Cisco Umbrella Data Loss Prevention (DLP)

Get visibility and control of sensitive data leaving your organization

Challenges

Keeping sensitive information safe has never been easy. With the widespread adoption of collaboration tools and cloud apps, enterprises face new security problems along with compliance challenges. As more companies unplug their on-premises systems and move to cloud-based services, company data becomes more vulnerable to both malicious exfiltration and unintentional misuse by inexperienced users.

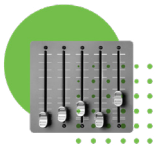
Solution

Cisco Umbrella data loss prevention (DLP) analyzes sensitive data in-line to provide visibility and control over sensitive data leaving your organization. It is easy to enable in conjunction with Umbrella secure web gateway (SWG) and simple to manage with flexible policies incorporating pre-built, customizable data identifiers. DLP is an integrated capability of Cisco Umbrella, one of the core components of Cisco's SASE architecture. Umbrella integrates multiple components that were once standalone security services and appliances in a single, cloud-native solution. With the cloud-native DLP function integrated into your existing Umbrella subscription, you can achieve your compliance goals while simplifying your security stack and taking the next step in your SASE journey.

58% of data breaches involve personal data[1]

64% of employees have access to 1,000 or more sensitive files[2]

Features



Define and control

- Leverage 75 pre-built data identifiers covering content such as personally identifiable information (PII), financial details, and personal health information (PHI) – customizable to target specific content and reduce false positives
- Create user-defined dictionaries using custom keywords such as project code names
- Create flexible policies for granular control – applying organization-specific data identifiers to target specific users, groups, locations, cloud apps, and destinations
- Manage DLP administration directly from the Umbrella dashboard

Detect and enforce

- Analyze sensitive data in-line with high throughput, low latency, and elastic scale
- Leverage the Umbrella SWG proxy for scalable SSL decryption
- Analyze sensitive data flows to select cloud apps and file uploads to any destination
- Discover and block sensitive data being transmitted to unwanted destinations and potential sensitive data exposure in sanctioned applications, preventing data exfiltration events from taking place

Monitor and report

- Gain rapid insights for quick discovery and investigation of potential sensitive data loss events
- Get drill-down reports with detailed information including identity, file name, destination, classification, pattern match, excerpt, triggered rule, and more

1. Verizon, 2020 Data Breach Investigation Report, 2020
2. Varonis, 2021 Global Data Risk Report, 2021