavioral policies to detect and block unauthorized agent access or risky data movements.
 - **Rewind Agent Errors:** Instantly remediate mistakes by "rewinding" specific files or folders to their known good state without a full environment rollback.

THE RUBRIK DIVIDEND: STRATEGIC OUTCOMES

Feature	Native Tools	Rubrik Cyber Resilience
Strategy	Passive Archiving	✔ Active Operational Recovery
Permission Fidelity	Stripped (Manual Rebuild)	✔ 100% Preserved (ACLs/Hierarchy)
Security Boundary	Shared Fate with Tenant	✔ Logically Air-Gapped Vault
Calendar, Contacts, Groups	Not Recoverable	✔ Point-in-time Restore with Full Fidelity
Org-Wide Recovery	Manual, User by User	✔ Mass Recovery + Prioritized Recovery
Identity Protection	None	✔ Full Okta & Super Admin Backup
AI Governance	No visibility into agent actions	✔ Active "Rewind" for Agent Errors

DELIVERING VALUE ACROSS THE ORGANIZATION

- **CIO / CISO:** Consolidates fragmented tools into one platform while eliminating the "Shared Fate" risk of the Google tenant.
- **Google Workspace Admins:** Replaces "wait and hope" recovery with a "point-and-click" experience that restores the business in minutes.
- **Security Architects:** Breaks the link between identity and data, ensuring a total takeover cannot destroy the ability to recover.

Stop managing backups and start building resilience. Don't let a 25-day cliff or a compromised control plane define your strategy. Secure your enterprise operating system with Rubrik today. Learn more at rubrik.com/google-workspace.

SAFE HARBOR STATEMENT

Any unreleased services or features referenced in this brief are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.



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, pioneering the AI Operations category as the enterprise control layer for artificial intelligence. We unify all AI agents across data, applications, and identity into one governed platform, transforming the way enterprises deploy, manage, and secure AI at scale. Built on our proven cyber resilience foundation, Rubrik uniquely delivers the visibility, control, and recovery capabilities that enable organizations to accelerate AI transformation while maintaining complete operational resilience.

For more information please visit www.rubrik.com and follow [@rubrikinc](https://twitter.com/rubrikinc) on X (formerly Twitter) and [Rubrik](https://www.linkedin.com/company/rubrik) on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.