Microsoft

Drive Down Risks of Data Disaster
with Microsoft Purview

MARCH 26, 2024

BDO

Our Agenda Today

Operating in a World Accelerated

The Data Hydra

Platform unified visibility with Purview

Get Started: One Step at a Time

With You Today

WAYNE ANDERSON
Data Security NA Service Line Leader

970-324-2276
wanderson@bdo.com

MARK RABORN
Data Security Architect

214-259-1448
mraborn@bdo.com

We Are Operating in a World Accelerated

84% | ## Must Accelerate Technical Innovation
Of leaders say their organization will only survive if it significantly accelerates its technological innovation.

**81%** | ## Require Technology to Enable Organizational Strategy
Of leaders say that technology is now the number one critical enabler of organizational strategy.
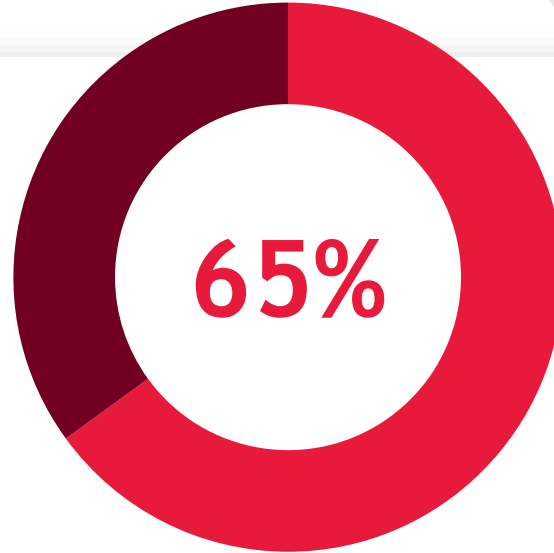
86% | ## See failure to leverage tech benefits as a risk to the org
Of leaders say that failure to leverage the benefits of technology – including data and AI – is a risk that will impact the organization over the next 3 years
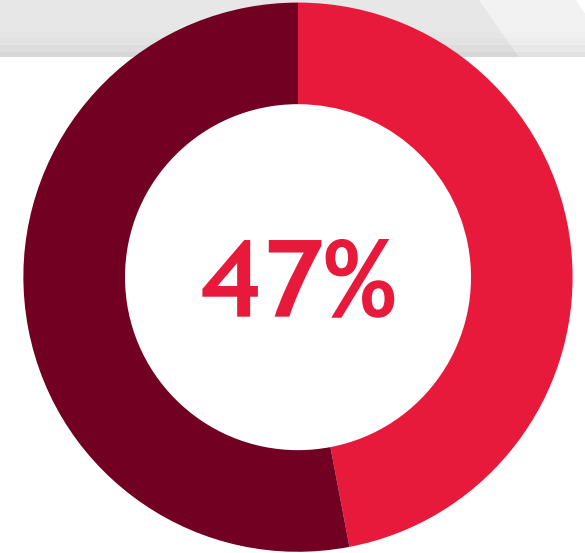
Security Tension With the Business

69%
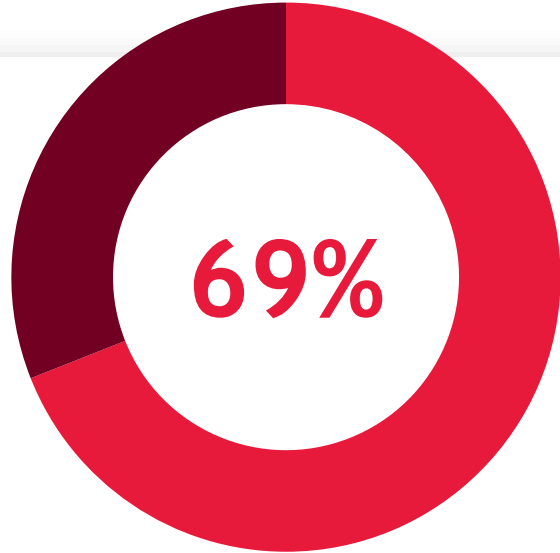
Of board members see "eye to eye" with Chief Information Security Officers (CISOs)

65%

Of Directors still believe their organizations are at risk of a material cyberattack within 12 months.

47%

Of board members reported having any recent contact with the Chief Information Security Officer (CISO)

Security Tension With the Business

76%

Of board members believe they have made "adequate investments" in cyber protection.

Of board m... ...orted to eye" with... Information Security Officers (CISOs)

organizations are at risk of a material cyberattack within 12 months.

having any recent contact with the Chief Information Security Officer (CISO)

For the Security Team...

▶ Demands cost efficiency

▶ Link with the Business
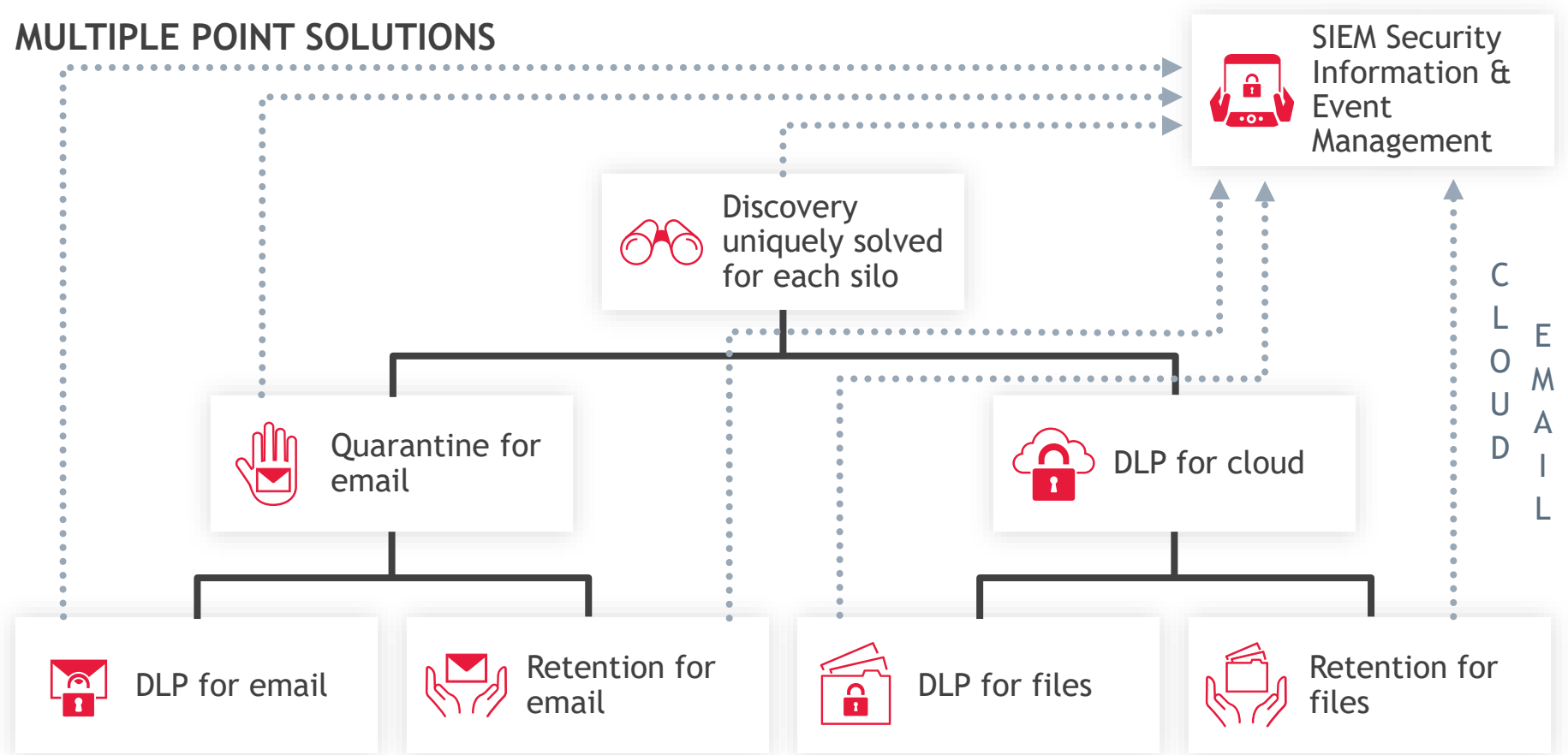
▶ Protect against Human-error

▶ Avoid distraction

... and "it's **your** fault"
if we have a breach event.

Approaches of the Recent Past

With data breaches and regulatory requirements increasing, security leaders historically have stitched together often disparate fabrics of siloed solutions attempting to gain coverage for data protection.

The result is numerous overlapping commitments, increased licensing costs, and a web of connectors and management approaches attempting to bridge gaps and consolidate signals.

MULTIPLE POINT SOLUTIONS

SIEM Security Information & Event Management

Discovery uniquely solved for each silo

CLOUD EMAIL

Quarantine for email

DLP for cloud

DLP for email

Retention for email

DLP for files

Retention for files

Microsoft Purview

Microsoft Purview empowers data security with a comprehensive set of unified solutions controlling governance, AI and machine learning driven discovery, data classification, controls, telemetry, security information and events across the digital estate.

Purview overcomes

▶ The fragmentation of data across solutions

▶ Lack of visibility and gaps associated with security silos

▶ Alignment of function solving the blur typically associated with with multiple IT/Security management roles

Purview unifies Azure and M365 compliance solutions: Data Classification, DLP & Rights Management, Data Lifecycle, Internal Risk, Case Management, Cloud App Security, and Audit into one unified XDR platform.

Purview Platform Enhancements

DATA CLASSIFICATION

Find, Know, Label… Automatically

▶ Discover, enumerate, and classify

Advanced Discovery Technologies

▶ File properties, sensitive data, exact data match, OCR, machine learning, document fingerprinting, and custom queries

DLP & RIGHTS MANAGEMENT

Information Protection

▶ Classify, label, and protect documents and files

Data Loss Prevention

▶ Safeguard data and files in use and in transit

DATA LIFECYCLE

Data Lifecycle Management

▶ Retain, review, dispose via automation

Records Management

▶ Protect business records irrevocably

Purview Platform Enhancements

INTERNAL RISK

Communications Compliance
- Manage communications for compliance

Information Barriers
- Segregate data from business units/depts

Insider Risk Management
- Intentional or accidental user actions

Privacy Risk Management
- Proactively identify and protect against privacy risks

CASE MANAGEMENT & AUDIT

eDiscovery
- Respond to legal matters or internal investigations intelligently at scale

Alerts
- Detailed and customizable alerting for SOC and Governance investigations

Audit
- Highly granular audit history retainable up to 10 years

CLOUD APP SECURITY

3rd Party SaaS
- Invoke Access Control, Session Control and DLP on 3rd party app estate

Shadow IT
- Discover, Sanction, Unsanction and Monitor

Integration Connectors
- Telemetry from on-premise devices & logs
- Built in API Connectors for deeper integration with cloud SaaS

Data Lifecycle

Lifecycle should satisfy **unique requirements** for unique assets.

Lifecycle should span unique data types and discover them **automatically**.

Lifecycle should identify risk and **block information loss** under the most difficult conditions.

Lifecycle should **allow change** to unique data while **providing resilient restoration** to protected points in time.

Lifecycle should **empower authoritative review** before required data disposal.

Lifecycle protections must be resilient, enforcing compliance and **eliminating or reducing legal exposure** and regulatory risk.

Purview is part of your Zero Trust Infrastructure

Microsoft Purview solutions help you implement a Zero Trust security strategy based on

Verify Explicitly

Always authenticate and authorize based on all available data points

Use Least Privilege Access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection

Assume Breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses

Data Classification

So, you can know your data

Information Protection

So, you can protect your data

Data Loss Prevention

So, you can prevent data loss

Data Lifecycle Management

So, you can delete what you don't need

Purview is part of your Zero Trust Infrastructure

Microsoft Purview solutions help you implement a Zero Trust security strategy based on

Role-based permissions

Administrative Units

Privileged Access Management

Double Key Encryption for Sensitivity Labels (documents & emails content)

Advanced Message Encryption (email in transit)

Insider Risk Management (risky user & data activity)

Information Barriers (segment access between depts)

Purview Now and in the Future

Whether adding new solutions to the Microsoft Purview governance compliance portals, updating existing features based on your feedback, or rolling out fresh and updated documentation, Microsoft Purview helps you stay on top of the ever-changing data governance, risk and compliance landscape.
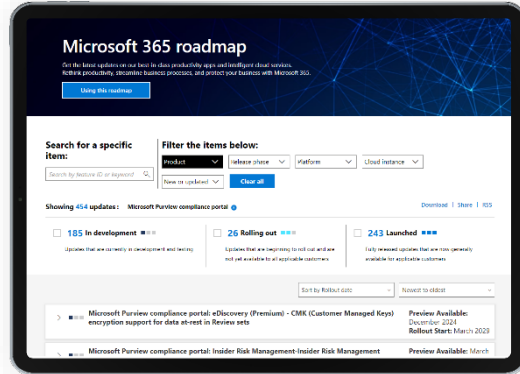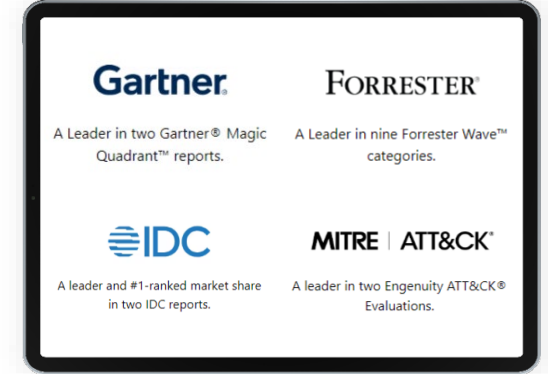

Roadmap

Purview Portal benefits from world class enterprise customers feedback and trillions of terabytes of signal telemetry to drive an industry leading roadmap in cybersecurity.

▶ 185 in development

▶ 26 rolling out

Feature Updates

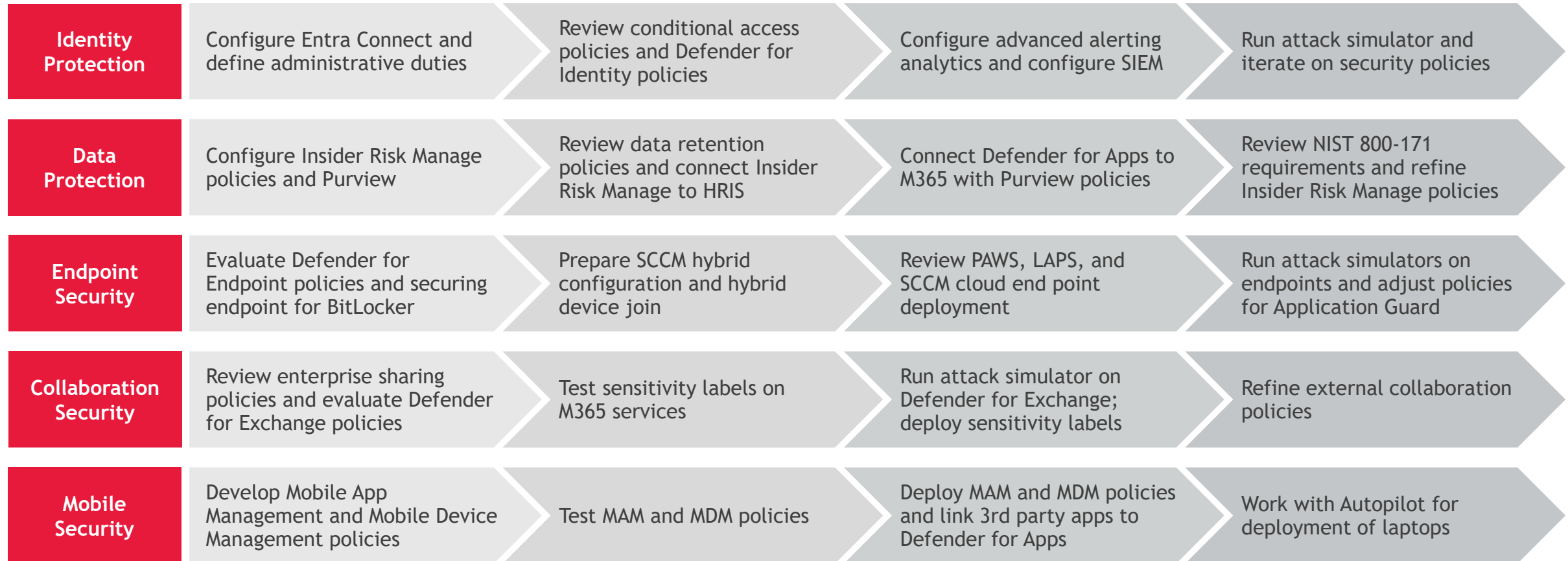Purview embodies a robust Feature Updates cycle with regular monthly updates across the platform.

Industry Recognition

Cybersecurity Leader Awards

(2) Gartner Magic Quadrant
(9) Forrester Wave
(2) Engenuity Mitre ATT&CK
… #1 in Cyber market share

Organizational Experience Protecting Data Is Variable

Identity Protection	Configure Entra Connect and define administrative duties	Review conditional access policies and Defender for Identity policies	Configure advanced alerting analytics and configure SIEM	Run attack simulator and iterate on security policies
Data Protection	Configure Insider Risk Manage policies and Purview	Review data retention policies and connect Insider Risk Manage to HRIS	Connect Defender for Apps to M365 with Purview policies	Review NIST 800-171 requirements and refine Insider Risk Manage policies
Endpoint Security	Evaluate Defender for Endpoint policies and securing endpoint for BitLocker	Prepare SCCM hybrid configuration and hybrid device join	Review PAWS, LAPS, and SCCM cloud end point deployment	Run attack simulators on endpoints and adjust policies for Application Guard
Collaboration Security	Review enterprise sharing policies and evaluate Defender for Exchange policies	Test sensitivity labels on M365 services	Run attack simulator on Defender for Exchange; deploy sensitivity labels	Refine external collaboration policies
Mobile Security	Develop Mobile App Management and Mobile Device Management policies	Test MAM and MDM policies	Deploy MAM and MDM policies and link 3rd party apps to Defender for Apps	Work with Autopilot for deployment of laptops

Link Your Program Investments to Your Business Goals

Revenue

▶ Unlock specific markets

▶ Enable sales through client contract commitments

▶ Maintain revenue producing accounts through assessment evidence

Cost Containment

▶ Reduce the risk of breach-based liability

▶ Reduce potential cost of incident response

▶ Streamline security tools and costs

▶ Streamline into platform based RBAC and visibility to the data pipeline

▶ Efficient training and operations

▶ Evidence export via PowerShell

▶ Compliance Manager toolset to identify and store configuration evidence

▶ Full audit logging for compliance and security features

▶ Comprehensive data management features,

▶ Including investments in privacy risk management supporting features

Build the Habit of Continuous Assessment

Assess Data Estate

Proactive Data Management

Control Data Exposure
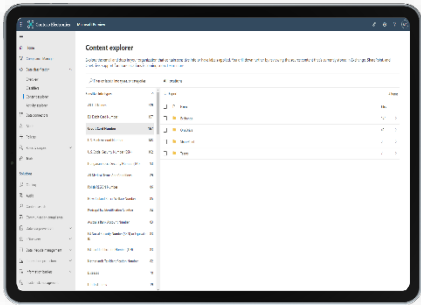
Operate and Improve

▶ Establish a baseline of what sensitive info you hold

▶ Talk to your business - what are they concerned about

▶ Set a definition of success – how do you know what good is?

▶ Do periodically as a habit
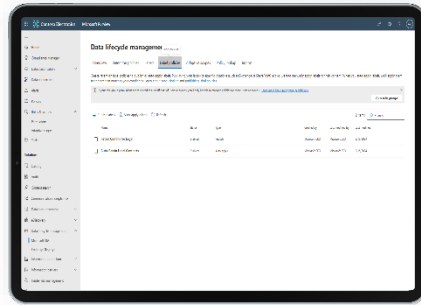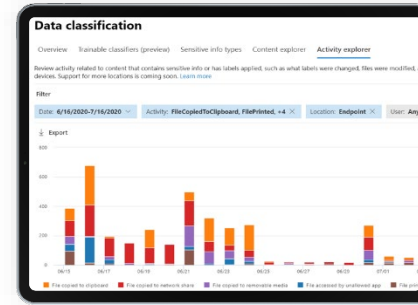
GET INTENTIONAL TO DRIVE DOWN DATA DISASTER RISKS
Proactive Data Management to Prune Risk from ROT
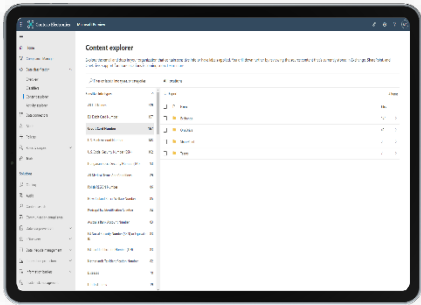
Assess Data Estate
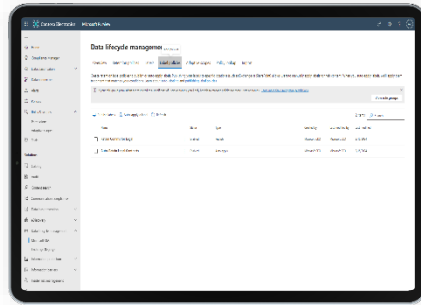
Proactive Data Management

▶ Identify redundant, outdated, trivial data for removal

▶ Make it easy to protect the business – label for retention, label for removal

▶ Auto-recognize and label data at scale for review

▶ Keep what regulations say you must
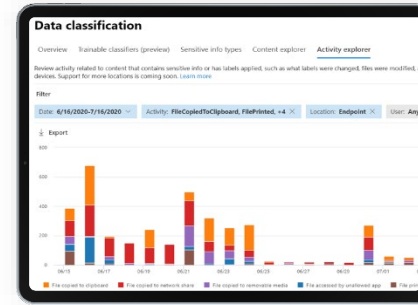
Control Data Exposure

Operate and Improve

Reduce Risk by Controlling Data Exposure with DLP
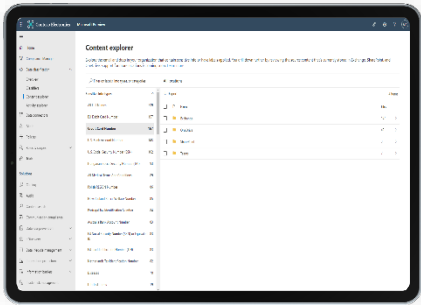
Assess Data Estate
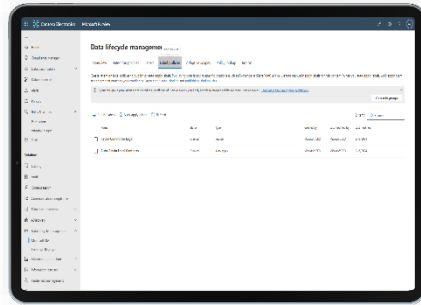
Proactive Data Management
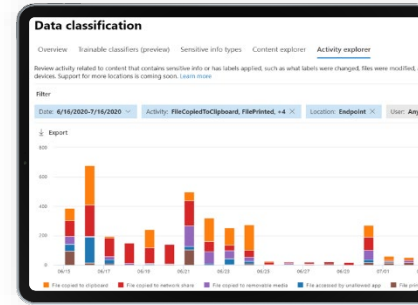
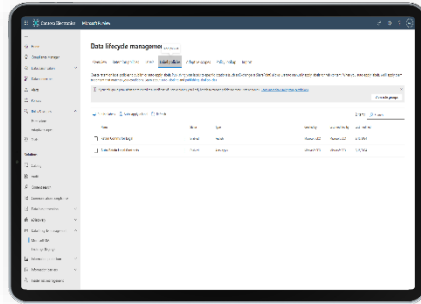**Control Data Exposure**

Operate and Improve

- ▶ Use sensitivity types to control easily identifiable data
- ▶ Powerful AI backed Trainable Classifiers can help with difficult/variable formats
- ▶ Build a matrix that reflects what protection the business needs
- ▶ Enforce with a powerful platform

GET INTENTIONAL TO DRIVE DOWN DATA DISASTER RISKS
Operate and Improve Over Time Internally or With Managed Services
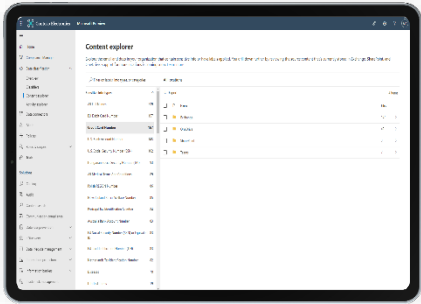
Assess Data Estate

Proactive Data Management

Control Data Exposure

Operate and Improve

▶ Use a platform strategy to enrich good decisions on what risks to respond to with insider risk management and/or Sentinel

▶ Consider a managed service provider to raise maturity quickly

▶ Refresh discovery and policies regularly

Assess Your Data Estate to Start Reducing Your Risk

DATA RISK ENGAGEMENT

Discovery Session

Detailed assessment of your strategic objectives, influences, and priorities for risk management and regulatory compliance

Data Assessment

Use Microsoft Purview to discover and rapidly assess sensitive data in the Microsoft 365 and related environments. Optionally evaluate insider risk and risky communications.
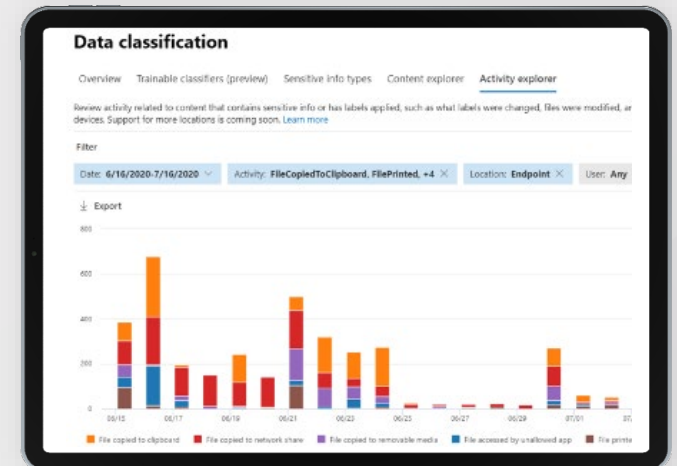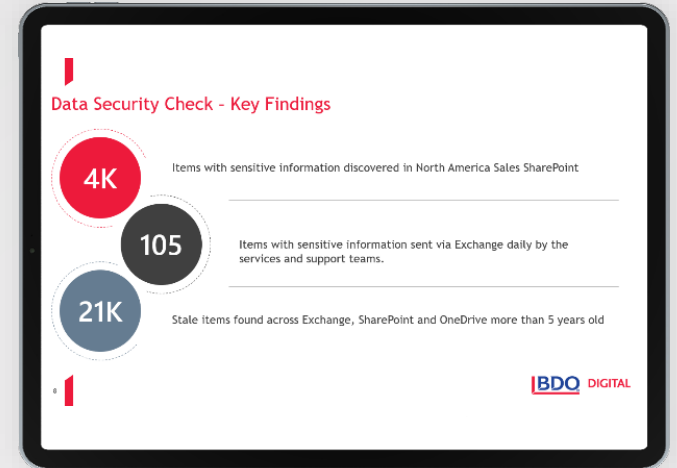
Analysis

Build a list of recommendations and actionable next steps that will help mitigate identified security and compliance risks in your production environment.

Roadmap

Provide a set of long-term recommendations in a roadmap with key initiatives and tactical next steps to reduce risk with new and existing capabilities.
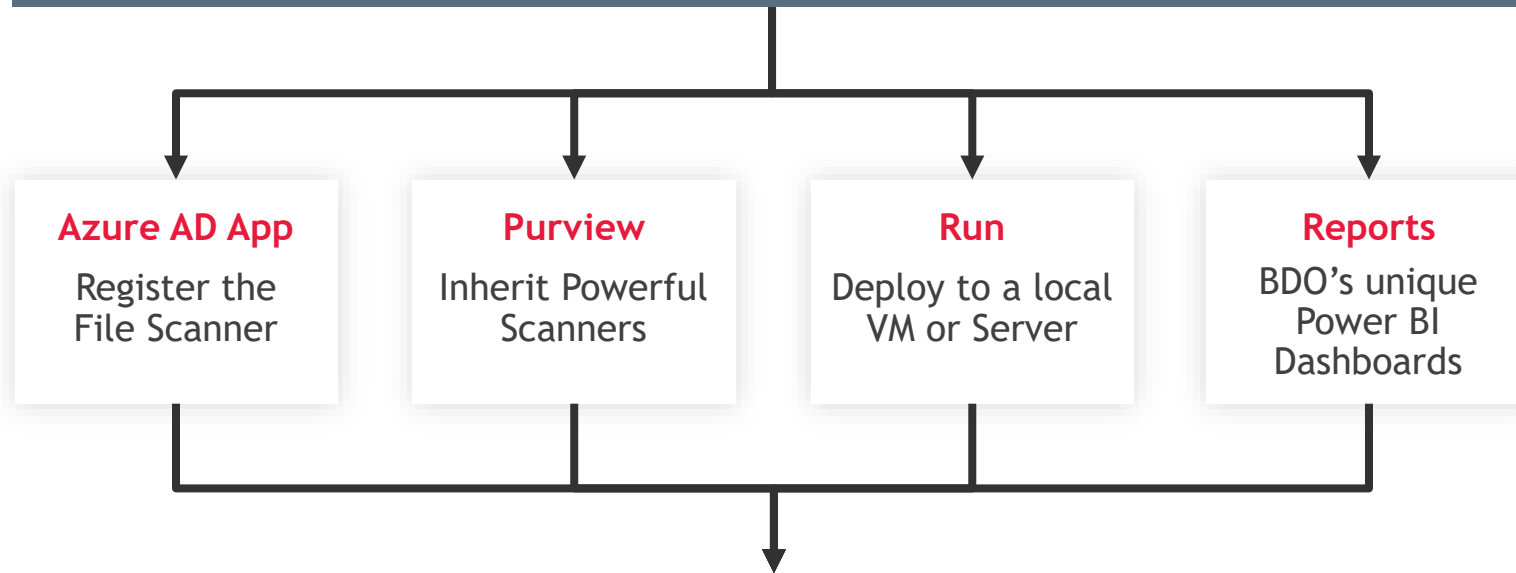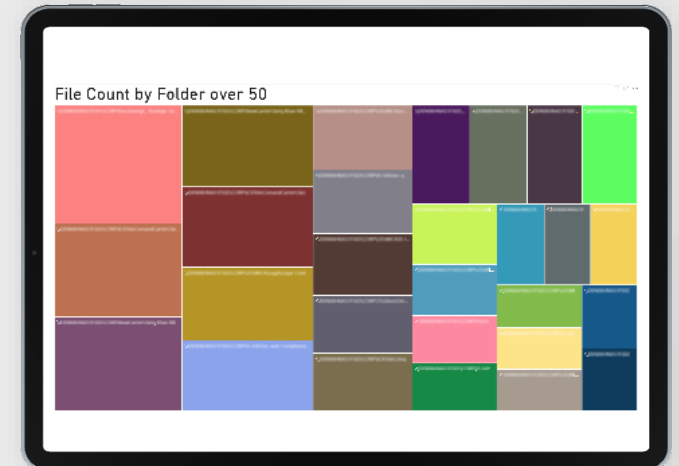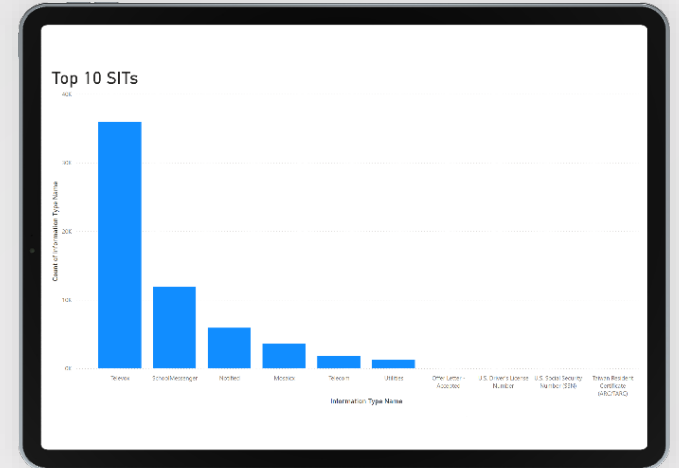
Extend Purview to your Dark Data to Start Reducing Your Risk

FILE SHARE ASSESSMENT

Planning: Get identities established, plan key file shares, target critical risks.

Azure AD App	**Purview**	**Run**	**Reports**
Register the File Scanner	Inherit Powerful Scanners	Deploy to a local VM or Server	BDO's unique Power BI Dashboards

Get Actionable insight reports on data aging, sensitivity, and more!

Top 10 SITs

File Count by Folder over 50

Renaissance 2024: Unleashing the Power of Microsoft 365 & Defender

Embrace the future with confidence, leveraging the formidable capabilities of Microsoft 365 and Defender.

▶ Explore the principles of a modern zero-trust architecture and understand how it transforms your security posture from the ground up.

▶ Discover how Defender goes beyond traditional antivirus solutions to provide holistic, proactive defense.

▶ Learn the latest techniques to secure your organization's devices, ensuring not only protection but also flexibility for the modern workforce.

▶ Explore innovative identity strategies that act as the new perimeter, offering enhanced security while accommodating the mobility and ease of use demanded by today's workforce.

Microsoft

Questions?

BDO

About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com