Cloud

On-Premises

Amazon S3 Buckets

Sensitivity labels

Azure SQL Database

Azure Blob Storage

Azure Synapse

Azure Datalake Storage

ADSLGen1 & ADSLGen2

Sensitivity labels

Via Client side readiness script

Azure Purview

Sensitivity labels and data classification

Data Connectors

REUTERS, webex, salesforce, zoom, servicenow, CISCO, Bloomberg, slack

Social-media data, instant messaging, documents

Solutions

Azure Security Center

Azure AD

Microsoft Defender for Endpoint

Office 365

Microsoft Defender for Office 365

Microsoft Intune

Microsoft Cloud App Security

Azure Information Protection

Azure Identity Protection

Microsoft Defender for Identity

Security Alerts

DLP Policies Enforcement

Policies, Alerts, Reports

DLP Policies Enforcement

Security Alerts

Microsoft 365 Compliance Center

https://compliance.microsoft.com

Compliance Manager

Control Access | Discover & Respond | Govern Information | Manage Compliance | Manage Devices | Manage Internal Risks | Protect Against Threats | Protect Information

Data Classification

Communication Compliance
Detect, capture and act on inappropriate messages in the organization communication channels

Data Loss Prevention
Prevent inside users from inappropriately sharing sensitive data

eDiscovery
Identify and deliver electronic information that can be used as evidence in legal cases

Information Governance (MIG)
Provide capabilities to govern the organization data for compliance or regulatory requirements.

Insider Risk Management
Data spillage, Confidentiality violations, IP theft, Fraud, Policy violation, Sensitive data leaks, security violations, regulatory compliance violation.

Records Management
Manage organizations legal obligations, demonstrate compliance, and increases efficiency with regular disposition of items that are no longer required to be retained

Privacy Management
Provide solutions for managing personal data in Microsoft 365 environment

Information Protection (MIP)
Discover, classify, and protect sensitive information wherever it lives or travels. (Label Policies)

Security Score | Policies | Alerts | Reports | Audit | Assessments

Compliance Monitoring, Reporting, Investigation

Endpoint DLP Policies Enforcement

Endpoint

Windows 10 device

Security Alerts

DLP incidents, eDiscovery

Microsoft Graph Security REST API

Security Alerts

Assessment Templates

Premium Templates E.g. CMMC, NIST, HIPAA Additional Fees applies

Email notifications (dispositions)

Compliance Administrator

Other logs

Azures Sentinel Log Analytics Workspace

Logs / Metrics

Kusto Query Language Queries

Azure Sentinel

Log Correlation

Security Alerts

Playbooks

Logic Apps

Incidents/Tickets/Reports

Security Operation Center (SOC)

BlueVoyant https://www.bluevoyant.com

Security Investigation

Custom Alerts

24x7 Managed Detection and Response

Managed Sentinel
www.managedsentinel.com

SOAR Automation

M365 Deployment

KPI Reporting & Monitoring

Third Party Risk

Threat Intelligence

Cyber Forensics Incident Response

Vulnerability Management

Microsoft 365 Compliance Licensing Requirements:

- *Microsoft 365 E5*

OR

- *Microsoft 365 E5 Compliance + Microsoft 365 E3 or (Office 365 E3+EMS E3)*

OR

- *Microsoft 365 E5/A5 Info Protection & Governance + (AIP Plan1 or EMS E3) + (Exchange Online, SharePoint Online or OneDrive for Business)*