Prevent sensitive data exfiltration with Cohesity and Zscaler

Key Benefits

- Prevent potential data breaches
- Improve compliance with regulations
- Extract security intelligence from your backup to unlock its full potential

Exfiltration of sensitive data is prevalent in double extortion ransomware attacks and insider threats, so it's a major concern for CISOs and business leaders. The unauthorized removal of sensitive and government-regulated data, including personally identifiable information (PII) and Protected Health Information (PHI), from an organization's network can lead to financial loss, reputational damage, and legal and regulatory consequences. It may also have implications for cyber insurance.

At the same time, organizations have a significant opportunity to derive additional value from backed-up data. For every terabyte of data in the production environment, 10 terabytes of that data are backed up or replicated across hybrid clouds and multiclouds for backup and recovery, disaster recovery, development and testing, and more. Use your secondary data estate to strengthen security intelligence and cyber resilience without impacting production environments.

Merge sensitive data discovery with advanced detection across all your cloud data channels

Stop the exfiltration of sensitive data by combining machine learning-based data classification from the Cohesity Data Cloud and comprehensive data loss prevention (DLP) from Zscaler Data Protection. Through API integration, you can fingerprint and index sensitive data within your organization using backups of your primary data assets. Use this information to detect sensitive data in outbound traffic, and block detected suspicious transmissions from your network. This safeguards your data assets against exfiltration and helps you maintain compliance with regulations like the GDPR and HIPAA.

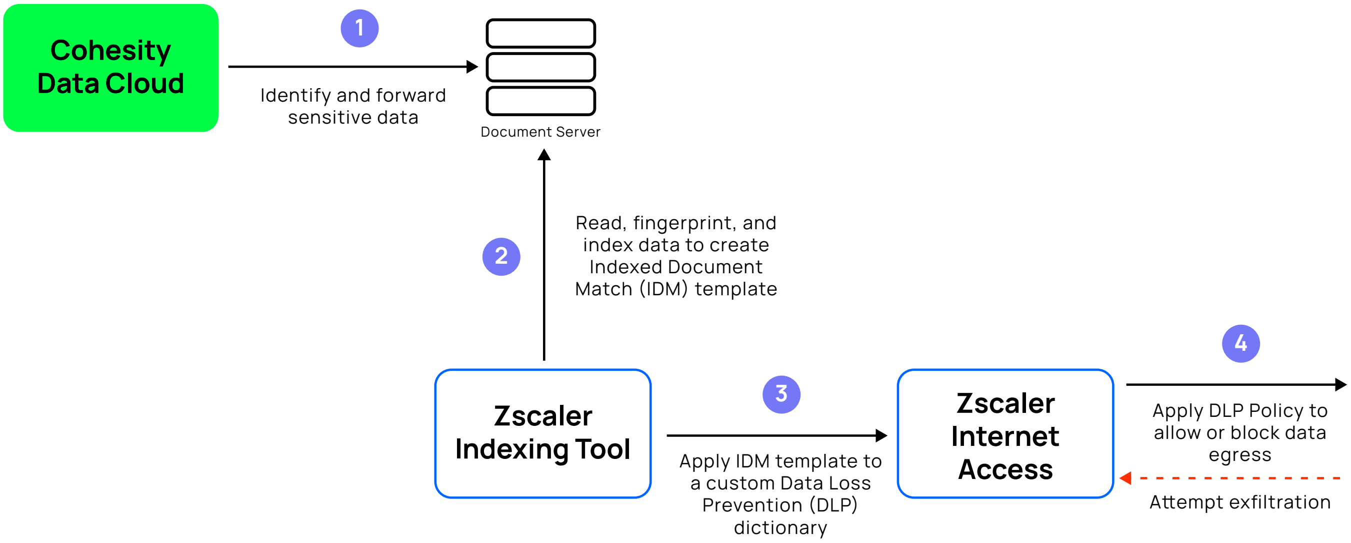
Cohesity Data Cloud
1
Identify and forward sensitive data
Document Server
2
Read, fingerprint, and index data to create Indexed Document Match (IDM) template
Zscaler Indexing Tool
3
Apply IDM template to a custom Data Loss Prevention (DLP) dictionary
Zscaler Internet Access
4
Apply DLP Policy to allow or block data egress
Attempt exfiltration

Fig. 1: High-level workflow: Cohesity and Zscaler integration

Solution Capabilities

Accurately classify sensitive data

Find sensitive and regulated data in workloads backed up on Cohesity using our ML-based data classification. Cohesity's highly accurate ML-based engine uses over 200 patterns to automatically discover and classify personal, health, and financial data automatically or on demand.

Stop data loss with indexed document matching (IDM) and security service edge (SSE)

With Zscaler IDM templates, you can fingerprint and index your organization's critical documents containing sensitive data and detect documents that match those templates across all channels of data loss—email, endpoint, SaaS, IaaS, and web. Inspect all traffic at scale with Zscaler Internet Access and block or allow transactions per your DLP policy.

Stop cybercriminals in their tracks and protect your sensitive data against exfiltration. See the configuration guidelines and get the integration from the Cohesity Marketplace.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY.com I 1-855-926-4374 I 300 Park Ave., Suite 1700, San Jose, CA 95110 3000154-001-EN 5-2024