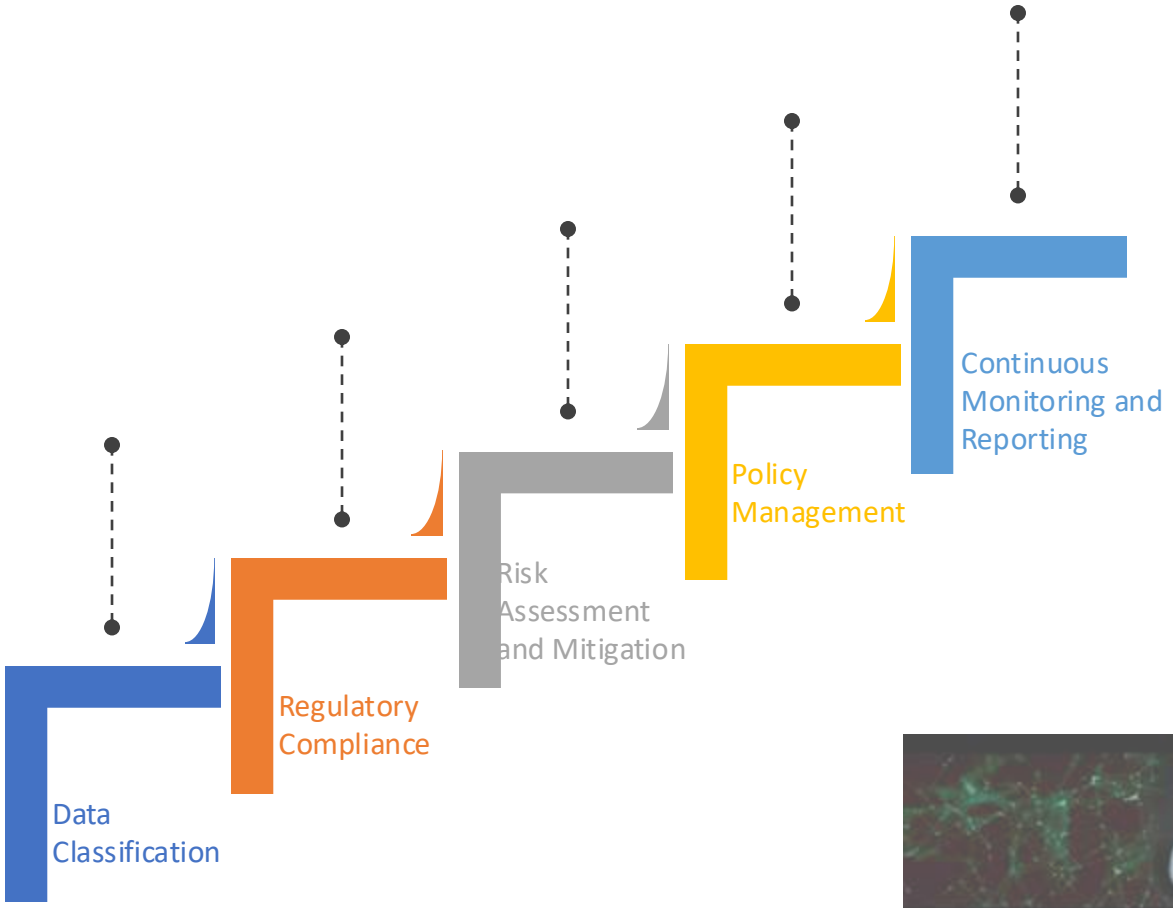
Unlocking Compliance Excellence with iLink Systems and Microsoft Purview

Empowering Your Compliance Journey

Primary areas of Focus of Microsoft Purview Compliance Manager

Here are the primary areas of focus and benefits that we emphasize when utilizing Microsoft's Purview compliance services



Microsoft Purview Compliance Manager is a comprehensive compliance solution that empowers organizations to manage their compliance requirements, data governance, and regulatory standards effectively.

What do we do

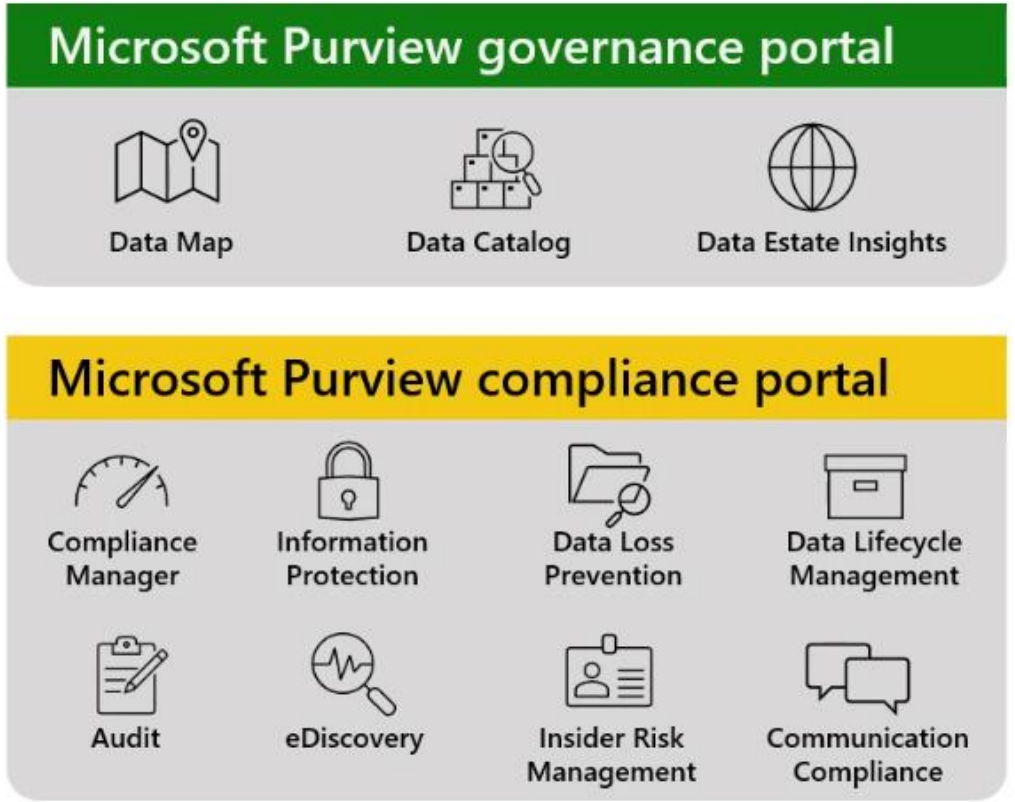
With our in-depth understanding of Purview compliance, we seamlessly integrate Microsoft's cutting-edge solutions to fortify data security and regulatory compliance within your organization.

- Deriving required sensitivity info Types based on the organization service model.
- Assisting in choosing the regulatory compliances required for the Organization standards.
- Sensitivity Labelling.
- Policy Controls (DLP).
- Integration of other services and end points to purview compliance.
- Data governance procedures and recommendations.
- Reporting and Administration of Purview compliance.
- Recommendations to improve the Security score.

By leveraging Microsoft's Purview compliance suite, our team implements robust strategies to safeguard sensitive data, mitigate risks, and ensure regulatory compliance

Microsoft Purview Compliance Manager

Microsoft Purview Compliance Manager is a comprehensive compliance solution that empowers organizations to manage their compliance requirements, data governance, and regulatory standards effectively.



Benefits for Organizations

- **Streamlined Compliance Management:** Purview Compliance Manager simplifies compliance management processes, reduces manual efforts, and provides a centralized platform for managing compliance requirements.
- **Enhanced Data Governance:** The platform enables organizations to establish and enforce consistent data governance policies, improving data quality, integrity, and security.
- **Proactive Risk Management:** Purview Compliance Manager helps organizations identify and mitigate data-related risks proactively, minimizing the likelihood of compliance violations and data breaches.
- **Improved Decision-Making:** By providing insights into compliance status, data usage, and risk exposure, Purview Compliance Manager enables informed decision-making and strategic planning.

Nonprofit legal advocacy organization – Purview Compliance Management

An Atlanta based company that is a nonprofit legal advocacy organization specializing in civil rights and public interest litigation

Business Scenario

The financial company prioritizes systematic data handling and precise classification to enforce stringent access controls. By deploying Auto Labelling and DLP policies, it proactively manages sensitive data, achieving robust data governance. Furthermore, integrating various endpoints such as file servers, BOX, and SQL servers with Purview Compliance ensures comprehensive data classification, governance, and monitoring from all perspectives for PCI, Biometrics and other compliances.

Challenge

Consolidating all endpoints, including file servers, SQL services, the BOX application, and files within Office 365 services, under one unified system with consistent labelling and policies for governance, demanded extensive fine-tuning and alignment of Sensitive Information Types (SIT) according to Microsoft standards.

Solution

Ilink carefully crafted the labelling policies, aligning them with Microsoft's recommended Sensitive Information Types (SIT). DLP policies were carefully crafted with diverse priority levels to minimize false positive alerts in data handling. Implementing strategic and uniform labelling policies across all endpoints effectively addressed the challenge. This streamlined administration of various data sources under Purview Compliance, ensuring seamless management.

Outcome & Benefits

iLINK offered advanced analytics and reporting capabilities, empowering organizations to gain valuable insights into their data, identify trends and patterns, and make informed decisions to optimize data governance and compliance strategies by deploying purview compliance across the customers organization.

- Data Classification
- Regulatory Compliance
- Risk Assessment and Mitigation
- Policy Management
- Security & Compliance
- Continuous Monitoring and Reporting

- Industry Vertical
  - Finance
- Headquarters
  - Atlanta
- Company Size
  - Enterprise
- Technologies
  - Microsoft Purview Compliance

iLink Systems expertise

With our in-depth understanding of Purview compliance, we seamlessly integrate Microsoft's cutting-edge solutions to fortify data security and regulatory compliance within your organization.

Deploying Auto labelling as required by the Regulatory and compliance standards will help the organization excel in data classification, data governance and policy controls at its best.

Email: info@ilink-systems.com Visit: www.ilink-digital.com

Project Scope - Sample

High-Level Scope:

- Assess the current Purview environment.
- Check compliance data classifications.
- Improve Purview Compliance readiness score.

Detailed Activities:

- Deploy agents and connect to platforms.
- Run initial.
- Create and apply classifiers.
- Fine-tune and label data.
- Develop queries and reports.
- Test and iterate.

Assessment Approach

Deploy Agents:

Installation on employee desktops/laptops and configuration for SharePoint Online, OneDrive, File Server, and Box.com.

Run Initial:

Across all connected platforms.

Create and Apply Classifiers:

Based on discussions with the insurance company for accurate identification of sensitive data.

Fine-tune and Label Data:

Encourage manual labelling for improved accuracy.

Develop Queries and Reports:

For monitoring and managing classified data.

Assumptions

Access and Permissions: "Assuming full access to all relevant data repositories and systems for assessment and implementation purposes."

Stakeholder Engagement: "Key stakeholders, including data owners and IT security teams, will be actively engaged and available for consultations throughout the project lifecycle."

Data Classification Standards: "Existing data classification standards are accurate and up-to-date, serving as a reliable foundation for compliance assessment."

Regulatory Environment Stability: "No significant changes in compliance regulations expected during the project timeline that could impact project scope or deliverables."

Technology Compatibility: "Current IT infrastructure and platforms are compatible with the deployment of compliance assessment and enhancement tools."

Key Deliverables

Project Schedule	Discovery Assessment Report	Gaps and Purview Optimization Scope	Recommendations and Best Practices
Purview Readiness Report	Remediation Path Recommendations	Queries and reports	Weekly Status Reports

iLink's Service Offerings

Overview of iLink's services related to Microsoft Purview Compliance Manager

- **Implementation and Configuration:** Setting up Purview Compliance Manager to align with your organization's compliance needs.
- **Data Classification and Governance:** Assisting in classifying and managing data assets for compliance and risk management.
- **Policy Enforcement and Monitoring:** Implementing policies and controls to ensure compliance with regulations and standards.
- **Compliance Reporting and Analytics:** Generating reports and insights to track compliance status and identify areas for improvement.
- **Training and Support:** Providing training and ongoing support to empower your team in utilizing Purview Compliance Manager effectively.

Why Choose iLink Systems for Microsoft Purview Compliance Manager?

- **Expertise and Experience:** Our team of experienced professionals with deep expertise in compliance and data management.
- **Tailored Solutions:** Customized solutions designed to meet your specific compliance requirements and objectives.
- **Proven Track Record:** Demonstrated success in implementing compliance solutions for organizations across various industries.
- **Strategic Partnership:** Strong partnership with Microsoft, ensuring access to the latest tools and technologies for compliance management.
- **Client-Centric Approach:** Commitment to delivering exceptional service and value, with a focus on client satisfaction and success.

SPLC Enhancing Data Governance and Compliance with Microsoft Purview

Business Scenario

SPLC, a nonprofit legal advocacy organization. They faced challenges in managing and protecting their growing data assets. With an increasing volume of sensitive information and regulatory compliance requirements, SPLC sought to implement a robust data governance solution.

Challenge

A non-profit legal advocacy organization, dedicated to providing legal aid and advocating for human rights, faced challenges in managing and securing sensitive legal data. To streamline their data governance and ensure compliance with various legal and regulatory standards, the organization sought an advanced data governance solution. The organization encountered several significant challenges:

Diverse and Sensitive Data Sources:

- Managed a wide range of data sources, including case files, client information, and legal documents.
- Required a unified platform to integrate and govern data from various sources while ensuring data integrity and confidentiality.

Regulatory Compliance:

- Need to comply with legal and regulatory standards such as GDPR, HIPAA, and various data protection laws.
- Required a solution that could ensure compliance and provide audit capabilities.

Data Security and Privacy:

- Handling sensitive legal and client information necessitated robust security measures to protect against data breaches and unauthorized access.
- Required advanced data protection features to ensure data privacy and maintain client trust.

Operational Efficiency: Lack of efficient data management tools resulted in increased operational costs and time-consuming manual processes.

Solution

Microsoft Purview provided a tailored, comprehensive solution to meet the organization's data governance needs:

Unified Data Governance Platform:

- Integrated data from diverse sources, providing a centralized platform for data management.
- Enabled data cataloging, classification, and lineage tracking to ensure comprehensive data governance.

Regulatory Compliance and Audit Capabilities:

- Provided tools to ensure compliance with legal and regulatory standards.
- Included audit capabilities to track data access and usage, ensuring transparency and accountability.

Advanced Data Protection:

- Implemented data protection measures such as encryption, access controls, and data loss prevention (DLP) policies.
- Ensured data privacy and security, protecting sensitive information from unauthorized access.

Scalability and Cost-Effectiveness:

- Offered a scalable solution that could grow with the organization's needs.
- Provided cost-effective data governance, maximizing the organization's limited resources.

- Industry Vertical
  - Nonprofit legal advocacy Management
- Employees : 1000+

Key Metrics

Data Governance Coverage

- Total data sources integrated: 20
- Total data assets cataloged: 150,000
- Data classifications applied: 60,000
- Data lineage tracks established: 15,000

Compliance and Security

- Compliance reports generated: 80
- Data access audits conducted: 250
- Data breaches prevented: 0
- DLP policies enforced: 75

Performance

- Average data classification time: 4 seconds per asset
- Average compliance report generation time: 8 minutes
- Overall data governance coverage: 100%

Results

Over a six-month period, Microsoft Purview achieved the following:

- Integrated 20 data sources and cataloged 150,000 data assets.
- Applied 60,000 data classifications and established 15,000 data lineage tracks.
- Generated 80 compliance reports and conducted 250 data access audits.
- Enforced 75 DLP policies, preventing data breaches and ensuring data security.

iLink Systems
Thinking Beyond

Select your M365 service:

All

Select your Business Unit

All

Select the Sensitive Information Type

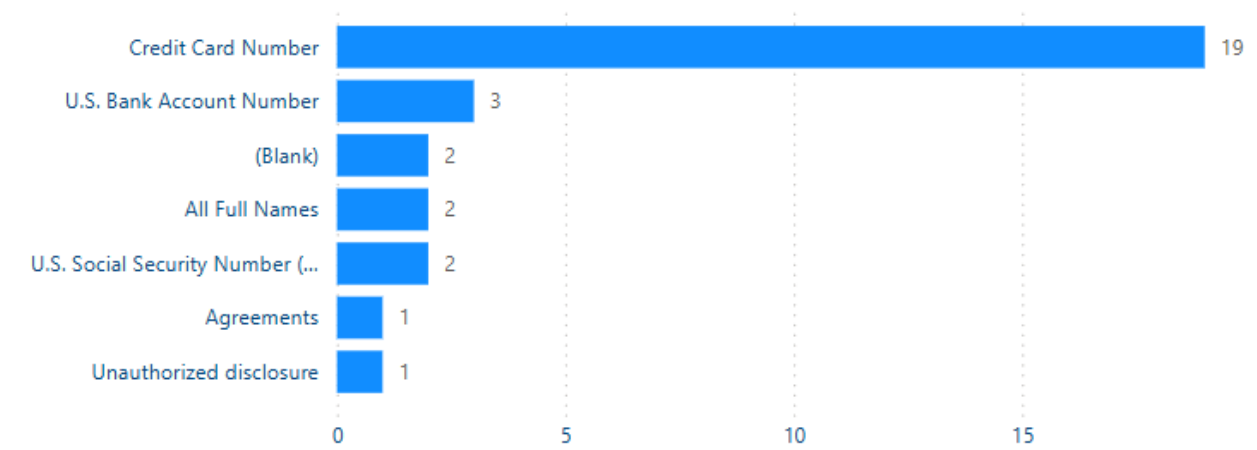
All

Select your DLP Policy

All

DLP matches by M365 services

DLP rule matches by SITs



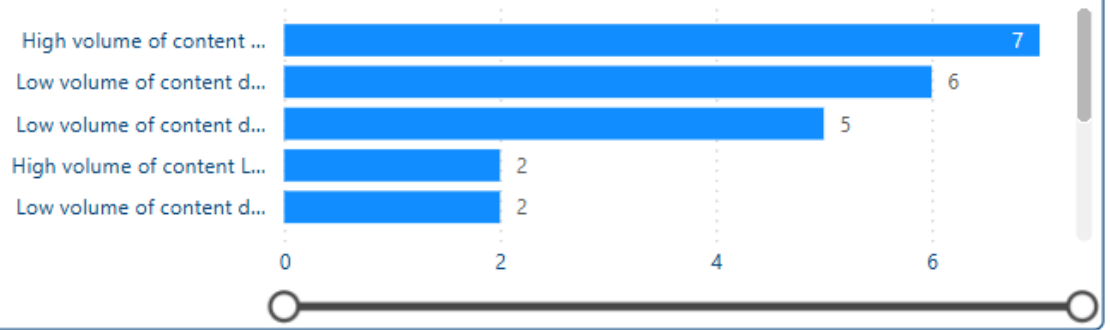
DLP rule matches by business unit

Timeline

1/1/2024

3/25/2025

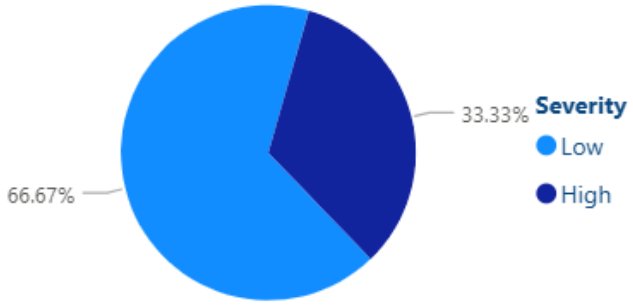
DLP matches by rule



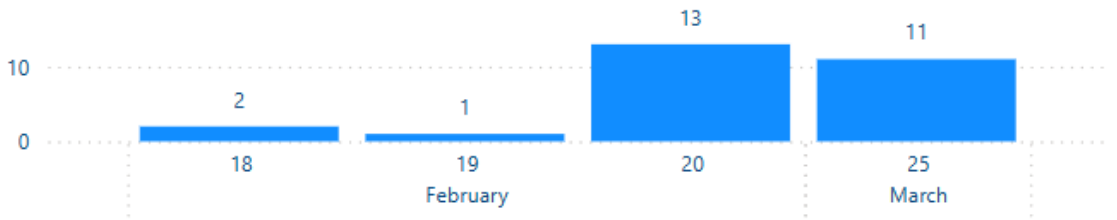
Lastest information update:

3/25/2025 2:14:45 AM

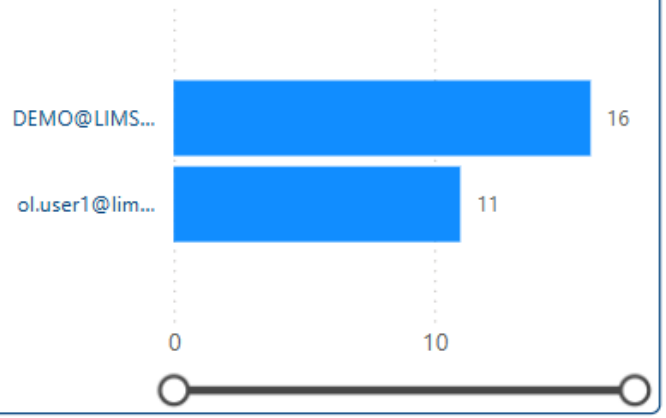
DLP rule matches by severity



DLP rule matches daily behavior



Top DLP rule matches by users



Timeline

1/1/2024 — 3/25/2025

Select your M365 service: All

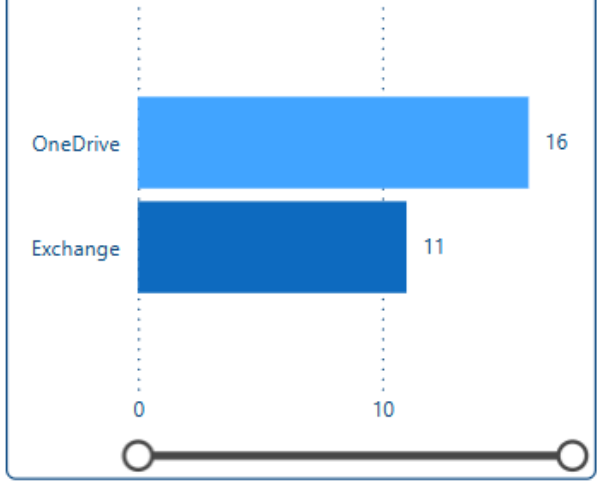
Select your Business Unit: All

Select your DLP Policy: All

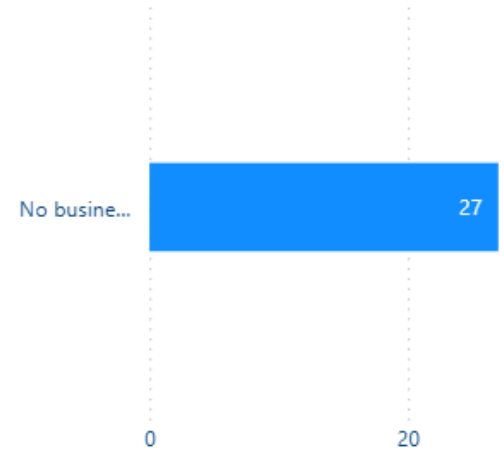
Select the Sensitive Information Type: All

Lastest information update: 3/25/2025 2:14:45 AM

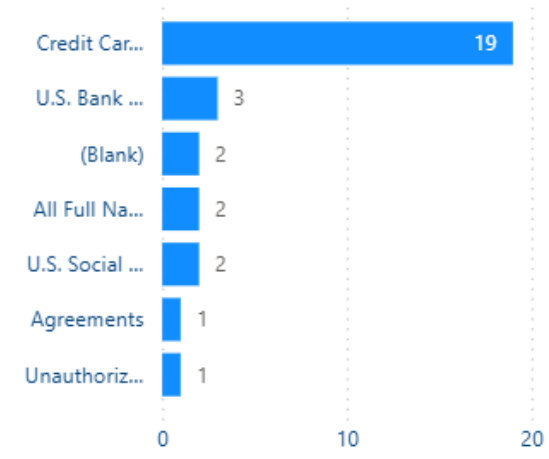
DLP matches by M365 services



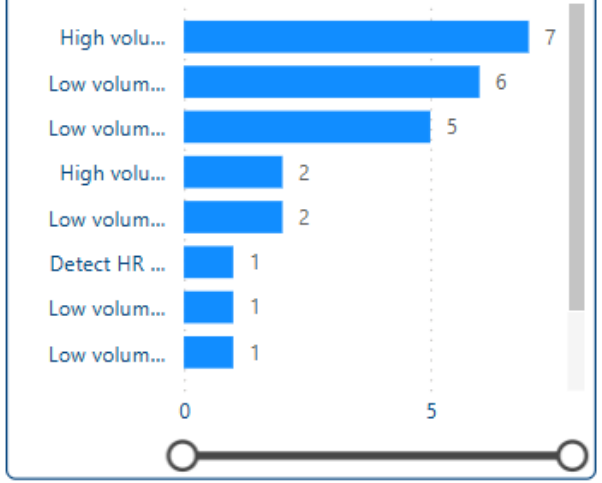
DLP rule matches by business unit



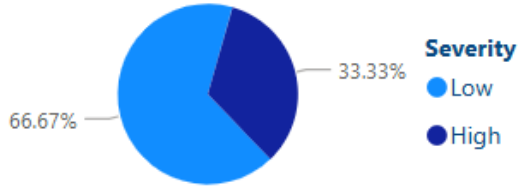
DLP rule matches by SITs



DLP matches by rule

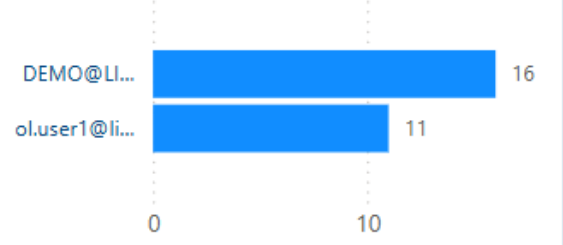


DLP rule matches by severity

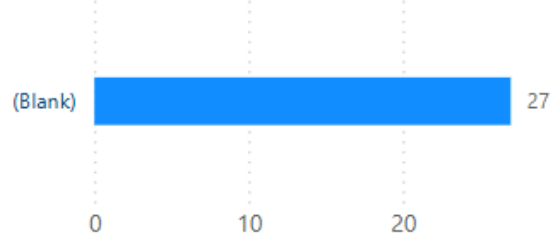


DLP rule matches daily behavior

Top DLP rule matches by users



Top DLP rule matches by IP



DLP rule matches by Label

DLP rule matches by Domain

Non-Profit Enhances Data Governance with Microsoft Purview

Company Overview

- A non-profit organization SPLC approached iLink for a Microsoft Purview Discover and Assessment to evaluate data protection for sensitive information (PCI, PHI, PII) across endpoints, including laptops, on-premises file/SQL servers, BOX, Azure File Share, and Office 365.

Objective

- Identify and classify Sensitive Information Types (SITs) to enable systematic data handling and prepare for future access controls. Identify exposure points.
- Align classifications with Microsoft SIT standards. Enable future Auto-Labelling & DLP policies.

Challenges & Risks

Data Challenge:

- Hybrid environment (on-prem file servers/SQL + BOX SaaS + Office 365).
- No centralized visibility into PII/PHI/PCI data

Blind Spots:

- Sensitive data scattered across legacy systems and SaaS

Compliance Exposure:

- Unclassified PII/PHI in file shares and user devices

Resource Gaps:

- Needed lightweight, scalable approach before investing in DLP

Data Location	PII	PHI	PCI	Key Findings
On-Prem File Servers	🔴	🔴	🟠	Unencrypted donor records
BOX (SaaS)	🟠	🔴	🟢	External sharing enabled
Azure File Shares	🟢	🟠	🟢	Data protection and Auto-labeling not in place
On-Prem SQL Server	🟠	🔴	🟠	Partial column encryption
Office 365	🔴	🔴	🔴	Data protection and Auto-labeling not in place

Our Solution

✅ **Holistic Discovery**:

- Scanned 100+ endpoints (laptops), on-premises (file servers, SQL), and cloud (BOX, Azure, Office 365)
- Mapped 100% of data flows and storage locations

✅ **Precision Classification**:

- Customized 25+ Sensitive Information Types (SITs)
- Aligned with Microsoft benchmarks for PCI/PHI/PII

✅ **Risk Intelligence**:

- Delivered prioritized findings with remediation roadmap
- Highlighted critical exposures in legacy systems

Key Business Outcomes

💰 **Data Security & Visibility**

⚡ ✅ **100% Compliance Success**

- **Passed all insurer audits with zero findings**

😊 **97% Employee Satisfaction**

- **Seamless transition with minimal training needed**

iLink Systems
Thinking Beyond

VCA Comprehensive Security Enhancement with Microsoft Defender

- Industry Vertical
  - Animal Healthcare
- Employees : 10000+

Business Scenario

VCA, one of the biggest animal hospital in US faced challenges in managing and protecting their growing assets. known for its advanced veterinary care and research, faced increasing cyber threats targeting its digital infrastructure. To protect sensitive patient data and ensure compliance with industry regulations, the hospital sought an advanced security solution.

Challenge

The animal hospital encountered several significant challenges:

Diverse and Sensitive Data Sources:

- Managed a wide range of data, including patient medical records, staff information, and research data.
- Required a unified security solution to protect data across various sources and systems.

Sophisticated Cyber Threats:

- **Phishing Attacks:** Increasingly sophisticated phishing schemes targeted staff, attempting to steal credentials and access sensitive information.
- **Ransomware Attacks:** Faced the threat of ransomware attacks that could encrypt critical data, disrupt hospital operations, and demand ransom payments..
- **Zero-Day Exploits:** Vulnerabilities in software and systems that were unknown to the hospital's IT staff, leaving systems exposed to undetected attacks.
- **Insider Threats:** Potential threats from within the organization, either through malicious intent or accidental data breaches by staff.
- **IoT Device Vulnerabilities:** Medical devices connected to the hospital's network presented new attack vectors for cybercriminals.
- **Email Spoofing and Business Email Compromise (BEC)**: Attackers used spoofed emails to impersonate executives or trusted partners, aiming to deceive staff into transferring funds or disclosing sensitive information.

Solution

iLink suggested to implement Microsoft Purview to address these challenges. The implementation involved:

1. Dedicated Support and Incident Response:

- 24/7 support from Incident Response and Customer Support teams.
- Proactive incident management, technical support, and issue resolution during and after deployment.

2. Flexible and Scalable Integration:

- Deployment segmented by region, allowing for customized security settings tailored to each location.
- Gradual rollout to ensure smooth integration without disrupting business operations.

3. Advanced Cloud-Native Platform:

- Adaptable to the client's specific requirements and scalable to handle the large user base.
- Real-time, dynamic scanning of all email content ensured high security without affecting performance.

4. Enhanced Protection Measures:

- Implemented real-time scanning of millions of files and URLs, providing robust protection.
- Specialized in preventing advanced threats such as phishing, malware, and ransomware.

Key Metrics

- **Traffic**
  - Total emails scanned: 28,760,432
  - Total artifacts scanned: 82,950,124
  - Embedded files/mail ratio: 0.5x
  - Embedded URLs/mail ratio: 1.1x
- **Events**
  - Attacks prevented: >350,000
  - Spam blocked: 1,200,000
  - Most prevalent attack: Malware (130,000 unique attacks)
  - Advanced attacks blocked by defender engine
- **Performance**
  - Average scan time for clean content: 8 seconds
  - 75% of content scanned within: 10 seconds
  - 100% of content scanned dynamically

Results

Over a five-month period, Microsoft Defender's email security system achieved the following:

- Intercepted over 350,000 malicious attacks.
- Blocked over 1,200,000 spam emails.
- Maintained an average scan time for clean emails of less than 10 seconds.

Our Expertise

Our team of experts provides end-to-end services, including assessment, planning, deployment, and ongoing support, ensuring our clients achieve their security goals efficiently.

Key Areas of Expertise:

- **Threat Detection and Response**
- **Endpoint Protection**
- **Vulnerability Management**
- **Security Monitoring**
- **Incident Response**
- **Compliance and Reporting**

iLink Systems
Thinking Beyond


iLink Digital
Thank you