CyStack

DATA SHEET

Data Loss Prevention

Preventing data loss, ensuring compliance

Overview

Data Loss Prevention (DLP) is a technology and set of processes that organizations use to ensure that sensitive or confidential information is not lost, stolen, or misused.

DLP is necessary because sensitive data is a valuable target for cybercriminals and can be used for malicious activities such as identity theft, fraud, and extortion. It's important for organizations to protect sensitive data to avoid financial losses, reputational damage, and legal penalties. DLP solutions can help organizations identify and protect sensitive data, block unauthorized access to that data, and respond quickly to data breaches.

DLP solutions also help organizations comply with various regulations and standards, such as HIPAA, PCI-DSS, and GDPR, that require organizations to protect sensitive data. Many organizations are also required to notify individuals and authorities when data breaches occur, and DLP can help organizations meet this requirement.

How CyStack Helps

The CyStack Audit Team is a group of highly skilled security testers who use a goal-oriented approach to testing, refined through years of experience and extensive testing. Our team members have a unique blend of software development and security testing expertise, enabling them to conduct comprehensive security evaluations that uncover potential risks for organizations. Members of this team are also regular speakers at world-known cyber security conferences and also talented bug hunters who discovered many critical vulnerabilities in the products and are acknowledged in the Hall of Fame of global tech giants such as HP, Microsoft, Sea Group, Alibaba, etc.

From our software development and audit experience, we understand the causes of data leaks and how to prevent them effectively. We will help you come up with effective DLP strategies and, most importantly, fit your current technology stack and policy.

Customer Benefits

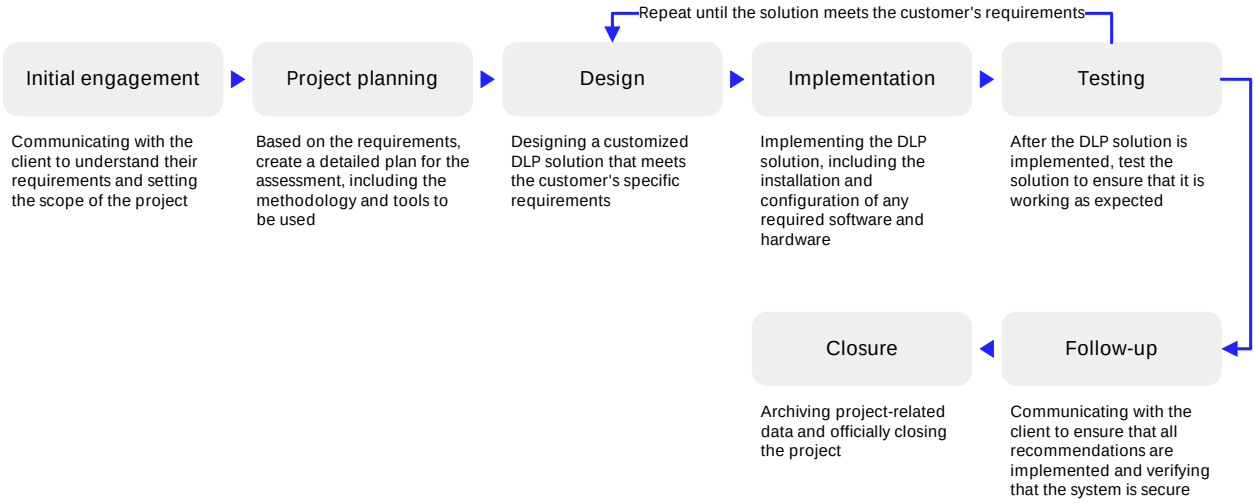
- Protect sensitive data from being lost, stolen, or misused
- Comply with various regulations and standards, such as HIPAA, PCI-DSS, and GDPR
- Reduce the risk of data breaches and other security incidents
- Identify and block the transmission of sensitive data
- Have visibility into the DLP solution and its performance

Methodology

CyStack DLP service methodology includes the following steps:

1. **Assessment**: In this step, a thorough assessment of the client's current data environment is conducted to identify sensitive data and potential vulnerabilities. This includes:
   - Identifying the types of data that need to be protected, such as personal information, financial data, and intellectual property.
   - Identifying where that data is located, such as on endpoints, in the cloud, or on email servers.
   - Identifying who has access to the data and how it is being transmitted.
   - Analyzing the client's current security controls and identifying any gaps or vulnerabilities.
   - Identifying the client's regulatory and compliance requirements and how they apply to the data environment.
2. **Design**: Based on the assessment, a DLP solution is designed that addresses the specific needs of the client. This includes:
   - Determining the appropriate technologies and processes to be used for data protection, such as network-based, endpoint-based, and cloud-based methods.
   - Identifying where DLP technologies should be deployed in the network.
   - Configuring DLP policies and rules to detect and protect sensitive data.
   - Identifying the necessary procedures and workflows for incident response and data recovery.
   - Designing a reporting and management console to provide visibility into the DLP solution's performance.
3. **Implementation**: Once the design is complete, the DLP solution is implemented. This may include:
   - Installing software and hardware, such as DLP software and endpoint agents. Or we will build a customized solution for the client.
   - Configuring network and endpoint devices, such as firewalls and intrusion detection systems.
   - Establishing policies and procedures for data protection, including incident response and data recovery procedures.
   - Testing the DLP solution to ensure it is configured correctly and working as intended.
4. **Monitoring and management**: After the DLP solution is implemented, ongoing monitoring and management are required to ensure that it is effectively protecting sensitive data. This includes:
   - Monitoring for data breaches and other security incidents, such as data exfiltration attempts.
   - Updating policies and procedures as needed to adapt to changes in the data environment or to improve the DLP solution's performance.
   - Providing regular reporting and analytics to the client to give visibility into the DLP solution's performance.
5. **Incident response**: In the event of a data breach or other security incident, incident response and remediation services are provided to help clients quickly and effectively respond to the incident. This includes:
   - Identifying the cause of the incident, such as a phishing attack or a malware infection.
   - Containing the incident to prevent further data loss.
   - Removing malicious code or actors from the environment.
   - Restoring normal operations, such as returning the data that was exfiltrated.
6. **Reporting**: Provide a centralized management console for monitoring and reporting, which allows clients to have visibility into the DLP solution and its performance. This includes:
   - Reports on the types of data that have been protected and the number of incidents that have been detected and blocked.
   - Reports on the DLP system's performance, such as the number of false positives and false negatives.
   - Reports on the effectiveness of the DLP solution, such as the number of data breaches that were prevented.

Flow To Work With Clients



About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net