Data Exfiltration Assessment

Solution Brief

Challenging Your DLP Controls

Cymulate's Data Exfiltration vector enables you to test the effectiveness of your Data Loss Prevention (DLP) security controls and optimize them. This vector challenges your DLP controls with a broad range of regulatory and custom data sets and exfiltration methods, that together with the results provides actionable remediation guidelines.

Attack Vector Overview

DLP solutions are designed to protect against both malicious and unintentional data exfiltration. Corporate-confidential data such as financial reports prior to publication, source code, and other intellectual property must be protected from corporate espionage. In addition, companies must comply with strict laws and regulations, regarding the handling of sensitive data or PII (personally identifiable information), such as GDPR, HIPAA, and PCI-DSS. DLP also protects employees from inadvertently storing and/ sharing sensitive information on unsanctioned cloud services (shadow IT).

Continuous Testing

Companies should be able to test their DLP controls frequently in the face of regulatory revisions, updates to corporate data security policies and new exfiltration methods. The Data Exfiltration vector evaluates the effectiveness of your DLP solution to prevent extraction of critical information. The security assessment is non-disruptive and can be performed continuously to validate that confidential and sensitive information assets remain secured on an ongoing basis.

How It Works

Test Setup - Select a test-template for the DLP assessment, or create your own from the library of data sets and exfiltration methods. Data types include synthetic data that apply to regulatory requirements and common types of corporate intellectual property. Additionally, you can test with your own data sets. Exfiltration techniques are grouped by the following methods:

- HTTP & HTTPS
- DNS & DNS Tunneling
- ICMP Tunneling
- Secure File Transfer Protocol
- Email
- Removable Device (USB)
- Cloud Services

The exfiltration techniques are updated in the platform on an ongoing basis

Test Execution: Once initiated, the Cymulate Agent will attempt to exfiltrate information using all the combinations of data types and exfiltration methods defined in the test-template. The data sets will be embedded in filetypes, including office documents, images, and other file types.

Test Results and Remediation: A comprehensive report is generated after each assessment, comparing the results to previous assessments and identifying the security gaps that need to be addressed.

Synthetic Confidential and Sensitive Data → **Export Techniques** → **Data Loss Prevention** → **Report**
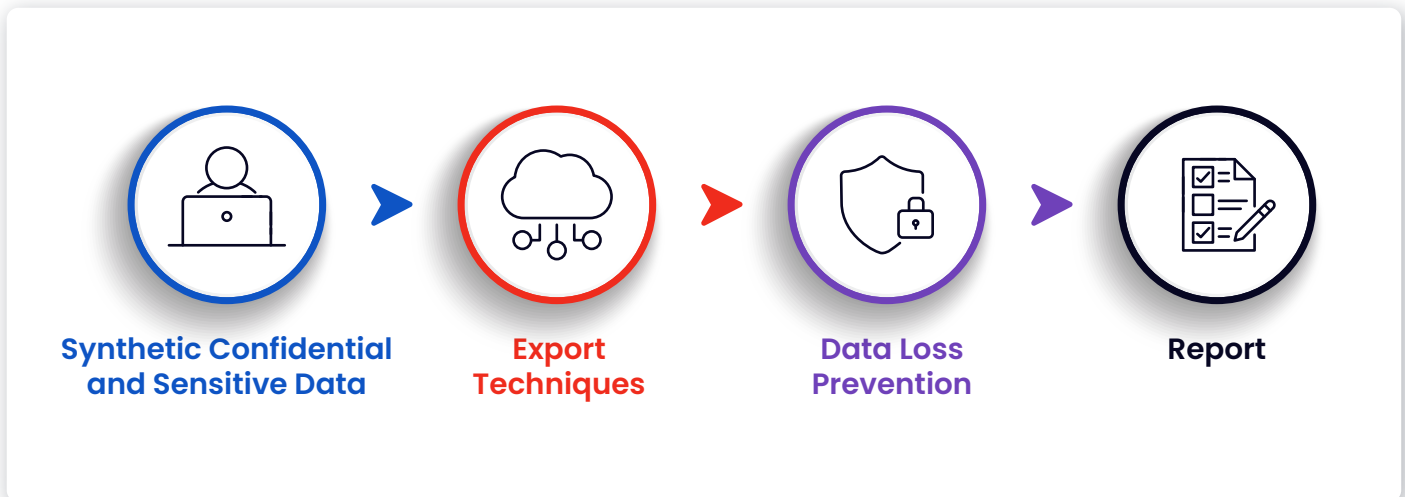
Key Features

- A broad library of synthetic regulatory and company confidential data types in addition to custom data sets are available for DLP testing.
- Assessments use multiple exfiltration methods and file types used by hackers.
- Uses a single agent to test your organization's security controls.
- Testing is non-disruptive and can be performed on the production network anytime, from anywhere.

Actionable Insights

The attack simulation results are presented in a comprehensive and easy-to-use format, allowing organizations to understand their DLP-related security gaps and take the appropriate measures using actionable mitigation recommendations.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial