Microsoft Purview: A Guided Tour

2024 Wyoming Spring Conference



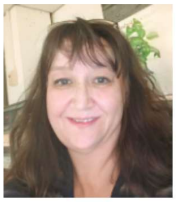
1

Special Thanks

Wyoming Chapter of ARMA International: Board of Directors



President
Geetha Murugesu
Wyoming Highway Patrol



Treasurer
Barbara Thomasee
Wyoming Dept. of Transportation



Secretary
Carmen Clayton
State of Wyoming - Archives



Social Media
Mindy Inman
Wyoming Public Service Commission

Today's Event Sponsors

WYOMING HIGHWAY PATROL DISPATCH

WYOMING TRANSPORTATION DEPARTMENT

ARMA WYOMING

Paintrock CONSULTING SERVICES

kristi@paintrockconsulting.com

2

Glad to meet you!

I left the oil and gas industry, and the heat of Houston, to form Paintrock Consulting in 2013 - initially focused on SharePoint & MS cloud adoption

Today I provide deep expertise in Governance and Compliance across multiple industry verticals and support organizations in US, UK, and EU

Fun facts:
- I live in rural NW Wyoming & have launched 2 non-profits
- Wyoming Woman Entrepreneur of the Year nominee in 2022
- Speak and mentor for Diversity in Tech and Women in STEM

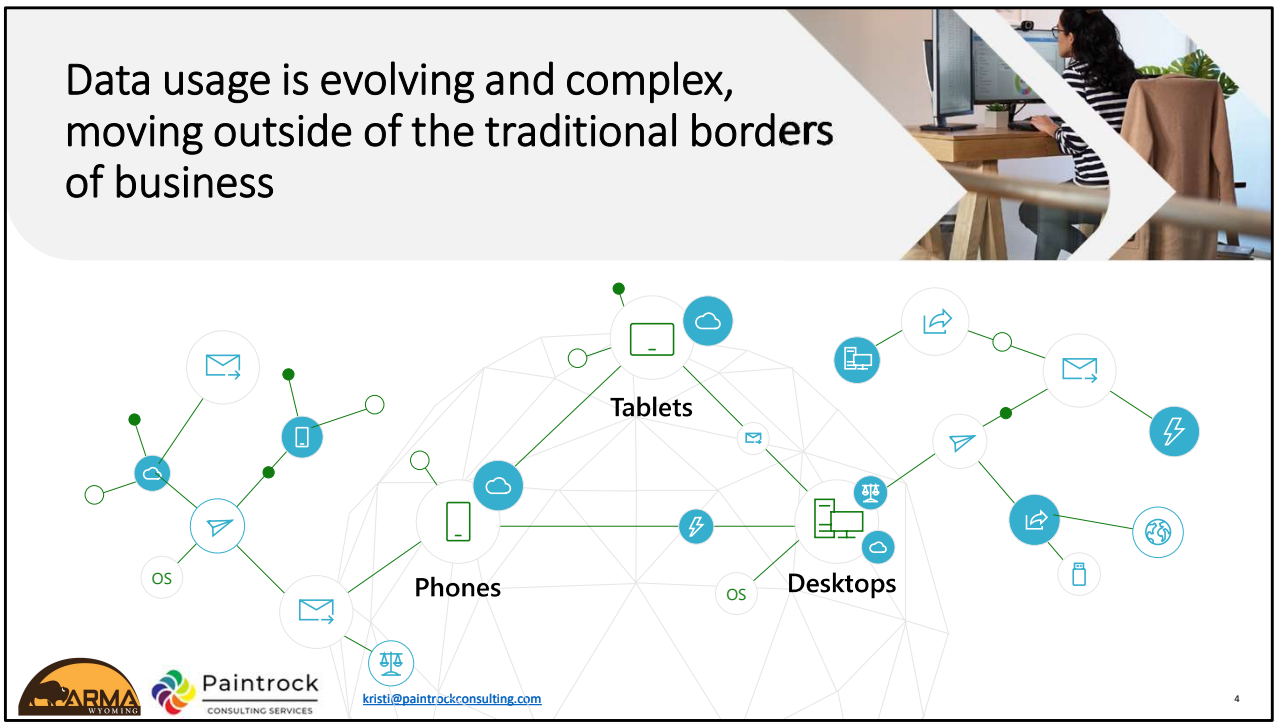


Kristi Robison, IGP

Paintrockconsulting.com
@klrobison
Kristi Robison, IGP | LinkedIn

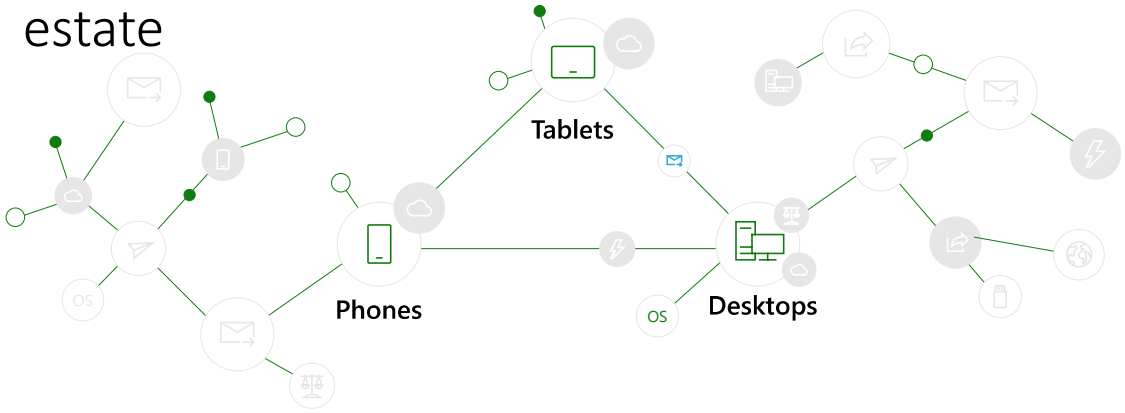
Paintrock
CONSULTING SERVICES

3



Data has become the lifeblood of every business, but with the shift to hybrid work and unprecedented levels of digital transformation, an organization's data now lives outside of the traditional borders of business.

Organizations lack visibility into their data estate



Year over year, the amount of data available doubles

93% of data within an organization is dark

kristi@paintrockconsulting.com

5

Over 30% of decision makers don't know where or what their sensitive business-critical data is, making it nearly impossible for organizations to protect that data, close exposure gaps, comply with regulatory requirements, or even manage access controls.

For data to fuel digital transformation, it must be readily discoverable, understandable, high quality, accessible and used in compliance with corporate, regulatory, privacy, risk and ethical standards. Considering over 93% of data within an organization is dark, customers are faced with solving an immediate need to cull the data surface area to protect more effectively against leaks or breaches.

The landscape is fragmented, creating risks



Exposure gaps | Missed regulatory requirements | Impeded digital transformation | Failed audits | Brand reputation at risk

kristi@paintrockconsulting.com

6

Not only is this data across a range of systems and applications, but it is also subject to rapidly evolving global regulations.

It's challenging to find a solution that integrates with hybrid environments

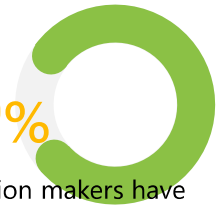


90%

of organizations are multi-cloud

80%

find it hard to manage fragmented compliance and risk related solutions



80%

of decision makers have purchased **multiple products** to meet compliance and data-protection needs

A majority have purchased **3+ products**

ARMA WYOMING | Paintrock CONSULTING SERVICES

kristi@paintrockconsulting.com

7

The market has responded with dozens of products that address fragments of the data governance and compliance landscape, forcing Chief Data, Security, Compliance, and Legal Officers to stitch together a patchwork of solutions that don't work together, expose infrastructure gaps and are costly and complex to manage. In fact, a recent survey of decision-makers showed that to meet their compliance and data-protection needs, almost 80% had purchased multiple products, and a majority had purchased 3 or more. It's not just more work; it's also ineffective. Security outcomes are worse. Audits are failed. Legal cases lost. Brand reputation damaged.

Microsoft Purview

Comprehensive solutions to help govern, protect and manage your data estate

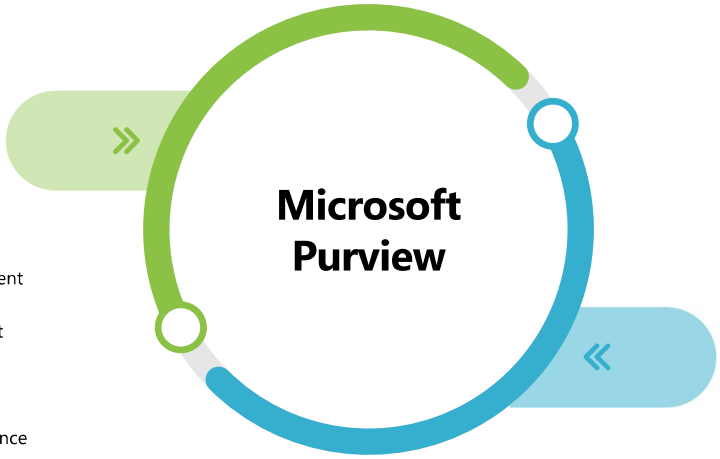


So, what comes with Purview?

Risk & compliance

For risk, compliance, and legal teams

- Information Protection
- Data Loss Prevention
- Data Lifecycle Management
- Data Connectors
- Insider Risk Management
- eDiscovery
- Audit
- Records Management
- Communication Compliance
- Compliance Manager



- Data Map
- Data Catalog
- Data Estate Insights

Unified data governance

For data consumers, data engineers, data officers

kristi@paintrockconsulting.com

Microsoft Purview

Comprehensive solutions to help govern, protect and manage your data estate



Understand & **govern** data

Manage visibility and governance of data assets across your environment



Safeguard data, wherever it lives

Protect sensitive data across clouds, apps, and devices



Improve risk & compliance posture

Identify data risks and **manage** regulatory compliance requirements

Microsoft ecosystem

Support for multi-cloud, hybrid, SaaS data | Third-party/partner ecosystem

Next we'll dive into the features in each of these 3 pillars: Govern, Protect, and Manage

kristi@paintrockconsulting.com

Understand and govern data

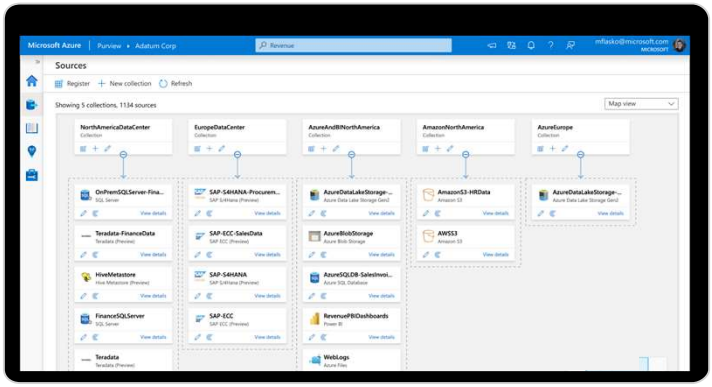
Manage visibility and governance of data assets across your environment



kristi@paintrockconsulting.com

Microsoft Purview Data Map

Unify and make data meaningful across your environment

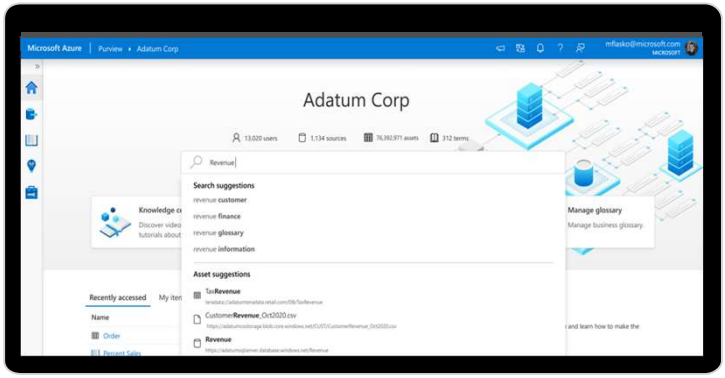


- Graph describes the data assets and their relationships across your data estate
- Automated data scanning, classification and lineage extraction of hybrid data stores
- 200+ built-in data classifiers
- Support for 35 data sources and growing

kristi@paintrockconsulting.com

Microsoft Purview Data Catalog

Enable effortless discovery of trusted data

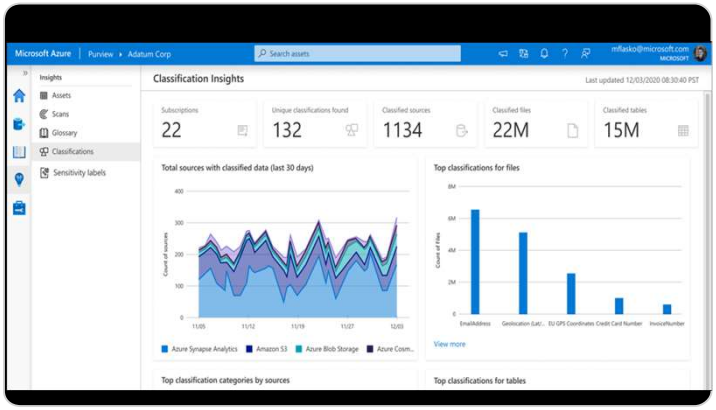


- Search, browse, and curate data
- Intelligent recommendations
- Lineage visualization

kristi@paintrockconsulting.com

Microsoft Purview Data Estate Insights

Gain a bird's-eye view of your data landscape

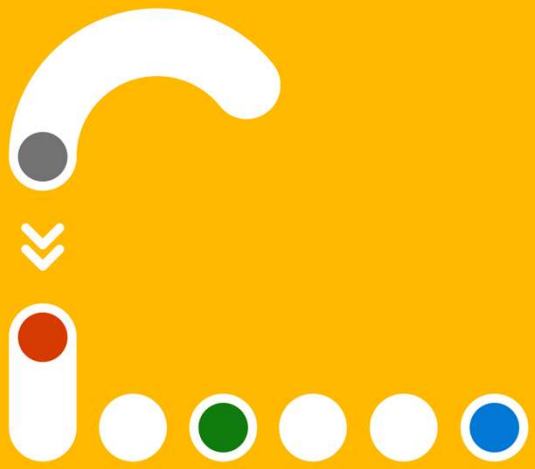


- Data asset distribution
- Data scanning coverage
- Business glossary utilization

kristi@paintrockconsulting.com

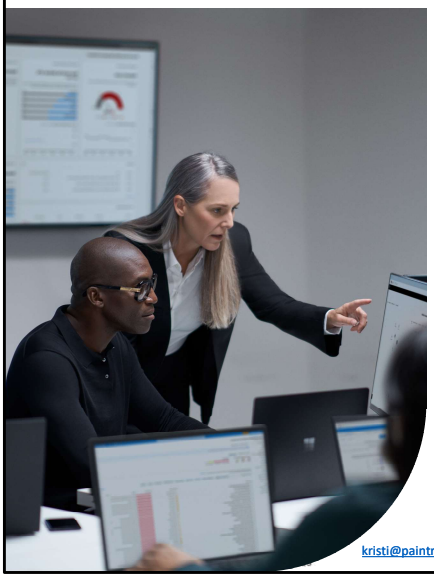
Safeguard data, wherever it lives

Protect sensitive data across clouds, apps, and devices



kristi@paintrockconsulting.com

Top data security concerns



Data security incidents are widespread	83%	of organizations experience more than one data breach in their lifetime[1]
Malicious insiders account for 20% of data breaches, adding to costs	$4.18M	Average cost of data breach with a malicious insider[2]
Organizations are struggling with a fragmented solution landscape	80%	of decision makers purchased multiple products to meet compliance and data protection needs[3]

1. Cost of a Data Breach Report 2022, IBM
2. Cost of a Data Breach Report 2022, IBM
3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

kristi@paintrockconsulting.com

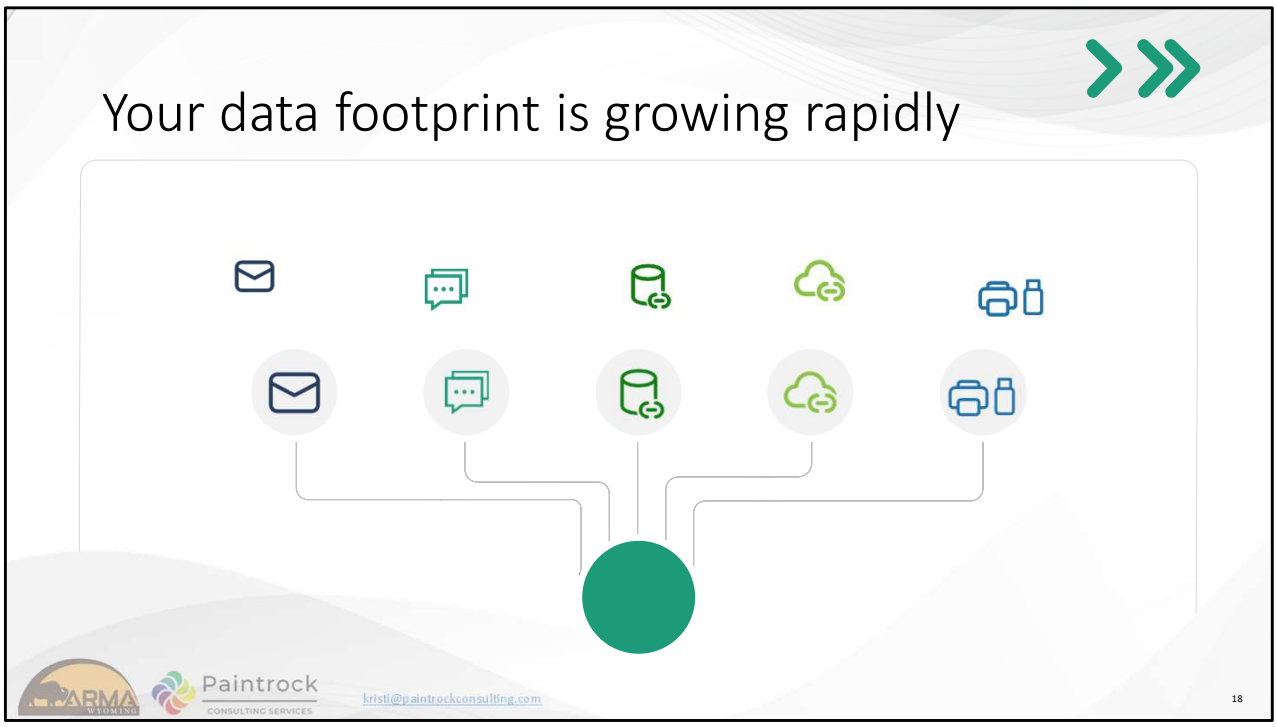
Cybersecurity is a constantly shifting landscape. As our digital world continues to grow, so do the risks. According to research, 83% of organizations experienced more than one data breach in their lifetime, of which 20% of data breaches are due to internal actors with an average cost of **$4.18M** when a malicious insider is involved. The potential cost is very significant and cannot be ignored. Data leaks and theft might be overshadowed by external threats in the past. However, they have become one of the most common vulnerability and risks that organizations need to address.

Recent Microsoft research also shows that 80% of the decision makers purchased multiple products to meet compliance and data protection needs, with majority of them purchase more than three products. Managing a fragmented solution landscape brings more complexity to the security teams with additional costs and efforts to bring siloed signals together while building a unified remediation plan across.

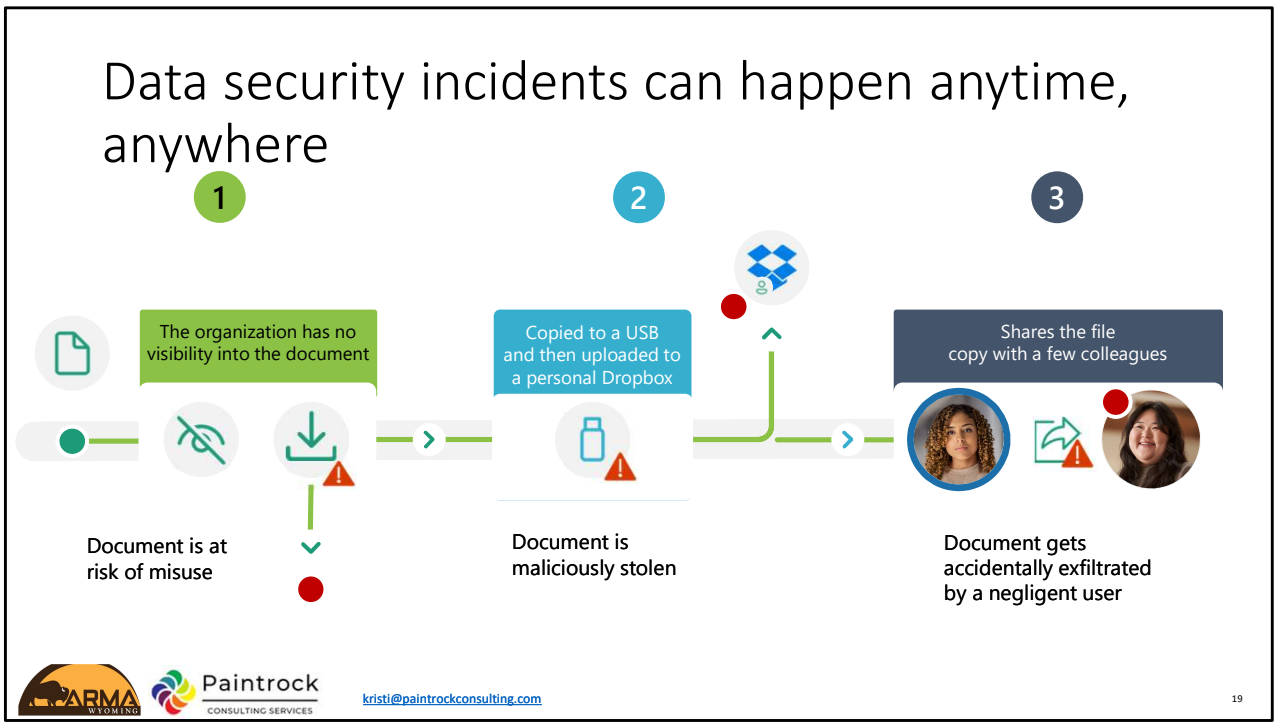
Why is data security so difficult?



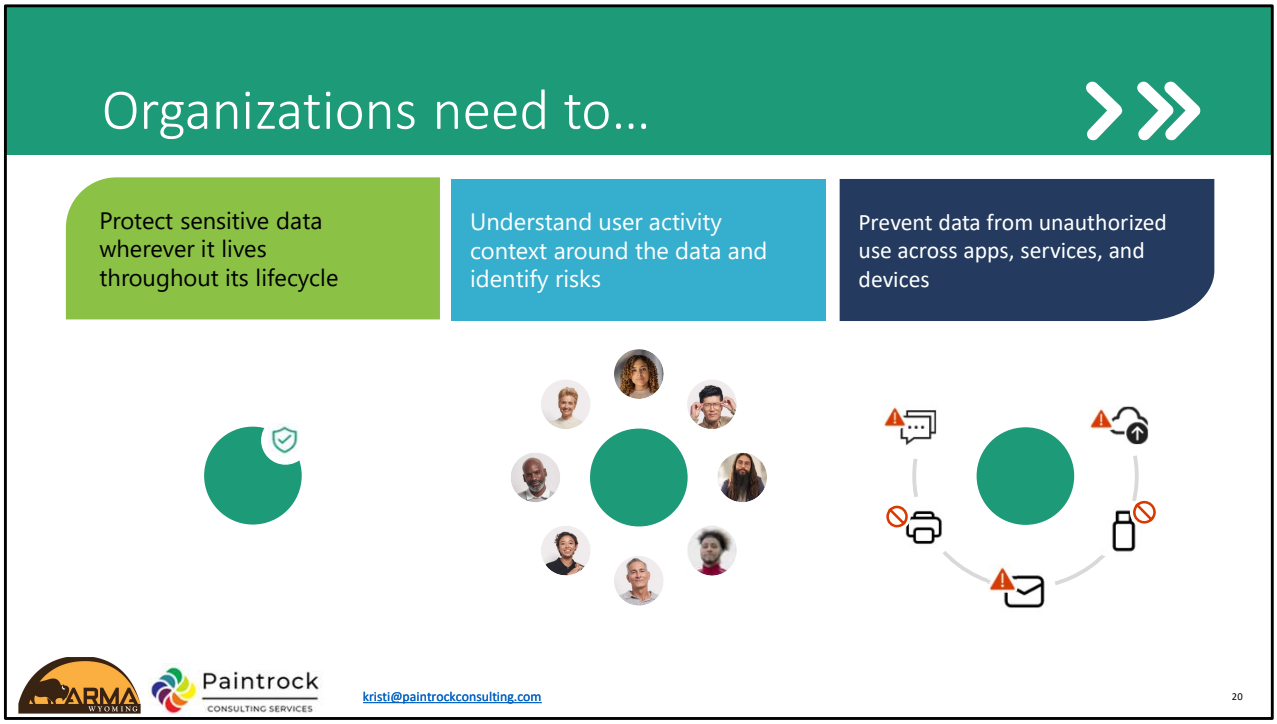
Why is data security so difficult? Organizations need to secure data in multiple channels, including emails, messages, shared storage, cloud apps, and devices, on top of managing a fragmented solution landscape we mentioned in the previous slide.



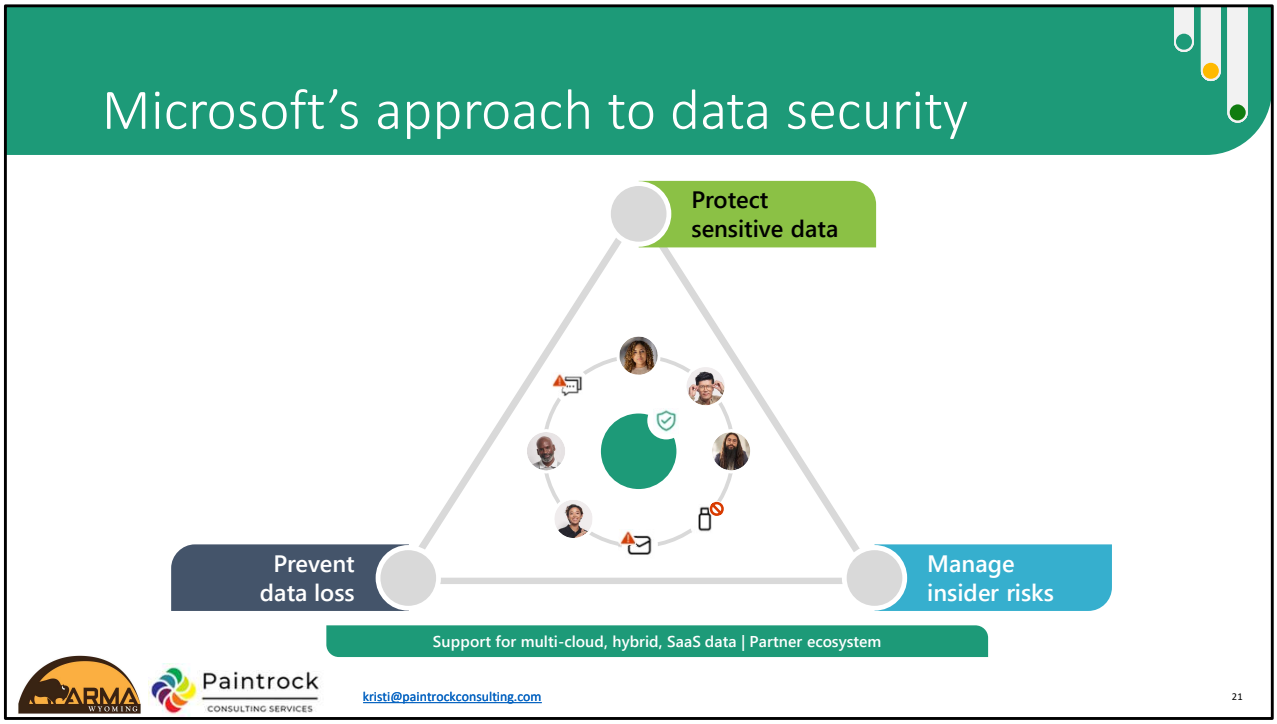
Data is like the oxygen of digital transformation. As organizations and individuals rely more and more on data, the creation and consumption of data are constantly growing. Can you imagine that people created 2.5 quintillion bytes of data and sent 333.2 billion emails every day? Every organization is experiencing the explosion of data growth and needs to rethink the approach they manage and protect data.



With more than 300 million people working remotely all over the world and collaborating across multiple environments and devices, **data security incidents can happen anytime anywhere**. There are three primary scenarios for data security incidents: 1) If your organization doesn't have visibility into it's data – the data is at risk of misuse (exfiltration, exposure, etc.). 2) If a user has malicious intent and is trying to exfiltrate the data and 3) If a user inadvertently takes a sensitive document and makes it visible.



To help address the data security challenges, organizations need to implement multiple controls, including preventing data from unauthorized use across workloads, protect sensitive data wherever it lives throughout its lifecycle, and understand user activity context around the data. You need to do all three to fortify your data security strategy, and Microsoft can help.

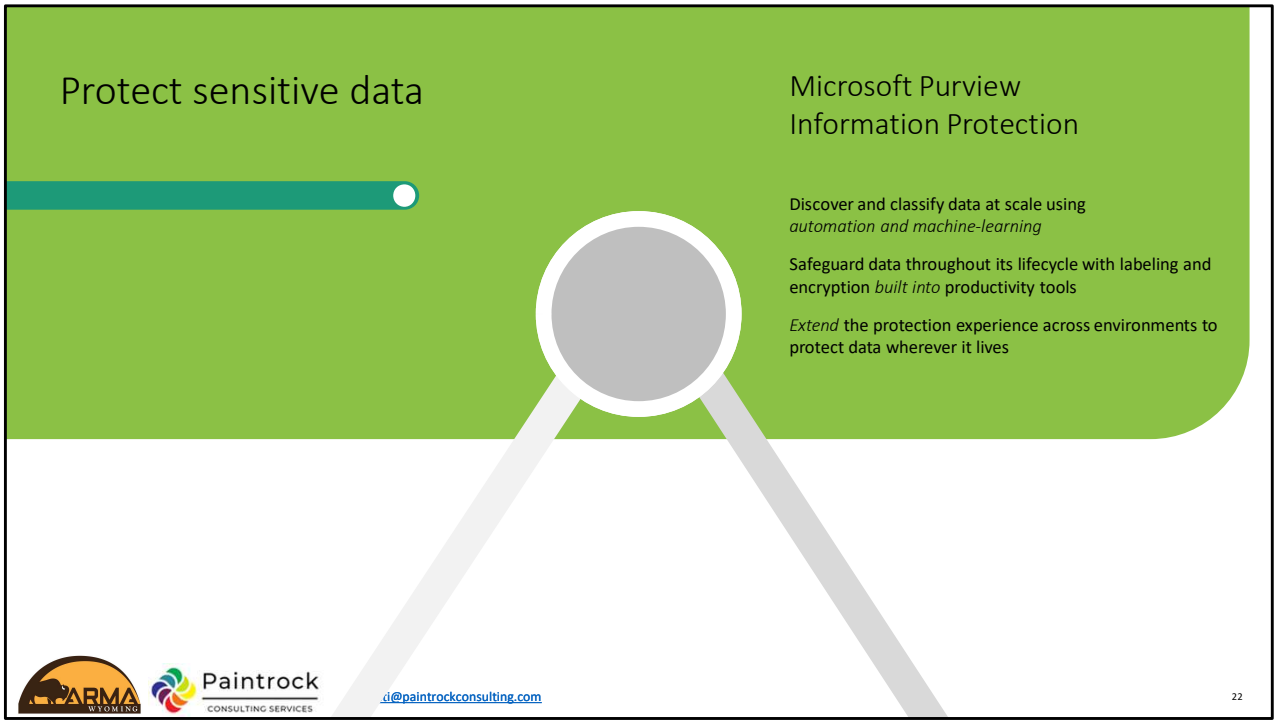


As organizations think about protecting their most important asset, their data, they ultimately need to create a defense in depth approach around it. There are three components to this strategy, but it is important to keep in mind that you don't need to do these in any particular order. This strategy should be tailored to your own organization's unique needs.

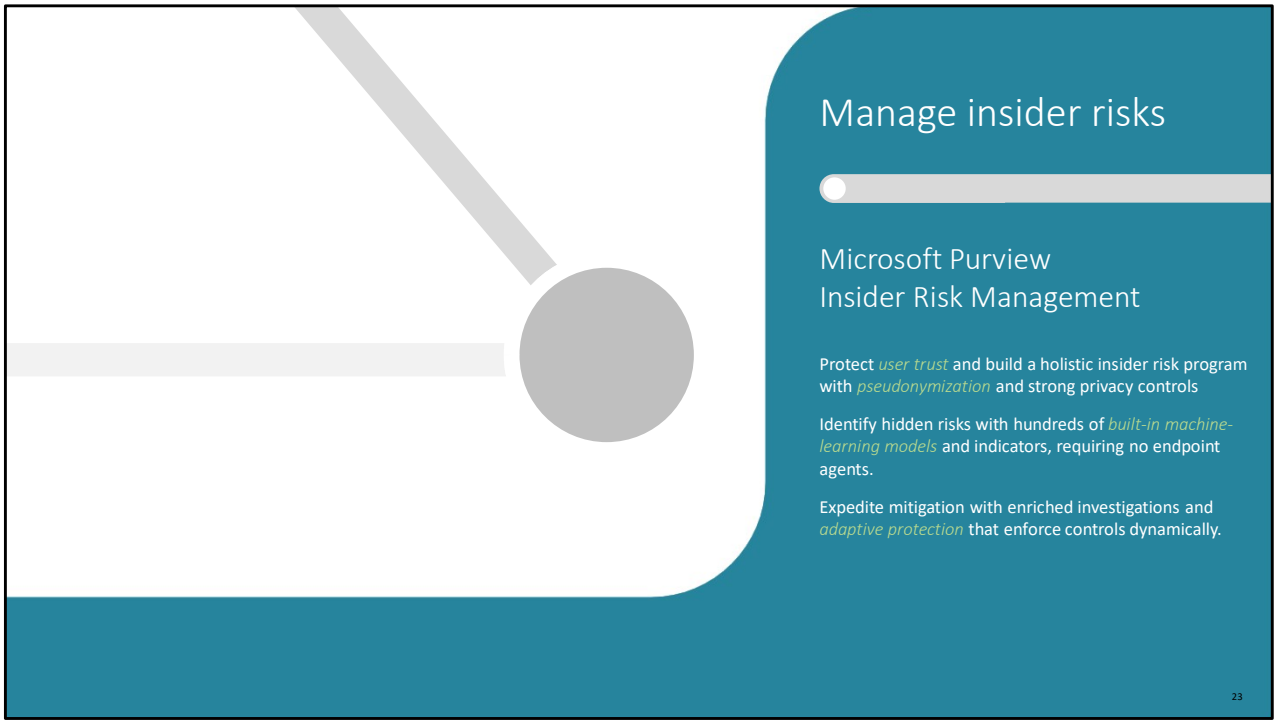
- Let's start with protecting sensitive data. It is important to understand and discover sensitive data within your organization. You need solutions that provide unparalleled visibility into your entire data estate, whether on-prem, hybrid, or multicloud. Microsoft Purview offers a single pane of glass which enables you to view and manage your data from one place, improving your team's efficacy for data security. You can see the volume, type, and location of sensitive information in your data estate. Discovering the data is beneficial when you can put protection policies in place to keep that data safe. To protect you at this line of defense, we offer solutions to help you classify and label your data and apply productions such as RMS, encryption and more.
- Data doesn't move itself; people move data. With all data in organizations, you need to understand the user context and intent around the data to effectively protect it with the right policy. This next layer of defense takes into account user context to identify potential data risks and/or risky activities that may lead to data security incidents, enabling security teams to quickly take mitigating action. Since data loss is usually caused by internal actors, organizations need to take a holistic approach to managing insider risk, which brings together the right people, processes, training and tools.
- The last layer of defense in this integrated in-depth approach is to prevent data loss or unauthorized use of data. Over 85% of organizations do not feel confident they can detect and prevent loss of sensitive data. Organizations need a way to balance protection and productivity, without compromising either. It's critical to ensure the proper access controls are in place and policies are set to prevent actions like improperly saving, storing, or printing sensitive data.

And of course, underlying everything here, is a strong ecosystem of partners, third party apps/platforms and clouds, as we know your data isn't just within the Microsoft

environments. Our aim is to make sure these layers are put in place to protect your data, no matter where it is.



Let's start with protecting sensitive data. Microsoft Purview Information Protection provides automation and machine-learning to help discover and classify data at scale, so you can know the volume, type, and location of sensitive information in your data estate in a single pane of glass. To protect your data at this line of defense, the solution also helps safeguard data throughout its lifecycle with persistent labeling and encryption built into productivity tools. Lastly, as we want to help you protect data in this modern workplace where users work from multiple environments, the visibility and protection of sensitive information are extended across your entire data estate, whether on-prem, hybrid, or cloud.



Data doesn't move itself; people move data. With all the sensitive data in your organization, you need to understand the user context and intent around the data to effectively protect it with the right policy. This next layer of defense takes into account user context to identify potential data risks and/or risky activities that may lead to data security incidents, enabling security teams to quickly take mitigating action.

Microsoft Purview Insider Risk Management is a privacy-first solution that help you manage insider risks while protecting user trust with pseudonymization on by default and other strong privacy controls including RBAC, explicit user opt-in, and audit logs.

With hundreds of built-in machine learning models and indicators, Insider Risk Management can help you correlate signals from various first- and third-party systems to identify hidden risks. One of the powerful models here is sequence detection. Most of the time, one single event, such as copying files to a USB, might not indicate good or bad intention. But if a user renamed the files to make it appear less sensitive prior to copy it to a USB, and then delete the files afterwards, that might show a user intent to evade detection of data exfiltration. With Insider Risk Management, security teams can detect this type of connected activities. This is just one example of the powerful ML models the solution provides. Along with other built-in ML models, Insider Risk Management helps identify the most critical risks for security teams to investigate. Best of all is that it requires no agents!

Lastly, Insider Risk Management provides enriched and interactive investigation tools to help security teams dive deeper into each alert or case. With the right permissions, admins can see the activity logs plotted on a risk score and timeline chart, see the content related to each activity in their native views, and get forensic evidence that help gain visual insights into user activities that may lead to security incidents. Insider Risk Management also enables Adaptive Protection that can enforce effective controls on high-risk users dynamically to contain insider incidents early on.



Equally important in to ensure that your egress channels such as applications, services, and devices prevent sensitive data from exfiltration and unauthorized use. Over 85% of organizations do not feel confident they can detect and prevent loss of sensitive data. Organizations need a way to balance protection and productivity, without compromising either. It's critical to ensure the proper access controls are in place and policies are set to prevent actions like improperly saving, storing, or printing sensitive data.

Microsoft's DLP solution is a **comprehensive solution** that works across different environments and services where sensitive data is stored, used or shared, including platforms native to Microsoft – as well as and non-Microsoft services and apps. Microsoft's DLP solution helps organizations consolidate the several individual solutions and save costs.

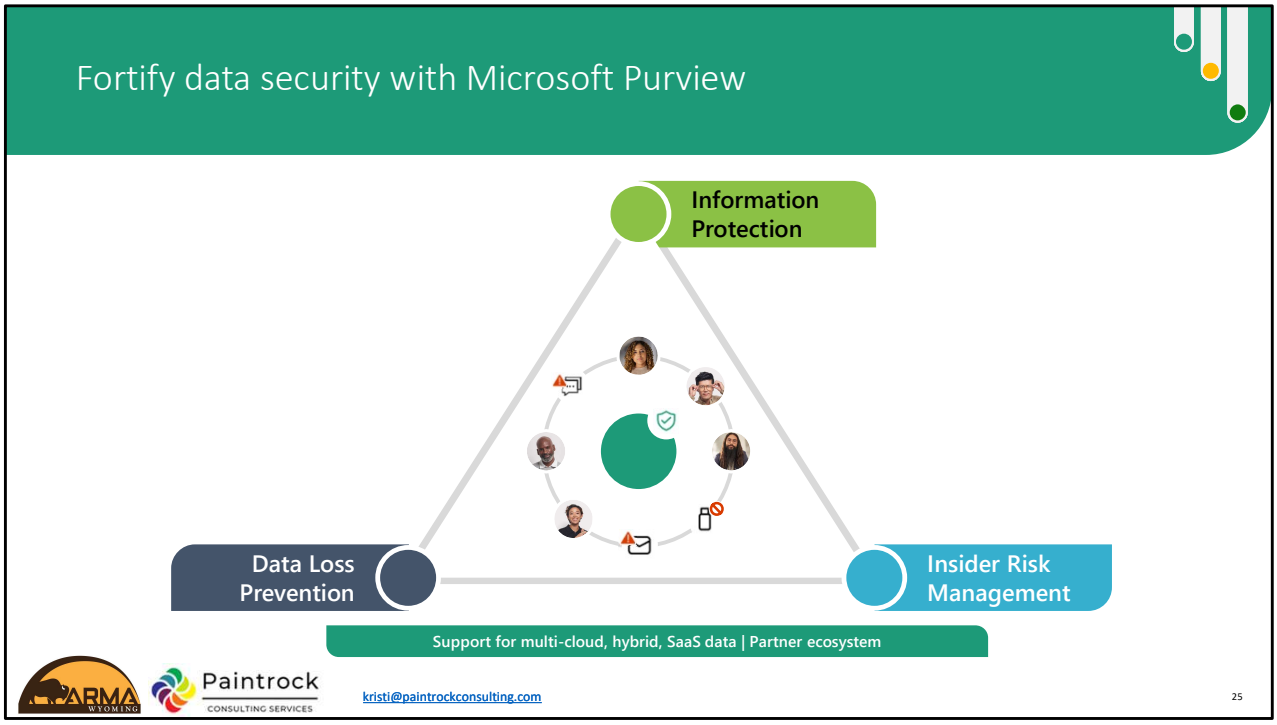
Microsoft Purview DLP is:

- **Cloud native,** which means that there is no need to deploy and maintain any on-premises infrastructure. Microsoft Purview DLP has protection built-in to Microsoft 365 cloud services such as Exchange Online, SharePoint Online, OneDrive for Business, and Teams, Office apps, and on endpoint devices with Windows and Microsoft Edge. DLP controls can also be extended to macOS endpoints and Chrome and Firefox browser, and various cloud apps such as Dropbox, Box, Google Drive, and others through the integration with Microsoft Defender for Cloud Apps.

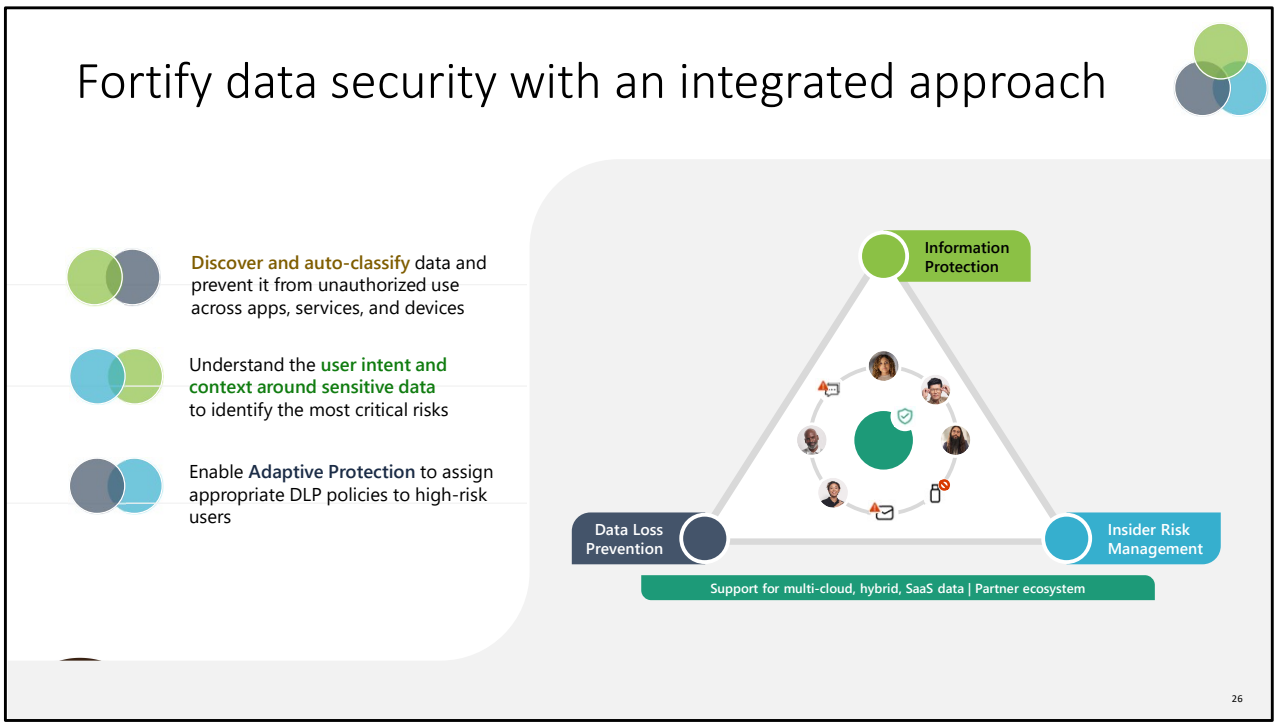
- **Unified,** as it allows you to create, deploy, manage your DLP policies across all workloads from a single location in Microsoft Purview compliance portal. You can balance protection and productivity by leveraging granular policies policy controls and restrict certain actions in specific situations while allowing others. Ex – you can allow printing on corporate printers and block it on personally owned printers.

- **Integrated,** because Microsoft's DLP solution is built from a common framework, DLP policies are consistently applied to all environments. Because DLP leverages Microsoft Purview Information Protection, you can use the built-in policy templates and classifiers to create and define DLP policies quickly. You can also make your DLP policies dynamic by leveraging the security risks levels of your users from Insider Risk

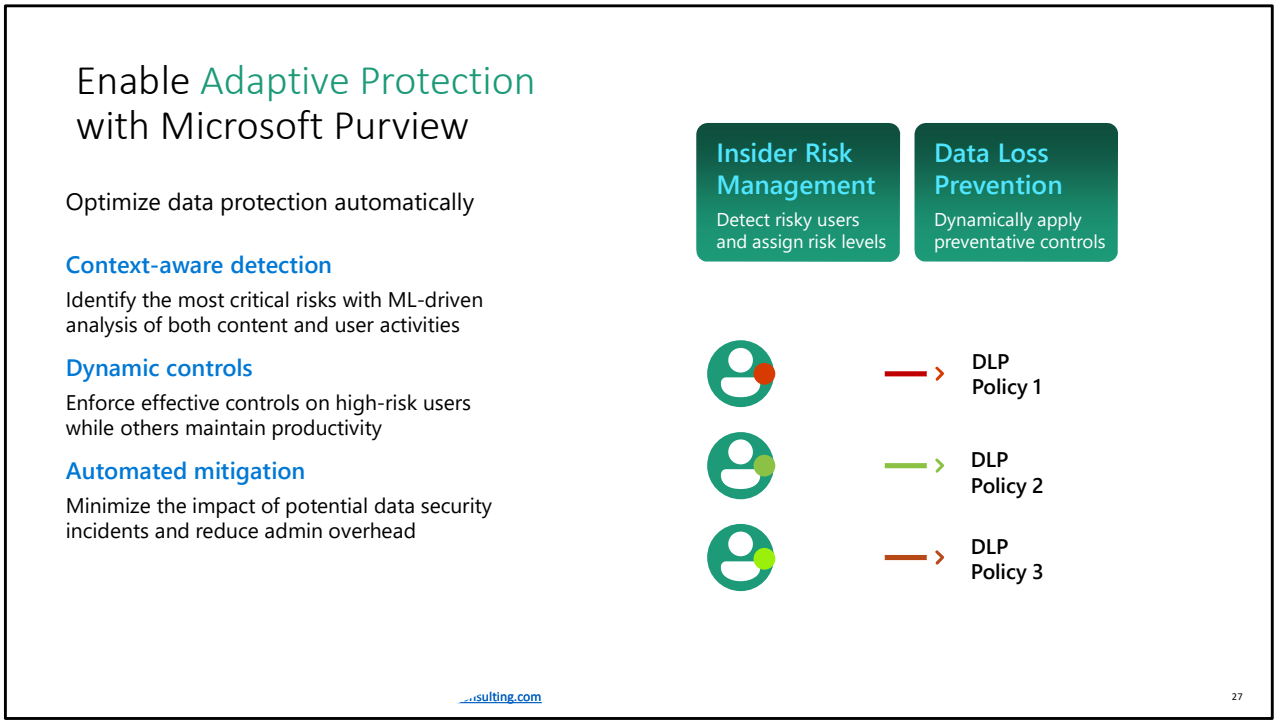
Management and automatically adjusting the strength of protection.



Microsoft Purview offers Information Protection, Insider Risk Management, and Data Loss Prevention on one unified platform that helps organization fortify data security effectively, so you can develop a defense-in-depth approach when it comes to protecting your sensitive data.



You need all three defenses of protection to effectively secure data from potential data security incidents and they work better together with reinforced synergy across the platform. For example, if you use Information Protection and Data Loss Prevention together, you are able to discover and auto-classify the data and prevent it from unauthorized use. Using Information Protection and Insider Risk Management together, you can understand the user intent around sensitive data to identify the most critical data risks in your organization. Another example is if you use Insider Risk Management and Data Loss Prevention, then you can enable Adaptive Protection which assign appropriate DLP policies based on user's risk levels. We will explain more about Adaptive Protection in the next slide. If you use all three products, then you can fortify your data security with a defense-in-depth approach.



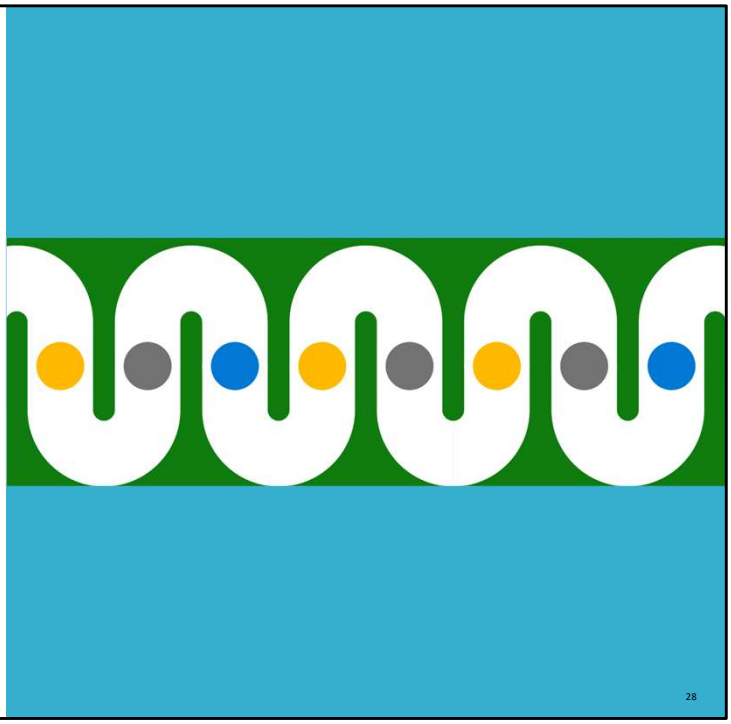
In the past, admins might receive many alerts when files containing sensitive information were shared, transferred, copied, or printed. It could be overwhelming or resources-draining to triage and address all the alerts while there is limited support to prioritize them. With Adaptive Protection, admins can continuously detect the most critical risks with ML-driven analysis on both content and users, identifying sensitive data in motion performed by risky users, such as an employee who just submitted a resignation. Remember, data doesn't move itself; people move data. By understanding the risk indicators of the user interacting with the data, admins can get more context-aware detection and reduce the overhead of reviewing an overwhelming number of alerts.

When you treat users with a static data protection policy, most of the time, the control would either be too loose that it didn't help remediate data loss risks or too strict about blocking users from working productively. Adaptive Protection can change that by automatically adjusting the right level of remediation controls based on the risks detected, so high-risk users would be scoped in a stricter control while low-risk users can work as usual. And it's constantly adjusting, so the control could be dialed up or down when the users' intent or behaviors change. The more precise remediation enables effective control enforcement while maintaining productivity.

Instead of treating risks separately in various solutions, Adaptive Protection brings signals and controls together across solutions. Here, you see how the risk indicators from Insider Risk Management and the data classification insights in DLP can help build a 1+1 > 3 protection. Organizations can take a defense-in-depth approach to prevent data loss, investigate insider risks, and leverage the integration between IRM and DLP to apply the right level of controls while maintaining productivity.

Improve risk and compliance posture

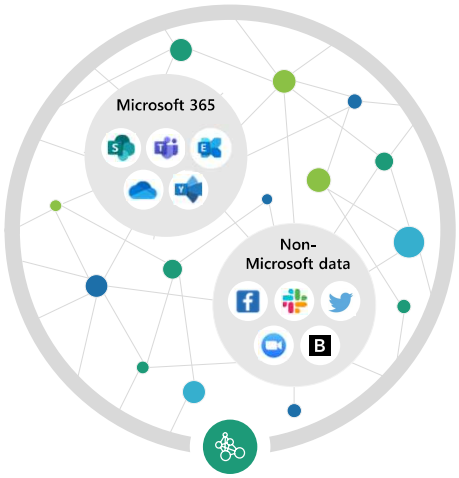
Identify data risks and manage regulatory compliance requirements



kristi@paintrockconsulting.com

Microsoft Purview Data Lifecycle Management

Classify and govern data at scale



- Retain or delete data and manage records where users collaborate to manage risk and prevent productivity loss
- Demonstrate compliance with label analytics insights, defensible disposal, and rich audit trails
- Manage non-Microsoft data import with pre-built data connectors*
- This is where Records Management features live

Powered by an intelligent platform

ARMA WYOMING Paintrock CONSULTING SERVICES

kristi@paintrockconsulting.com

*Pre-built data connectors include connectors built by Microsoft and by partners – Veritas, Telemessage, CellTrust and 17a-4 LLC. Except for Veritas, Telemessage, CellTrust and 17a-4 LLC, Microsoft does not have direct relationships with the data source companies in bringing these data connectors to the platform.

29

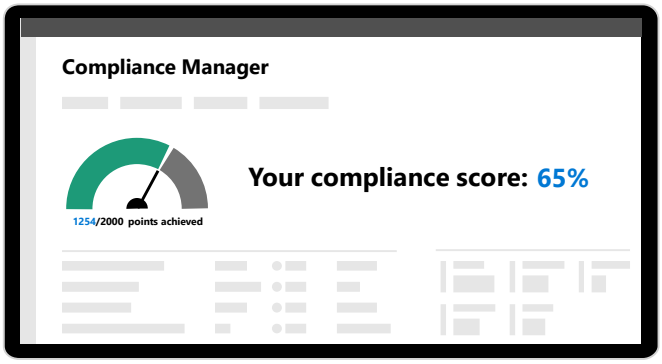
You can now put retention and deletion policies in place to help you manage information lifecycle and meet recordkeeping obligations for data in Microsoft 365 and beyond. Microsoft Information Governance helps classify and govern data at scale with the following capabilities:

- **In-place management:** On average, organizations are wrestling with five different content systems and repositories. Duplicate information across platforms not only causes productivity loss but also increases risks. In-place management enables companies to retain information and manage records where data is created to prevent productivity loss and reduce operational and legal risks.
- **Automated policy:** The volume of information is expected to grow 4.5 times over the next two years. Relying on manual classification is ineffective since users usually care the most about the value of the information, less about the risks it generates. It's challenging to hold them accountable to classify and manage information accurately. By automating information governance, companies can leverage various auto-classification capabilities such as file properties (e.g., Content Type defined in SPO), pattern recognition, and machine-learning classifiers to classify and govern data at scale.
- **Defensible process:** Multiple regulations, such as SEC 17a-4 and FINRA, require companies to meet stringent information governance requirements like record immutability. Companies also need to demonstrate compliance by proving they follow a defensible process to dispose of content. Microsoft 365 provides transparent insights on how data is classified to help you audit and finetune classification and policies. Moreover, the records management capabilities within Microsoft Information Governance can help companies follow a defensible process to retain and dispose of information with proof of disposals that can be kept for 7 years, disposition reviews, and rich audit trails.
- **Pre-built data connectors:** To help companies leverage the capabilities above to govern data beyond Microsoft cloud, we provide pre-built data connectors for social media, text messages, chats, and collaboration data. Microsoft not only builds its own connectors but also works with hand-picked partners like TeleMessage and Globanet to enable ongoing and high-fidelity data import. In addition to the pre-built ones, customers and partners can build their own custom connectors to continuously ingest data into Microsoft 365.
- You can leverage these four key capabilities to govern both the general and high-value information across various data sources:
  - General information governance: Retain only what you need and delete what you don't to reduce risks and liability.
  - High-value information management: Classify, retain, review, dispose, and manage records to meet recordkeeping obligations.

Microsoft Purview Compliance Manager

Intuitive end-to-end compliance management

- Manage end-to-end compliance from easy onboarding to control implementation
- Configure out of the box assessments to meet your requirements across all assets
- Simplify compliance with continuous assessments, automated control mapping, and a compliance score



kristi@paintrockconsulting.com

With Microsoft Purview Compliance Manager, you can now continuously assess and monitor data protection controls, get clear guidance on how to improve your score and thus reduce compliance risks, and leverage the built-in control mapping to scale your compliance effort across global, industrial, and regional standards.

- **Intuitive management:** The complexity of regulations makes it challenging for organizations and IT administrators to know specific actions they can take to meet their compliance requirements. Compliance Manager provides easy, guided onboarding and supports twenty four languages. With simple design that works out of box, IT admins and Compliance / Audit Officers can quickly collaborate to address compliance. With Compliance Manager, you don't need to be an expert in complex regulations like the General Data Protection Regulation (GDPR) to know the actions you can take to improve compliance effectiveness. Compliance Manager now combines the functionality of compliance score and the existing Compliance Manager solutions, making it a single portal for end-to-end compliance management.
- **Scalable assessments:** Compliance Manager provides access to a vast library of 150+ assessment templates – from global regulations such as the GDPR, PCI-DSS, COBIT 5, to regional assessments such as Brazil's LGPD data protection law and Malaysia's Personnel Data Protection Act. Industry-specific assessments such as HITRUST and Cybersecurity Maturity Model Certification (CMMC) are also covered. Compliance Manager now provides the ability to quickly customize these assessments to meet your unique business requirements. With the custom assessments feature, you can manage compliance across your assets in one location by bringing your own assessments into Compliance Manager. For example, if you are currently tracking compliance of your SAP data in an Excel file, you can bring that into Compliance Manager.
- **Built-in automation:** Compliance management can be tedious, and organizations often find it difficult to know their degree of compliance with specific regulations. Translating ever-changing regulatory requirements into specific actions and controls is also challenging and not all organizations have the resources to do this accurately. Point-in-time assessments (e.g., for quarterly/semi-annual/annual audits) also mean that organizations tend to have 'blind spots' between these assessment windows. To help you with these challenges, Compliance Manager comes built-in with the following capabilities: **compliance score, control mapping, continuous regulatory updates, and continuous assessments**

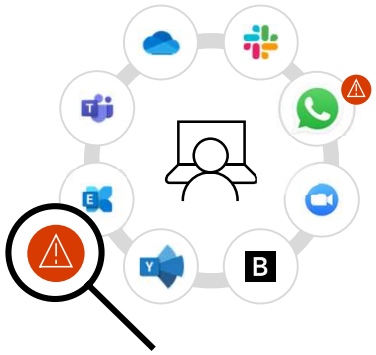
Microsoft Purview Compliance Manager measures your progress towards completing recommended

actions that help reduce risks around data protection and regulatory standards.

Microsoft Purview Communication Compliance

Quickly identify and act on code-of-conduct policy violations

- Intelligent customizable playbooks detect violations across Teams, Exchange, and third-party content
- Flexible remediation workflows enable quick action on violations, like remove incriminating messages on Teams
- Identify and investigate communications risks while maintaining end-user privacy



ARMA WYOMING Paintrock CONSULTING SERVICES kristi@paintrockconsulting.com 31

1. Intelligent Customizable playbooks:
   There are four pre-configured templates within Communication Compliance: regulatory compliance, offensive language, sensitive information types, conflicts of interest.
   - These are available across first- and third-party content, in 8 languages, with the ability to customize policies.
   - ML models continue to learn with trainable classifiers including gory, racy, adult images, harassment, discrimination, threats, profanity.

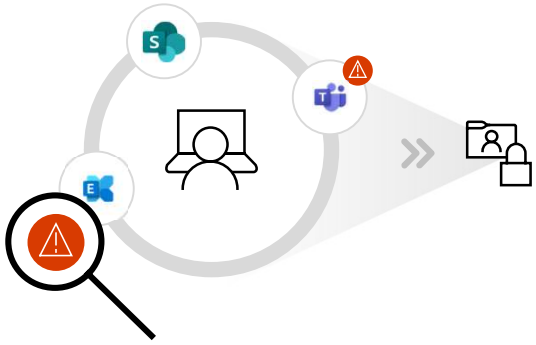
2. Remediation workflows:
   - Collaborative and easy-to-navigate
   - Identify risk communication with keyword highlighting and prioritization through past user behavior
   - Ability to send notification to employee, escalate the case for investigation, remove message from Teams channels
   - Able to provide feedback to improve the model

3. Privacy built in:
   - Rules-based access controls
   - Admin opt in of users/reviews
   - Pseudonymization and audit trails to scan behavior

Microsoft Purview eDiscovery

Discover, preserve, collect, process, cull, and analyze your data in place

- Preserve content by custodian, send hold notifications, and track acknowledgements
- Review and manage static sets of documents within a case, that can be independently searched, analyzed, shared, and acted upon
- Near duplicate detection, email threading, themes, and ML models to identify potential high value content and make the review process more efficient



ARMA WYOMING Paintrock CONSULTING SERVICES kristi@paintrockconsulting.com 32

Microsoft built whole new stack –from ground up.

1. Custodian Management
   It's looking to simplify the process. For example, a typical case requires hunting down mailbox addresses and SharePoint urls in order to use scripts to find out the addresses, *plus* give the export of the scripts. Now, with eDiscovery, you have the ability to just tell us who has been escalated. Our solution then goes in the background and maps the content for you – these are the sources in play that you can hold to get started on a case.

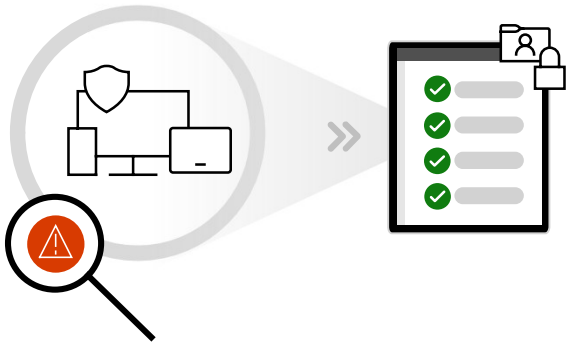
2. Review
   Before a user exports, we wanted to provide a view of the content in review. These review tools help with analytics for culling decisions (to show related content), near duplicate detection, email threading, and redaction of content.

3. Deep Indexing
   Microsoft is using a search that is tuned for performance – finding the most relevant content quickly becomes critical. Because we tune it for speed, we give it rules to look for specific items (and skip specific items that may take too long). For example, if you put a file with too many attachments, this would be skipped to optimize for speed. In our new stack, we will look at that content before we search. For example, if Jane is the custodian, looking at her content will pick up any partially and unindexed content. Jane then has the ability to index that content, so that when she searches for something specific, she is able to access primary and secondary indexes.

Microsoft Purview Audit

Power your forensic and compliance investigations

- Tap into additional events that are important for forensic investigations (e.g. mail items accessed, mail send, user search)
- Preserve audit logs for up to a year, with option for 10-year retention add-on
- High bandwidth access to data with ~2x the baseline

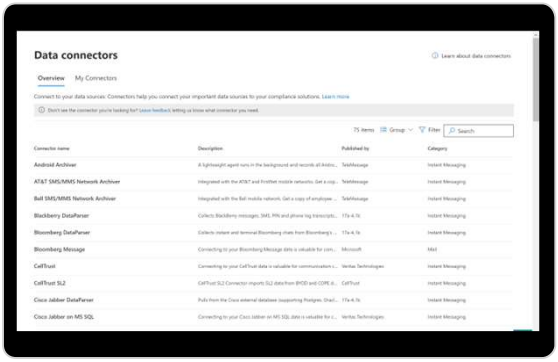


kristi@paintrockconsulting.com

- There are 3 key capabilities we offer customers in Audit to help with their regulatory, legal and compliance obligations.
  - The first are additional audit events that help with forensic investigations. Earlier this year we delivered new events that helps investigators understand if mail items were accessed through the mail sync and mail bind operation. This is extremely helpful to organizations with regulatory obligations that require breach notifications, because now they can scope mail items that may have been compromised to reduce fines and penalties.
  - Another key area is around retaining audit logs. According to the latest Ponemon research, it takes roughly 6 months to detect a data breach and organizations need a way to go back to the audit logs to conduct forensic investigations. Advanced Audit extends audit log retention from 90 days to 6 months. And new to Audit – optionally add 10-year retention for highly regulatory customers that need to keep audit log data for longer.
  - And lastly, for those using activity API, Audit provides 2 times the bandwidth compared to other customers – which is valuable especially if customers are using audit data in 3rd party solutions.

Microsoft Purview Data Connectors

Ingest non-Microsoft data and benefit from Microsoft Purview solutions



- One catalog for all connectors built by Microsoft and partners (TeleMessage,Veritas,17a-4,CellTrust) in one place
- Simplified deployment and monitoring with few clicks to setup data import for most connectors*
- Hi-fidelity data ingestion available for Purview solutions
- 73 built-in connectors including Bloomberg Message, Slack eDiscovery, Zoom Meetings, Webex, Twitter etc.

kristi@paintrockconsulting.com

*Pre-built data connectors include connectors built by Microsoft and by partners – Veritas, Telemessage, CellTrust and 17a-4 LLC. Except for Veritas, Telemessage, CellTrust and 17a-4 LLC, Microsoft does not have direct relationships with the data source companies in bringing these data connectors to the platform.

Microsoft Purview ecosystem

Extend, integrate and automate compliance solutions beyond Microsoft 365



- High fidelity multi-cloud data ingestion from 70+ sources, benefitting from multiple Microsoft Purview solutions
- In-place multi-cloud data classification covering 35+ sources
- APIs to integrate and automate Microsoft Purview solutions with existing applications and services (e.g. McAfee, Netskope, Relativity)
- Identify and protect sensitive information that is unique to your organizations using ML and built-in customizations
- Built-in workflow automation with Power Automate

kristi@paintrockconsulting.com

The value of Microsoft Purview is that it can be extended to third-parties

- Customers can access their data using APIs
- Partners can use APIs to integrate solutions
- Service providers to manage at scale

Questions?

I would greatly appreciate your feedback! Please scan this code to submit an anonymous feedback survey.



Thank You

kristi@paintrockconsulting.com



Why I Focus on Microsoft Purview

Experience-based perspective

In my experience as an Information Governance Professional across multiple industry verticals, I have yet to see a successful implementation of Google Workspace Vault since its inception.

Yes, it does have a simple, clean interface, because all it really does is manage minimal retention and disposition. It is ineffective for organizations or enterprises that have more than 20 people, are responsible for managing records (not just simple retention), have regulatory compliance responsibilities, privacy requirements, or have geographically diverse people and data. ~ my $0.02

Addendum

Feature Comparison	Google Workspace Vault	Microsoft Purview
Information Lifecycle Management (Retention, Disposition)	✓	✓
eDiscovery	✓	✓
Information Protection (Role-based access controls)	*	✓
Data Lifecycle Management	*	✓
Records Management	*	✓
Insider Risk Management	*	✓
Communication Compliance	*	✓
Compliance Manager	*	✓
Unified Data Governance	*	✓
Data Map, Catalog	*	✓
3rd party platform integration	*	✓
Integration with Google Big Query	n/a	✓

ARMA WYOMING
Paintrock CONSULTING SERVICES
kristi@paintrockconsulting.com