Solution Brief

Zscaler and Rubrik

Data at rest intelligence combined with data in motion security to deliver Zero Trust Security

Introduction

Enterprises today are experiencing an explosion of business application adoption to boost productivity. These business applications—combined with public cloud and private data centers—host a phenomenal volume of your data. Your data includes sensitive data stored by your users in diverse environments like AWS S3, Azure, GCP, and in approved and unapproved applications.

The number one threat of data exfiltration from these environments is no longer limited to physical devices like USB drives, but is now expanded to users' personal cloud storage, collaboration, and cloud-based personal email applications.

Ransomware attacks increasingly threaten organizations due to distributed content footprint. Earlier ransomware was limited to encryption of the content to extort money from the victim organizations. Attackers are now weaponizing your data with double extortion ransomware attacks that involve encrypting the critical content and exfiltrating it out of the organization, thus making it more complex to recover from such attacks and maintain business continuity.

Zscaler ThreatLabz State of Ransomware report shows a 120% increase in double extortion attacks. Traditional approaches to stop such attacks have been inadequate in providing protection to users.

Securing organizations from double extortion ransomware attacks needs a new solution that combines focused visibility with fine-grain control to prevent data loss and exfiltrations.

The Zscaler-Rubrik Joint Solution

Zscaler and Rubrik have partnered to help customers secure sensitive data with the identify, evaluate, and control paradigm, thus preventing exfiltration and unauthorized access.

The joint solution enables customers to gain visibility of sensitive data in the Rubrik security cloud and forward it to Zscaler Data Protection for Indexed Document Matching (IDM). The index is then used to create a document repository that Zscaler Data Protection can use while evaluating outbound traffic with the Data Loss Prevention (DLP) policy.

These protection measures can ensure sensitive data isn't accidentally lost or maliciously exfiltrated due to a breach.

The security leads can now design policies to control access and movement of sensitive data classified by the Rubrik Security Cloud. The compliance team now will have visibility, control, and reports of the entire digital estate, thus improving the compliance posture of the organization.

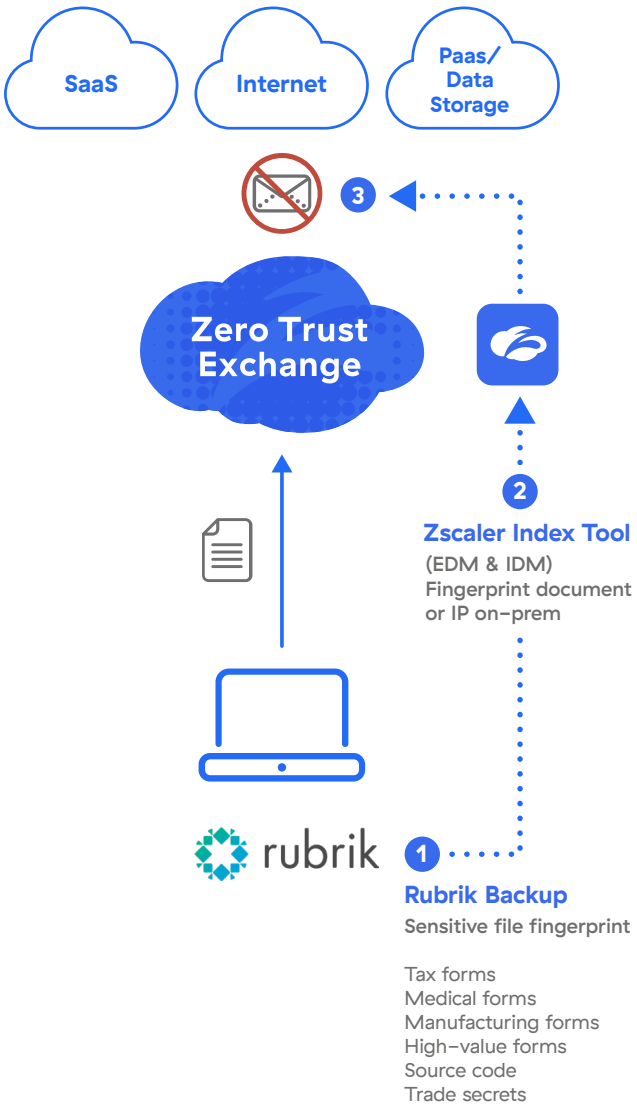
How it works

Step 1: Sensitive data discovery
The customer identifies and configures the assets that are needed to be backed up with Rubrik Security Cloud. Rubrik Sensitive Data Discovery then scans backups for sensitive data aligned with security and compliance policies.

Step 2: Indexing sensitive data
The data files identified as sensitive are now recovered to a known Zscaler Indexed Location in the document server. The servers will create an index and forward it to Zscaler Internet Access for further processing.

Step 3: Zscaler policy configuration
The index is added to the document registry maintained by Zscaler Data Protection and can be used to configure policies regarding the movement of the files.

Step 4: Traffic evaluation and action
Zscaler Internet Access will assess and evaluate the traffic of the sensitive content, within and beyond the infrastructure, and enforce policies—including blocking the files from being uploaded to unmanaged online storage or as an attachment to an email.



Key benefits

- **Identify Sensitive Data**
  Identify what types of sensitive data you have, where it lives, and who has access to it.
- **Inspect traffic for violations**
  Find completely or partially matching documents when inspecting outbound traffic with a data protection policy.
- **Enforce policies and prevent data loss**
  Use comprehensive knowledge of sensitive data to more effectively enforce data protection policies.

Summary

Application and infrastructure administrators and security/compliance teams working in tandem can demonstrate a large impact on the security of the organization's data. Persistent exfiltration threats posed by malicious internal or external users can jeopardize an organization's reputation and incur heavy penalties from regulatory aurthorities. A comprehensive data protection program can enhance protection of sensitive data across the organization with prompt discovery and monitoring.

Together, Rubrik and Zscaler present valuable data security insights to the security and compliance teams with reliable data protection policies and prevent the loss of critical business data through finely tuned enforcement methods.

To learn how Zscaler and Rubrik together can help you better secure sensitive data across your organization, visit our website:

www.zscaler.com/partners/rubrik

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com