

## N26 IT Security Take Home Assignment

Data Loss Prevention is defined as a strategy that detects potential data breaches or data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while *in use* (endpoint actions), *in-motion* (network traffic), and *at rest* (data storage).

I have listed the few of the best DLP solutions available based on the required parameters provided, like scalability, cost-effectiveness, seamless integration, and compatibility.

### 1. Symantec Data Loss Prevention (DLP):




- Symantec is a well-established name in the cybersecurity industry, and their DLP solution is known for its comprehensive features.
- It offers content discovery and monitoring, policy enforcement, and incident response capabilities.
- Symantec DLP is recognized for its scalability and integration capabilities with other security tools.

### 2. McAfee Total Protection for Data Loss Prevention:

- McAfee is another prominent player in the cybersecurity space, and its DLP solution is designed to protect sensitive data across various channels.
- It provides content discovery, policy enforcement, and encryption features.
- McAfee's DLP solution is often praised for its ease of use and management.

### 3. Forcepoint Data Loss Prevention:

- It offers content inspection, contextual analysis, and behaviour analytics to identify and mitigate risks.
- Forcepoint's DLP is recognized for its ability to adapt to evolving threats and user activities.

DLP Software	Best for	Platforms	Deployment
<a href="#">McAfee DLP</a> 	Small to large businesses.	Windows, Mac, Linux.	Cloud-based & on-premise.
<a href="#">Symantec DLP</a> 	Enterprises.	Windows, Mac, Linux.	Cloud-based & on-premise.
<a href="#">Forcepoint DLP</a> 	Small to large businesses, Agencies, and Enterprises.	Windows, Mac, Linux and Web App.	Cloud-based & on-premise.

### *Why an invest in an DLP solution is important?*

In simple terms, this is because the unintentional leakage or loss of sensitive data due to a malicious actor, an inside job, or an unknowing employee, can lead to significant financial loss and reputational damage to our organization.

DLP solutions are crucial for organizations to safeguard sensitive data and prevent unauthorized access or disclosure. When considering DLP solutions, it's essential to analyse and compare various options to make an informed decision. Below, I will provide a general analysis of the importance of investing in a DLP solution and then focus on my recommended DLP solution.

### **Importance of Investing in a DLP Solution:**

#### 1. Data Security:

- DLP solutions play a vital role in ensuring the security of sensitive information. They help identify, monitor, and protect data from unauthorized access, sharing, or theft.

#### 2. Regulatory Compliance:

- Many industries and regions have stringent data protection regulations. Implementing a DLP solution helps organizations comply with these regulations and avoid legal consequences and fines, e.g. GDPR etc.

#### 3. Intellectual Property Protection:

- For businesses that rely on proprietary information, DLP solutions are crucial to safeguard intellectual property from both internal and external threats.

#### 4. Reputation Management:

- A data breach can severely damage an organization's reputation. DLP solutions mitigate the risk of data leaks, preserving the trust of customers, partners, and stakeholders.

#### 5. Operational Continuity:

- Data breaches can disrupt business operations. DLP solutions contribute to maintaining operational continuity by preventing data incidents that could lead to downtime or loss of critical information.

### **Forcepoint DLP Solution:**

After thoroughly analysing multiple vendors, I recommend Forcepoint DLP solution for the provided scenario in N26 as Forcepoint is a recognized player in the cybersecurity industry, and their DLP solution offers several features that make it a compelling choice.

### **Justification for choosing Forcepoint DLP:**

#### 1. Unified DLP Approach:

- Forcepoint provides a unified DLP approach that covers endpoints, networks, and cloud environments. This comprehensive coverage ensures that data is protected across the entire organization, regardless of where it resides or how it is accessed.

## 2. Behaviour Analytics:

- Forcepoint DLP incorporates advanced behaviour analytics to detect and prevent insider threats. This proactive approach goes beyond rule-based detection, identifying abnormal user behaviour that might indicate a potential data breach.

## 3. Cloud-Centric DLP:

- With the increasing adoption of cloud services, Forcepoint DLP offers robust protection for data stored in cloud environments. It ensures that data is secure, whether it's on-premises or in the cloud, addressing the challenges of modern, hybrid IT infrastructures.

## 4. Scalability and Flexibility:

- Forcepoint DLP is designed to scale with the growing needs of an organization. It provides flexibility in deployment options, allowing organizations to tailor the solution to their specific requirements.

## 5. User-Friendly Interface:

- The user interface of Forcepoint DLP is intuitive and user-friendly. This simplifies the implementation and management of DLP policies, reducing the learning curve for administrators.

## 6. Threat Intelligence Integration:

- Forcepoint integrates threat intelligence into its DLP solution, enhancing its ability to identify and respond to emerging threats promptly.

## 7. Proven Track Record:

- Forcepoint has a history of providing effective cybersecurity solutions. A vendor's reputation and track record are critical factors when selecting a DLP solution.

Investing in Forcepoint DLP, is a strategic decision that aligns with the N26's overall cybersecurity strategy, regulatory compliance needs, and the goal of protecting sensitive data from both internal and external threats. At the same time, it fulfils the required compatibility with AWS, GCP, Windows, Linux and MacOS client, Gsuite and coverage of critical corporate IT SaaS solutions like Workday and Atlassian.

I am also attaching the datasheet of comparison of Forcepoint DLP with its competition DLP vendors along with this file as provided by Forcepoint in its official website.

## Implementing the DLP solution across the company can be carried out in multiple phases:

- Phase 1: Assessment (Duration: 1 month)
  - *Task 1:* Conduct a thorough assessment of current data flows and vulnerabilities.
  - *Task 2:* Identify and categorize sensitive data.
  - *Task 3:* Document existing security policies and protocols.
- Phase 2: Policy Design (Duration: 2 months)
  - *Task 1:* Define DLP policies tailored to N26's specific needs and compliance requirements.
  - *Task 2:* Develop incident response procedures.
  - *Task 3:* Establish criteria for categorizing data sensitivity.
- Phase 3: Deployment (Duration: 2 months)
  - *Task 1:* Deploy Forcepoint DLP agents on all relevant endpoints (Windows, Linux, MacOS).
  - *Task 2:* Configure DLP policies and monitoring rules.
  - *Task 3:* Conduct pilot testing in a controlled environment.
- Phase 4: Training and Awareness (Duration: 1 month)
  - *Task 1:* Develop training materials on DLP policies and best practices.
  - *Task 2:* Conduct training sessions for employees across departments.
  - *Task 3:* Launch awareness campaigns to highlight the importance of data protection.
- Phase 5: Monitoring and Optimization (Ongoing)
  - *Task 1:* Implement continuous monitoring of DLP alerts and incidents.
  - *Task 2:* Fine-tune DLP policies based on feedback and evolving security needs.
  - *Task 3:* Regularly update incident response procedures.

This completes the first stage of deployment.

- Required Resources:
  - *DLP Experts:* TAC engineers from Forcepoint DLP.
  - *IT Administrators:* 2 Security administrators for deployment and ongoing maintenance.
- Stakeholders:
  - *IT/Security Teams:* Responsible for implementation, monitoring, and incident response.
  - *Employees:* End-users who must adhere to DLP policies.
  - *Management:* Provides oversight, change management, support, and resources. Monthly or quarterly meetings will provide input and will help to continuously drive the program and ensure the quality of the investment is operating optimally.

However, like any significant IT initiative, there are potential problems and risks associated with the implementation of this new DLP solution. Here are some common challenges:

1. **False Positives and Negatives:**
  - **False Positives:** DLP solutions may sometimes incorrectly identify normal activities as potential security threats, leading to unnecessary alerts. This can result in frustration for users and the risk of important business processes being disrupted.
  - **False Negatives:** On the other hand, false negatives occur when the DLP system fails to detect actual security incidents, allowing sensitive data to be leaked. This poses a significant risk to the organization.
2. **Complexity of Policies:**
  - Defining and configuring DLP policies can be complex, especially in large organizations with diverse data types and numerous communication channels. Overly complex policies may lead to misconfigurations and, consequently, security vulnerabilities.
3. **Integration with Existing Systems:**
  - Integrating a new DLP solution with existing IT infrastructure, applications, and security systems can be challenging. Incompatibilities may arise, leading to disruptions in business processes and potential security gaps.
4. **User Resistance:**
  - Users may resist the implementation of DLP measures, especially if they perceive them as intrusive or hindering their workflow. Resistance can result in circumvention of security controls and decreased overall effectiveness.
5. **Performance Impact:**
  - Implementing DLP solutions can sometimes introduce latency or performance issues, particularly when inspecting and monitoring large volumes of data. This can affect system responsiveness and user experience.
6. **Data Classification Challenges:**
  - Properly classifying and identifying sensitive data is essential for effective DLP. Organizations may face difficulties in accurately categorizing all sensitive information, leading to incomplete protection.
7. **Encryption and Data Handling:**
  - DLP solutions need to handle encrypted data appropriately. If the solution cannot inspect encrypted traffic or mishandles encryption, it may miss potential threats or create a false sense of security.
8. **Costs and Resource Allocation:**
  - Implementing and maintaining a DLP solution can be resource-intensive and costly. Organizations may need to allocate significant financial and human resources for initial deployment, ongoing management, and updates.
9. **Regulatory Compliance:**
  - Failure to properly implement DLP measures can result in non-compliance with data protection regulations. This can lead to legal consequences, fines, and damage to the organization's reputation.
10. **Evolution of Threats:**
  - DLP solutions need to continually evolve to address new and emerging threats. If the solution becomes outdated or lacks regular updates, it may become less effective over time.

To mitigate these risks, planning the DLP implementation plays a very crucial role, i.e. involving key stakeholders, providing user education and training, conducting thorough testing, and regularly reviewing and updating policies and technologies to stay ahead of evolving threats.

I would also want to highlight another important point regarding the cost involved: It would not be a wise investment to purchase an expensive Enterprise DLP solution that offers an entire suite of DLP features if N26 doesn't manage unstructured data on-premise or in the cloud as the cost of implementing a DLP platform can be expensive.

**Conclusion:**

I would suggest configuring the required policies one at a time, instead of turning on every single policy checkbox available as doing so could overwhelm the system and generate massive amounts of incidents, therefore, defeating the purpose of the investment. Best practice would be to start with a small subset of policies, then gradually build the system over time as our understanding of the product matures.