Versa Data Loss Prevention

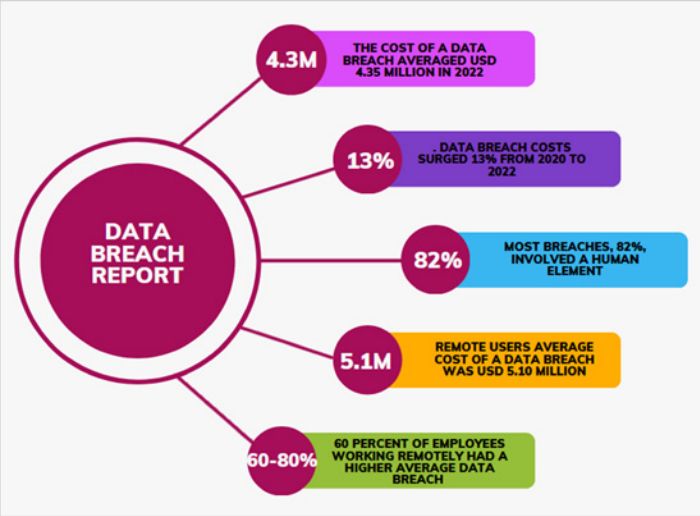
Protect and govern data with Versa DLP Solution

Introduction

Data is the most valuable asset for any organization. In today's world, data is scattered across different geographies, storages, and cloud computing. Controlling and protecting sensitive data has become more challenging due to the data landscape. Data volumes that are generated in a digital world are exploding to exponential levels.

4.35M
average cost of a data breach

Data breaches have serious forfeits for individuals and businesses, including financial losses, reputational damage, legal liability, and regulatory penalties. **According to IBM Data Breach Report 2022, Data breach costs surged 12.7% from 2020 to 2022 and the average cost of a data breach is USD 4.35 million.**



Protecting data from unauthorized/ malicious users and sophisticated attacks is extremely important for any organization. With modern attacks and evading techniques, the data need to be protected in all states Data at Rest, in transit, and in use. To protect data, one should be aware of what needs to be protected, how it needs to be protected, and when it needs to be protected.

In the Current rise of hybrid workplace models, cloud computing, and complex trust models, organizations need a data-centric approach that allows a single unified data protection model that can be used throughout the enterprise. Organizations can use Versa's unified SASE/SSE architecture with Application visibility and Zero Trust approach to prevent data exposure.

The best way to prevent security threats is to build a layered defense strategy. Organizations need to reduce the attack surface, actively look for suspicious activity and insider threats that could lead to data breaches, and plan an effective response strategy. Here Versa DLP solution comes in with proficiency with security services that include Secure SD-WAN, SASE capabilities that include NGFW, ATP, CASB, DLP, ZTNA, VSA.

Though organizational data is complex and unique with specific customization requirements, there are some critical functionalities that an ideal DLP solution should include to meet the industry standards.

What Are the Key Considerations for DLP Solution?

Deeper Data Visibility

Data around the internet is 95% encrypted using SSL/TLS traffic in Digital World. Organizations need comprehensive capabilities to monitor and control encrypted traffic to identify the risk and make business decisions. Versa Single-Pass architecture with native decryption functionality allows decrypting the traffic and identifying the Sensitive data for applying data security policies.

Versa Deep Packet inspection(DPI) engine can identify 3800+ applications and URL categorization to inspect the applications and categorize the URLs to apply data security policies based on the dynamic requirements.

Also, the Versa Antivirus / File filtering feature scan/inspect the traffic to protect the network from threats such as malware, worms, and virus that are embedded with files.

At the same time, sensitive data need to be masked using DLP redaction so that only authorized people have privileges to view the sensitive data.

Cloud Data Protection

Cloud adoption has evolved and become standard for any organization to host their services in the cloud. Most cloud platforms provide security to protect their virtual instances and services, but the most critical part is securing the data. Versa CASB solutions seamlessly integrated with the DLP module provide regulatory compliance, data security, and threat protection with granular access for cloud applications. Ex: Protecting data theft from uploading sensitive information to personal storage accounts EXCEPT for corporate cloud storage or cloud applications.

Regulatory Compliance

Whether you run your workloads in the public cloud or a private cloud or a hybrid infrastructure, or a multi-cloud with several cloud providers organization, sensitive information needs to comply with data regulations and ensure the security of your data. Financial organizations need to comply with PCI-DSS and Healthcare organizations need HIPAA Compliance, Privacy compliance, etc. Any non-compliance will undergo a law enforcement policies act and financial regulations. Versa Unified DLP/CASB solution has inbuilt regulatory compliance that helps organizations to adhere data regulatory policies and safeguard the data.

Network Protection

Most of the organization traffic is through web channel HTTP/HTTPS which includes email, web applications, and chat. The data flowing through the channel needs to be monitored and controlled based on the organization's requirements. Versa Secure web gateway and On-Prem solution can assess the traffic and define granular policies based on the Zero Trust Network Model by using different elements such as user identity, location, operating system, and device type to protect the data.

With the above consideration, Versa Advanced Data Loss Protection solution helps you in protecting critical data with controls and policies based on defined risk and data sensitivity. Versa DLP delivers data protection to build Robust data security policies and controls around your critical sensitive data irrespective of where data flows.

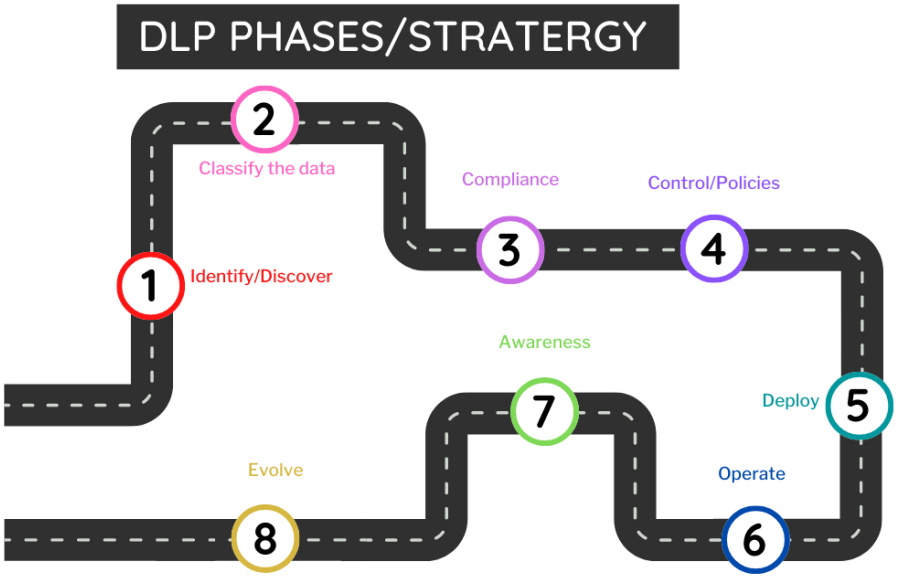
Data Loss Prevention

Data loss prevention (DLP) helps to prevent potential data leaks from being lost or stolen by unauthorized communication channels through the network, endpoint etc. DLP controls help to reduce the risk of data leakage, data loss and data exfiltration by ensuring that sensitive information is identified, and risk-appropriate controls are deployed.

DLP lifecycle has different strategies that need to be followed to have a successful DLP solution.

- **Identify and Discover:** Identify the business-sensitive data, create an inventory of data, and locate sensitive data wherever it is stored. Data can be stored in file shares, cloud storages, etc. Identifying critical data is the first key step to prevent data theft.
- **Classification:** Data classification is one of the important processes in the data protection life cycle. Classifying sensitive data based on business risk and impact will allow organizations to manage data effectively. Data can be classified as Personal, Public, Critical, Confidential and so on to control the accessibility of the data, based on the Data classification DLP controls that are applied to protect the valuable information.
- **Compliance:** Data Privacy and regulations are key aspects of security and compliance, as data breaches usually aim to extract Personal Identifiable Information/ Sensitive information. Regulations like PCI-DSS, HIPAA, GDPR, and CCPA are imperative in certain regions based on the regulation of laws. Failure to maintain compliance with these regulations can result in serious penalties and possibly private rights of action.
- **Deploy:** DLP solution should be flexible in defining the policies for any dynamic and agile business requirements. Policies can be defined based on user, application, file types, geography and various other DLP controls.
- **Operate:** DLP systems require continuous monitoring or alerting mechanism to identify the data loss. DLP solutions can be integrated with the ITSM tool for auto-recording the incidents and SIEM tool for real-time monitoring and alerting.
- **Awareness:** User should be educated that the data are being monitored. Awareness sessions about data loss and its impact will prevent users from falling into any type of attack.

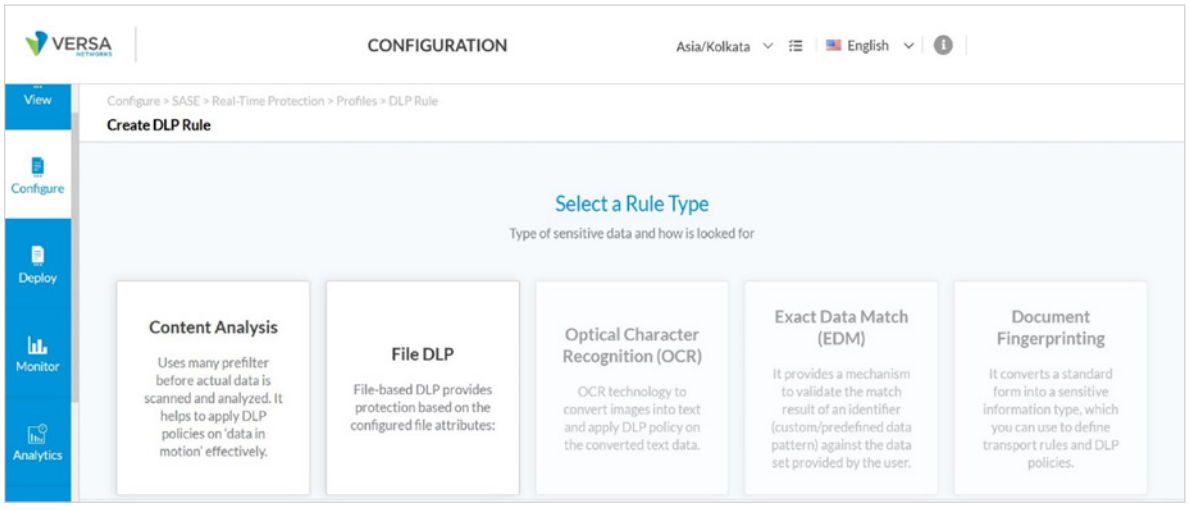
- **Evolve:** As per Gartner, DLP is not a set-it-and-forget program. It needs continuous monitoring and fine-tuning process. Changes in Data types may happen in organizations at any time so adapting and change in DLP policies will be a constant effort.



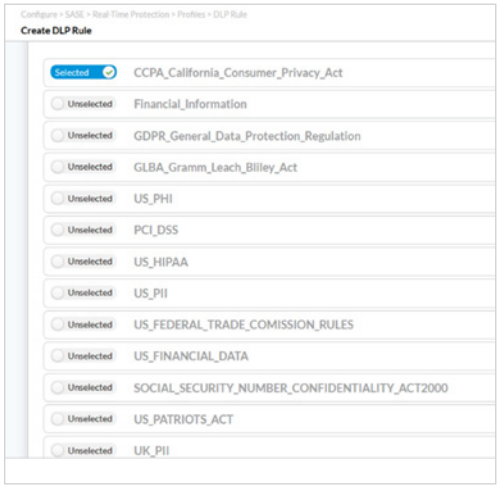
In the following section, we will discuss Versa's Key DLP features. Versa DLP solution provides deeper content analysis through various features to protect organization data. Versa DLP solution is agile and flexible enough to define the policies through a unified SASE solution.

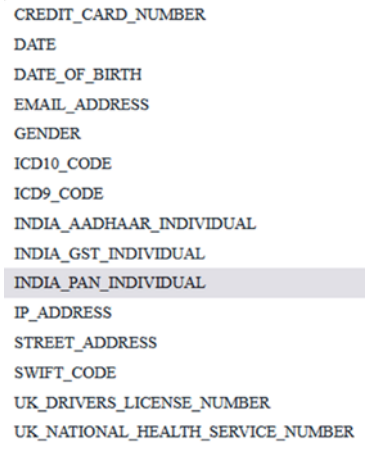
Key Features and Benefits

1. **Fingerprinting:** Document fingerprinting can help to protect sensitive documents that are available in storage/file servers by defining the DLP policy. Versa fingerprinting solution can take an identical copy of the files and convert them into sensitive file types based on the classification and protect the data loss that occurs via the network. Ex: The user trying to send confidential billing information to an unauthorized network can be protected by fingerprinting that matches the unique pattern of the document.
2. **Exact data match:** Exact data match (EDM) is a precise data loss prevention (DLP) technique that monitors and protects sensitive data exfiltration such as PII, Financial records, Intellectual property etc. EDM matches the exact data values with high accuracy that are important to the organization and reduces the false positive alerts triggered. Ex: scanning for credit card information would lead to a bunch of alerts. With the support of EDM combination of fields can be used to match the exact credit cards, names, and phone numbers can be matched for additional validation to get more accurate results.
3. **OCR (Optical Character Recognition) Roadmap:** Strengthening the DLP protection using Versa OCR features helps to detect the data loss that occurs via various image file types. Data loss can occur through network and email channels via jpeg, png, pdf image files, images in documents and power points, etc. To protect the sensitive data leak from image files OCR can be enabled along with DLP and CASB policies.

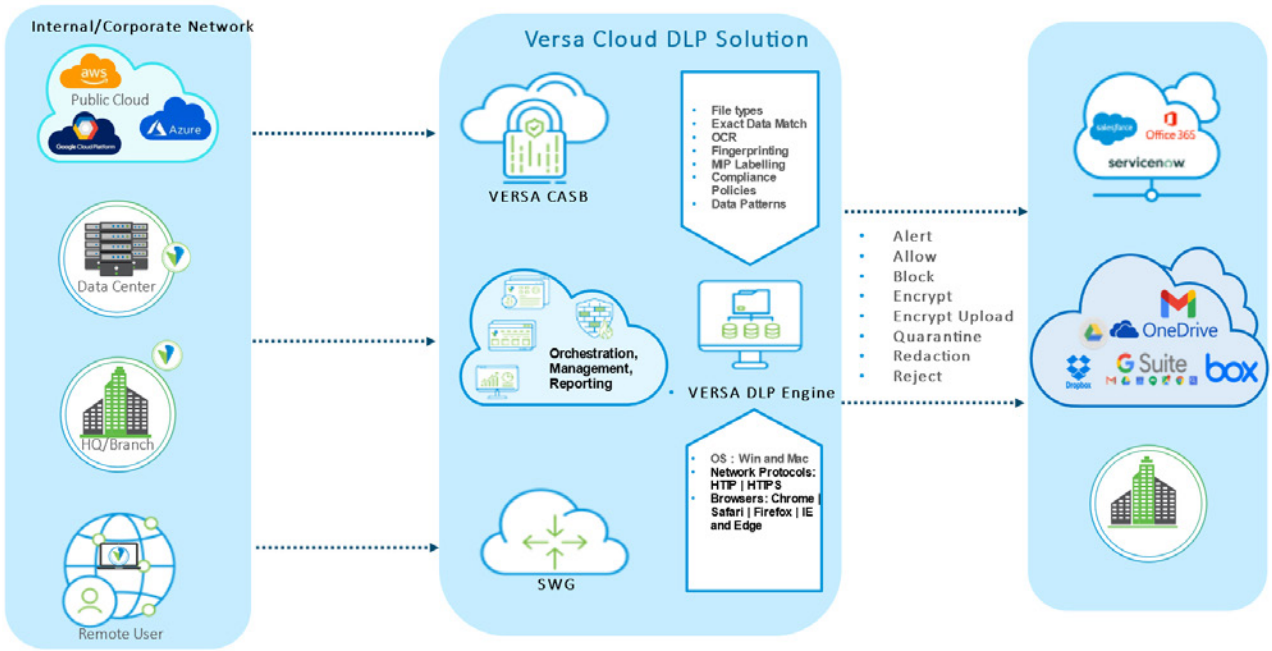


4. **Compliance Policies:** Organizations collect and store customer data in the form of Personally Identifiable Information (PII) (SSN, AADHAR, Passport details etc), Protected Health Information (PHI), or payment card information (PCI), etc. To safeguard and meet the compliance regulations organization need to adhere to standards like HIPAA, PCI-DSS, GDPR, CCPA, etc. Versa Predefined compliance profiles (15+) and patterns (120+) helps to map the required standards in DLP policies to meet regulatory compliance and prevent data leak.





5. **Classification:** Organizations will store and process countless documents, therefore it will be difficult to monitor those documents whether they have sensitive information or not. With the help of labelling, documents are associated with a tag/label that can classify the document and DLP systems can apply appropriate policies/labels. Labelling helps to define the criticality of the document types and the risks associated. Versa DLP system has been integrated with MIP (Microsoft Information Protection) for the classification policies. MIP has 100+ labelling types by default (Public, Personal, Confidential, etc.) and custom labels can be created. DLP systems can act based on the policy defined for labelling.
6. **Data Patterns/File Types:** the most commonly enabled feature for DLP Protection is pattern match and file types, Versa supports regular expression-based pattern match with predefined and custom profiles. Standard file types are supported for file analysis.



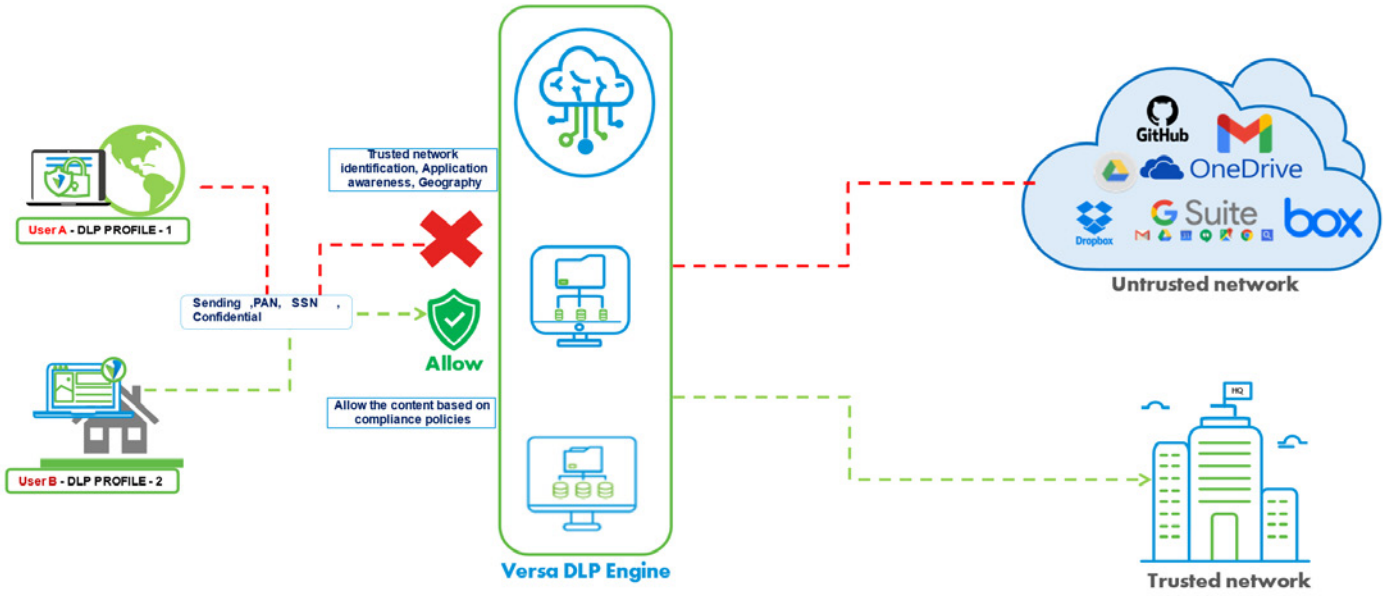
With the above Versa DLP features, Organizations can deploy the Versa DLP solution that can fit in easily and combat over the data protection. Versa DLP provides a wide range of solutions for various environments; the common use-case solutions are laid out below.

DLP for Remote Workforce

Due to the Pandemic, the traditional On-Prem workforce has been shifted to a remote or hybrid workforce and hence controlling the data over remote users becomes difficult and crucial. Organizations apply different policies such as restricting internet access and download/upload restrictions to control users from exposing to cyber-attacks. With the current evasive techniques and encrypted traffic, controlling sensitive data becomes cumbersome for an organization to have full-blown visibility and control. To control and Manage Remote Workforce data security, Versa Unified SASE solution with DLP solution provides secure access and control over sensitive data. To protect the remote workforce from intentional and unintentional data thefts, DLP policies with regulatory compliance, Labeling controls, ZTNA, Pre-built DLP policies, custom DLP policies, and OCR can be enforced. Along with Data Protection other security features like application control, AV engine, File filtering, and Best VPN gateway can be added security advantages for remote users to protect against threats.

Scenario: The DLP policy needs to be enabled to protect the data leak for PAN, SSN, and confidential documents when the user is sending anything to an untrusted network.

Remote VPN Users - DLP Flow



1. User Identity is identified based on the Zero Trust network access policy (Identity the user location, application, user and device identity, and Compliance) for the remote user.
2. User A belongs to the Finance department and DLP policy is set to block confidential documents as per labelling.
3. Versa systems integrated with Microsoft Purview Information protection sensitivity labels seamlessly integrated and fetch the labeling information and apply the DLP policy.
4. If a user tries to send confidential documents towards an external zone or untrusted network DLP policy will be inspected and blocked. In Addition, the incident will be reported to the Analytics console for SOC analysis.
5. When the same user is in a corporate network, the user can send confidential documents internally within the organization.

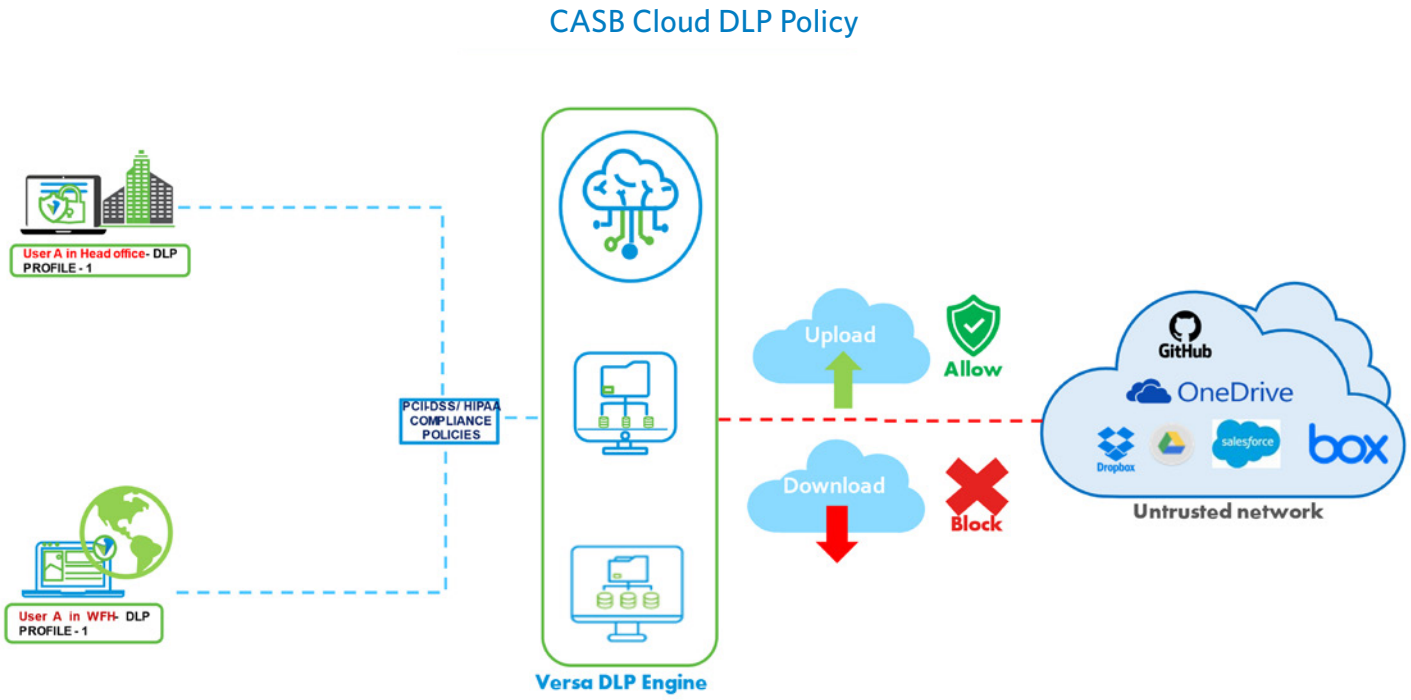
Solution: Implement Versa Cloud gateway and On-Prem Network DLP Solution for Roaming Users.

DLP for Cloud Resources

Organizations adopting the cloud and digital transformation have been growing at a faster rate and becoming the new normal for enterprises. As per Hashicorp, 76% of organizations use the cloud to host their services. Data exists in cloud SaaS services such as O365, Salesforce, and GitHub that need data protection and masking. Versa's Cloud DLP Solution extends the data security policy via CASB and Network DLP services to protect the cloud data by encrypting or tokenizing sensitive content to enforce privacy. Versa CASB solution can be deployed in a different deployment mode to have cloud data visibility, prevent data leakage, and enable compliance. In addition, embedded security features such as Cloud ATP, ZTNA and Next Gen firewall services reduce cloud attack exposure.

Scenario: DLP policy needs to be enabled to protect the data leak from cloud SaaS Applications/storage.

Deploy Cloud CASB solution in Inline or Reverse proxy with the integration of API to scan for sensitive information, configure data security policies to protect against sensitive information data leakage by applying advanced techniques such as data identities, regular expressions, Compliance Policies, exact data matching and OCR.



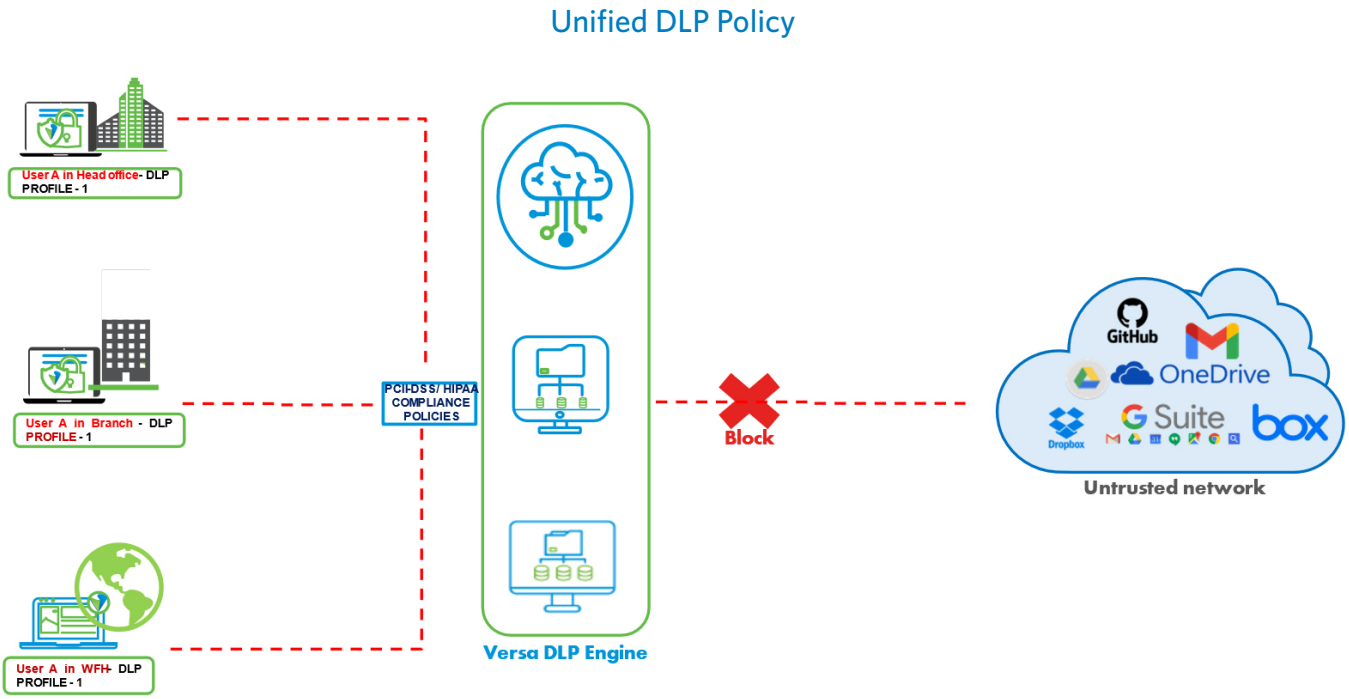
Users can upload the information to corporate cloud SaaS applications but cannot download any PCI-DSS/HIPAA related information based on the DLP policy.

Solution: Implement Versa CASB Solution to protect against data leakage from Cloud SaaS / Infrastructure Applications.

DLP for Web/Network

Enterprise-wide traffic need to be inspected and monitored to protect against data loss because data in motion or transit is the most vulnerable point, protect the information in this state requires a comprehensive data security approach where Versa Unified User policy will be dynamically enforced to users across all work environment (Datacenter, Remote user or hybrid). Versa solution will decrypt and monitor web email traffic, chats, online file transfers, etc, and apply the dlp controls that can protect PII, Financial Data, and Intellectual property information.

Scenario: DLP policy needs to be enabled for the User to protect against the data leak for PCI-DSS/HIPAA for the external network.



1. DLP Profile -1: Versa Unified DLP policy is enabled in On-Prem VOS gateways to achieve PCI-DSS/HIPAA compliance, Versa inbuilt patterns and DLP profiles are applied to inspect the data traffic.
2. Users trying to send credit card information outside the network can be blocked by enabling a PCI-DSS compliance profile or pre-defined patterns that match credit card details or Exact data match condition DLP policy.
3. DLP violation rules will be sent to the Analytics console for Soc Analysis.

Solution: Implement Network DLP Solution for On-Prem Users.

Versa DLP Solution Benefits

1. Robust and Unified DLP policy management for a remote workforce, network users, and cloud applications.
2. Data Visibility and Application aware policies with embedded security features to protect Sensitive Data.
3. Versa DLP solution's key features Fingerprinting, Exact Data Match, OCR, Labeling, and Compliance policies can help organizations to comply with industry standards and prevent data leakage.
4. Versa DLP solution can scale and extend to On-Prem Datacenter, Cloud or Hybrid environments.
5. Inspect Encrypted traffic and get Unmatched Data Visibility, Configure the DLP policies with Automation and Monitor the data flow with big data Analytics solution with Versa Unified Architecture.
6. Versa Advanced security services like Remote Browser Isolation, Advanced Threat Prevention, and Zero Trust Network Access can prevent zero-day attacks and enable borderless and granular user access.

Other Considerations

The DLP process needs strategic planning to combat data theft. Based on organization requirements, choose the type of DLP solution your organization is looking for, whether network DLP or cloud DLP or Hybrid.

Versa DLP solution gives visibility and control over the data points and sensitive information that flows through the network or cloud application.

Training and user awareness sessions help to educate and prevent them from becoming victims of any attacks.

Versa Concerto provides a single pane of glass for Management, Reporting, and a complete set of end-to-end orchestration functions of services including configuration design, implementation, zero-touch-provisioning, deployment, monitoring, and analytics capabilities.

Versa big data Analytics solution provides powerful reporting functionalities, holistic real-time and historical view of the Logs related to Threats, DLP, Application visibility, Remote Users, SDWAN, etc. Versa solution can be integrated with the SIEM tool to provide real-time security incident response.

Versa advanced security services include Remote Browser Isolation, ATP, NGFWaaS, ZTNA, and CASB provide embedded security.

Conclusion

Overall Versa DLP solution is going to be an effective way to safeguard your data from data loss and theft whether the data is in Remote sites, On-Prem, roaming users, or in Cloud. Organizations had challenges in deploying successful DLP solution. Choosing the right tool, and process and applying the appropriate policies will give insight into where sensitive data transit and how well the data is being protected.

Versa DLP solution meets industry requirements with its advanced feature sets (Exact Data Match (EDM), Regulatory Compliance, Optical Character Recognition (OCR), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), etc) and unified SASE solution. Versa is recognized as the SASE leader in the global market and choosing Versa SASE solution will be a smart choice for any organization.

Versa DLP is available both as a cloud-delivered solution and On-Prem Solution DLP is available in the Versa SASE Service (SASE-as-a-Service), the Versa CASB solution, the Versa Secure SD-WAN solutions, or the stand-alone Versa Secure Internet Access Service (SWG-as-a-Service)

For more information on Versa Networks, please visit https://versa-networks.com, contact us at https://versa-networks/contact or follow Versa Networks on Twitter @versanetworks

Roadmap Items: Cloud Advanced Threat Prevention, Remote Browser Isolation and Optical Character Recognition.

Reference and Resources

[1] IBM data breach report 2022 " https://www.ibm.com/reports/data-breach

[2] Verizon, 2022 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[3] https://transparencyreport.google.com/https/overview?hl=en

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com