



MIP and Power BI Compliance and Protection for Sensitive Business Data

Anton Fritz – Principal Program Manager, Power BI

Igor Bekerman – Program Manager, MIP, Customer Acceleration Team

Pandemic | Online work | Security



Online collaboration



145M

Daily active users in
Microsoft Teams, 4x vs
before pandemic



Security staff



82%

Of business leaders plan
on adding security staff



Costs



81%

Of business leaders feel
pressure to reduce
security costs

Data Breaches Since Covid-19

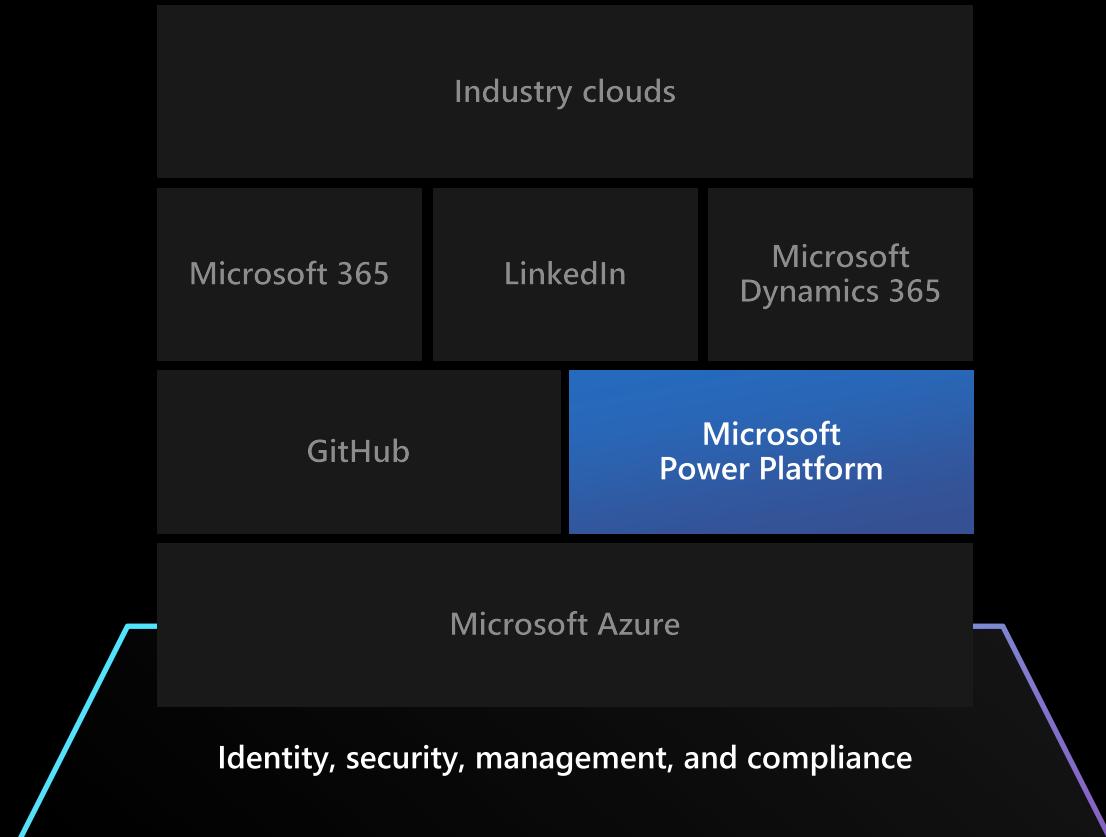
News events, criminal activity, and Microsoft's response



Benefits of MIP + Power BI

- Meet compliance requirements for sensitivity data in the cloud
- Centralized policies management and monitoring
- End-To-End protection as data travels across systems
- Don't compromise on productivity
- Reduced COGs

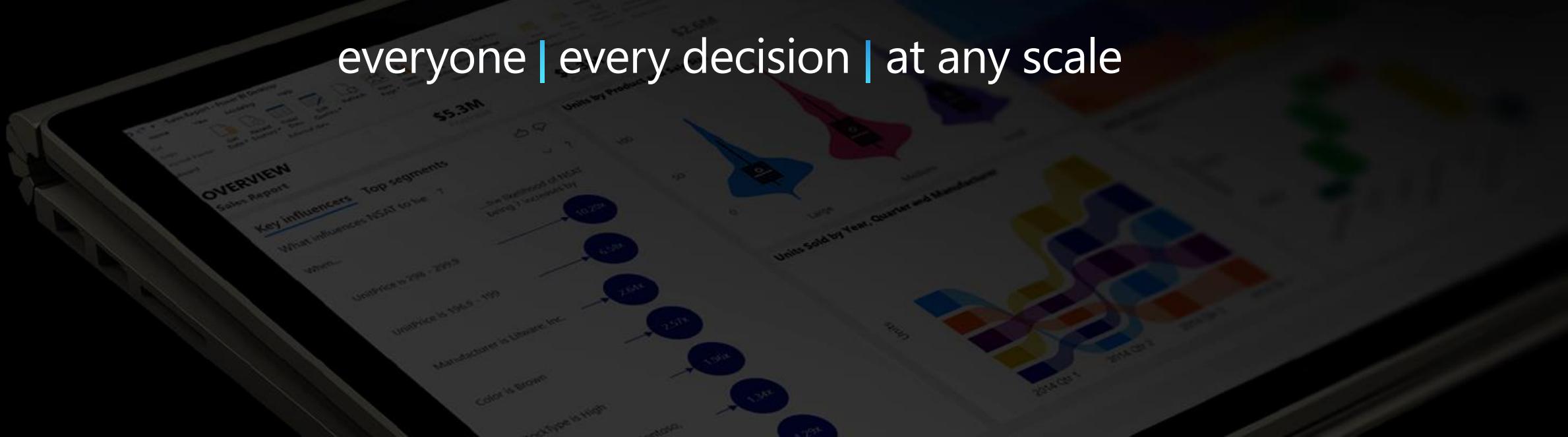
Microsoft cloud





Drive a data culture

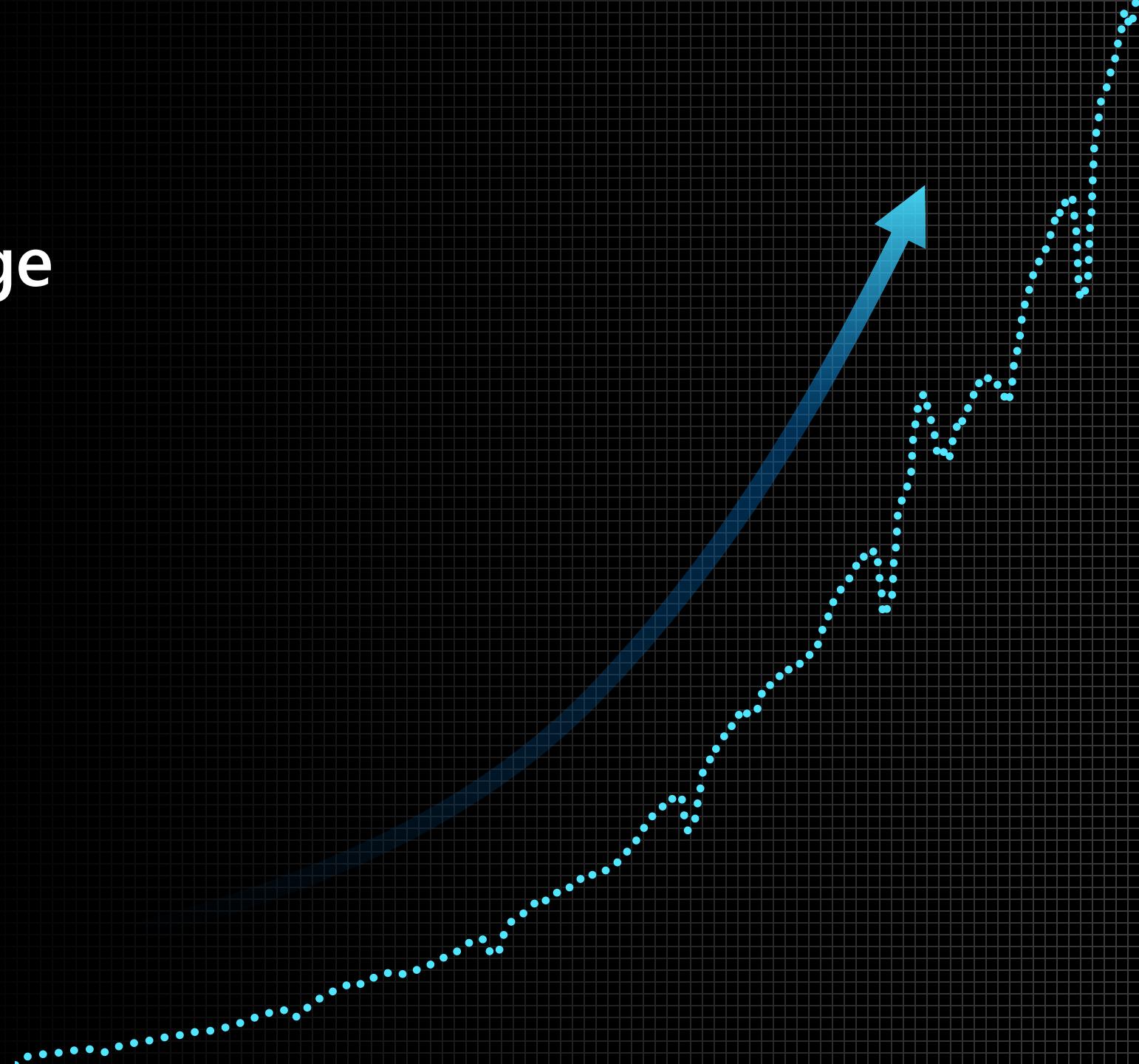
everyone | every decision | at any scale



Power BI monthly active usage

6 years
of rapid growth

260k+
Organizations



Industry Leadership

Gartner®

Figure 1: Magic Quadrant for Analytics and Business Intelligence Platforms



Source: Gartner (February 2021)

FORRESTER®

FORRESTER® RESEARCH

THE FORRESTER WAVE™

Enterprise BI Platforms (Vendor-Managed)

Q3 2019



Why the world's largest organizations are standardizing on Power BI



Leading BI
capabilities



Fully governed
& trusted



Best
economics

Why the world's largest organizations are standardizing on Power BI



**Leading BI
capabilities**



PowerPoint for data

The screenshot shows the Power BI Desktop interface with the title "Game Analysis - Power BI Desktop". The ribbon menu includes File, Home, Insert, Modeling, View, Help, External Tools, Format, and Data / Drill. The Home tab is selected, showing options like Cut, Copy, Paste, Format painter, Get data, Power BI Server, Enter data, Dataverse, Recent sources, Transform Refresh data, New visual, Text box, More visuals, New measure, Quick measure, Sensitivity (preview), Publish, Insert, Calculations, Sensitivity, and Share.

The main workspace displays two visualizations:

- Number of games by publisher:** A donut chart showing the distribution of games by publisher. The data is as follows:

Publisher	Count	Percentage
_publisher1	619	(18.21%)
_publisher2	809	(23.79%)
_publisher3	627	(18.44%)
_publisher4	700	(20.59%)
_publisher5	645	(18.97%)
- Sentiment by platform:** A bar chart showing sentiment scores for different platforms. The data is as follows:

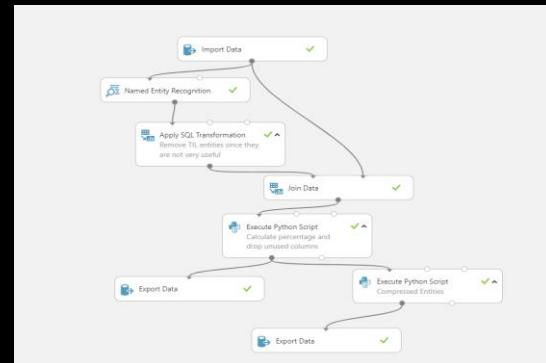
Platform	Sentiment Score
PS2	0.63
DS	0.63
Wii	0.61
PS3	0.56
X360	0.56

On the right side, there is a Q&A panel titled "Ask a question with Q&A" with a text input field and suggestions like "top genres by #games" and "top rating by #games". The bottom navigation bar includes tabs for "Q&A Demo", "Decomp Tree", "Decomp Tree Analysis", "Page 1", and a plus sign icon. The status bar at the bottom left shows "Page 1 of 4".

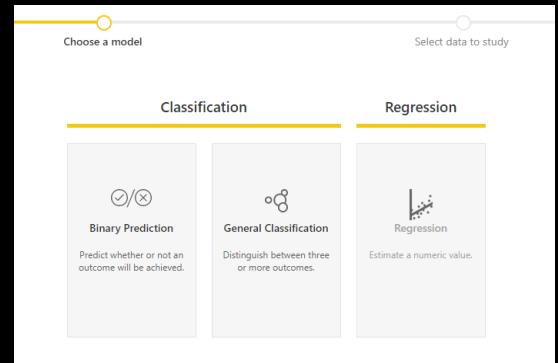


The most complete AI capabilities in a BI product

Extend with Azure ML



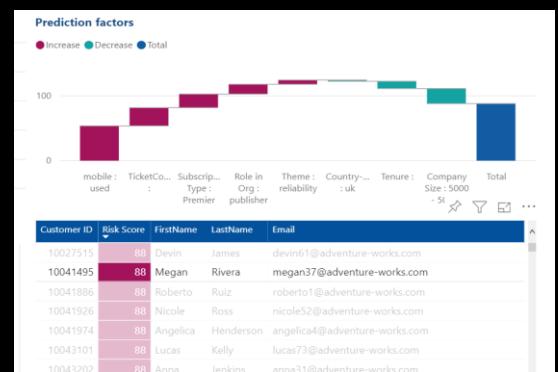
Create ML models



Python & R Integration



Explore Predictions





Power BI + Teams

Your data is where you collaborate

As fundamental as "chat", "calendar" and "files"

The screenshot shows a Microsoft Teams interface with a Power BI dashboard titled "Sales Pipeline" embedded in a "Pages" tab. The dashboard includes the following components:

- EXECUTIVE KPIs:** Revenue (\$3,978,178, +18%), Deals (35,870, +23%), Opportunity Value (\$906,069, +06%).
- Revenue and Pipeline:** A bar chart showing Actual Revenue (dark blue bars) and Opportunity Value (light blue bars) from Jan 2018 to Sep 2019.
- Open Opportunities:** A table listing opportunities with columns: Opportunity Name, Account Name, Owner, Estimated Close Date, Close Probability.
- Pipeline Gap by Account:** A bubble chart showing Current Relationship Strength (Y-axis, 40% to 100%) versus Opportunity Value (X-axis, 0K to 1500K). Accounts like Mundopolis, Venasor, and Contoso are highlighted.
- Filters:** On the right side, there are filters for Account, City, Current Relationship Status, Opportunity Value, Risk Status, and Sum of Risk.

Why the world's largest organizations are standardizing on Power BI



Fully governed
& trusted



Power BI security strategy

Cloud & remote work

Data residency

Certifications

Network security

Data encryption

Data loss prevention



Power BI security strategy

Cloud & remote work



Data residency

Large global footprint,
offering storage in 54
data centers WW

Multi-geo capacities



Certifications

119 local and
international
compliance standards

34 local and
international industry
certifications



Network security

Service tags
Private links

VNet
TLS 1.2 enforcement



Data encryption

BYOK encryption via
Azure Key Vault
Double encryption
at rest



Data loss prevention

Classify and protect
data with MIP

Monitor and protect
data with MCAS

Integrated security policy
management, audit and
compliance

Power BI tenant admin
governance - permissions,
settings, metrics



Power BI security strategy

Cloud & remote work



Data loss
prevention

Classify and protect
data with MIP

Integrated security policy
management, audit and
compliance



SharePoint



OneDrive



PowerBI



Teams



Office

MIP

Microsoft Information Protection is a built-in, intelligent, unified and extensible solution to protect sensitive data

It is a massive cross team effort



Azure



MCAS



Exchange



Windows



Edge

Microsoft Information Protection (MIP)

Key customer benefits



BUILT-IN

Built-in labeling and protection experience in Microsoft 365 apps, Microsoft 365 services, other MS services like Power BI, Edge and Windows



INTELLIGENT

Accuracy in classification via ML based trainable classifiers and exact data match



UNIFIED

Single admin console to configure and manage your policies and view analytics across on-premises, Microsoft 365 apps, Microsoft 365 services, 3rd party services and Windows devices



EXTENSIBLE

MIP platform extends the protection experience, in a consistent way, to popular non-Microsoft apps and services

The screenshot shows the Microsoft 365 Security & Compliance center. On the left, a navigation pane includes Home, Alerts, Permissions, Classifications (which is expanded), Labels (selected), Label policies, Sensitive info types, Data loss prevention, Data governance, and Threat management. On the right, the 'Sensitivity' tab of the Labels page is active, with a sub-header 'Labels'. Below this are sections for 'Label policies', 'Sensitive info types', and 'Data loss prevention'. A 'Create a label' button and search controls are at the top. To the right of the interface, a Microsoft Word document titled 'M&A Plan – "Shanghai"' is displayed. The document has a red 'Highly Confidential' watermark and contains text about an M&A proposal regarding the potential merger with a company codenamed 'Shanghai'. It also includes a note about being prepared by the M&A & Acquisitions sourcing department at Contoso, Colorado during Q2 2018.

Microsoft Information Protection is a **built-in, intelligent, unified** and **extensible** platform and solution to protect sensitive data.



MIP and Power BI

- **Classify Power BI content with MIP labels**
- **Label and protect files when data leaves Power BI (Excel, PowerPoint, PBIX and PDF).**

The screenshot shows the Microsoft Power BI service interface. The top navigation bar includes 'Power BI', the 'ContosoFinanceDepartment' workspace name, a search bar, and user profile icons. Below the navigation is a toolbar with icons for creating new content, pipelines, and various report types. The main area displays a list of five items under the 'All' tab:

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Business Units & Regions	Report	ContosoFinanceDepa...	4/21/21, 10:38:10 AM	—	Promoted	—	Yes
Company Metrics	Dataset	ContosoFinanceDepa...	4/21/21, 10:38:10 AM	N/A	Promoted	Confidential\Internal...	...
Executive Summary	Dashboard	ContosoFinanceDepa...	—	—	—	Highly Confidential\In...	Yes
Finance	Report	ContosoFinanceDepa...	4/21/21, 10:38:10 AM	—	Promoted	Highly Confidential\In...	Yes
HR Metrics	Report	ContosoFinanceDepa...	4/21/21, 10:38:10 AM	—	Promoted	Highly Confidential\In...	Yes



MIP in Power BI Desktop app

Label and protect PBIX files

The screenshot shows the Microsoft Power BI Desktop application interface. The ribbon at the top has the 'Home' tab selected. On the right side of the ribbon, there is a 'Sensitivity' dropdown menu that is open and highlighted with a red box. This menu lists several sensitivity levels: Non-business, Public, General, Confidential, Highly confidential, and More info. To the right of the sensitivity levels, there are options for 'Recipients only', 'Microsoft FTE', 'Microsoft extended', and 'Any user (no protection)'. Below the ribbon, the main workspace displays a report titled 'Contoso'. The report features a bar chart titled 'Top 10 Customers in Revenue' showing revenue for five companies: Proseware, Inc., Litware, Humongous Insurance, Wide World Importers, and Blue Yonder Airlines. A donut chart shows status distribution with 220M (78.67%) Won, 54M (19.2%) Open, and 11M (2.13%) Lost. A table titled 'Open Opportunity by' is also visible. The overall theme of the application is dark, with blue and white highlights.

Demo



Inherit labels when connect to Power BI data from Excel

Automatic Excel
Workbook labels

The screenshot shows a Microsoft Excel window titled 'Book2 - Excel'. The ribbon is visible at the top, with the 'Data' tab selected. In the 'Get Data' section of the ribbon, the 'From Power BI' option is highlighted. The main area of the Excel window is a blank sheet labeled 'Sheet1'. The status bar at the bottom indicates 'Ready' and 'Accessibility: Good to go'.



Inherit MIP label from data source

Securing the full data journey from Azure to Office

Coming soon

- Inherit MIP label from source Excel file
- Get data from protected Excel file

The screenshot shows the Microsoft Azure Purview Data Catalog interface. A specific asset, 'ip_address', is selected, which is described as 'Highly Confidential/Internal Only'. The asset details include its classification as 'IP Address' and 'Personal IP Address'. The properties listed include:

Property	Value
qualifiedName	mssql://ress
precision	0
length	20
encryptionType	0
columnEncryptionKeyId	0
description	
scale	0
isXmlDocument	false
isMasked	false
encryptionTypeDesc	
xmlCollectionId	0

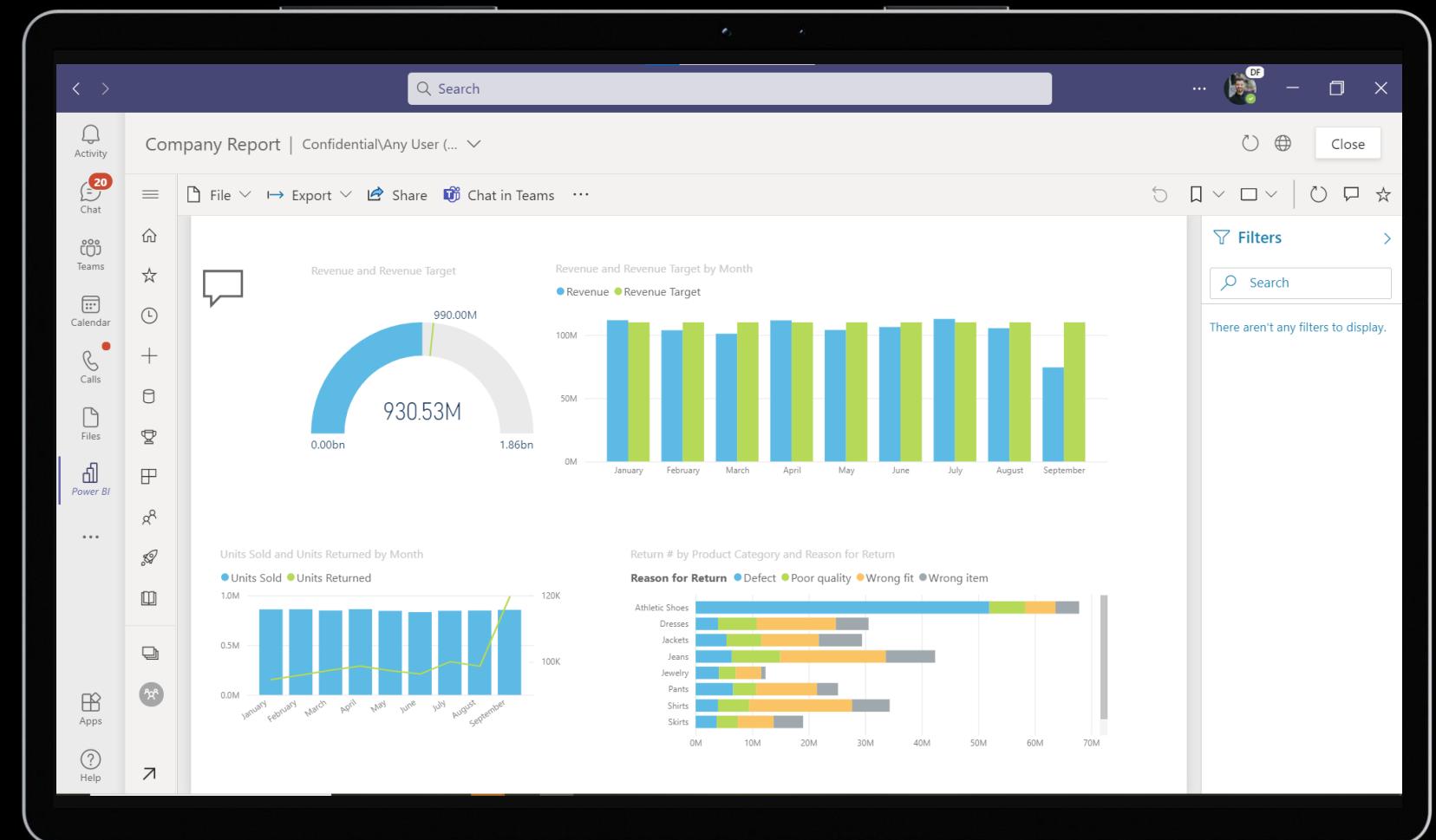


Demo



MIP Labels in Microsoft Teams

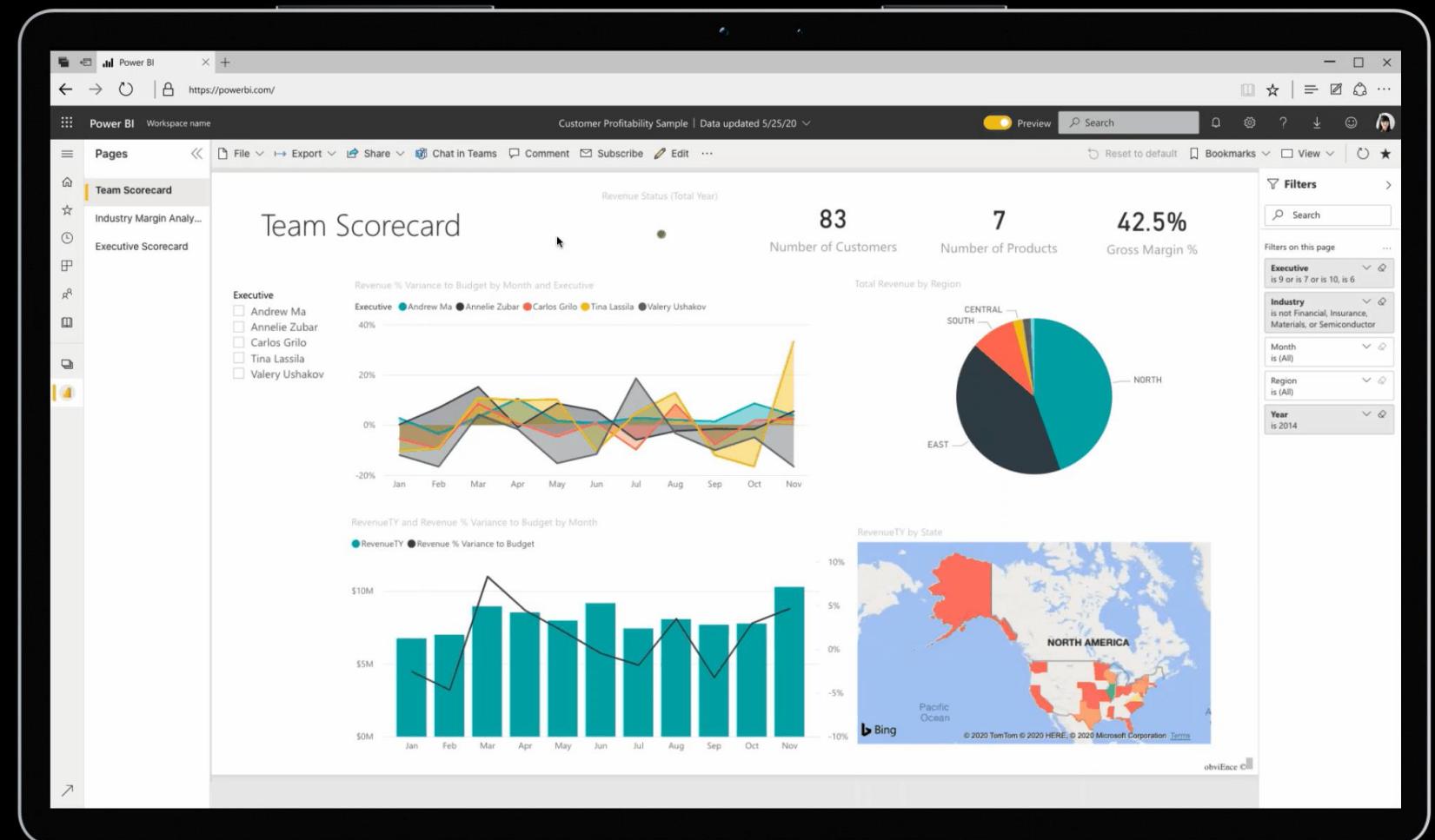
- Sensitivity labels visible in embedded views
- Protection persists when data is exported.





MIP label policies

- Mandatory label policy
- Default label policy -
Coming soon
- Admin APIs to
set/remove MIP labels





O365 audit logs

Every user and system event are captured by the standard enterprise audit log

Office 365 | Security & Compliance

Home > Audit log search

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search [Clear](#)

Activities: Accessed out-of-box entity, ... (9)

Date: 2018-07-16 00:00 - 2018-07-24 00:00

IP address: Unknown

User: Unknown

Activity: Accessed other entity type

Item: Get Organization

Detail: "AdminCenter" @ "https://..."

Start date: 2018-07-16 00:00

End date: 2018-07-24 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Results 150 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity	Item	Detail
2018-07-23 23:59:21	40.118.175.16:31760	Unknown	Accessed other entity type	Get Organization	"AdminCenter" @ "https://..."
2018-07-23 23:59:21	40.118.175.16:31760	Unknown	Accessed other entity type	Get Organization	"AdminCenter" @ "https://..."
2018-07-23 23:59:15	40.118.175.16:23425	Unknown	Accessed other entity type	Get Organization	"AdminCenter" @ "https://..."
2018-07-23 23:59:15	40.118.175.16:23425	Unknown	Accessed other entity type	Get Organization	"AdminCenter" @ "https://..."
2018-07-23 23:58:44	71.197.217.152:14473	BenW@BAPpartners.onmicrosoft.com	Accessed other entity type	Configure Organization	"AdminCenter" @ "https://..."
2018-07-23 23:58:42	104.42.186.44:1249	Unknown	Accessed other entity type	Post UpdateInstanceSetting	"AdminApi" @ "https://ad..."
2018-07-23 23:58:42	104.42.186.44:1249	Unknown	Accessed other entity type	Post RetrieveInstancesOperat	"AdminApi" @ "https://ad..."
2018-07-23 23:58:41	104.42.186.44:1249	Unknown	Accessed other entity type	Post RetrieveInstancesOperat	"AdminApi" @ "https://ad..."
2018-07-23 23:56:08	71.197.217.152:14473	BenW@BAPpartners.onmicrosoft.com	Accessed other entity type	Edit Organization	"AdminCenter" @ "https://..."
2018-07-23 23:53:54	40.83.145.50:27916	Unknown	Accessed other entity type	Post RetrieveInstancesOperat	"AdminApi" @ "https://bap..."

[Search](#) [+ New alert policy](#)

Activity Explorer

A better understanding of activities related to your data



Visibility into document-level activities like label changes and label downgrades

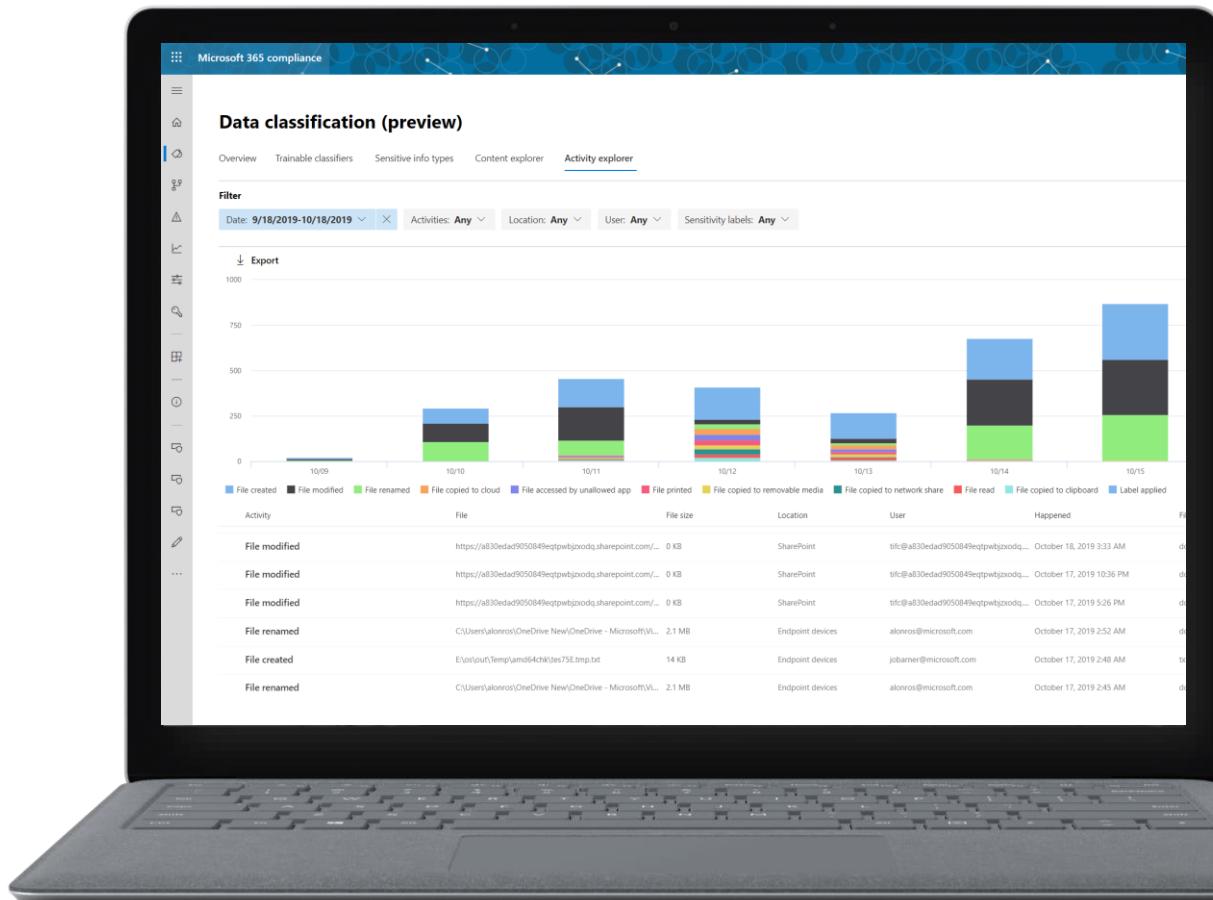


Ability to filter the data to see all the details for a specific label, file, file types, user and importantly interesting activities



Understanding of a broad-spectrum of activities across documents by location

Coming soon: Power BI label activities





Enable MIP labels in Power BI admin portal

Publish label policy in M365 Compliance

Enable MIP label in Power BI admin portal

Users

Audit logs

Tenant settings

Capacity settings

Embed Codes

Organizational visuals

Dataflow settings

Workspaces

Custom branding

Protection metrics (preview)

Featured content

◀ Enable Microsoft Information Protection sensitivity labels
Enabled for the entire organization

Sensitivity labels can be applied to datasets, dataflows, reports, and dashboards, and will be visible in Power BI. [Learn more](#)

Enabled

⚠ After applying this setting, enable the "Set sensitivity labels" setting, below. Otherwise labels can't be set and will appear empty in Power BI.

Apply Cancel

ⓘ This setting applies to the entire organization

◀ Set sensitivity labels for Power BI content and data
Enabled for the entire organization

Users in the organization can set sensitivity labels for Power BI datasets, dataflows, reports, and dashboards. [Learn more](#)

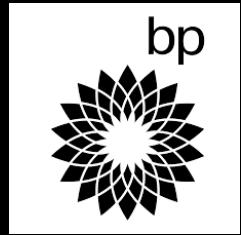
Enabled

⚠ The setting below determines which users in the organization can set and change sensitivity labels. All other users in the organization can only view the labels.

Licenses

- To view and apply sensitivity labels in Power BI, in addition to Power BI licenses, users must have Governance (IP&G) at minimum
- The license is sold stand alone or through one of Microsoft's licenses suites, Microsoft 365 E5 / E5 Compliance (Power BI included in E5)
- For more details go to:
<https://aka.ms/PowerBIDataProtectionOverview>





“Our data owners can now classify their data with ease within Power BI and align with our existing Microsoft Information Protection labels. The integration with Microsoft Information Protection means that we can see where our important data is being used and be assured that exported data is automatically labelled and protected in accordance with our policies. In this way our users practice security by choice because it is easy. The ability to monitor activity and block or protect downloads of classified data in real-time using [Microsoft Cloud App Security] is a very powerful control, which gives us increased flexibility on collaborating and sharing securely.”

Why use MIP labels in Power BI?



Compliance



Centralized



End-To-End
protection



Easy to deploy



Don't
compromise on
productivity



“We've seen two
years' worth of
digital transformation
in two months.”

Satya Nadella



Resources and information?

Sensitivity labels in Power BI documentation –
<https://aka.ms/PowerBIDataProtectionOverview>



Questions?





Thank you!

