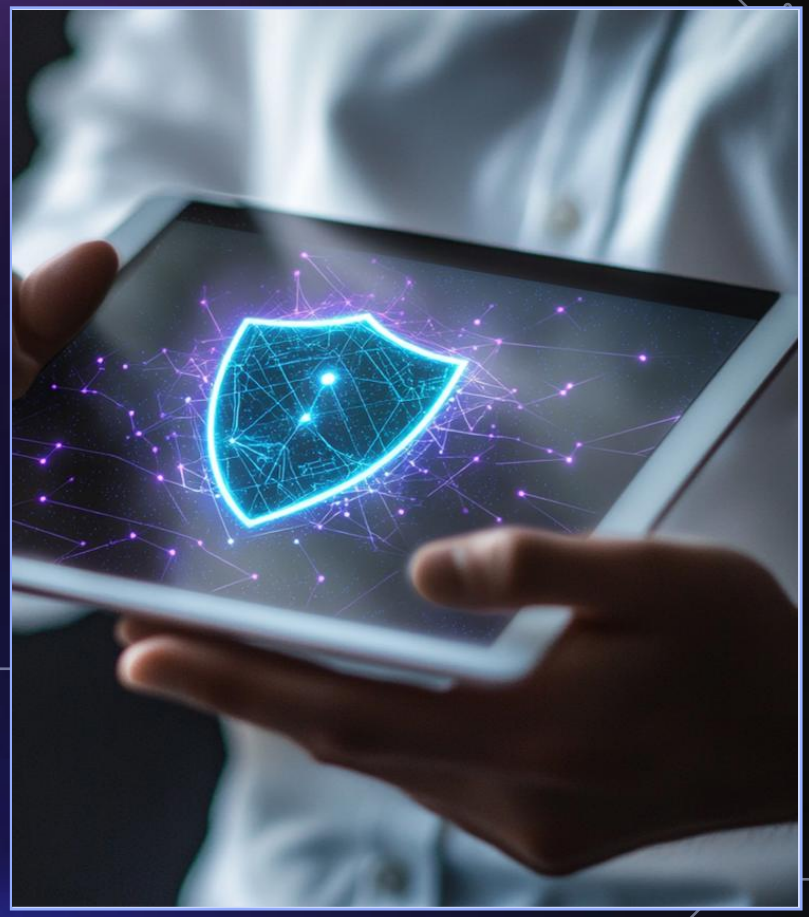
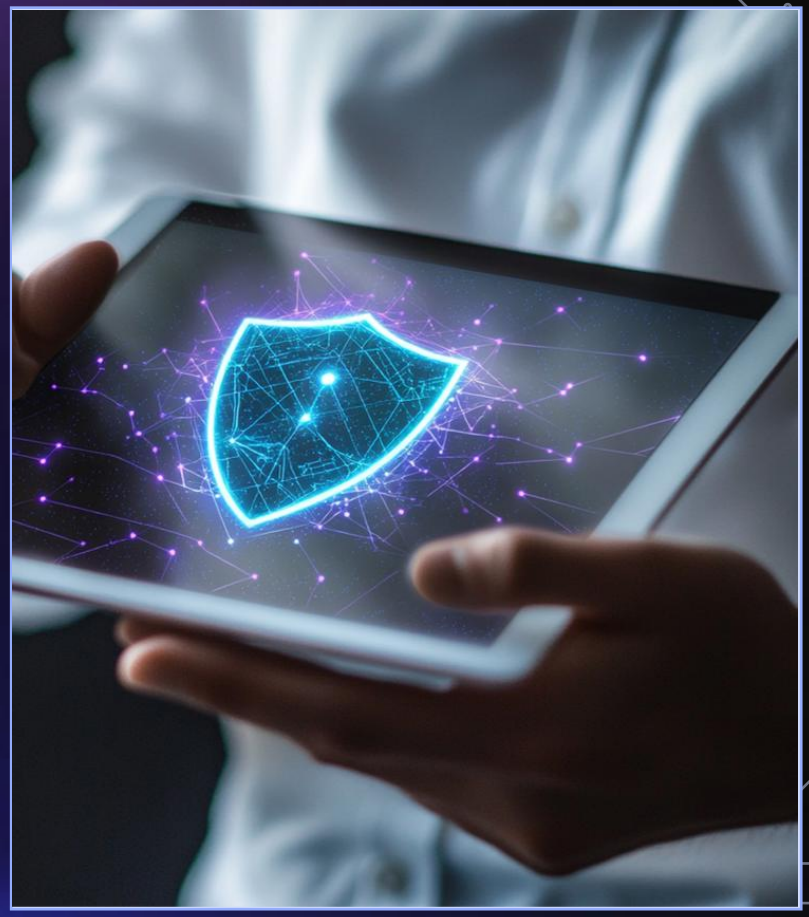
Microsoft Purview

Summary & Conclusion



01

Integrated Strategy and Governance

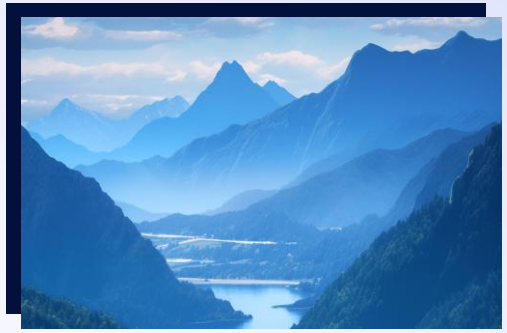


Governance and Compliance Solution

01

Microsoft Purview

Microsoft Purview enables organizations to comprehensively govern, protect, and manage sensitive information across their entire digital estate.



02

Microsoft Defender

Microsoft Defender offers advanced threat protection to secure your organization’s sensitive data against sophisticated cyber- attacks.

03

Microsoft Sentinel

Microsoft Sentinel provides intelligent security analytics to detect and respond to threats in real- time, ensuring a proactive defense strategy.

Protecting Sensitive Data

01.

Data Classification

Identify and classify sensitive data to ensure appropriate protection measures are implemented throughout the data lifecycle.

02.

Data Encryption

Utilize encryption technologies to safeguard sensitive data both at rest and in transit, ensuring data confidentiality and compliance.

03.

Access Controls

Implement robust access controls to limit data access to authorized personnel, minimizing the risk of data breaches and leaks.

Designing Retention and DLP Strategies

Retention Policies

Create and enforce retention policies to manage data lifecycle, ensuring compliance with regulatory requirements and organizational policies.

01

DLP Policies

Deploy Data Loss Prevention (DLP) policies to detect and prevent data leaks by monitoring and controlling data transfers.

02

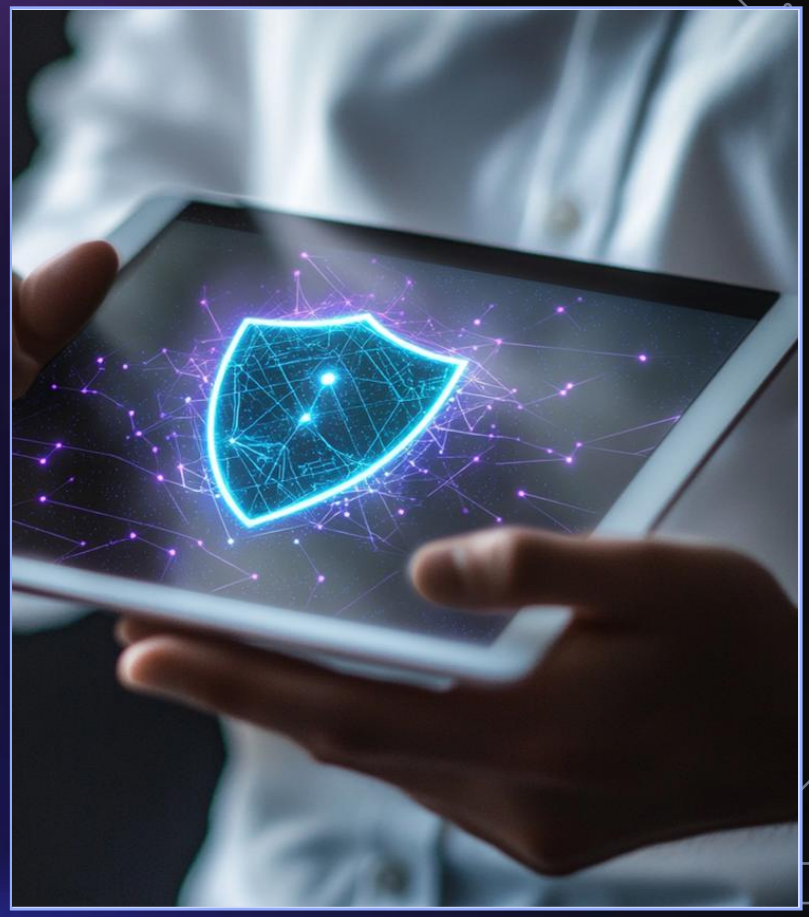
Policy Implementation

Ensure the successful implementation of retention and DLP policies through continuous monitoring, assessment, and adjustment as needed.

03

02

eDiscovery for Incident Response



Configuring eDiscovery

eDiscovery Tools

Utilize eDiscovery tools to identify, collect, and preserve electronically stored information (ESI) for legal and investigative purposes.

Search and Collection

Perform comprehensive searches to collect relevant ESI, ensuring it is readily accessible for analysis and review.

Data Preservation

Implement measures to preserve data integrity and prevent spoliation, maintaining the evidentiary value of collected data.

Incident Management

01

Incident Identification

Develop strategies for the early identification of security incidents, enabling a prompt and effective response.

02

Response Protocols

Establish incident response protocols to manage and mitigate the impact of security incidents, reducing potential damage.

03

Forensic Analysis

Conduct forensic analysis to understand the root cause of incidents, aiding in the prevention of future occurrences.

Legal and Regulatory Compliance

Regulatory Requirements

Stay informed of relevant regulatory requirements to ensure compliance and avoid legal penalties.

Legal Hold

Implement legal hold processes to prevent the alteration or destruction of potentially relevant ESI during legal proceedings.

Compliance Audits

Conduct regular compliance audits to verify adherence to legal and regulatory standards, identifying areas for improvement.

03

Building an Auditing Plan

Security Audits

01 Audit Framework

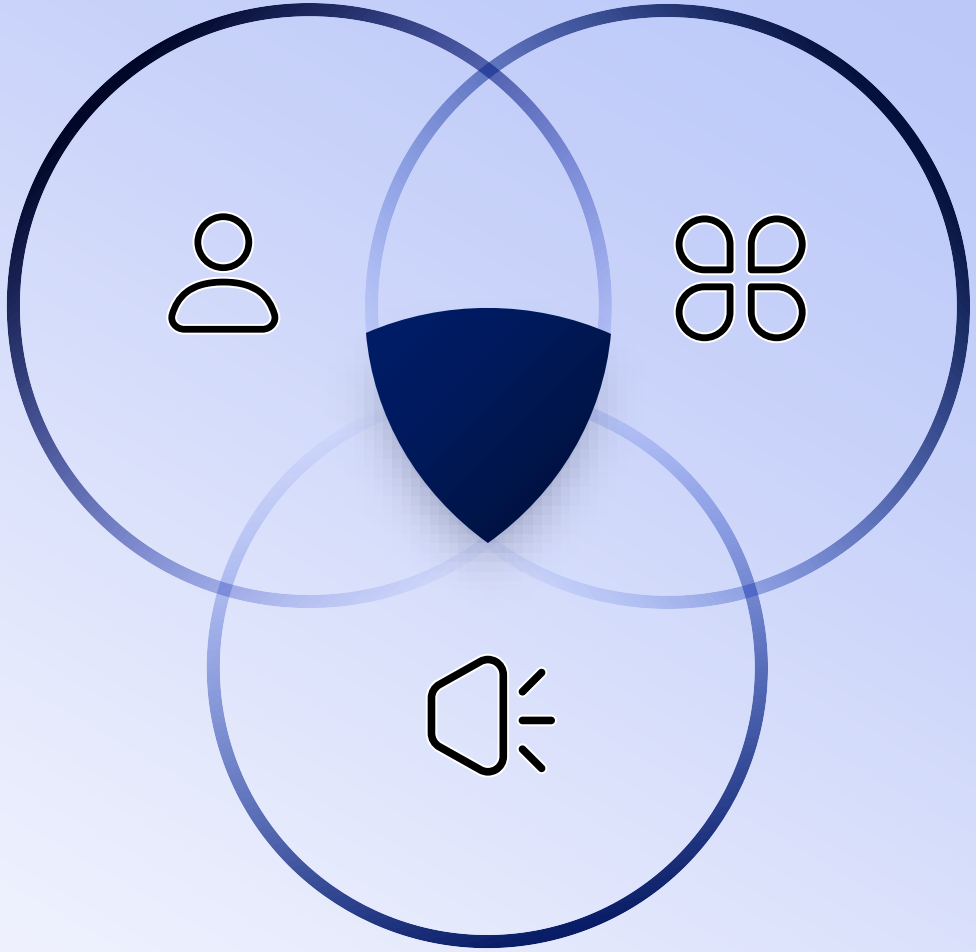
Develop a comprehensive audit framework to systematically evaluate the security posture and compliance of the organization.

02 Audit Tools

Leverage advanced auditing tools to automate the auditing process, increasing efficiency and accuracy.

03 Audit Reporting

Generate detailed audit reports to document findings, recommendations, and corrective actions required to enhance security and compliance.



Compliance Audits

Internal Audits

Conduct internal audits to assess adherence to internal policies and procedures, identifying areas for improvement.

External Audits

Engage external auditors to perform independent assessments, providing an unbiased evaluation of the organization's compliance status.

Continuous Monitoring

Implement continuous monitoring practices to ensure ongoing compliance and timely identification of non-compliance issues.

Risk Management

Risk Assessment

Perform regular risk assessments to identify potential threats and vulnerabilities, allowing for proactive risk management.

Risk Mitigation

Develop and implement risk mitigation strategies to reduce the impact and likelihood of identified risks.

Risk Reporting

Communicate risk findings and mitigation efforts to stakeholders through comprehensive risk reports, ensuring transparency and informed decision- making.

Thanks