



M365
SECURITY,
COMPLIANCE &
MANAGEMENT

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

Microsoft blog 2021



Security staff



82%

Of business leaders plan
on adding security staff

Microsoft survey 2020



Costs



81%

Of business leaders feel
pressure to reduce
security costs

Microsoft survey 2020

Data Breaches Since Covid-19

News events, criminal activity, and Microsoft's response

Microsoft detections and response



Machine learning detections built to spot Emotet's malicious behavior protect customers from updated campaigns.



Machine learning detections analyze behaviors to reliably detect and block new Emotet, Lokibot, Trickbot, and other campaigns shifting to COVID-19 lures.



EARLY MAR Focused COVID-19-themed threat hunting and research intensifies.



MAR 14 Microsoft proactively notifies hospitals with vulnerable VPN infrastructure of human-operated ransomware.



MAR 15 Microsoft sees AND processes more than 18K malicious COVID-19-themed URLs and IPs daily.



MAR 18 Specialized machine learning models designed for COVID-19 threats deployed.



Microsoft correlates signals across emails, identities, endpoints, and apps to detect entire attack chains and prevent resurgence.



Ransomware attacker is known threat actor tracked by Microsoft.



Microsoft threat intelligence team detects and investigates Ryuk attack.



Each day, Microsoft blocks ~50K emails with COVID-19-related malicious attachments or URLs, ~2% of all threats.

Criminal activity



JAN 28 Emotet switches to COVID-19 lures starting in Japan.



FEB 4 Lokibot follows Emotet's lead, using COVID-19-themed lures in campaigns observed in China and US.



FEB Emotet sustains operations using COVID-19 lures spreading to Italy, Spain, and English-speaking countries.



MAR 3 Trickbot starts to use COVID-19 lures in campaign targeting Spain, France, and Italy. Trickbot goes on to become the most prolific malware operation using COVID-19-themed lures.



MAR 13 A Czech hospital is hit by a known ransomware actor.



MAR 15 Malware using COVID-19-map-themed lures start appearing.



MAR 17 COVID-19-map-themed malware observed in Europe leads to human-operated ransomware Ryuk.

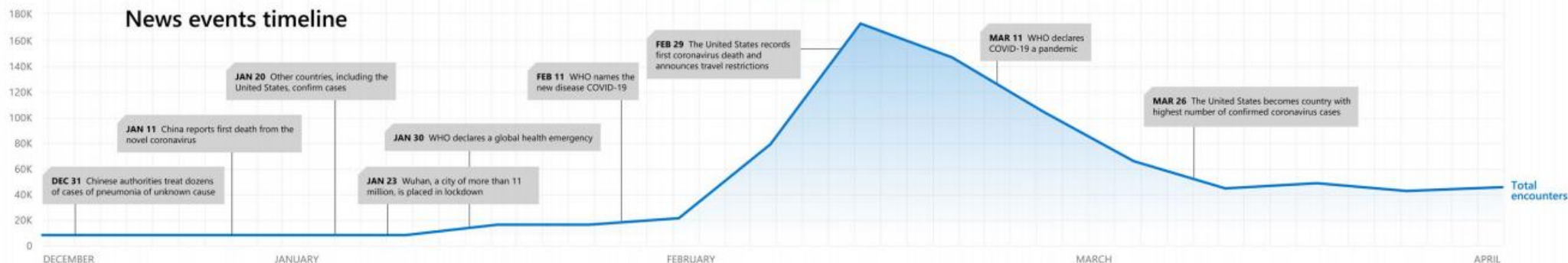


The ransomware actor that attacked Czech hospital continues to actively target healthcare, software, and critical infrastructure.



By late March, every country in the world has seen at least one COVID-19-themed attack.

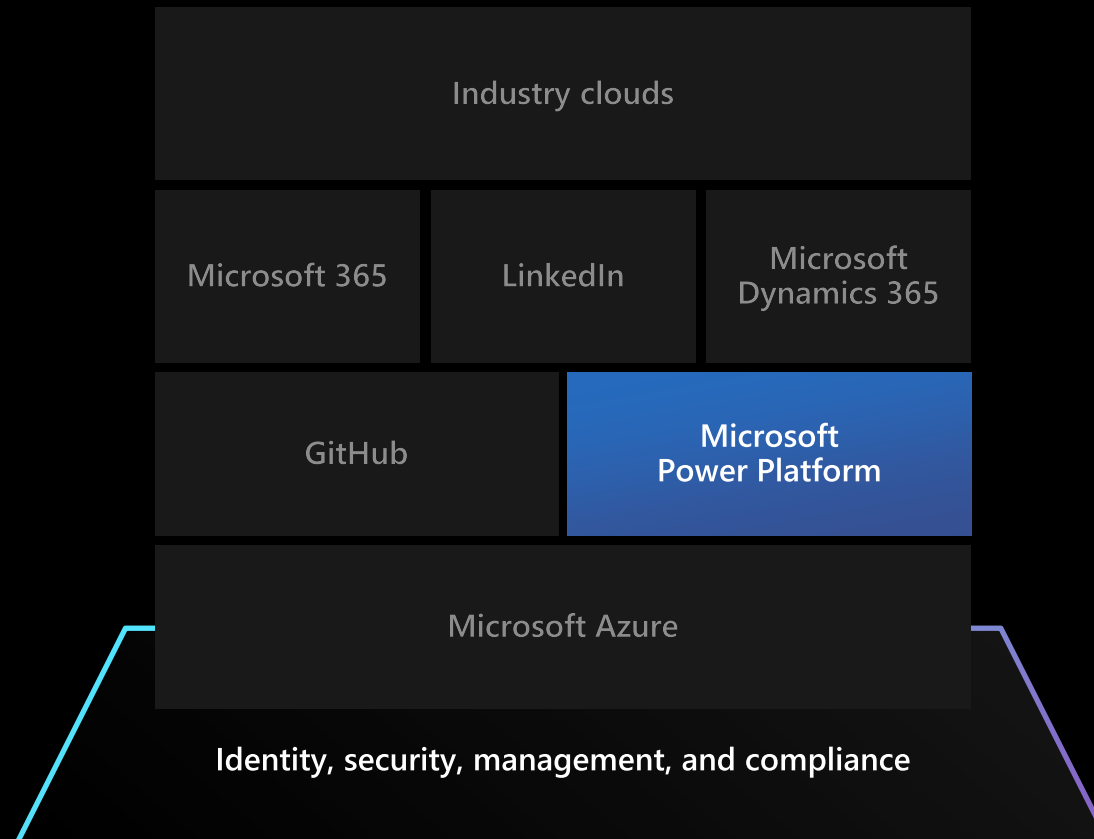
News events timeline



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





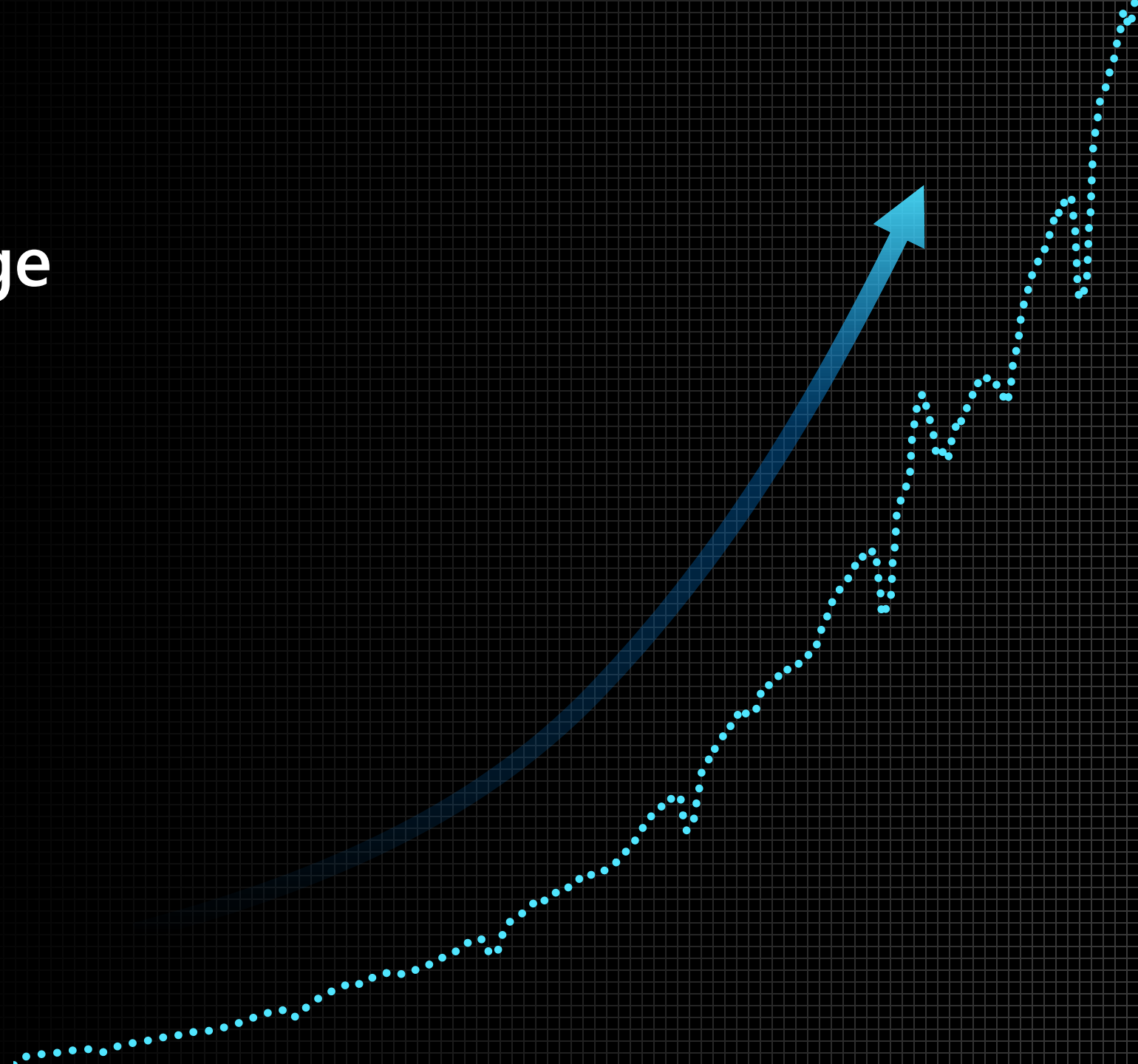
Drive a data culture

everyone | every decision | at any scale

Power BI
monthly active usage

6 years
of rapid growth

260k+
Organizations



Industry Leadership



Figure 1: Magic Quadrant for Analytics and Business Intelligence Platforms



Source: Gartner (February 2021)



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

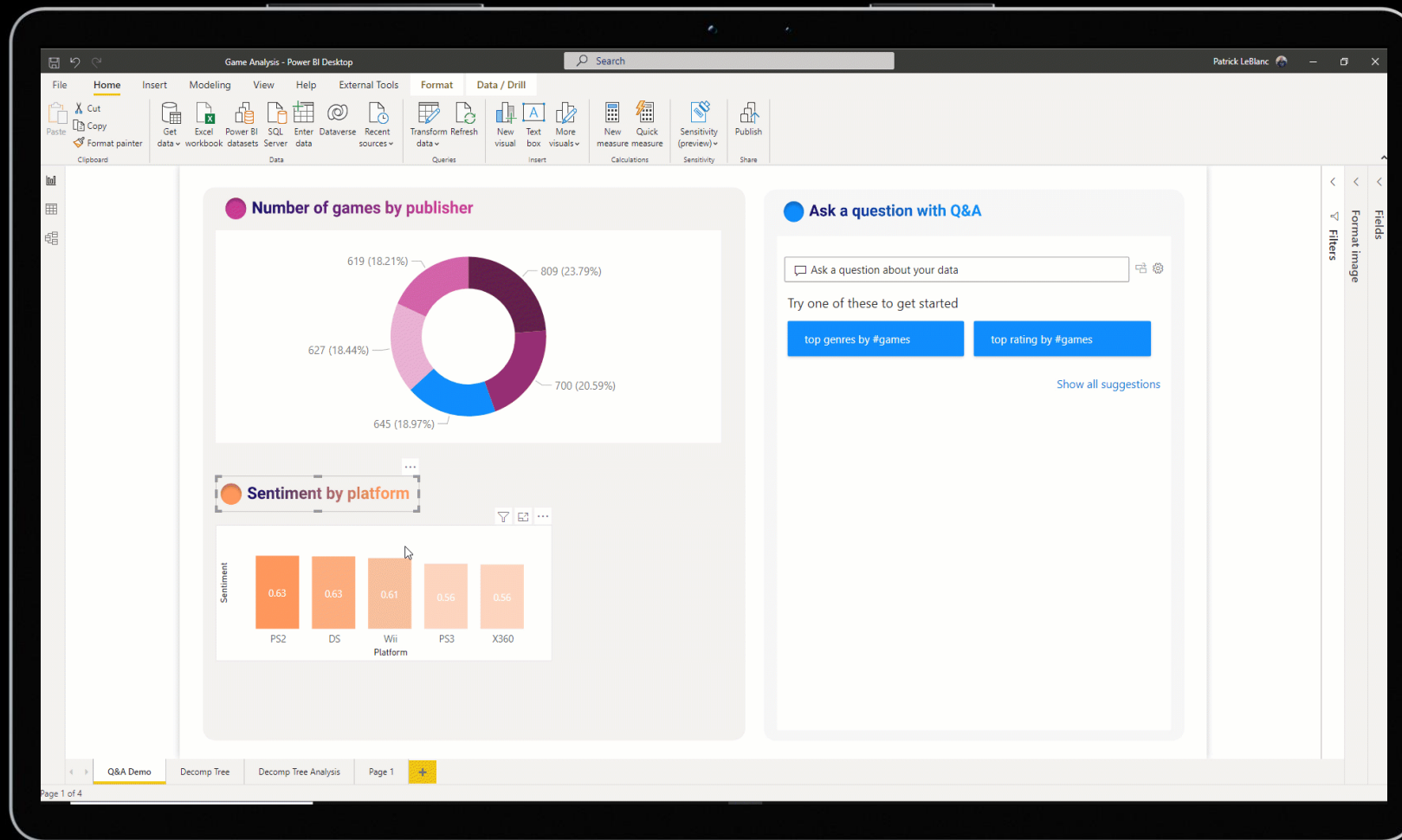
Why the world's largest organizations are standardizing on **Power BI**



**Leading BI
capabilities**

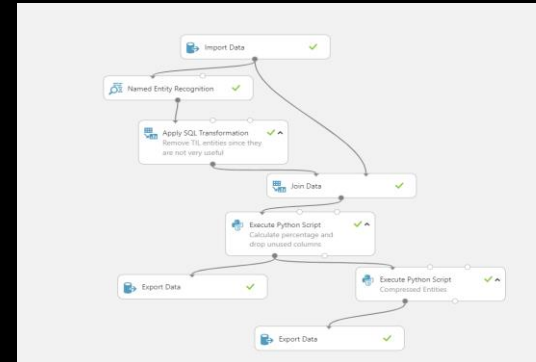


PowerPoint for data

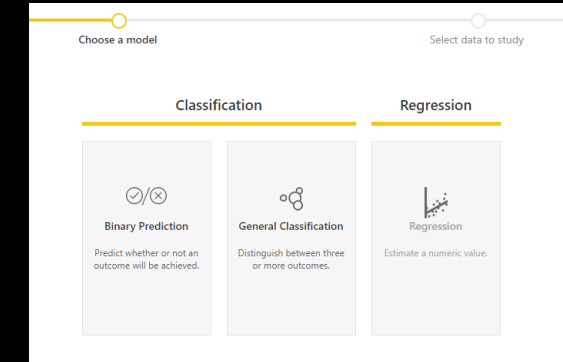


The most complete AI capabilities in a BI product

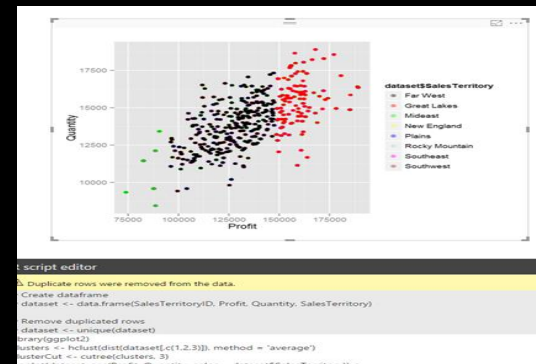
Extend with Azure ML



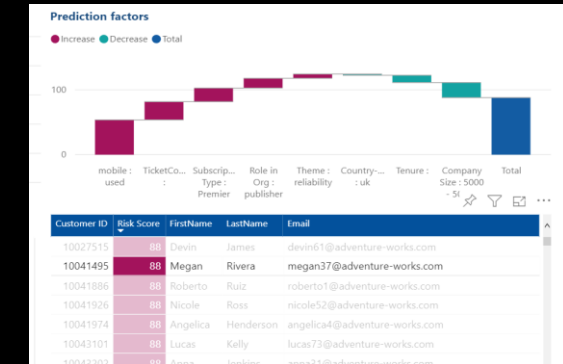
Create ML models



Python & R Integration



Explore Predictions

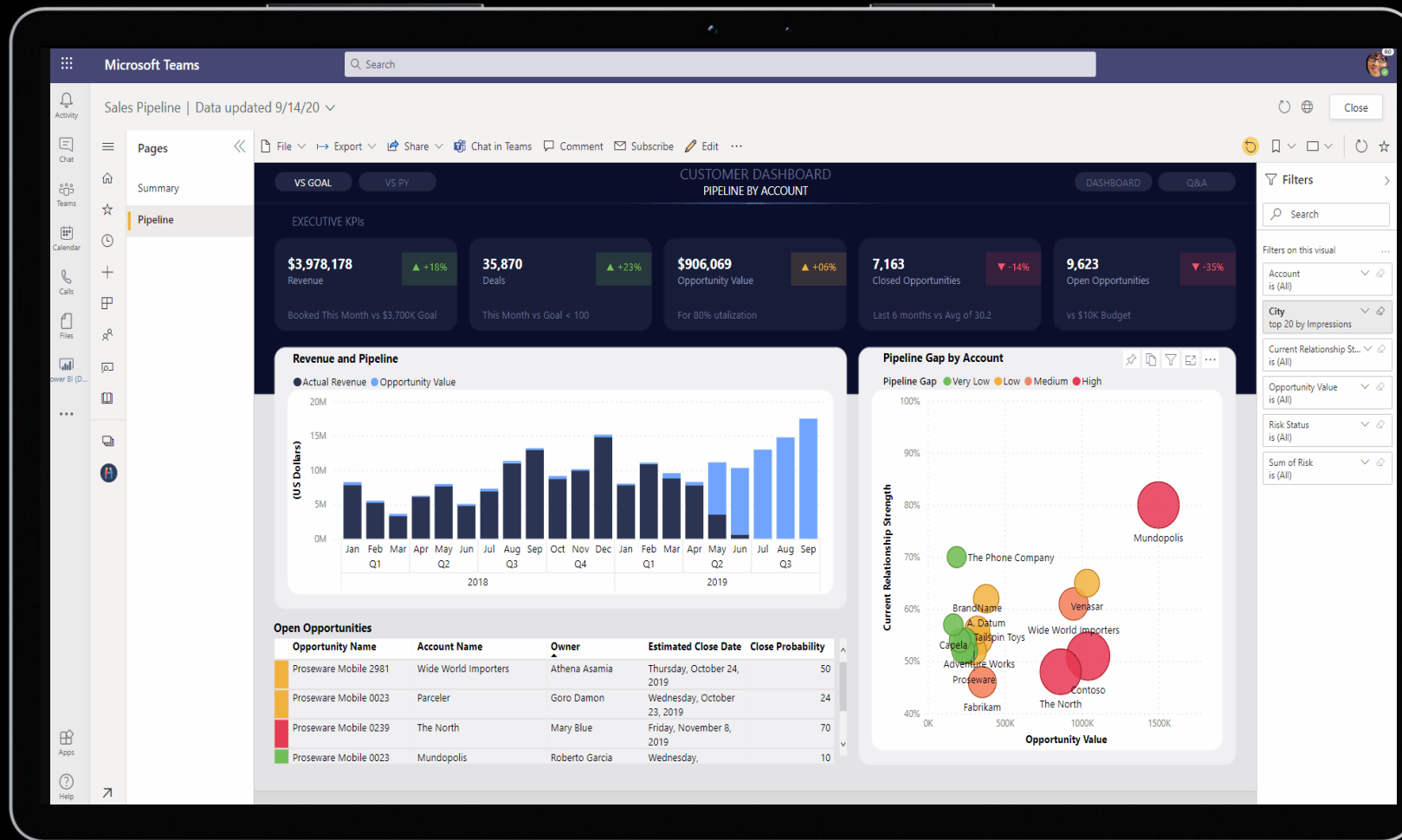




Power BI + Teams

Your data is where
you collaborate

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



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



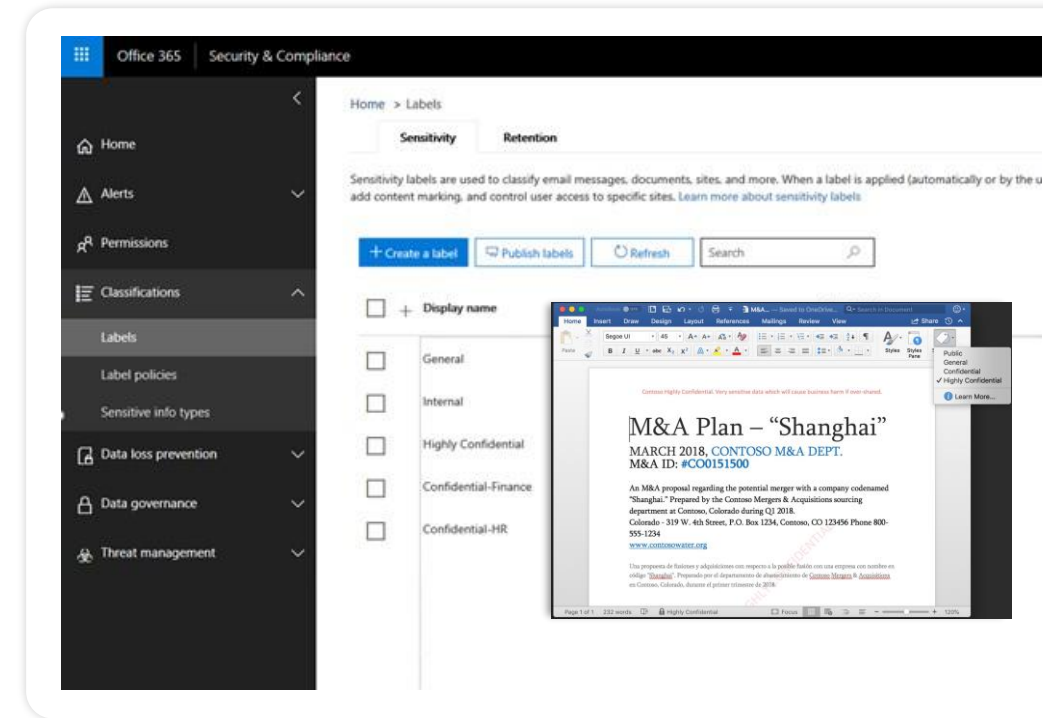
UNIFIED

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

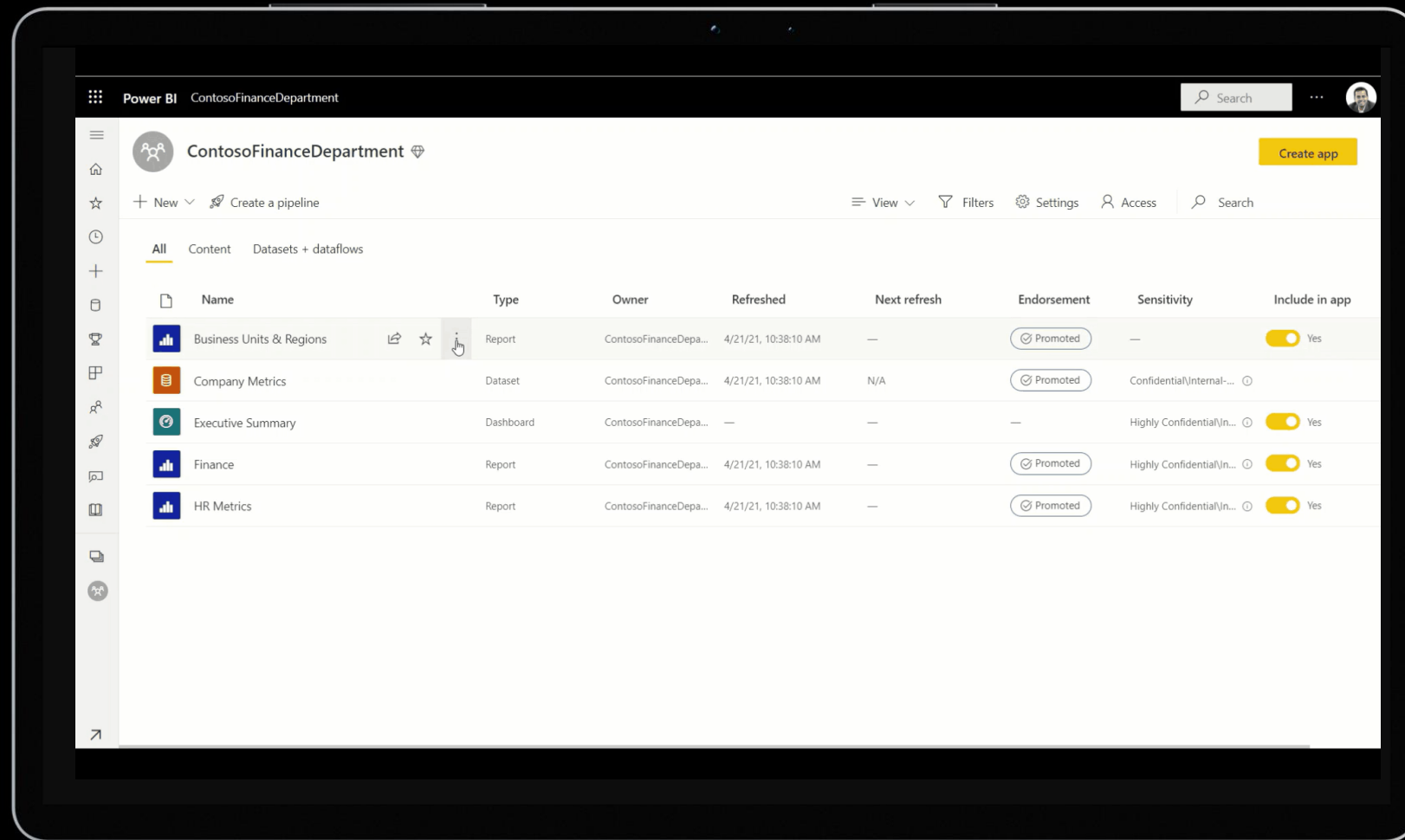


Microsoft Information Protection is a **built-in, intelligent, unified** and **extensible** platform and solution to protect sensitive data.



MIP and Power BI

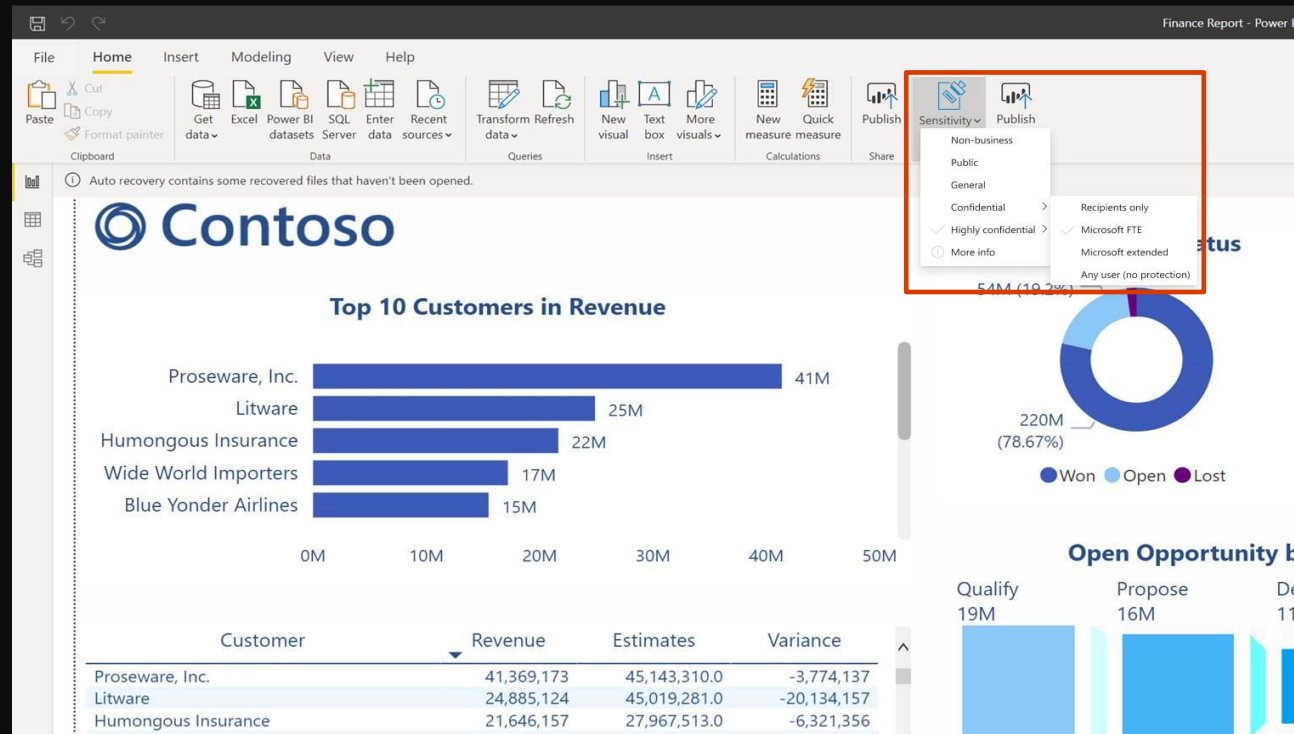
- Classify Power BI content with MIP labels
- Label and protect files when data leaves Power BI (Excel, PowerPoint, PBIX and PDF).





MIP in Power BI Desktop app

Label and protect PBIX files

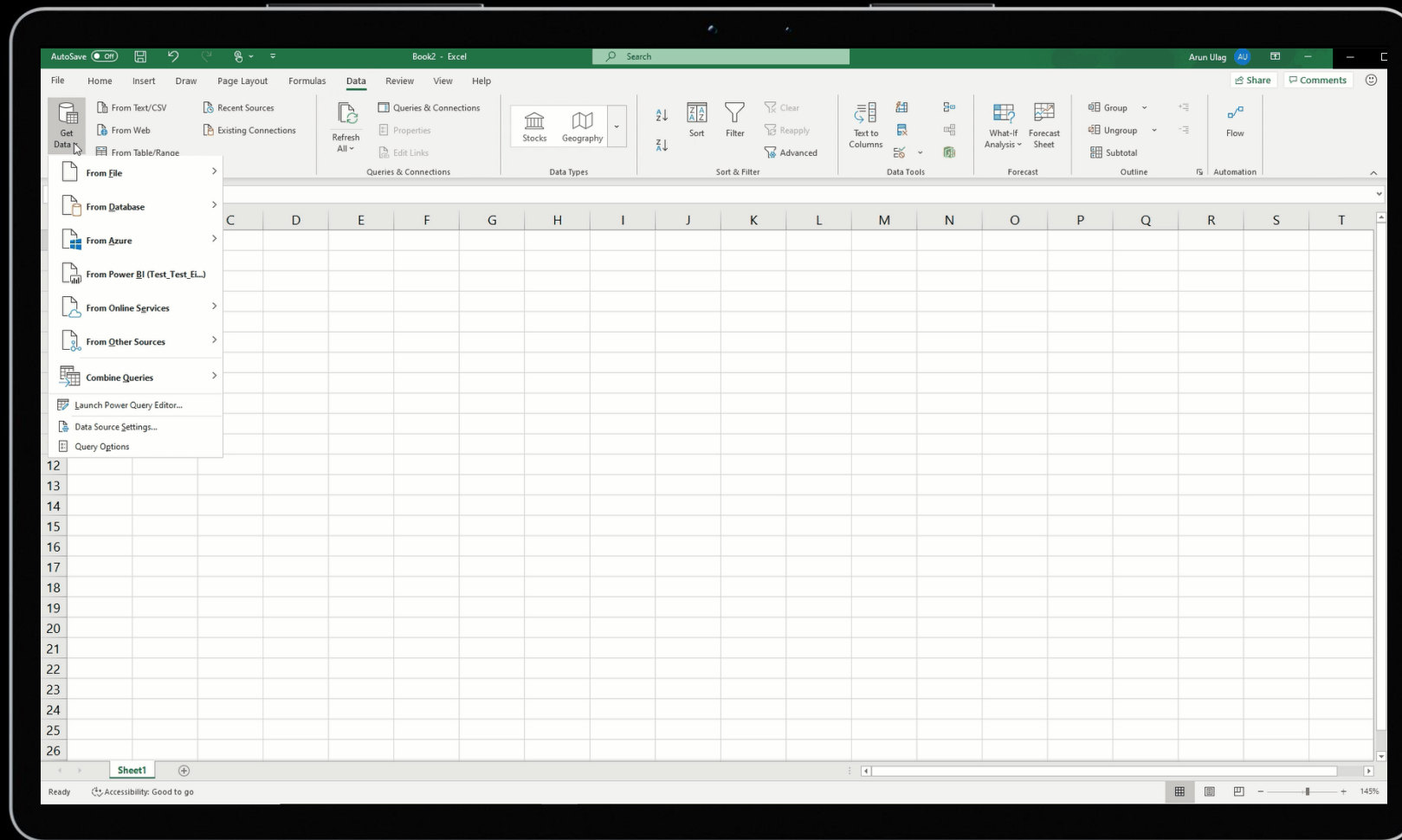


Demo



Inherit labels when connect to Power BI data from Excel

Automatic Excel
Workbook labels



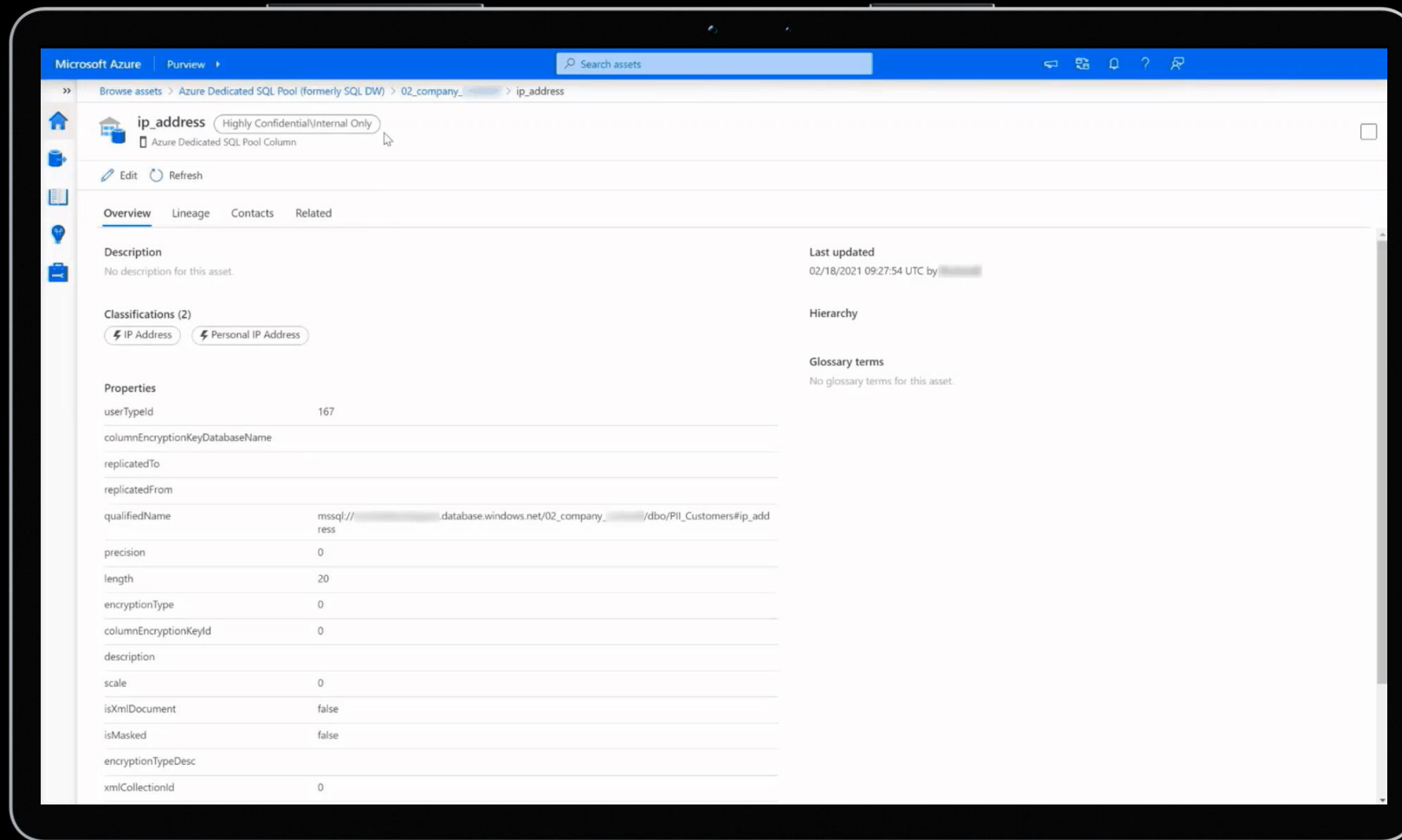


Inherit MIP label from data source

Securing the full data
journey from Azure to
Office

Coming soon

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

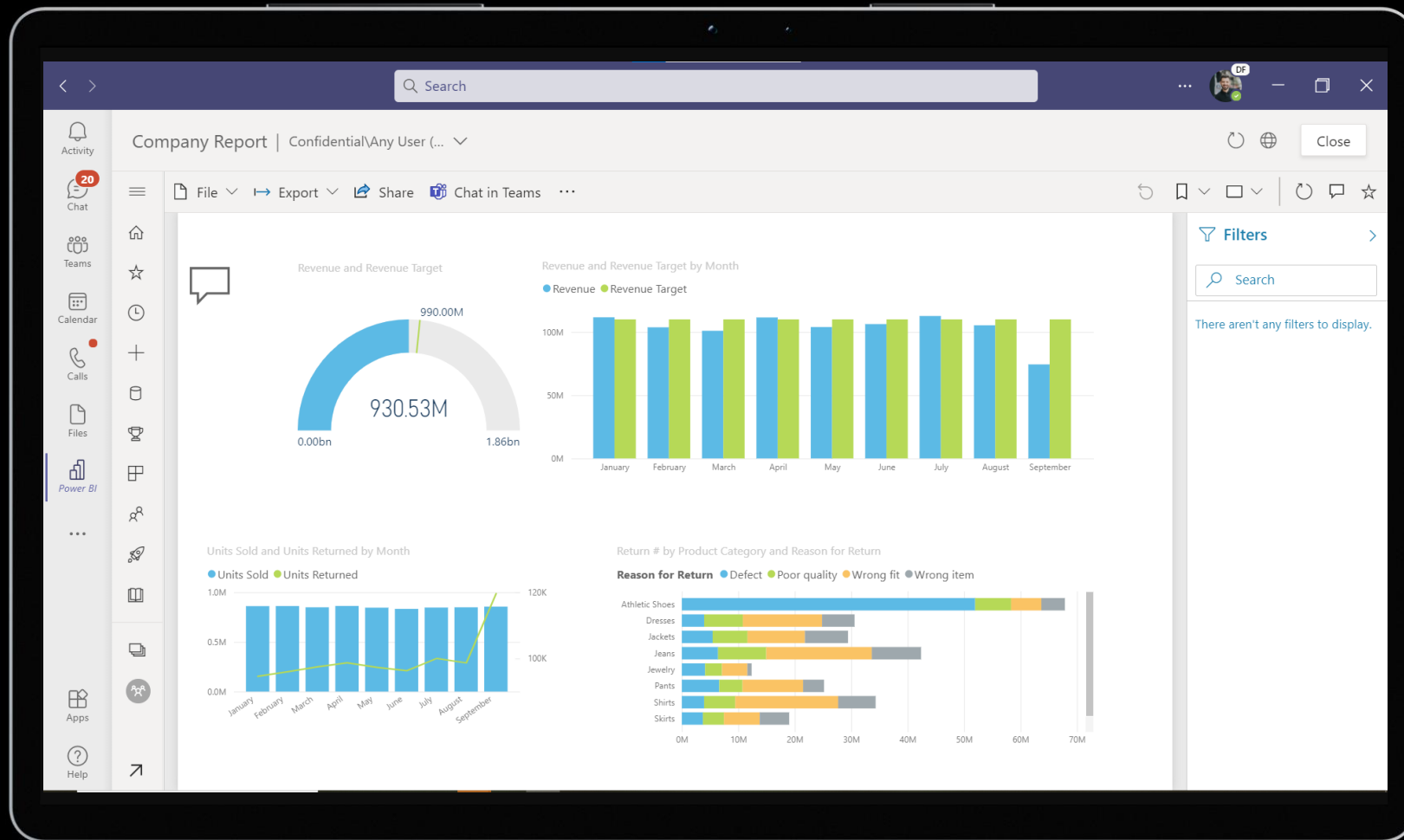


Demo



MIP Labels in Microsoft Teams

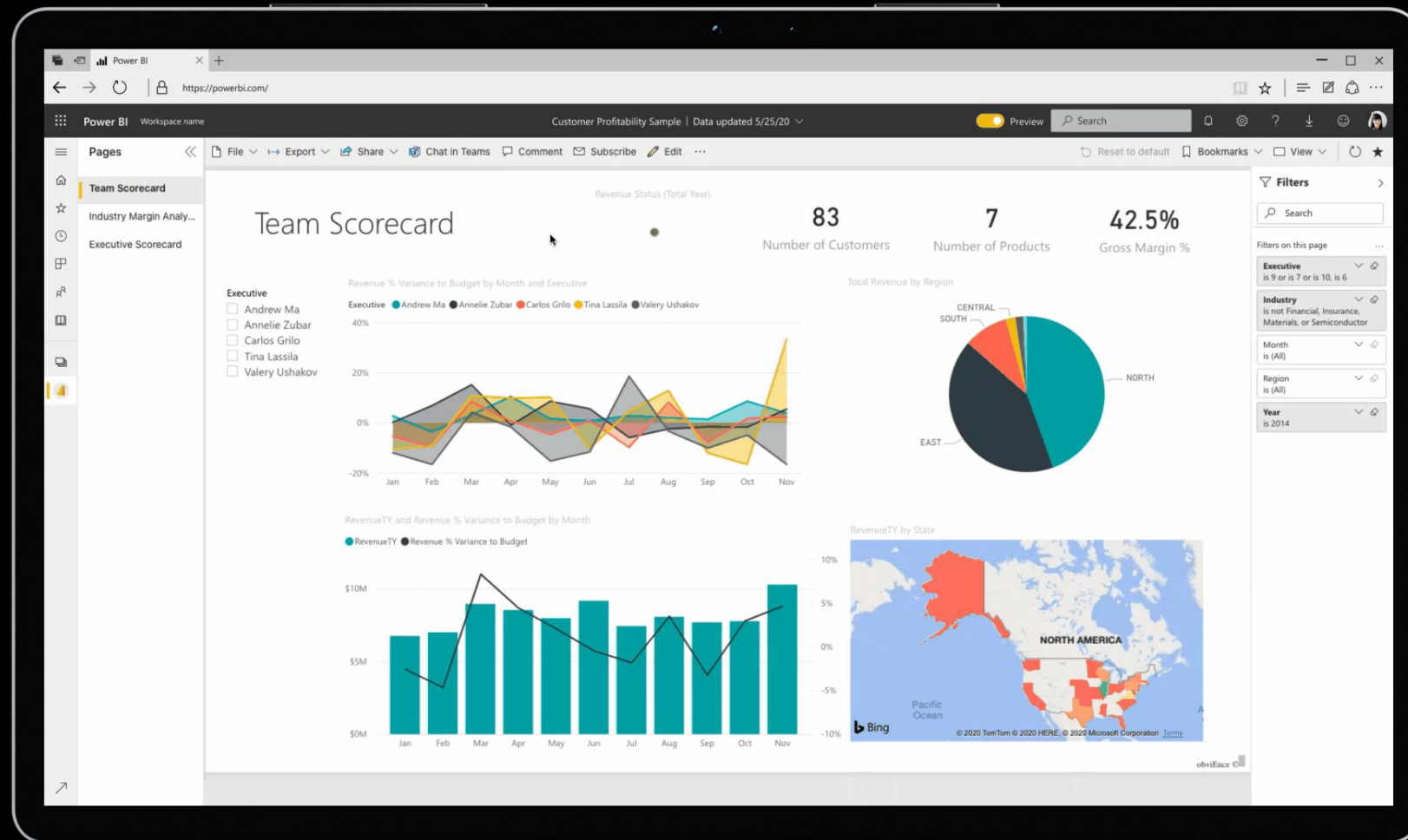
- Sensitivity labels visible in embedded views
- Protection persists when data is exported.





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)

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.

Search

+ New alert policy

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

Hide filtering

Export results

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.onmic...	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 UpdateInstanceSettin...	"AdminApi" @ "https://ad...
2018-07-23 23:58:42	104.42.186.44:1249	Unknown	Accessed other entity type	Post RetrievalInstancesOper...	"AdminApi" @ "https://ad...
2018-07-23 23:58:41	104.42.186.44:1249	Unknown	Accessed other entity type	Post RetrievalInstancesOper...	"AdminApi" @ "https://ad...
2018-07-23 23:56:08	71.197.217.152:14473	BenW@BAPpartners.onmic...	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 RetrievalInstancesOper...	"AdminApi" @ "https://bap...

Activity Explorer

A better understanding of activities related to your data



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

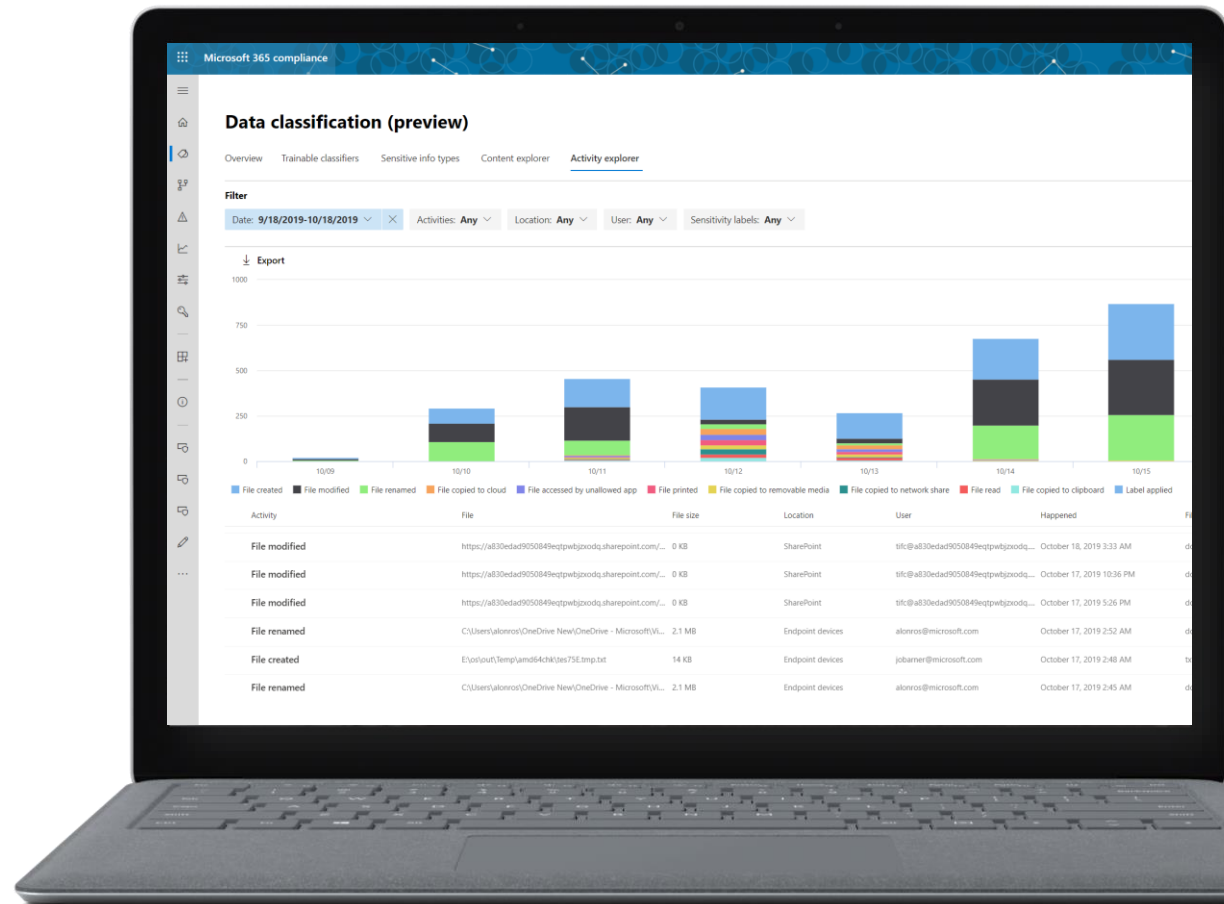


Ability to filter the data to see all the details for a specific label, file, file types, user and importantly interesting activities



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

Coming soon: Power BI label activities

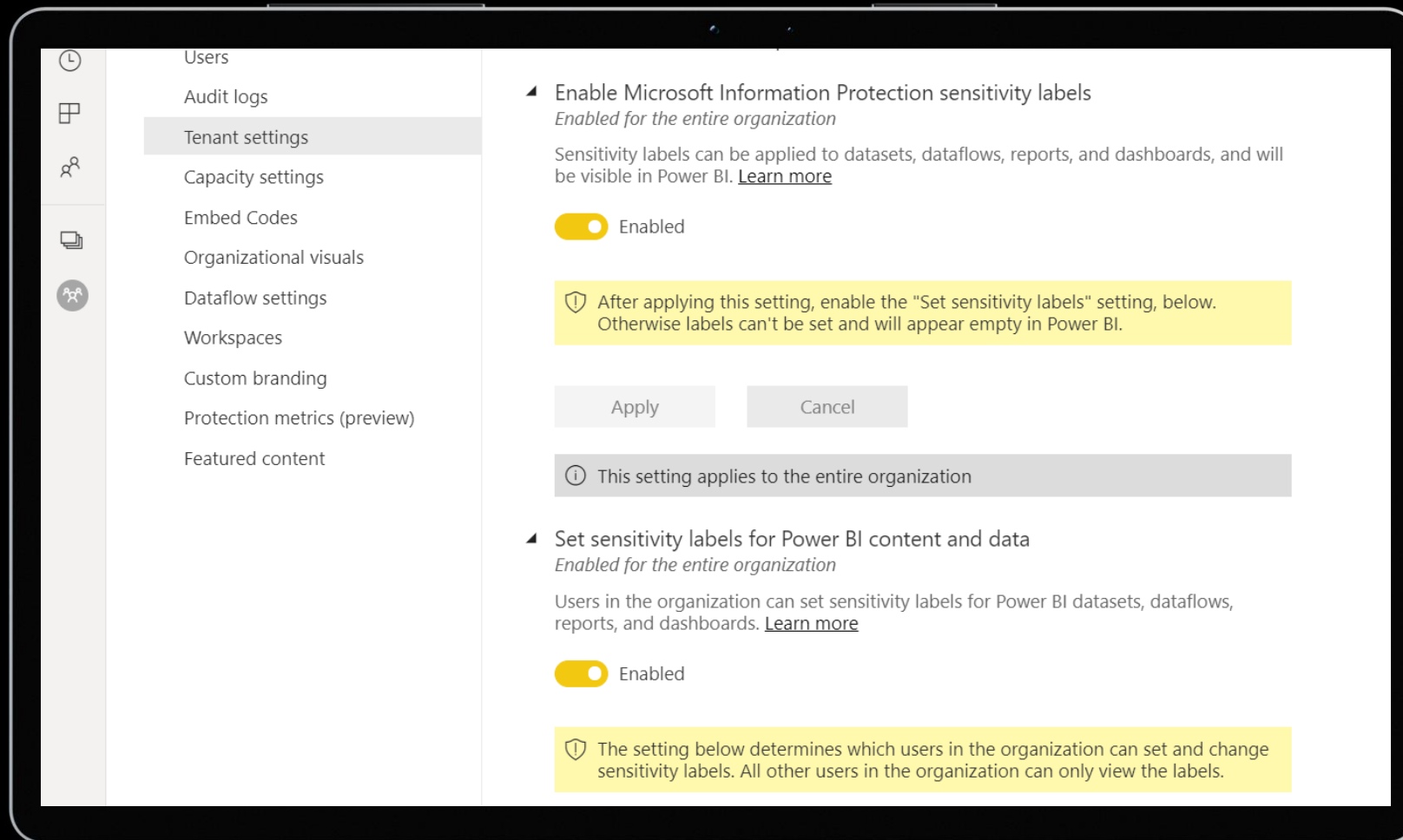




Enable MIP labels in Power BI admin portal

Publish label policy in
M365 Compliance

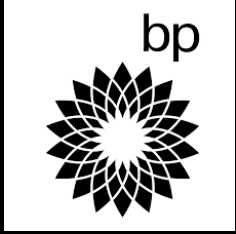
Enable MIP label in Power
BI admin portal



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 license 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



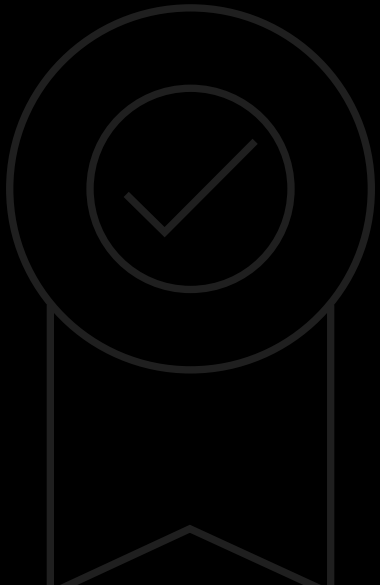
End-To-End
protection



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!

