



rubrik

Zero Trust  
Data Security™

WHITE PAPER

# The Trusted Data Security Solution for Cyber Recovery



# Table of Contents

- 3 CYBER ATTACKS: A PERVASIVE AND GROWING RISK**
- 3 THE BUSINESS IMPACT OF RANSOMWARE**
- 3 LEGACY BACKUP: UNTRUSTWORTHY FOR CYBER RECOVERY**
- 4 DATA SECURITY: THE TRUSTED APPROACH TO CYBER RECOVERY**
- 5 RUBRIK SECURITY CLOUD PROTECTS DATA FROM CYBER ATTACKS, CONTINUOUSLY MONITORS DATA RISKS, AND QUICKLY RECOVERS DATA AND APPLICATIONS.**
  - 6 Data Protection
  - 6 Data Threat Analytics
  - 6 Data Security Posture
  - 7 Cyber Recovery
  - 7 Zero Trust
- 8 WHY RUBRIK**
- 8 ESTÉE LAUDER SECURES AT-RISK DATA FOR GROWING BEAUTY EMPIRE WITH RUBRIK**

## CYBER ATTACKS: A PERVASIVE AND GROWING RISK

Digital transformation has brought significant benefits to organizations, including increased agility and flexibility, but it has also led to a rise in cyber attack vectors. 66% of organizations were hit with ransomware within the last year, according to a [2022 Sophos survey](#). The widespread adoption of cloud services and Software-as-a-Service (SaaS) applications has expanded the attack surface, making it more challenging to manage and secure data. Additionally, the increased use of mobile devices and remote work have made it easier for cybercriminals to launch attacks from anywhere, at any time.

## THE BUSINESS IMPACT OF RANSOMWARE

Ransomware attacks can be crippling. Ransom payments can cost millions of dollars without any guarantee that paying the ransom will restore impacted data. Beyond the cost of the ransom itself, attacks can also result in downtime, lost revenue, recovery costs, reputational harm, regulatory compliance requirements, loss of customer goodwill, increased cyber insurance premiums, and more. All in all, total costs are often in the millions of dollars, with full recoveries taking weeks to months. [Ransomware cost the world \\$20 billion in 2021](#) and that number is expected to rise to \$265 billion by 2031. The impact is clear: when an organization's data is down, its business is down.

## LEGACY BACKUP: UNTRUSTWORTHY FOR CYBER RECOVERY

Many organizations still rely on legacy backup as their last-resort cybersecurity option. However, these systems often lack critical security features and are not designed to protect against modern cyber threats. Amongst all the weaknesses and deficiencies of legacy backup, here are a few reasons why it cannot be trusted for cyber recovery:

- Legacy backups are vulnerable to cyber attacks. Organizations that use legacy backup likely have open storage protocols, which can expose their data to unauthorized access and manipulation by hackers. This is particularly problematic when coupled with windows operating systems, and multi-factor authentication that's not deployed or enforced. Without proper authentication and access controls, cyber attackers can exploit vulnerabilities in these systems to gain unauthorized access to sensitive data and compromise an organization's security posture.
- Legacy backups do not provide critical insights or visibility into what data is at risk or what has been affected during a cyber attack. As a result, organizations can't respond promptly and effectively to the incident. The task of determining what data has been lost or compromised can be overwhelming and can take weeks or even months to complete, extending costly downtime.
- Legacy backups were designed to restore individual files, virtual machines, or databases from a known point in time associated with a disaster. However, with cyber recovery, it can be incredibly challenging to determine what to restore, when the attack occurred, how far the bad actor went, and the extent of the damage they caused. This piecing together of information is very time-consuming and can significantly delay the recovery process.

- Cyber recovery also requires a whole new level of concern around sensitive data. Unlike legacy backups, determining the scope of the attack and potential sensitive data exposure is crucial for cyber recovery, especially where organizations are required to notify compliance units such as GDPR.
- Legacy backups do not offer protection against the reinfection of malware. In a cyber recovery scenario, restoring backups that contain malware to a clean environment can trigger the attack all over again, potentially causing even more damage and data loss. The aftermath of such an attack can be devastating for organizations, causing them to lose money and customer trust for months or even years to come.
- Finally, legacy backup systems don't provide organizations with the capability to simulate and test their recovery processes, which leaves them in a precarious position in the event of a cyber attack. Organizations have to rely on luck or chance to restore their systems fully, leading to potential data loss, system downtime, and significant reputational damage.

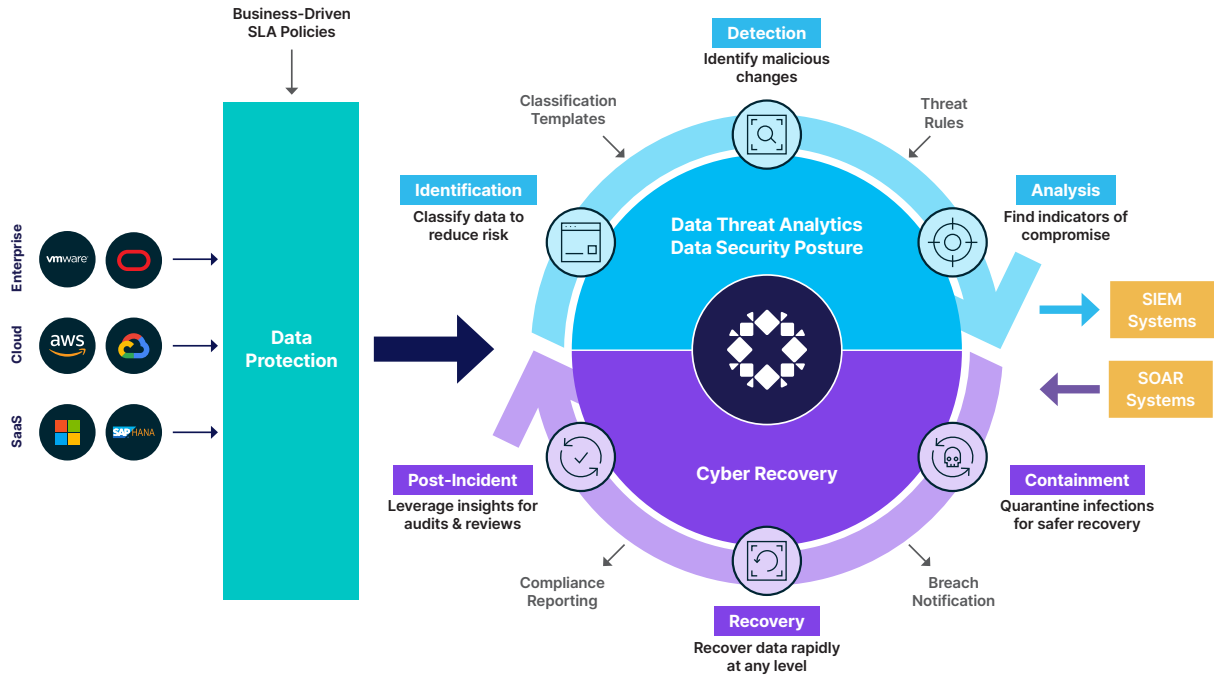
It's clear that legacy backup systems are no match for modern cyber threats. In today's competitive environment, organizations cannot afford to be complacent about cyber recovery and must invest in solutions specifically designed for cyber recovery to avoid significant pain in the long run.

## DATA SECURITY: THE TRUSTED APPROACH TO CYBER RECOVERY

Given this dynamic threat environment, organizations must adopt an “assume breach” mindset. Securing data is the only way an organization can truly secure its business, especially at a time when ransomware is such a pervasive threat that remains financially rewarding for attackers. IT and cybersecurity teams must ensure that data is available, safe, and recoverable in the event of an incident. Because data is the target of attackers, organizations need security at the point of data—“data security”—to keep data safe and recover it faster.

Data security is composed of three pillars:

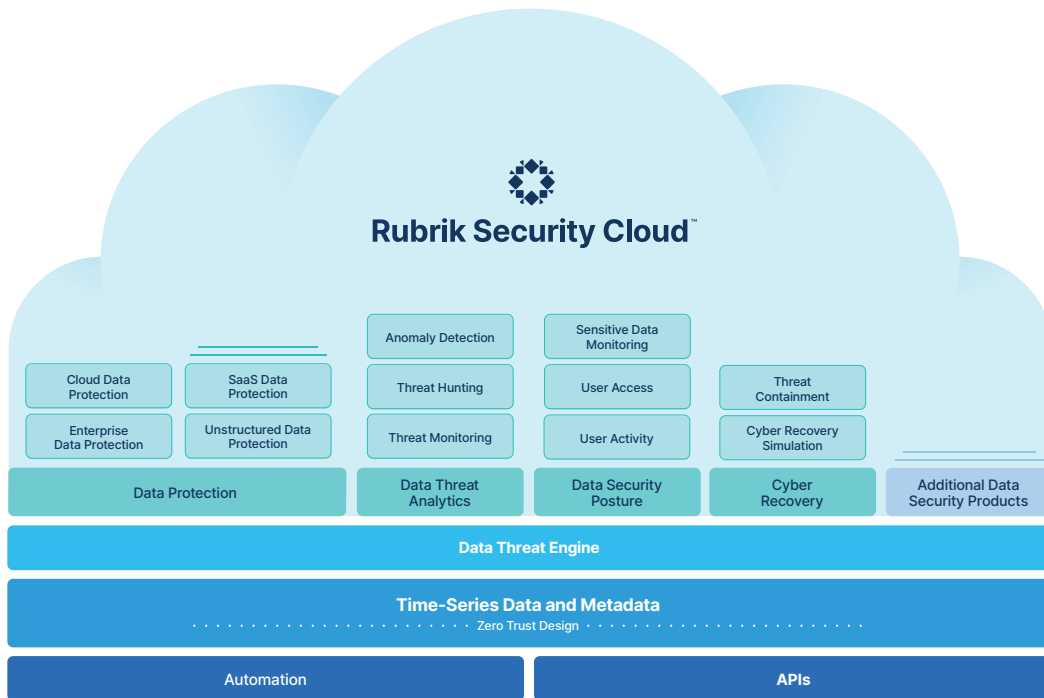
1. **Data Protection** – Protect your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups.
2. **Data Threat Analytics** – Continuously monitor for threats to your data, including ransomware, data destruction, and indicators of compromise.
3. **Data Security Posture** – Identify and monitor sensitive data exposure and use intelligent risk insights to maximize data security posture.
4. **Cyber Recovery** – Improve cyber readiness and incident response by easily testing and orchestrating recovery workflows.



Data security keeps data safe and makes it easier to respond to cyber attacks.

## RUBRIK SECURITY CLOUD PROTECTS DATA FROM CYBER ATTACKS, CONTINUOUSLY MONITORS DATA RISKS, AND QUICKLY RECOVERS DATA AND APPLICATIONS.

Rubrik Security Cloud gives organizations a single place to secure their data wherever it lives—across enterprise, cloud, and SaaS applications.



Rubrik Security Cloud provides zero trust data security, which is made up of data protection, data threat analytics, data security posture, and cyber recovery.

## DATA PROTECTION

With Rubrik, organizations can be confident that their critical data is safe from deletion, compromise, or encryption. This is because air-gapped, immutable, access-controlled backups enable organizations to withstand cyberattacks, malicious insiders, and operational disruptions.

Data is stored in an immutable format and cannot be read, modified, or deleted. Additionally, data is encrypted in-flight and at rest, and backup data is stored in a purpose-built append-only file system.

Lastly, backed up data is logically air-gapped so it's offline and not accessible through standard network protocols. System interfaces are secure, role-based, least privileged, and protected by multifactor authentication (MFA) to further reduce the risk of intrusion.

Data Resilience services include:

- **Enterprise Data Protection** – to keep your enterprise data safe from attacks or disasters.
- **Cloud Data Protection** – to ensure your cloud data is secure from compromise.
- **SaaS Data Protection** – to secure your SaaS application data with automated protection.
- **Unstructured Data Protection** – to protect, monitor, and rapidly recover unstructured data at petabyte-scale.

## DATA THREAT ANALYTICS

Organizations using Rubrik are well positioned to recruit their data in the fight against ransomware. This is because Rubrik captures the longitudinal time-series history of data. Additionally, Rubrik manages metadata—including its content, users, and access privileges. By scanning hundreds of snapshots, Rubrik's Data Threat Analytics engine generates signals that are fed into a highly trained machine learning model – building a historical baseline against which new data can be compared to find anomalous modifications, deletions, and encryptions.

Data Threat Analytics services include:

- **Anomaly Detection** – to determine the scope of ransomware attacks, using high fidelity machine learning to detect deletions, modifications, and encryptions.
- **Threat Monitoring** – to detect threats early by automatically identifying indicators of compromise within backups using an up-to-date feed of threat intelligence.
- **Threat Hunting** – to prevent malware reinfection by analyzing the time-series history of data for indicators of compromise to identify the initial point, scope, and time of infection.

## DATA SECURITY POSTURE

Sensitive data discovered by the data security posture engine can be correlated with data anomalies found earlier to determine if any sensitive data was impacted, which could pose a potential double extortion risk. And scanning the time series history of data for indicators of compromise makes it easy to find the last known clean copy for recovery operations.

Additionally, organizations can continuously assess whether their data managed by Rubrik is safe and ready to recover from a cyber attack with Data Security Command Center. From an easy-to-use dashboard with risk scores, IT and security teams can get visibility into data risks, identify security gaps, and get actionable guidance to make their data more secure.

Data Security Posture services include:

- **User access** – to reduce data exposure risk by identifying and limiting who has access to sensitive data.
- **Sensitive Data Monitoring** – to reduce sensitive data exposure and manage exfiltration risk by discovering what types of sensitive data you have and where it lives.
- **Data Security Command Center** – to identify security gaps, quantify data risk, and provide actionable recommendations to improve data security posture.

## **CYBER RECOVERY**

Rubrik's Cyber Recovery capabilities allow organizations to improve cyber readiness and incident response by easily testing, validating, and orchestrating recovery workflows. Rubrik enables organizations to test whether their recovery playbook works, including sequence, timing, and failure points. Organizations can also clone production data into isolated recovery environments to investigate snapshots for malware and use their own choice of security tools to conduct cyber readiness assessments, such as penetration tests or red teaming, without impact to production.

Rubrik also provides the ability to scan backups using file patterns, file hashes, and YARA (Yet Another Recursive Acronym) rules to look for indicators of compromise (IoCs) across all objects in the backup. Organization can also analyze a time-series history of backup snapshots to pinpoint clean uninfected snapshots for recovery. Additionally, they can leverage the insights that Rubrik provides to quickly recover at scale, with less risk of reintroducing malware.

Cyber Recovery capabilities include:

- **Threat Containment** – to ensure safe and quick data recovery by quarantining data infected with malware.
- **Cyber Recovery Simulation** – to improve cyber readiness and incident response by easily creating, testing, and validating cyber recovery workflows.

Additionally, integrations with common security solutions allow security operators to use their existing tools (i.e., SIEM and SOAR solutions) to view alerts generated by Rubrik's Data Threat Analytics and Data Security Posture services and invoke Rubrik Threat Monitoring & Hunting and Cyber Recovery workflows without touching the Rubrik interface. By bringing data protection and data security into a single platform with a unified control plane and integrated workflows, Rubrik Security Cloud fosters tighter collaboration between IT and Security Operations and helps reduce ransomware remediation time.

## **ZERO TRUST**

All Rubrik Security Cloud capabilities follow the zero trust principle that users, admins, and network traffic not be trusted unless strongly authenticated. This helps ensure that Rubrik keeps data safe, aligned to standards set forth by the US government's National Institute of Standards and Technology (NIST).

## WHY RUBRIK

Rubrik Security Cloud is the leading data security platform built upon a unique backup architecture that secures data. Rubrik is designed with zero trust principles to incorporate a logical air gap, secure protocols, native immutability, encryption, and access controls. With global policy-driven automation, Rubrik helps ensure data availability, policy compliance, and streamlined recovery workflows, while the data classification engine identifies sensitive data exposure and the anomaly detection engine enables faster threat investigation and prevention of malware reinfection. Additionally, the API extensibility feature facilitates collaboration with cross-functional teams by providing a shared view of data risk and threat insights across tools.

The principal economic benefit of Rubrik is reduced costs associated with combating cyber threats. Data Protection safeguards data with secure backups. Data Threat Analytics makes it easy to monitor data risk and investigate threats faster. Data Security Posture helps to proactively reduce data exposure risk. Cyber Recovery helps restore business operations faster.

## ESTÉE LAUDER SECURES AT-RISK DATA FOR GROWING BEAUTY EMPIRE WITH RUBRIK

**90%+ Reduction in time to backups of 10 TB+ databases**

Cosmetics company Estée Lauder has over 25 beauty brands throughout 150 countries. Its IT department supports over 48,000 global employees and protects several petabytes worth of data. One of its biggest challenges is accommodating changing data and different platforms with different operating systems, especially as it introduces and acquires new brands. It is now focused on standardizing on Rubrik as the unified enterprise data security fabric across locations and for all SLA use cases as well as improving backup performance and restore times. In addition, Estée Lauder had blind spots regarding its at-risk sensitive data and often found PCI information in files where it should not have been. The team leveraged Rubrik's Data Security Posture engine to discover, classify, and report on locations of files containing sensitive data without any impact to production. This helped them take steps to remove and remediate the sensitive data, keeping both customers and the company protected from exposed information.



ESTÉE LAUDER

**We are very impressed with Rubrik's ability to instantly recover. While other solutions were offering similar capabilities, Rubrik stood apart by the ease at which we were able to take a backup and instantly make it available through Live Mount. It was an important selling point for us, and we constantly use it to have our data readily available.**

**Pankaj Govil**

Executive Director, Global Storage Infrastructure



### Global HQ

3495 Deer Creek Road  
Palo Alto, CA 94304  
United States

1-844-4RUBRIK  
inquiries@rubrik.com  
[www.rubrik.com](http://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](http://www.rubrik.com) and follow @rubrikinc on X (formerly Twitter) and 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.

wp-the-trusted-data-security-solution-for-cyber-recovery / 20230918