Rubrik and Mandiant

Partnership designed to improve cyber resilience for organizations with a tightly integrated, end-to-end solution for cyber threat detection, incident response, and data recovery.

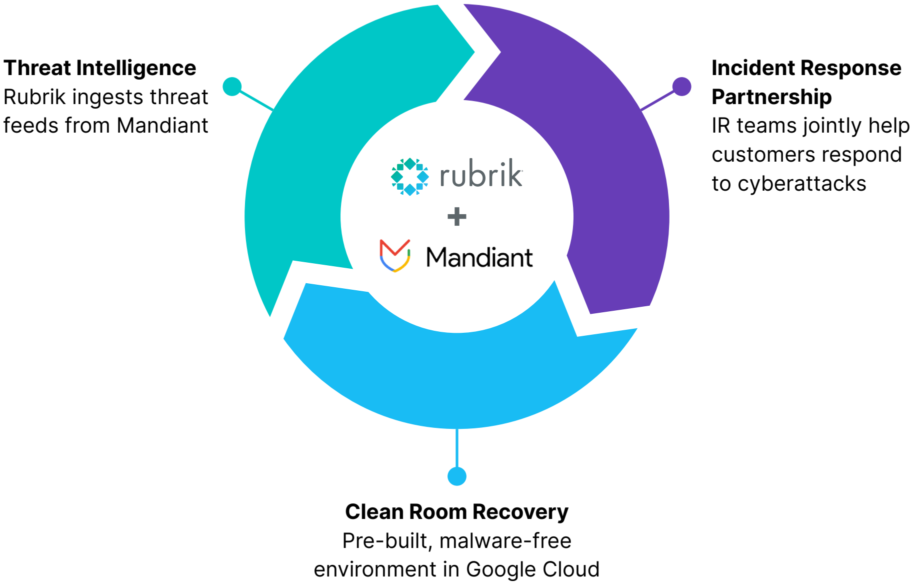
In the ever-evolving world of cybersecurity, dealing with cyberattacks has become a daunting challenge for organizations across the globe. The aftermath of such attacks can be catastrophic, leaving organizations stymied for weeks or even months as they scramble to determine the true scope of an attack through recovering their data and systems. The partnership between Rubrik and Mandiant, part of Google Cloud, turns the tables on these malicious actors, and aims to dramatically reduce the entire intrusion lifecycle from initial detection through recovery—all with the goal of keeping businesses running during ransomware attacks.

Partnership aims to:

Accelerate incident response with Mandiant's deep frontline expertise combined with Rubrik's cyber recovery capabilities

Identify malware and safe recovery point quickly and confidently with Rubrik threat scanning technology powered by best-in-class threat intelligence from Mandiant

Recover confidently into a clean room environment in Google Cloud with minimal business disruption



Threat Intelligence
Rubrik ingests threat feeds from Mandiant

Incident Response Partnership
IR teams jointly help customers respond to cyberattacks

Clean Room Recovery
Pre-built, malware-free environment in Google Cloud

BEST-IN-CLASS TECHNOLOGY MEETS BEST-IN-CLASS EXPERTISE

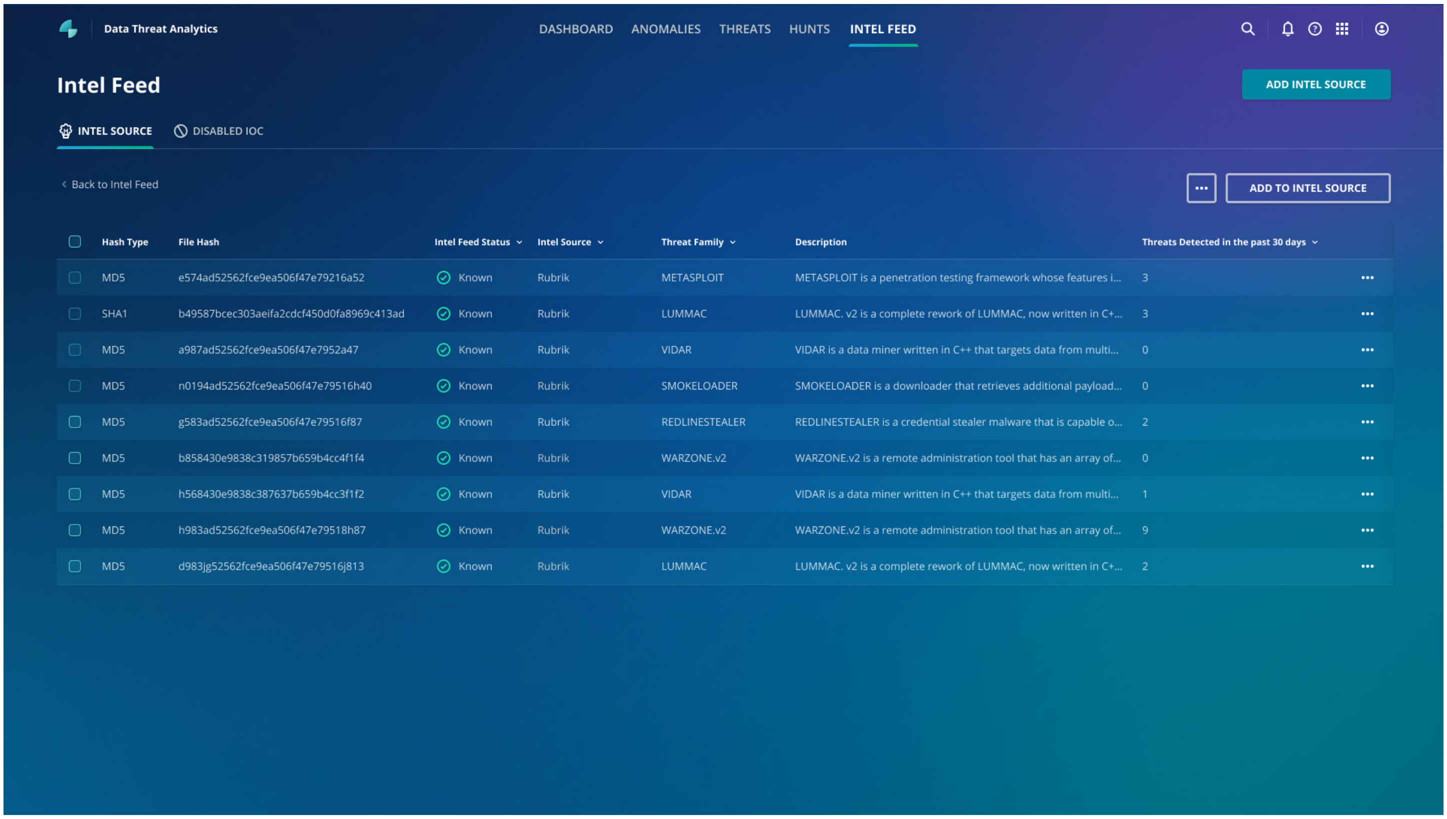
The Rubrik-Mandiant partnership combines best-in-class technology and expertise. Together, Rubrik's technology combined with Mandiant's expertise aims to empower organizations with an unparalleled level of resilience against cyber threats, to help ensure business continuity even in the face of the most sophisticated attacks.

The partnership focuses on three key elements:

1. **Threat Intelligence:** Integrating intelligence from Mandiant into Rubrik's security capabilities to better identify malware, potentially before ransomware is deployed. Our combined capabilities manifest in hundreds of new malware families per year and over 4,000 threat groups tracked by Mandiant, that can be actively pursued across more than 47 exabytes of data within Rubrik—continuously and automatically.

2. **Incident Response Partnership:** For Rubrik's Ransomware Response Team and Mandiant's incident response team to be fully trained in each other's offerings and prepared to respond to intrusions during a crisis. Qualifying customers will have access to Mandiant Consulting.

3. **Clean Room Recovery:** For quick recovery of data into a safe instance in Google Cloud with minimal business disruption, regardless of whether the intrusion is fully remediated.



□	Hash Type	File Hash	Intel Feed Status	Intel Source	Threat Family	Description	Threats Detected in the past 30 days	
□	MD5	e574ad52562fce9ea506f47e79216a52	✓ Known	Rubrik	METASPLOIT	METASPLOIT is a penetration testing framework whose features i...	3	•••
□	SHA1	b49587bcec303aeifa2cdcf450d0fa8969c413ad	✓ Known	Rubrik	LUMMAC	LUMMAC. v2 is a complete rework of LUMMAC, now written in C+...	3	•••
□	MD5	a987ad52562fce9ea506f47e7952a47	✓ Known	Rubrik	VIDAR	VIDAR is a data miner written in C++ that targets data from multi...	0	•••
□	MD5	n0194ad52562fce9ea506f47e79516h40	✓ Known	Rubrik	SMOKELOADER	SMOKELOADER is a downloader that retrieves additional payload...	0	•••
□	MD5	g583ad52562fce9ea506f47e79516f87	✓ Known	Rubrik	REDLINESTEALER	REDLINESTEALER is a credential stealer malware that is capable o...	2	•••
□	MD5	b858430e9838c319857b659b4cc4f1f4	✓ Known	Rubrik	WARZONE.v2	WARZONE.v2 is a remote administration tool that has an array of...	0	•••
□	MD5	h568430e9838c387637b659b4cc3f1f2	✓ Known	Rubrik	VIDAR	VIDAR is a data miner written in C++ that targets data from multi...	1	•••
□	MD5	h983ad52562fce9ea506f47e79518h87	✓ Known	Rubrik	WARZONE.v2	WARZONE.v2 is a remote administration tool that has an array of...	9	•••
□	MD5	d983jg52562fce9ea506f47e79516j813	✓ Known	Rubrik	LUMMAC	LUMMAC. v2 is a complete rework of LUMMAC, now written in C+...	2	•••

Google Threat Intelligence is directly integrated into Rubrik Security Cloud via Rubrik's Threat Monitoring capability.

"Organizations have been responding to ransomware attacks with months-long recovery processes, which can result in irreparable damage to the business. With Mandiant, we are able to demonstrably lessen the impact window of ransomware attacks while simultaneously increasing the capabilities available to customers in need—from threat intelligence to rapid access to incident response teams. Together, we connect the dots in a time of crisis to deliver true cyber resilience." **– Steve Stone, Head of Zero Labs, Rubrik**

Safe Harbor Statement: Any unreleased services or features referenced in this document 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.

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 on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

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