rubrik

Anomaly Detection

Detect and Recover from Cyber Attacks

CYBER ATTACKS HAPPEN

Cyber attacks are becoming more common—and more expensive. It is not easy to play perfect perimeter defense against ransomware and other cyber threats. In the face of this challenge, organizations are looking to adopt a holistic, multi-level incident response strategy that integrates detection, analysis, and rapid recovery.

Global ransomware damages predicted to reach

$265 billion

in 2031

Every **2** seconds

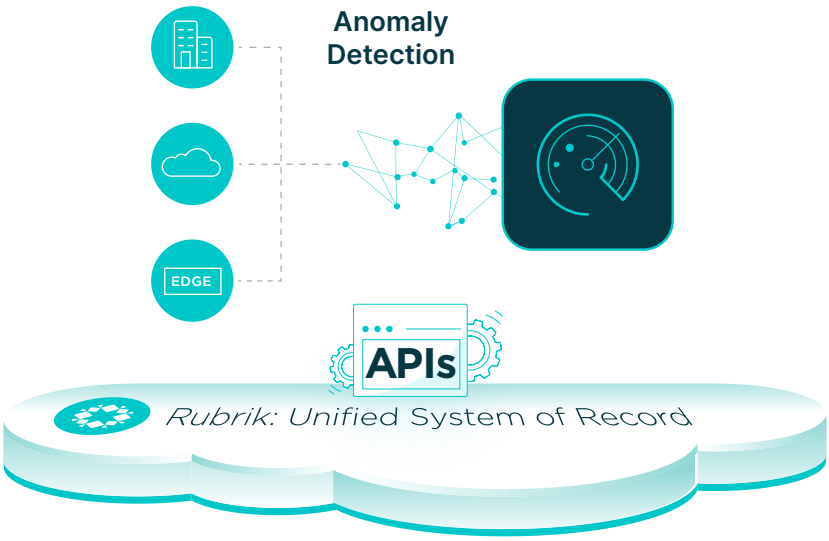
a ransomware attack on businesses predicted in 2031

Source: Cybersecurity Ventures

The most effective strategy for preventing and recovering from cyber attacks is defense in depth. A defense in depth approach keeps your backups safe from threats, identifies when you are under attack, and accelerates recovery to minimize business impact in the event of an attack.

ANOMALY DETECTION: RECOVER FASTER. STAY SMARTER.

Anomaly Detection determines the scope of cyber attacks using machine learning to detect deletions, modifications, and encryptions. Anomaly Detection helps you ***recover faster*** by providing a simple, intuitive user interface that tracks how your data changed over time. It replaces manual recoveries with just a few clicks for minimal business disruption. It also ***increases intelligence*** by using machine learning to actively monitor and generate alerts for suspicious activity.



RECOVER FASTER

Minimize downtime. Restore to the most recent clean state with just a few clicks.

INCREASE INTELLIGENCE

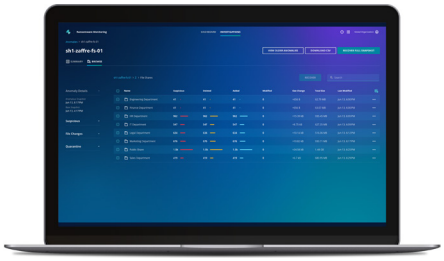
Leverage machine learning to detect and alert on anomalous behavior.

See how your data has changed to quickly identify what was impacted where.

A MULTI-LEVEL DEFENSE: HOW ANOMALY DETECTION WORKS

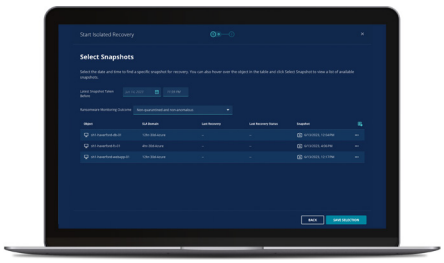
DETECT ANOMALIES VIA MACHINE LEARNING

Anomaly Detection applies machine learning algorithms against application metadata to establish normal baseline behavior for each machine. It proactively monitors the system by looking at behavioral patterns and flagging any activity that varies significantly from the baseline. Anomaly Detection analyzes several file properties, including file change rates, abnormal system sizes, and entropy changes. Additionally, Anomaly Detection detects encryption at the VM level. Once an anomaly is detected, Anomaly Detection alerts you to the unusual behavior via the Rubrik UI, by email, or by SOAR and SIEM applications like Palo Alto Networks Cortex XSOAR or Microsoft Sentinel. By using machine learning, Anomaly Detection can continuously refine its anomaly detection model over time and stay ahead of the most advanced threats.



ANALYZE THREAT IMPACT WITH DATA INTELLIGENCE

Anomaly Detection continuously scans the backup environment to provide insights on how your data has changed over time. In the event of an attack, you can quickly identify which applications, VMs, and files were impacted and where they are located through simple, intuitive visualizations. Using the UI, browse through the entire folder hierarchy and drill-down to investigate what was added, deleted, or modified at the file level. With Anomaly Detection, you minimize the time spent discovering what happened and the data loss with granular visibility into the latest unaffected files.



ACCELERATE RECOVERY TO MINIMIZE BUSINESS DISRUPTION

Anomaly Detection's simple user experience is powered by the Rubrik global management interface. After completing the analysis, you can simply select all impacted applications and files, specify the desired location, and restore to the most recent clean versions with just a few clicks. Rubrik automates the rest of the restore process, and users can track the progress through the UI. Since Rubrik captures all data in an immutable format, malicious actors cannot access and encrypt or delete backups.

WHAT OUR CUSTOMERS ARE SAYING

"When we were hit by ransomware a few years ago, we leveraged Rubrik's fast recovery and APIs to recover in under an hour with zero data loss. Today, ransomware is much more sophisticated than it was a few years ago. With Anomaly Detection, we could leverage its data intelligence to alert us on suspicious behavior and better understand what was impacted at a granular level." **– Paul LaValley Former CIO, Yuba County, California**

"Backups are one of the most, if not the most, important defenses against ransomware. Rubrik's file system was built to be immutable, meaning backups cannot be encrypted or deleted by ransomware. I am very fortunate to say that 100% of what we had on Rubrik we were able to recover." **– Matthew Day CIO, Langs Building Supplies**

"Anomaly Detection will help us protect our bottom line and potentially save us millions of euros in case of an attack. If we did not have Anomaly Detection, we would not have been approved for a cyber insurance contract." **– Fabrice De Biasio CIO, ASL Airlines**

rubrik

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

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

Rubrik 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.

ds-anomaly-detection / 20231018