SOLUTION BRIEF

VERSA

Versa Data Loss Prevention

Comprehensive Data Security

Data is an organization's most valuable asset, yet controlling and securing it has become increasingly complex. Modern enterprises navigate a complex digital landscape where data flows across on-premises systems, cloud storage, and BYOD setups. Data volumes are also expanding exponentially, creating additional challenges for managing and securing data.

Data breaches have serious consequences for individuals and businesses, including financial losses, reputational damage, legal liability, and regulatory penalties. According to IBM's Cost of a Data Breach Report 2024, the average cost of a data breach is $4.88 Million. The average cost of a malicious insider attack was even costlier at $4.99 Million.

With distributed workforces the norm, data residing in diverse locations, and data breaches financially crippling, organizations need advanced Data Loss Prevention (DLP) to protect sensitive information, ensure compliance, and maintain robust data visibility and control.

Heightened Needs for DLP

As organizations strive to protect their assets in this intricate, digital landscape, the critical need for DLP becomes evident. First, there is the pressing need to protect sensitive data from unauthorized exposure, especially as it travels across various environments and devices. Insider threats also pose significant risks, with employees or other internal users potentially exposing data either accidentally or with malicious intent. Regulatory compliance is another key driver — organizations must adhere to strict data protection standards outlined by laws such as GDPR, HIPAA, and PCI-DSS.

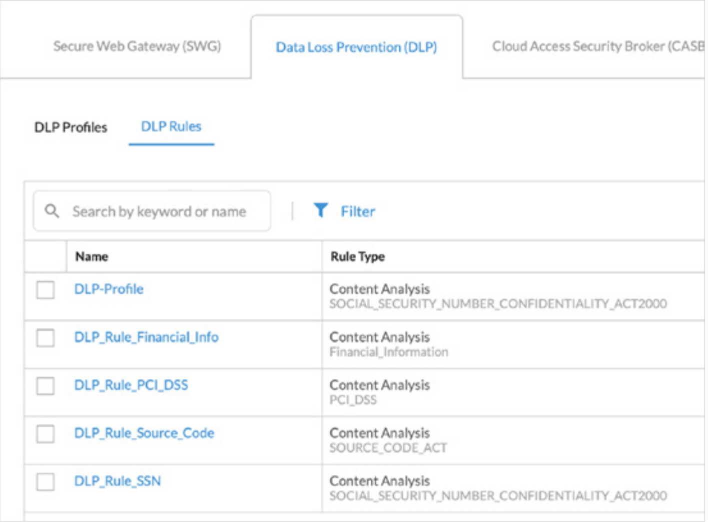
A comprehensive DLP solution plays a crucial role in helping enterprises safeguard data and meet regulatory mandates by ensuring that sensitive data is properly controlled and managed. A DLP solution monitors and prevents unauthorized data access or transfers. DLP policies can be put in place to ensure organizations are handling data according to relevant data compliance rules. Finally, detailed logs provide data visibility and aid in potential investigations.

Versa DLP Solution

Versa offers a comprehensive DLP solution that addresses the unique data security challenges of today's enterprises. Versa DLP combines inline network and endpoint DLP capabilities, allowing for a consistent, unified security framework that adapts to various data flow scenarios.

Network DLP

Versa Network DLP includes 15+ pre-defined compliance profiles and 120+ customizable data patterns that support regulatory compliance including HIPAA, PCI-DSS, GDPR, and CCPA. With advanced data-matching techniques like exact data match (EDM), indexed document match or document fingerprinting, and OCR (Optical Character Recognition), sensitive data identification can be identified across multiple protocols including HTTPS, or email protocols, multiple file types - PDFs, Microsoft Office files, and images. In addition, Microsoft Information Protection (MIP) label integration allows alignment of Versa DLP policies with existing data standards. Versa Network DLP provides flexible data-handling options—including allow, block, redact, and tokenize—allowing organizations to tailor responses to the sensitivity and requirements of their security policies.

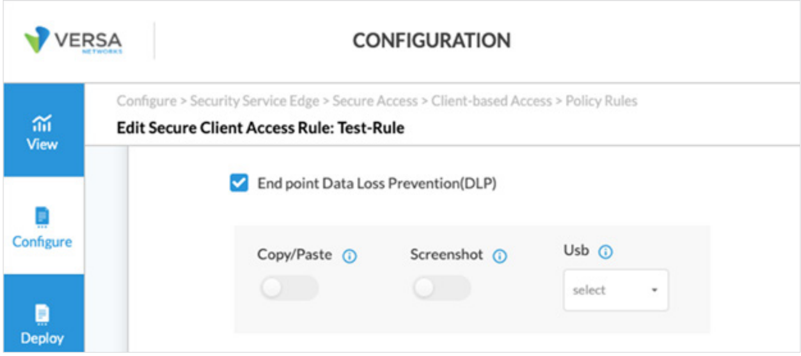

Secure Web Gateway (SWG)
Data Loss Prevention (DLP)
Cloud Access Security Broker (CASB
DLP Profiles
DLP Rules
Search by keyword or name
Filter

	Name	Rule Type
□	DLP-Profile	Content Analysis SOCIAL_SECURITY_NUMBER_CONFIDENTIALITY_ACT2000
□	DLP_Rule_Financial_Info	Content Analysis Financial_Information
□	DLP_Rule_PCI_DSS	Content Analysis PCI_DSS
□	DLP_Rule_Source_Code	Content Analysis SOURCE_CODE_ACT
□	DLP_Rule_SSN	Content Analysis SOCIAL_SECURITY_NUMBER_CONFIDENTIALITY_ACT2000

Easily comply with regulatory requirements with predefined compliance profiles and customizable policies.

Endpoint DLP

Versa Endpoint DLP further strengthens data security by preventing unauthorized actions on endpoints such as copy/paste, screenshots, and data removal to external devices (USB). These capabilities are especially useful in highly regulated industries and scenarios where the act of copying or removing any information is strictly prohibited (e.g. call centers working with customer PII, point-of-sale stations, healthcare workstations, etc.).



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Secure Client Access Rule: Test-Rule

☑ End point Data Loss Prevention(DLP)

Copy/Paste ⓘ

Screenshot ⓘ

Usb ⓘ select ▾

Prevent data exfiltration on endpoint from copy/paste, screenshots, and USB removal (block or read-only).

Versa Endpoint DLP also helps organizations preserve end user experiences. Consider scenarios where virtual desktop infrastructure (VDI) are used. Since VDIs are centralized services, they often have high latency and performance issues for users at branch locations, negatively affecting user experience and productivity. Versa Endpoint DLP can replace virtual desktops in environments where strict controls are necessary. Since enforcement happens on the endpoint itself, endpoint DLP does not introduce latency or performance issues, allowing users to maintain optimal user experience and improving productivity.

Versa's Endpoint DLP is enabled through Versa's lightweight and feature-rich SASE client.

Benefits of Versa DLP

Versa DLP provides comprehensive data security for distributed and hybrid environments, unifying DLP policy management across campus networks, distributed workforces, cloud applications, and endpoints. This enables organizations to enforce consistent policies regardless of where data resides, while also allowing for granular control over data flow through application-aware policies. Versa's unified architecture scales seamlessly across on-premises, cloud, and hybrid environments, making it an adaptable solution for enterprises of all sizes. With capabilities to decrypt and inspect encrypted traffic and monitor data flow, Versa DLP leverages big data analytics for enhanced visibility and insight.

Integration with Versa's advanced security services, such as Remote Browser Isolation (RBI), Advanced Threat Protection (ATP), and Zero Trust Network Access (ZTNA), ensures that data protection is layered within a comprehensive security framework. This helps prevent data breaches and insider threats, enforces compliance, and protects sensitive information. With the ability to cover diverse data protection requirements, organizations can use Versa DLP to ensure secure collaboration on cloud applications, data sharing with third parties, and protection of sensitive information within emails and messaging apps.

BENEFITS OF VERSA NETWORK AND ENDPOINT DLP

- Enforce consistent compliance and data usage policies across on-premises locations, cloud, and endpoints
- Prevent data exfiltration from data breaches and insider threats
- Protect financial data, IP, PII, and other sensitive information
- Secure collaboration with cloud apps
- Protect sensitive information in emails and messaging apps
- Secure data sharing with third parties
- Gain detailed data visibility and control

Versa DLP can be deployed in multiple form factors, including cloud-delivered and on-premises, offering flexible options to fit diverse organizational needs. Versa DLP is available with the Versa Unified SASE platform, Secure SD-WAN, and Secure Service Edge (SSE). With its robust capabilities, Versa DLP offers a scalable, flexible solution for data security, empowering enterprises to maintain data integrity and compliance across complex, distributed environments.

Learn more about Versa Inline and Endpoint DLP at versa-networks.com.

VERSA