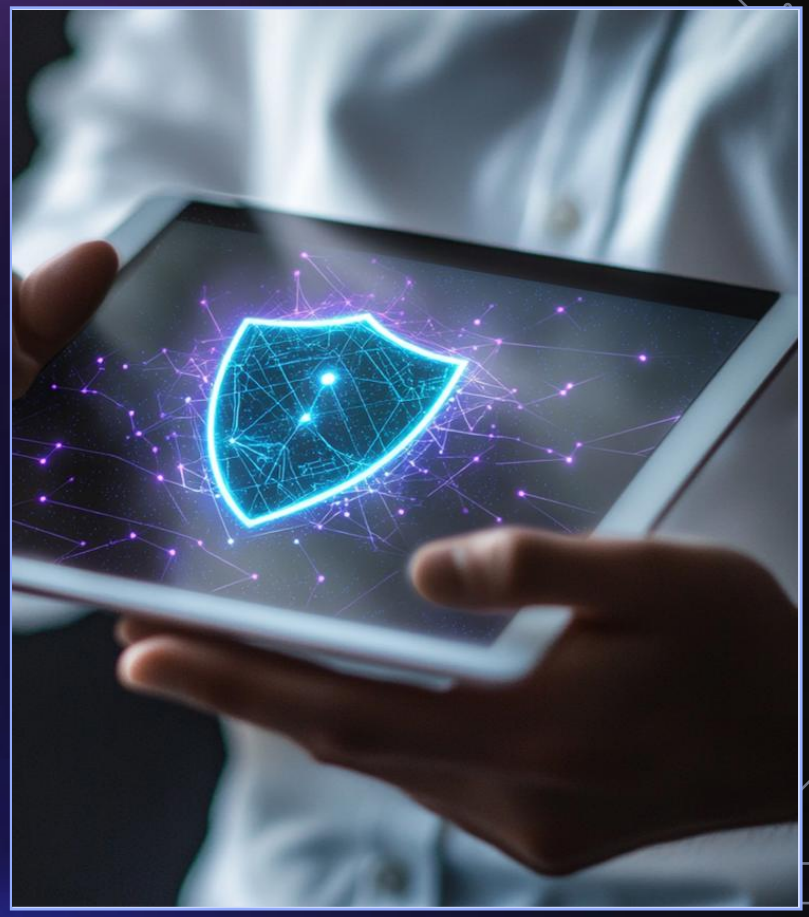
Microsoft Purview

Data Loss Prevention (DLP)

CONTENTS

01

Planning & Designing DLP Policies



Analyzing DLP Requirements

01

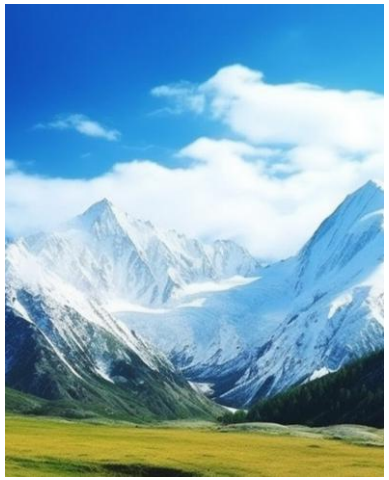
Identifying sensitive data

Determine the types of sensitive data that need protection based on organizational requirements and data classification standards.

02

Assessing regulatory compliance

Evaluate the regulatory requirements that impact data protection strategies like GDPR, HIPAA, and others relevant to the business.



Policy Framework Creation

Defining policy templates

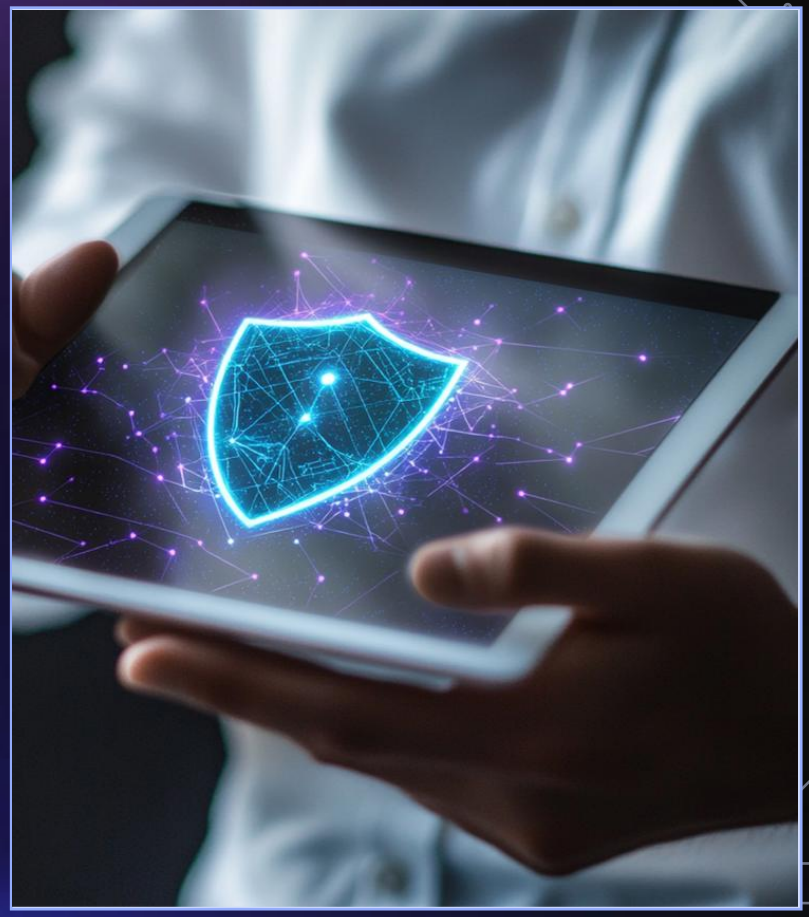
Create reusable templates for DLP policies that address common protection scenarios and streamline policy implementation.

Setting policy scopes

Define the scope of each DLP policy, including specific users, locations, and data types to ensure targeted protection measures. Not over-targeting, not under-targeting, but targeting at the right levels.

02

Creating & Managing DLP Policies



Policy Configuration

Configuring protection rules

- Set up detailed rules within DLP policies to detect and prevent sensitive data leaks based on preset conditions.

Customizing user notifications

- Tailor the notifications that end-users receive when a DLP policy blocks or restricts certain actions to ensure awareness and compliance.

Policy Deployment

01

Policy testing and validation

Test DLP policies in a controlled environment to ensure they work as intended before widespread deployment.

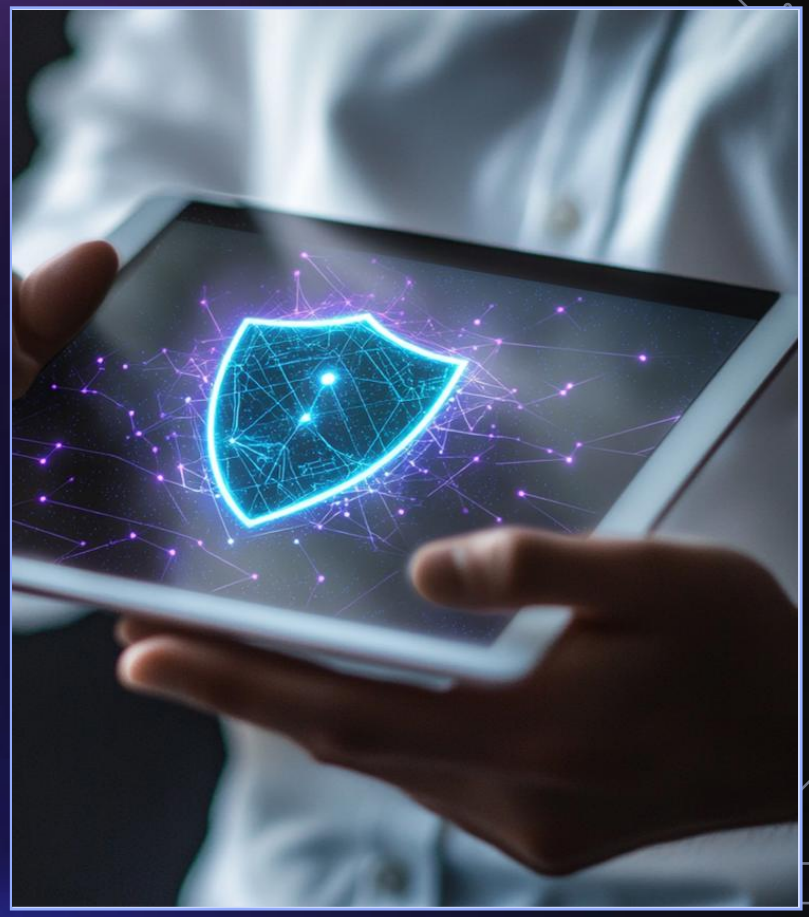
02

Policy rollout strategies

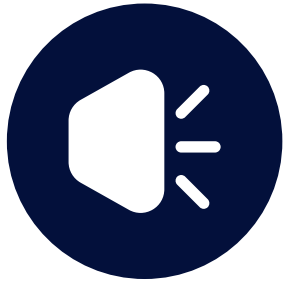
Develop a strategic plan for deploying DLP policies across the organization, including phased rollout and employee training.

03

Leveraging Adaptive Protection with DLP



Dynamic Policy Adjustments



Real-time risk assessment

Use real-time analytics to adjust DLP policies dynamically based on current risk levels and detected threats.

Behavior-based policy modification

Modify DLP policies based on observed user behavior patterns to enhance protection and reduce false positives.

Integration with Other Security Tools

Coordinated incident response

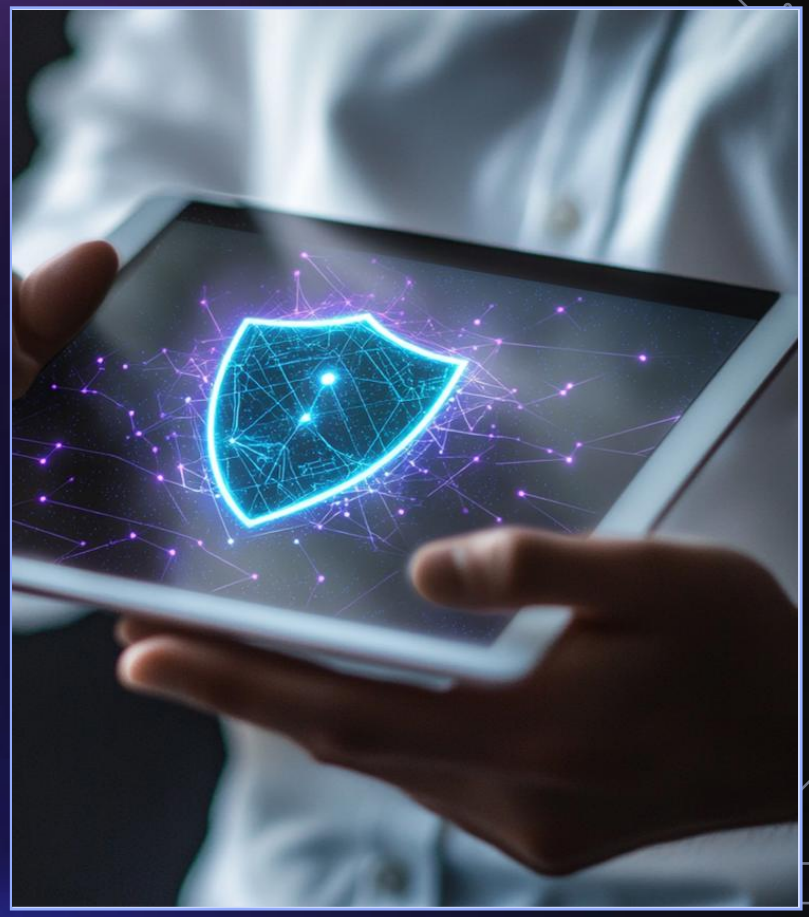
Integrate DLP with other security tools to enable coordinated response to data loss incidents, improving overall incident handling.

Enhanced threat detection

Leverage integration capabilities to augment threat detection by combining data from multiple security systems.

04

DLP Alerts & Activity Tracking



Alert Configuration

01

Custom alert criteria

Set up alerts based on specific criteria such as data sensitivity, user actions, or locations to ensure timely detection of potential data loss.

02

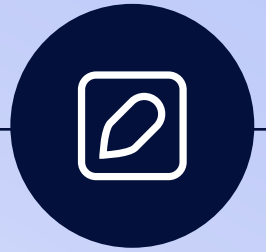
Alert prioritization settings

Prioritize alerts based on the severity of the detected issues to streamline response efforts and mitigate risks more effectively.

Activity Monitoring

Detailed event logging

Ensure comprehensive logging of all relevant activities related to DLP policies for auditing and tracking purposes.

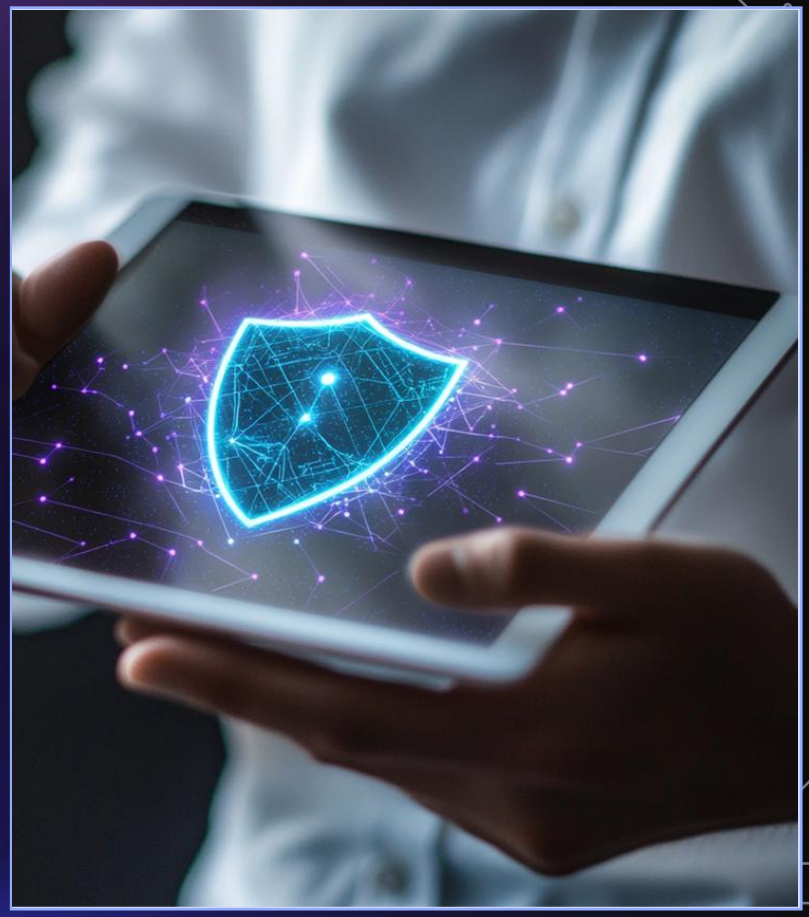


User activity analysis

Analyze user activities to identify patterns or anomalies that might indicate potential data loss or security breaches.

05

SC-100 Tie-in



DLP within Enterprise Security Strategy

Integrated security architecture

Explore how DLP integrates within broad enterprise security architecture, reinforcing layers of protection and ensuring coherent security measures.

Role of DLP in risk management

Focus on the role of DLP in managing enterprise risk, minimizing data loss impacts, and maintaining compliance with security policies.

Training for Security Professionals

01

DLP education programs

Develop comprehensive DLP training programs to ensure security professionals understand policy design, implementation, and management.

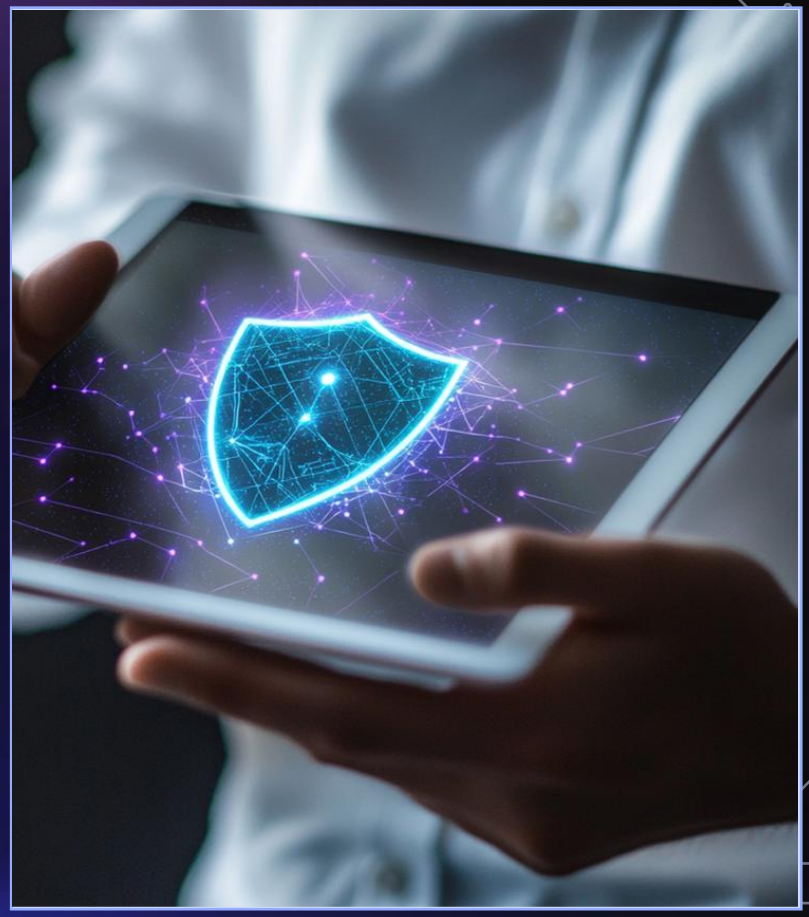
02

Continuing education and certification

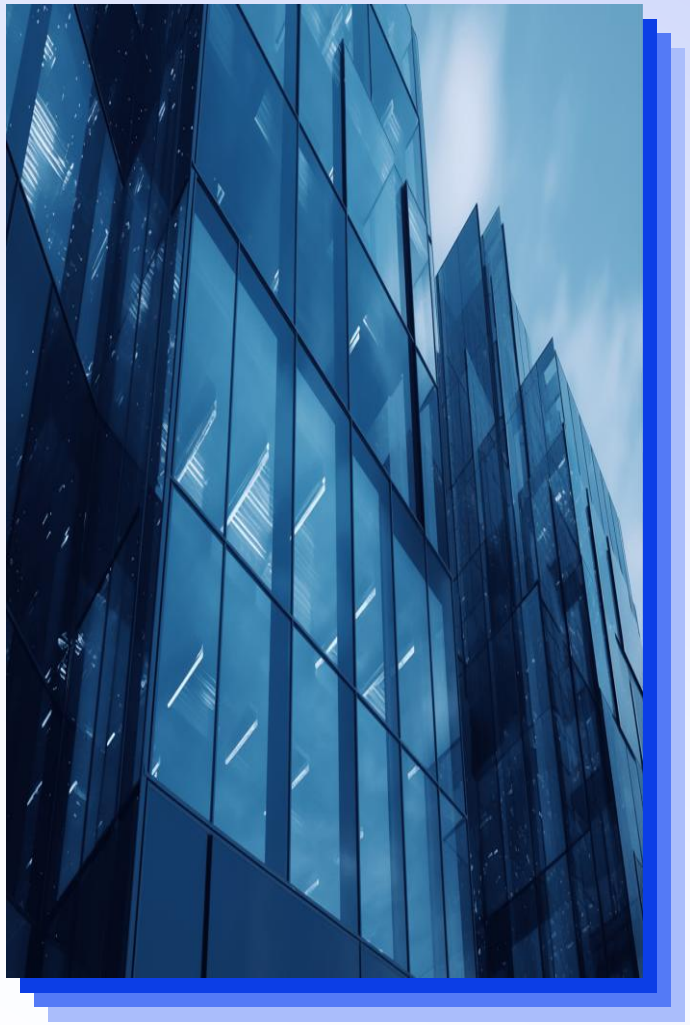
Encourage ongoing education and certification for security professionals to stay updated with latest DLP techniques and practices.

06

Future Trends in DLP



Emerging Technologies



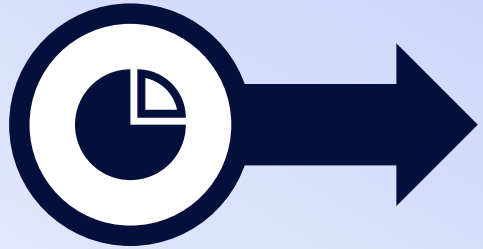
01. AI-driven data protection

Artificial intelligence (and application of the associated technologies) provided potential in enhancing DLP capabilities through better threat detection and automated policy adjustments.

02. Blockchain for data integrity

Explore how blockchain technology could be leveraged to track and ensure data integrity within DLP frameworks. See https://www.dataexpertise.in/blockchain-technology-data-integrity-security/.

Evolving Regulatory Landscape

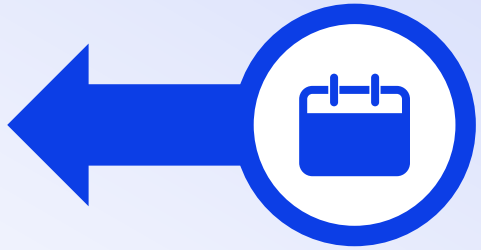


Impact of new legislation

Examine the impact of new data protection laws on DLP strategies and how organizations can adapt to stay compliant.

Global data protection standards

Understand the significance of developing unified global standards for data protection to streamline DLP implementation across multi-region enterprises.



Thanks