rubrik

Rubrik Identity Resilience

# The Identity Intelligence Fabric

Unify Your Security Stack to Detect, Reconcile, and Recover at AI Speed.

In June 2026, researchers uncovered FortiBleed, a campaign that harvested more than 86,000 valid credentials from Fortinet firewalls and VPNs across 194 countries. Roughly half of the exposed devices still had working credentials attached. The attackers needed no malware and no foothold. They logged in and moved through networks looking like legitimate users making routine changes. Once an adversary holds a valid credential, AI lets them escalate privileges and move laterally at inference speed, often with no human in the loop: AI-enabled cyber incidents rose 89% year over year in CrowdStrike's 2026 Global Threat Report. Detection and response playbooks were built for humans attacking at human speed. That world is gone.

## The Fragmentation Problem

The average enterprise runs about 61 security tools and 58 dashboards (Panaseer 2026 Security Leaders Peer Report), and Gartner projects security spending to keep growing at roughly 10% a year. More tools were supposed to mean more security. Instead they produced more silos, and that fragmentation shows up in two places:

- **Slow Detection:** when a signal fires in one tool, confirming it means manually correlating alerts across endpoint detection and response (EDR) platforms, the security information and event management (SIEM) system, and identity systems, then pulling several teams into a room to reconstruct what happened and what changed.
- **Slow Reconciliation:** once an attack is confirmed, sorting the changes made since the last known clean state needs identity context that lives across the whole stack: workforce data in human resources (HR) systems like Workday, access data in an identity governance and administration (IGA) tool like SailPoint, native object data in identity providers like Entra ID and Okta, and privileged access data somewhere else entirely. Scattered context turns reconciliation into a cross-tool investigation run in spreadsheets. It takes days, and the business stays down.

### Reconciliation Is Not a Data Problem. It Is a Context Problem.

The Identity Intelligence Fabric, part of Rubrik Identity Resilience, closes this visibility gap. It gathers signals from the identity threat detection and response (ITDR), HR, and IGA tools an enterprise already runs and aggregates identity context in a single, integrated layer, so security and Identity and Access Management (IAM) teams can detect, investigate, and recover from AI-driven attacks at machine speed. Two sets of integrations begin that vision today: CrowdStrike and Microsoft Defender for faster detection, Workday and SailPoint for faster reconciliation.

**89%**
year-over-year rise in AI-enabled cyber incidents (CrowdStrike 2026 Global Threat Report)

**61 Tools**
and 58 dashboards in the average enterprise security stack (Panaseer 2026)

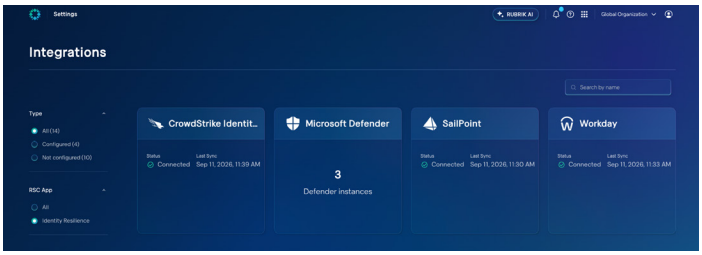
**86,000+**
valid credentials harvested by FortiBleed across 194 countries, half of them still working

## Faster Detection with CrowdStrike and Microsoft Defender

Rubrik Identity Resilience now ingests alerts from CrowdStrike and Microsoft Defender and correlates them against the enterprise's identity snapshot data. When a critical identity attack signal appears, such as a Golden Ticket, DCSync, or Golden SAML, it becomes a single decisive trigger for IAM admins to loop in the security team and start recovery. From the moment that alert fires, every new snapshot for the affected domain or tenant is marked suspicious until it is resolved. Admins see the status inline, on the Entra ID calendar view and in the Active Directory Forest Recovery (ADFR) flow, with the triggering alert attached, and the most recent clean snapshot is recommended as the restore point. This does not replace the analyst's work. It brings security and IAM to the same signal at the same time, closing the gap between detection and response.

## Faster Reconciliation with Workday and SailPoint

Detection tells you when an attack happened. Reconciliation tells you which changes are legitimate, which are malicious, which to undo, and which to keep. Identity First Recovery (IFR) simplified a full ADFR; surgical rollback, one of Rubrik's biggest value propositions, undoes unwanted changes without one. The Fabric now feeds that rollback with context from across the identity stack: Workday verifies joiner, mover, and leaver changes such as new hires, terminations, and role moves, and SailPoint cross-references changes against approved access requests. Rubrik separates malicious changes from legitimate ones in a unified console, and IAM teams stop reconciling context across systems by hand.




CrowdStrike, Microsoft Defender, SailPoint, and Workday connected in Rubrik Security Cloud.

## The Value Delivered

- **Faster Detection:** alerts from ITDR tools correlated against identity snapshots, so both teams know when and where to begin recovery.
- **Faster Reconciliation:** HR and IGA context sorts every change, and manual cross-tool reconciliation disappears.
- **One Console for Security and IAM:** both teams look at the same picture, without the spreadsheets.

## Where the Identity Intelligence Fabric Goes Next

These integrations are the start. Rubrik plans to connect the Fabric to more ITDR platforms and identity systems of record, including additional HR, IGA, privileged access management (PAM), and IT service management (ITSM) platforms, so that one console is where security and IAM teams detect an attack, investigate it, and begin recovery.

**Available Now:** the CrowdStrike, Microsoft Defender, SailPoint, and Workday integrations are part of Rubrik Identity Resilience. Learn more at rubrik.com/identity.

Schedule a Demo >



rubrik


**Global HQ**
3495 Deer Creek Road
Palo Alto, CA 94304
United States

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


Rubrik (RBRK), the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.




Identity-Intelligence-Fabric_Data-Sheet_v1.1 / 20260921