CYBER RESILIENCE FOR YOUR DATA ON AMAZON S3

rubrik

Reduce Risk, Minimize Impact, and Accelerate Incident Response

Today, more than a million organizations around the world rely on Amazon S3 to store billions of files and to run business-critical applications. As data volumes grow and cyber crime increases, it's never been more important to manage and secure that data.

CYBER ATTACKS ARE INEVITABLE, MATERIAL DAMAGE IS NOT

Despite increased investments in cyber security, ransomware attacks continue to rise. Between 2021 and 2023, data breaches rose by 72%[1]—with over 343 million ransomware victims in 2023. And it has become more difficult to stop these threats because 80% of cyber attacks[2] exploit legitimate access credentials to avoid detection. Once threat actors bypass perimeter, network, and endpoint defenses, they can easily gain access to sensitive data—especially unmonitored and unprotected data. They can then encrypt and exfiltrate the data for double extortion.

In this threat landscape, the most effective strategy is to assume breach—and to become cyber resilient. With Rubrik, you can gain resilience by proactively reducing the risk of sensitive data exposure, detecting data threats early, and accelerating incident response.

1 Forbes Advisor, *Cyber Security Stats: Facts and Figures You Should Know*
2 CrowdStrike, 2023 Global Threat Report Report

CYBER RESILIENCE ACROSS THE ATTACK TIMELINE

Pre-Attack

Reduce data exposure risk

- Discover and classify sensitive data likely to cause material damage if compromised.
- Identify unprotected, overexposed, redundant, and misplaced data so you can remediate and minimize risk.
- Locate identities with extensive access to sensitive data so you can reduce the blast radius of attacks.

At Time of Attack

Detect data threats early

- Detect threat actors that have bypassed perimeter, network, and endpoint defenses.
- Get alerted to anomalous activity on sensitive data (e.g. excessive file enumeration or downloads).
- Detect data encryption.

Post-Attack

Accelerate incident response

- Identify what data was compromised, its sensitivity, and when it was accessed.
- Determine the blast radius of the attack.
- Quarantine the ransomware and recover without reinfecting the environment.

To learn more about how Rubrik can help your organization become cyber resilient, contact our data security experts.

TWO RESPONSES TO ONE CYBER ATTACK: THE RUBRIK DIFFERENCE

The following attack timeline compares how two companies might respond to the same ransomware attack—illustrating how Rubrik helps minimize the risk, duration, and impact of cyber attacks.

Threat Actor

Company WITHOUT RUBRIK

Company WITH RUBRIK

Initial Access with Compromised Credentials

Large Amounts of Sensitive Data Accessed

Threat actors gained **access to thousands of files with sensitive data**, including personally identifiable information (PII), financial data, and health records.

Minimal Amount of Sensitive Data Accessed

Threat actors gained access to only a few files with sensitive data as the credentials **did not have access to a broad amount of sensitive data**.

How Rubrik helped:

- Identified entities with access to large amounts of sensitive data, which helped the company implement **least privilege access**.
- Discovered redundant data, which the company archived or deleted. This **reduced the attack surface and decreased cloud costs**.

Discovery

Did Not Detect File Enumeration

Threat actors enumerated shared directories and files to locate sensitive data. **This went undetected.**

Identified Excessive Enumeration

The company was **alerted to excessive enumeration** and began to investigate the breach.

How Rubrik helped:

- **Found S3 buckets without activity logs.** The company enabled logs through a one-click command in the Rubrik platform.
- Monitored activity logs and **detected excessive enumeration** of sensitive files.
- Sent a high-priority alert. The data context and sensitivity **accelerated the incident response**.

Data Exfiltration

Notified About Breach by Threat Actor

Threat actors exfiltrated sensitive data from an S3 bucket without activity logs. The exfiltration **went undetected**.

Threat actors also exfiltrated sensitive data from an S3 bucket with activity logs. Alerts were sent but were not noticed due to the high volume of alerts—and **no prioritization based on data context or sensitivity**.

Rapidly Responded to Alert on Data Exfiltration

Threat actors began to exfiltrate sensitive data from an S3 bucket with activity logs enabled, but the compromised **account was quickly suspended**.

How Rubrik helped:

- **Detected anomalous downloads** of files with sensitive data.
- Sent an alert marked as critical due to the sensitivity of the data—making it **easier for the incident response team to recognize**.

Data Encryption

Business Operations Disrupted

Threat actors encrypted thousands of sensitive files.

The company **struggled to identify the source and extent of the attack**. It took days to remove the ransomware and to test and implement the recovery.

Identified Encrypted Data and Removed Ransomware

Threat actors encrypted some sensitive files. The company **removed the ransomware and** quickly restored business operations.

How Rubrik helped:

- **Located the impacted data**, initial point of compromise, and time of infection.
- Identified the **blast radius**.
- Diagnosed the **ransomware infection type**.
- **Recovered data** without reinfecting the environment.

Impact

Significant Material Damage

No Material Damage