Secure Your Organization's Critical Data

VMware Cloud Web Security with DLP

Data loss prevention (DLP) is a key capability of VMware Cloud Web Security™ and the VMware SASE portfolio. Part of VMware's 'defense-in-depth' approach to cloud security, the DLP solution helps organizations:

- Identify sensitive data in the organization and protect it during its transit within and outside the organization
- Navigate through a complex regulatory landscape and achieve compliance

In today's hyperconnected world, a company's sensitive data resides across a myriad of user devices, IT applications, and in the cloud. This data is stored and processed by external entities and freely exchanged across geographies. While a larger global digital footprint is helping businesses thrive, it is also leading to an increased incidence of data breaches and making it harder for companies to comply with regulatory requirements.

Data breaches are expensive

According to IBM's Cost of a Data Breach Report 2022, the average cost of a data breach was $4.35M[1]. Further, 82% of all data breaches worldwide had human involvement[2] either accidentally (e.g., phishing, social engineering attacks) or through malicious intent (e.g., insider attacks). Given the de-centralized IT environments in organizations today, these numbers are bound to go up without a comprehensive data loss prevention (DLP) strategy.

DLP is a set of tools, capabilities, and processes to track and safeguard data at each stage of its lifecycle:

- **Data at rest:** Data that is stored in a physical or logical form, e.g., system logs stored on a server, medical records in a database.
- **Data in use:** Data that is actively being processed, accessed, or read, typically on an endpoint, e.g., a spreadsheet being edited by a user.
- **Data in motion:** Data that is being transmitted within or outside the corporate network perimeter, e.g., files exchanged over email or instant messaging platforms.

[1] IBM – Cost of a Data Breach Report 2022
[2] Verizon – Data Breach Investigations Report 2022

The regulatory landscape is complex and evolving

Consider an enterprise that operates in the US and processes transactions. Customers' financial data is considered highly sensitive and must comply with Payment Card Industry Data Security Standard (PCI DSS) regulations. If the enterprise has a branch that operates in the European Union (EU), customer data needs to be processed differently in line with the EU General Data Protection Regulation (GDPR) requirements. While many organizations may have dedicated IT and security teams to implement such complex data security and privacy policies, there is a need for a solution to audit and ensure that there are no blind spots in regulatory compliance.

Introducing VMware's approach to DLP

The DLP solution offered by VMware Cloud Web Security is an agentless, cloud-hosted solution that applies policies inline and monitors the data in motion between end users and external applications to prevent sensitive data from ever leaving the enterprise.

No "one-size fits all" approach

Using the DLP solution, IT and security administrators can set and enforce fine-grained security policies that inspect file uploads and control the types of data that specific users and user groups can share based on the organization's data classification policy. For example, interns and contractors could not upload files that contain sensitive data outside the organization, while full-time employees could do so. This ensures that data loss is prevented while still allowing users to collaborate.

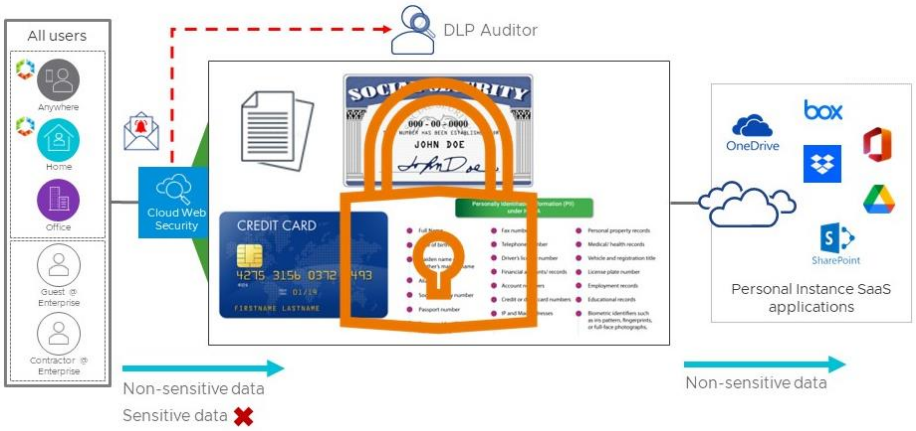

Figure 1: DLP in action enforcing policies based on data classification

Key benefits

- DLP is an effective approach to prevent sensitive data from being exfiltrated
- VMware's approach enforces DLP policies in real-time when data is in motion between end users and external applications
- The solution is flexible and easy to set-up with out-of-the-box dictionaries and customizable definitions to meet business needs

Learn more

- VMware Cloud Web Security, *sase.vmware.com/products/cloud-web-security*
- VMware SASE, *sase.vmware.com*

Easy setup and customization

Implementing DLP policies from scratch can be difficult and time-consuming. With VMware Cloud Web Security, IT and security admins have a great starting point with 350+ out-of-the box dictionaries covering 11 regional localizations of sensitive data types, and the option to create custom dictionaries aligned to their unique business requirements.

Ongoing regulatory compliance

DLP combines core data security and privacy tenets to deliver a solution that can help you maintain compliance with relevant regulatory requirements including GDPR, PCI-DSS and HIPAA, among others. Organizations can start viewing regulatory compliance as a key differentiator instead of a roadblock.

Early detection and response

A potential violation of a DLP rule is immediately blocked and triggers an audit trail that notifies the auditors with details of the incident. This promotes early detection and response, preventing security incidents from turning into data breaches.

Why adopt the DLP solution from VMware?

VMware Cloud Web Security with DLP combines robust data security and effective regulatory compliance without impeding business performance. Its benefits for different stakeholders within the organization are as follows:

Stakeholder	Benefits provided by DLP in VMware Cloud Web Security
Senior management	✓ More confidence in security posture ✓ Enhanced data governance ✓ Lower incidence of data breaches
IT and security teams	✓ Real-time control over data-in-motion ✓ Simple policy creation and customization ✓ Regulatory compliance and audit checks
End users	✓ Centrally controlled data sharing ✓ Prevention of accidental data leakage ✓ Data privacy requirements fulfilled