Microsoft Security

Mastering the Microsoft Purview Customer Pitch

Stephanus Schulte
Sr Partner Solution Sales Manager SMB Security
Microsoft

AI transformation is happening now

95% of organizations are implementing or developing an AI strategy[1]

75% of knowledge workers already using AI at work (doubled in the past 6 months)[2]

1% of risk leaders are thoroughly prepared for mass GenAI availability risks[3]

1. Microsoft internal research May 2023, N=638, 2. Work Trends Index,
3. Gartner®, Executive Pulse: Organizations are not prepared for Generative AI risks Sept 2023.

Top concerns from risk leaders

Leakage of sensitive data

80%+

of leaders cited leakage of sensitive data as their main concern with 48% of them expect to continue banning all use of GenAI in workplace[2].

Lack preparedness for deploying GenAI

31%

of organizations have established a global data architecture and 25% have a global data quality program[3].

Regulatory evolution + uncertainty

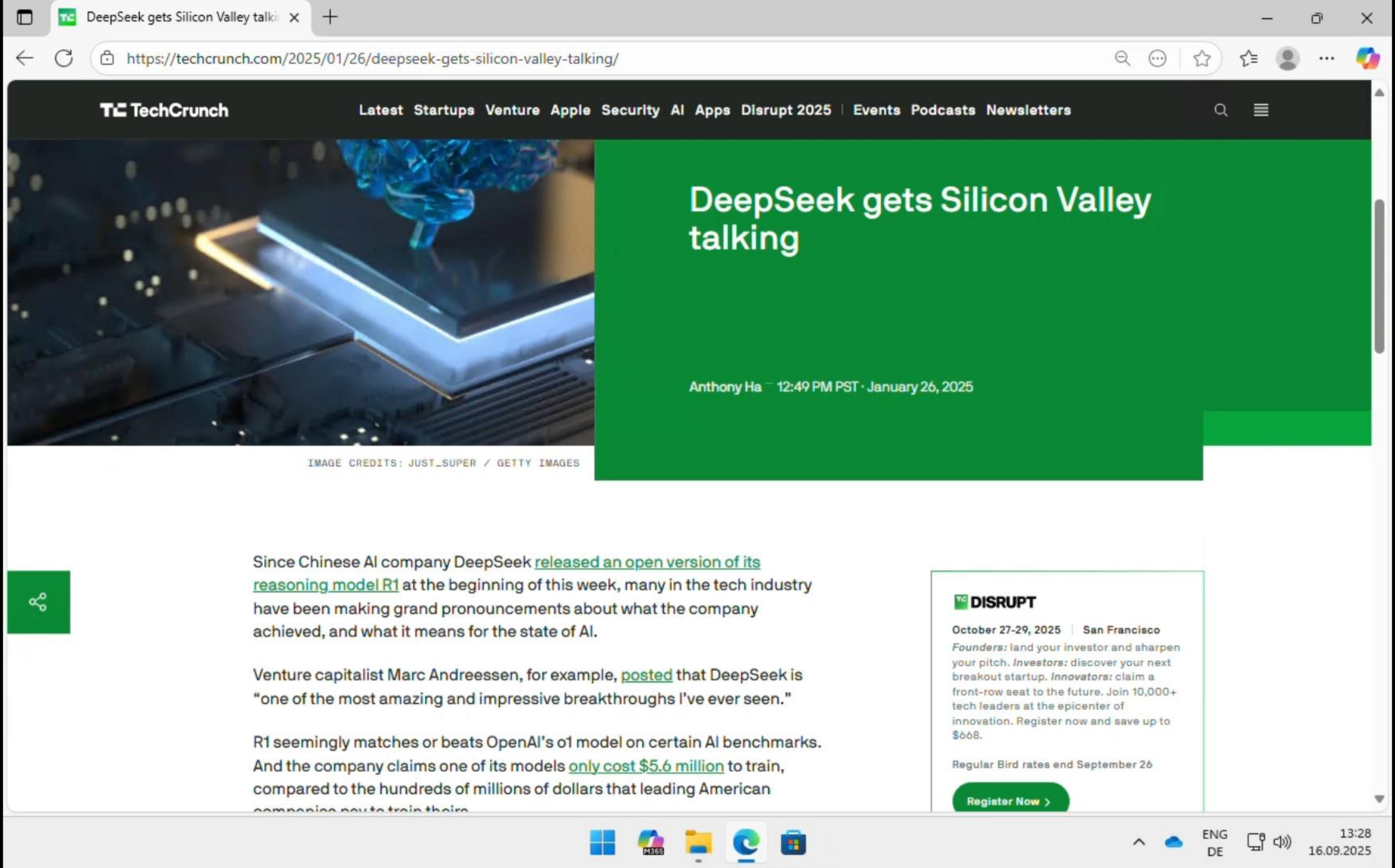
2027

at least one global company will see its AI deployment banned by a regulator for noncompliance with data protection or AI governance legislation[1].

[1] Gartner Security Leader's Guide to Data Security, Sep 2023

[2] First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

[3] Voice of the Chief Data Officer 2024, 4. DSI Report



DeepSeek gets Silicon Valley talking

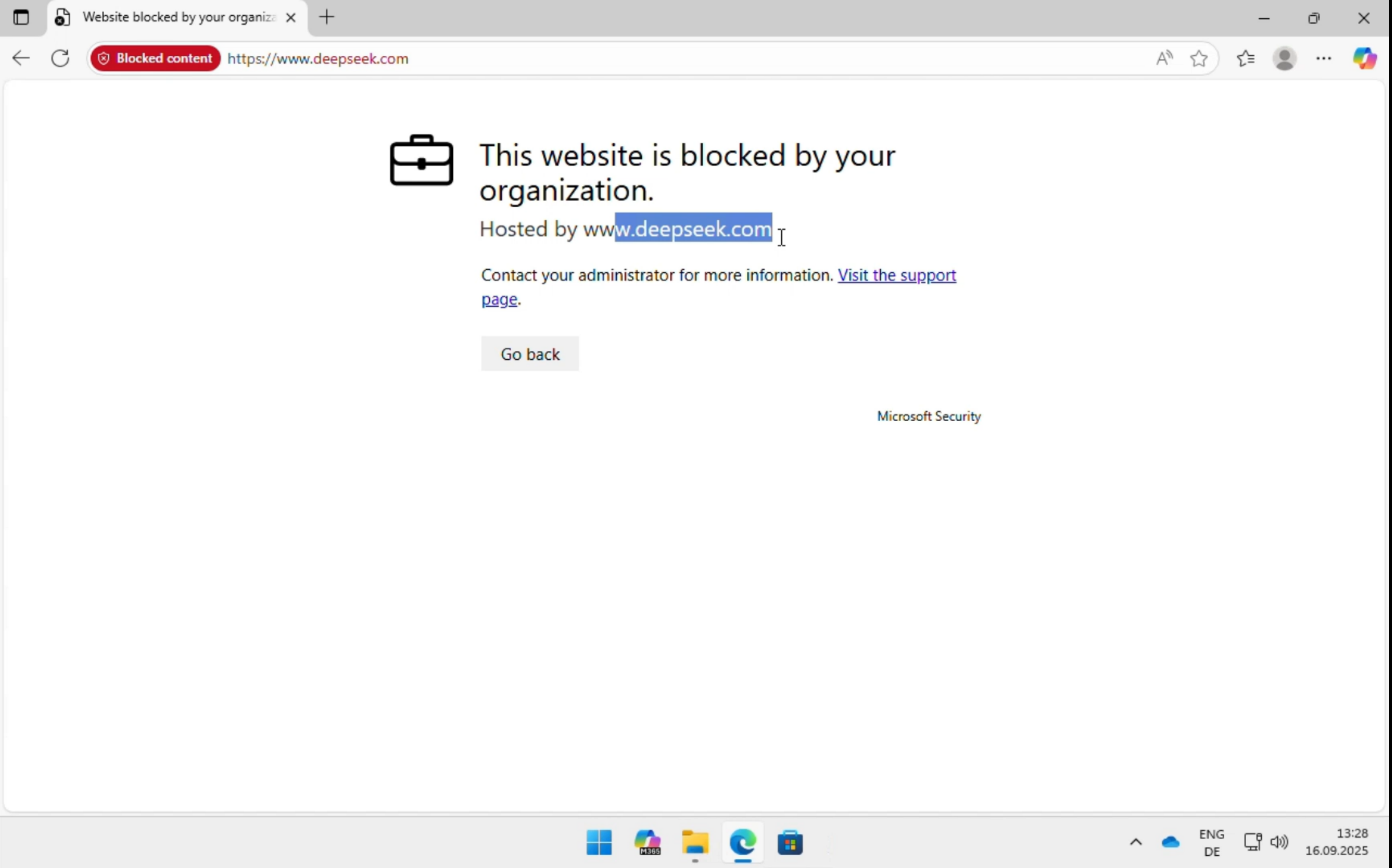
Anthony Ha 12:49 PM PST · January 26, 2025

IMAGE CREDITS: JUST_SUPER / GETTY IMAGES

Since Chinese AI company DeepSeek released an open version of its reasoning model R1 at the beginning of this week, many in the tech industry have been making grand pronouncements about what the company achieved, and what it means for the state of AI.

Venture capitalist Marc Andreessen, for example, posted that DeepSeek is "one of the most amazing and impressive breakthroughs I've ever seen."

R1 seemingly matches or beats OpenAI's o1 model on certain AI benchmarks. And the company claims one of its models only cost $5.6 million to train, compared to the hundreds of millions of dollars that leading American companies pay to train theirs



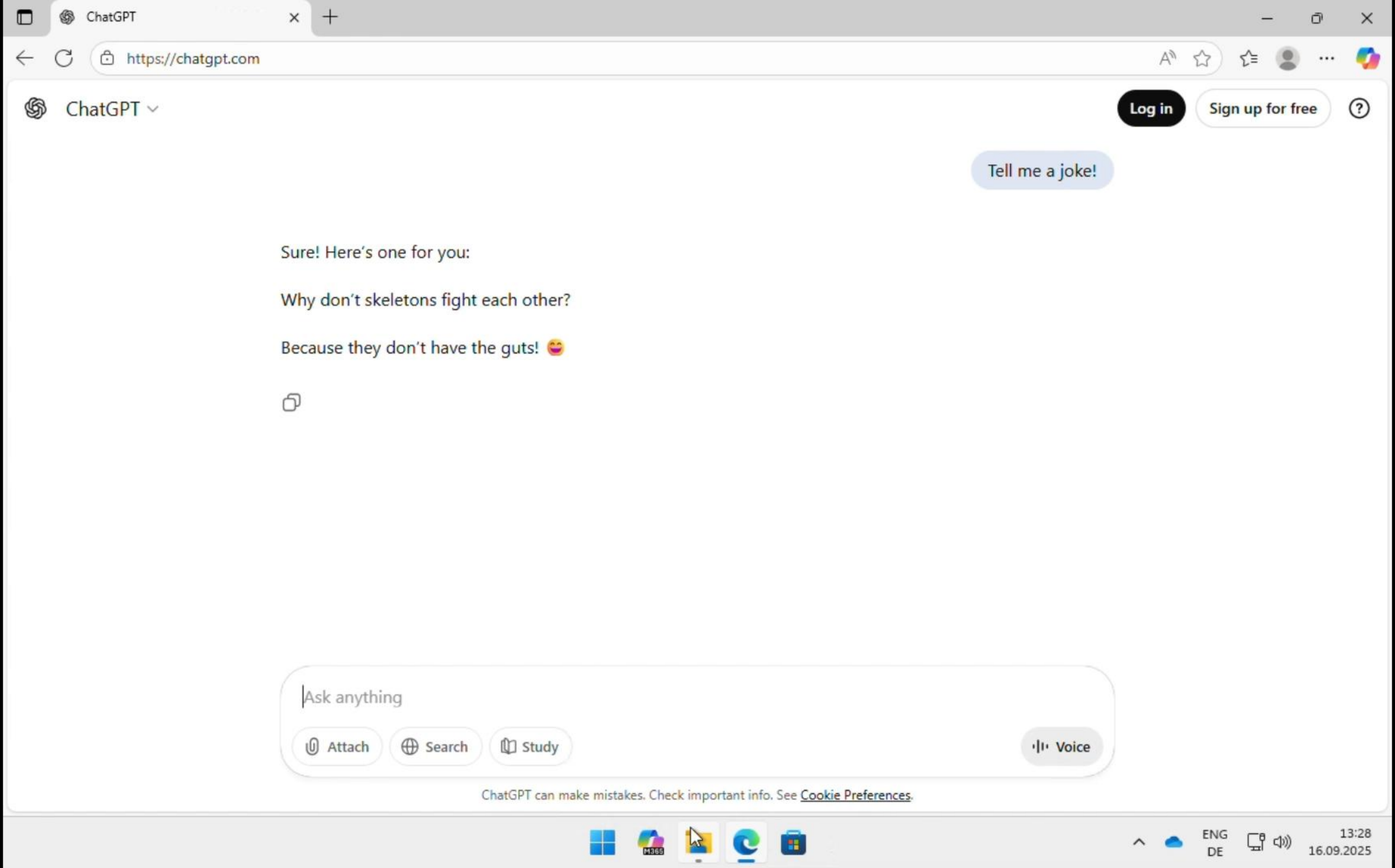
This website is blocked by your organization.

Hosted by www.deepseek.com

Contact your administrator for more information. Visit the support page.

Go back

Microsoft Security



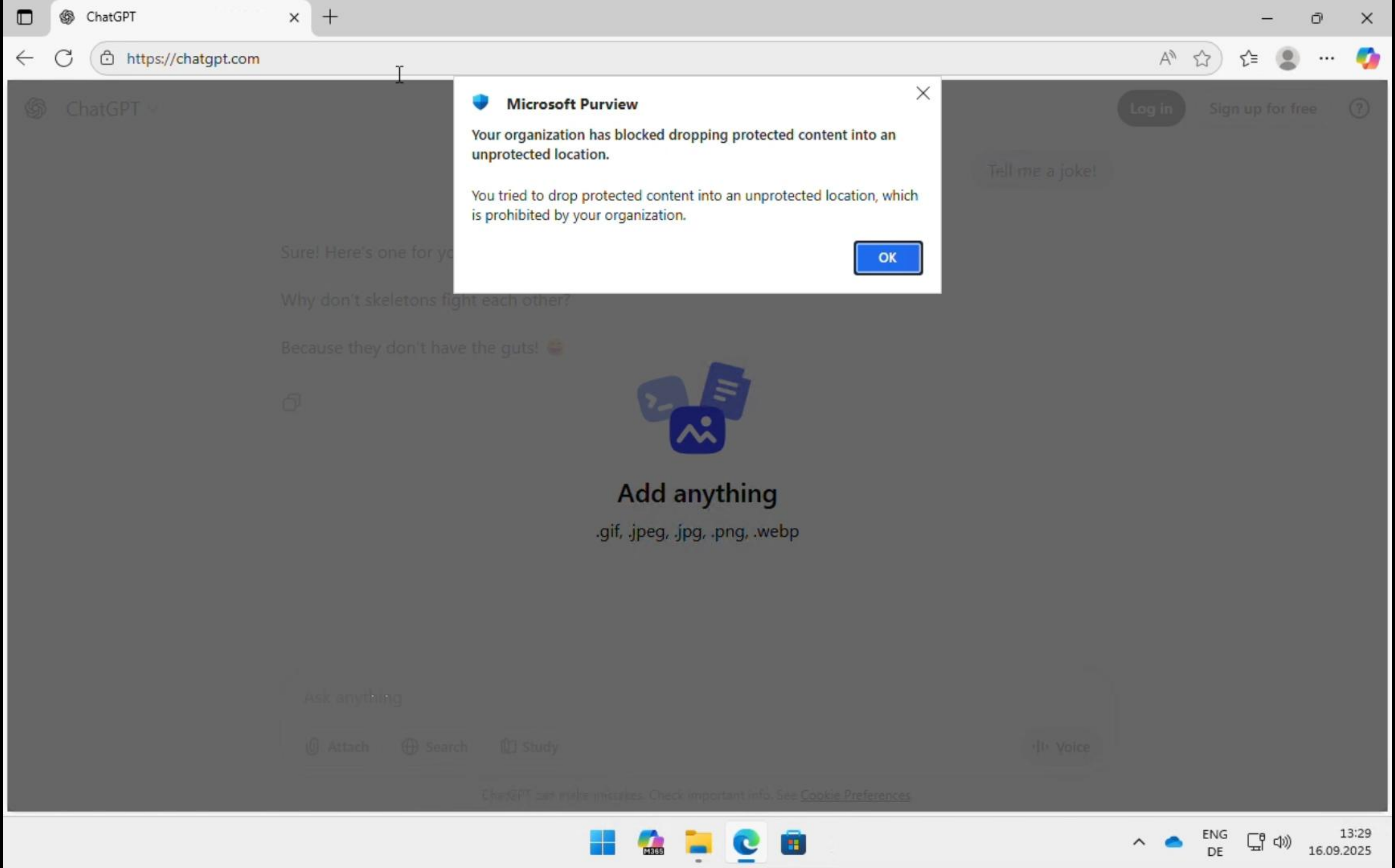
Tell me a joke!

Sure! Here’s one for you:

Why don’t skeletons fight each other?

Because they don’t have the guts! 😄

ChatGPT can make mistakes. Check important info. See Cookie Preferences.



Microsoft Purview

Your organization has blocked dropping protected content into an unprotected location.

You tried to drop protected content into an unprotected location, which is prohibited by your organization.

Tell me a joke!

Sure! Here's one for yo

Why don't skeletons fight each other?

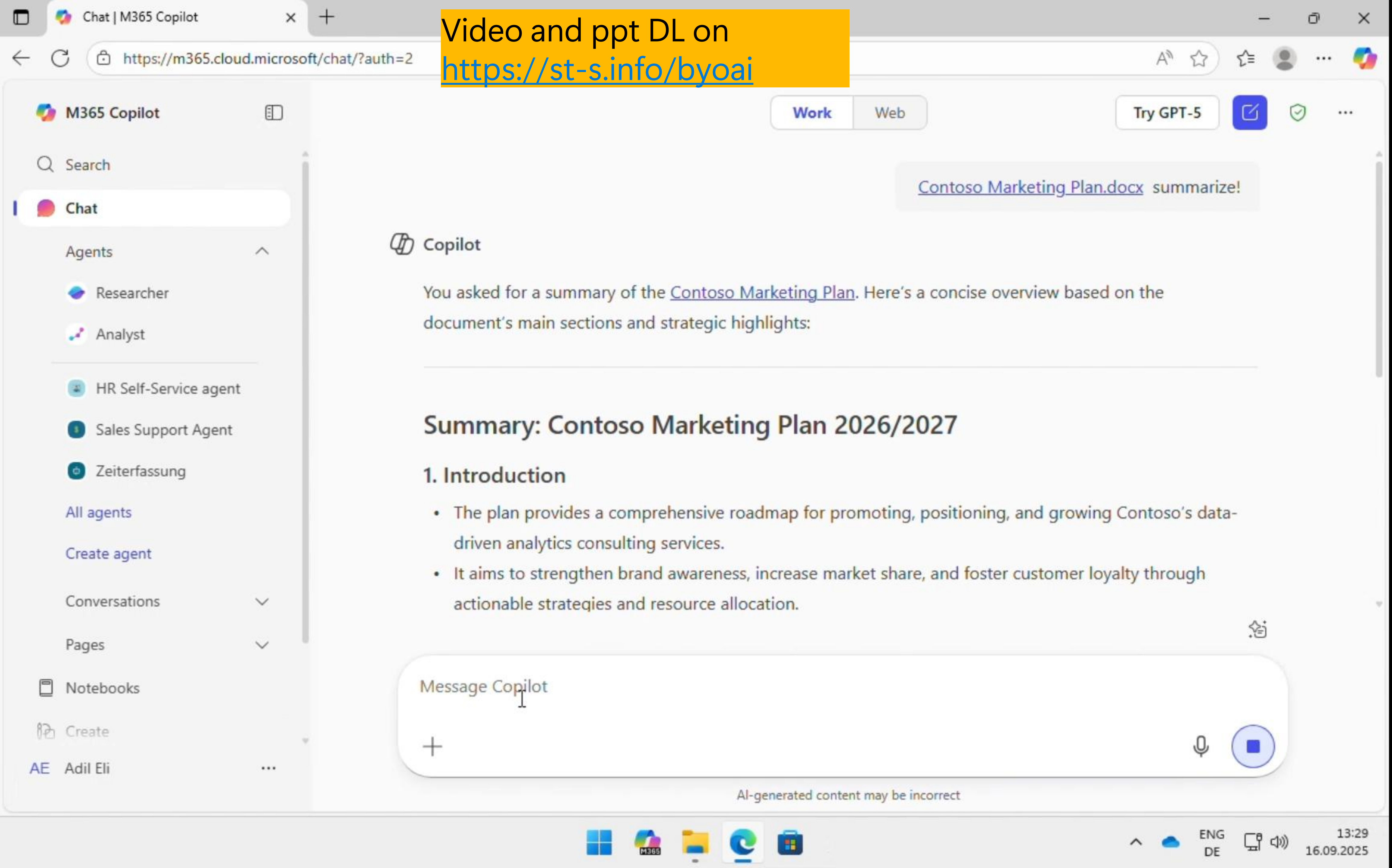
Because they don't have the guts! 😄

Add anything

.gif, .jpeg, .jpg, .png, .webp

ChatGPT can make mistakes. Check important info. See Cookie Preferences.

Video and ppt DL on
https://st-s.info/byoai



Contoso Marketing Plan.docx summarize!

Copilot

You asked for a summary of the Contoso Marketing Plan. Here's a concise overview based on the document's main sections and strategic highlights:

Summary: Contoso Marketing Plan 2026/2027

1. Introduction

- The plan provides a comprehensive roadmap for promoting, positioning, and growing Contoso's data-driven analytics consulting services.
- It aims to strengthen brand awareness, increase market share, and foster customer loyalty through actionable strategies and resource allocation.

Disparate solutions perpetuate data risk in the era of AI

10+

organizations use an average of 10 data security solutions for their data estate[1].

The count jumps when you also consider data governance, compliance, and privacy solutions.

Creating infrastructure gaps that are costly and complex to manage and traverse during incident responses.

[1] Source: Microsoft Data Security Index report

Microsoft Purview via M365 Purview Suite

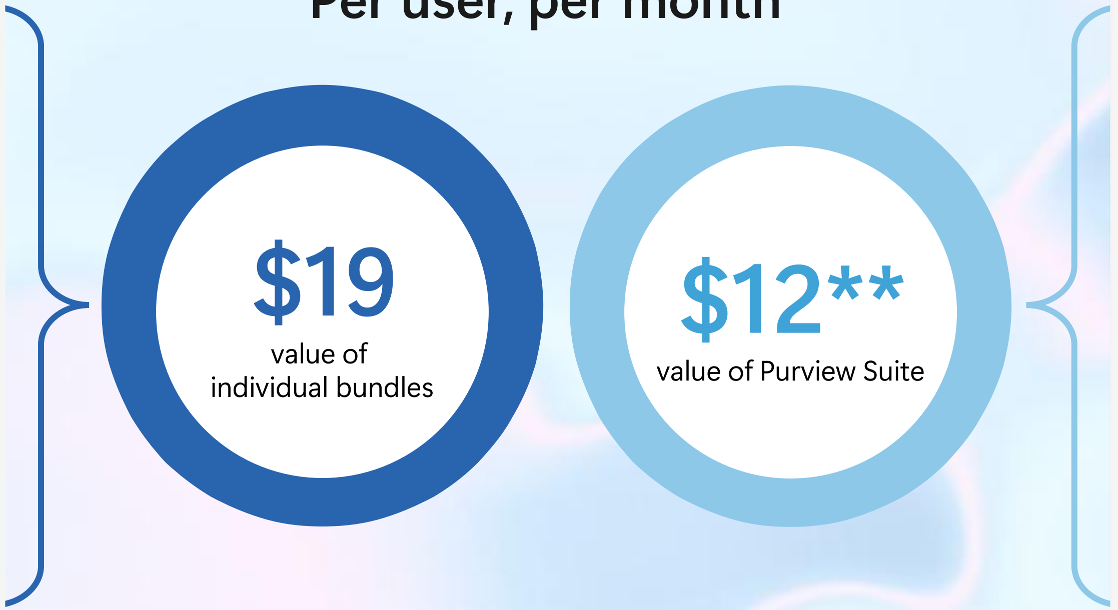
- Effective data protection that removes silos and takes action to ensure data security
- Intelligent tooling supports more efficient data and regulatory compliance
- Purpose-built innovation helps safeguard Microsoft 365 Copilot data

Microsoft Purview

Standalone bundles

Information Protection + Governance Data Loss Prevention Information Protection Data Lifecycle Management ...and more	$7
Insider Risk Mgmt. Insider Risk Management Communication Compliance Privileged Access Management ...and more	$6
eDiscovery + Audit eDiscovery (Premium) Audit (Premium)	$6
Add on Compliance Manager	$8,500 per template

Per user, per month



$19

value of individual bundles

$12**

value of Purview Suite

Microsoft 365 Purview Suite

Save ~36% per license

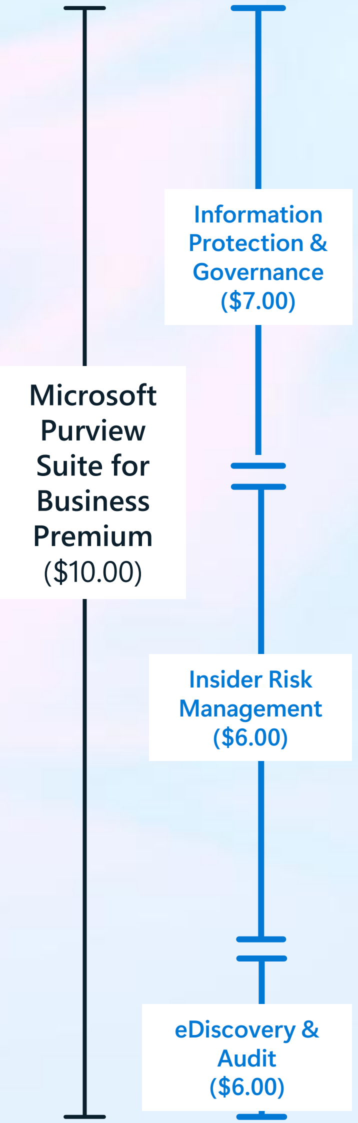
- Enable end-to-end data security + compliance
- Prepare for GenAI + regulatory requirements

*Prices are USD list and per user, per month. Prices may vary by region, currency, and customer pricing agreements

**.Purview Suite for Business Premium for $10; Defender and Purview Suite for Business Premium $15

Microsoft Purview Suite for Business Premium

Manage risks, protect and govern sensitive data, and respond to regulatory requirements



Microsoft Purview Suite for Business Premium ($10.00)

Information Protection & Governance ($7.00)

Insider Risk Management ($6.00)

eDiscovery & Audit ($6.00)

Purview Data Lifecycle and Records Management
Use retention labels and policies to retain and delete information.

Purview Data Loss Prevention (DLP)
Identify, monitor, and automatically protect sensitive information stored across Microsoft 365 locations.

Purview Information Protection
Identify and protect sensitive data including credit card, bank account, and passport numbers.

Purview Message Encryption
Send and receive encrypted email messages to people inside and outside your organization.

Microsoft Defender for Cloud Apps
A multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud service.

Purview Customer Key
Help meet compliance requirements by exercising control over your organization's encryption keys.

Purview Data Connectors
Apply various Microsoft Purview solutions to third-party data that has been imported and archived in Microsoft 365.

Purview Customer Lockbox
Maintain control over your content with explicit access authorization for service operations.

Purview Communication Compliance
Minimize communication risks by detecting, capturing, and taking remediation actions on inappropriate messages in your organization.

Purview Privileged Access Management
Help protect your organization from breaches through granular access control over privileged admin tasks.

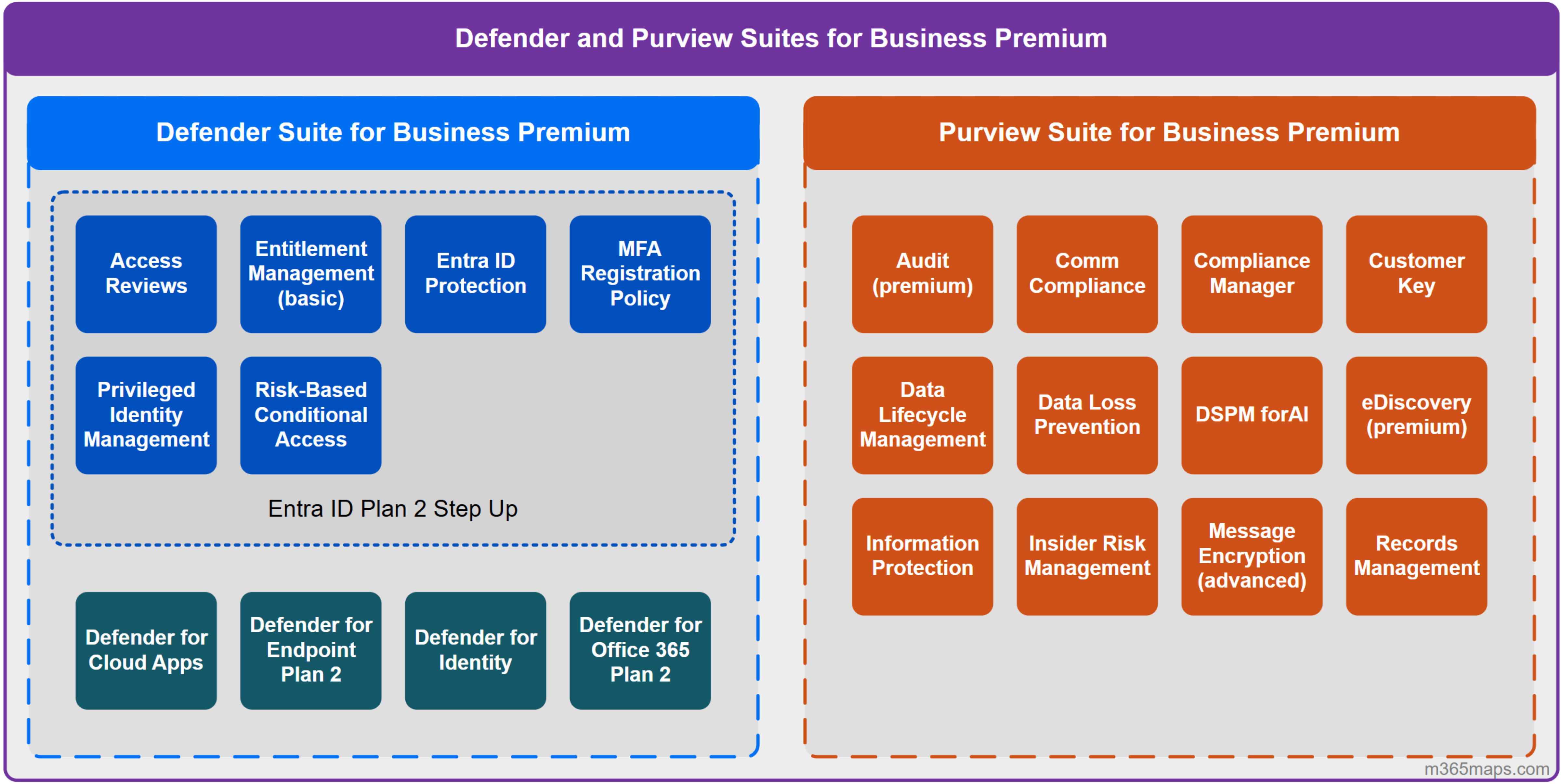
Purview Insider Risk Management
Detect, investigate, and take action on risky activities in your organization.

Purview Information Barriers
Restrict communications between specific groups of users inside your organization to safeguard internal information.

Purview eDiscovery (Premium)
Manage the end-to-end workflow of internal and external investigations.

Purview Audit (Premium)
Gain visibility with new auditing capabilities that help with forensic and compliance investigations.

Enterprise Security & Compliance Technologie now available for SMB!



Defender and Purview Suites for Business Premium

Defender Suite for Business Premium

- Access Reviews
- Entitlement Management (basic)
- Entra ID Protection
- MFA Registration Policy
- Privileged Identity Management
- Risk-Based Conditional Access

Entra ID Plan 2 Step Up

- Defender for Cloud Apps
- Defender for Endpoint Plan 2
- Defender for Identity
- Defender for Office 365 Plan 2

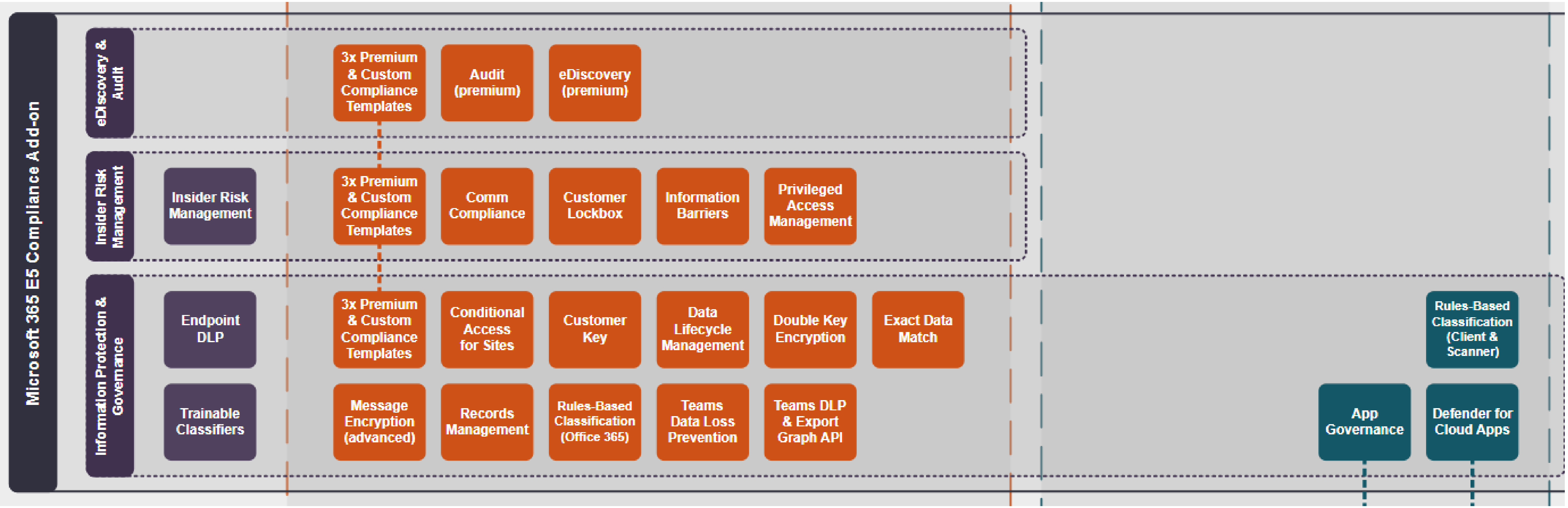
Purview Suite for Business Premium

- Audit (premium)
- Comm Compliance
- Compliance Manager
- Customer Key
- Data Lifecycle Management
- Data Loss Prevention
- DSPM forAI
- eDiscovery (premium)
- Information Protection
- Insider Risk Management
- Message Encryption (advanced)
- Records Management

m365maps.com

https://aka.ms/bp-map

Microsoft Purview Suite


Microsoft 365 E5 Compliance Add-on
eDiscovery & Audit
3x Premium & Custom Compliance Templates
Audit (premium)
eDiscovery (premium)
Insider Risk Management
Insider Risk Management
3x Premium & Custom Compliance Templates
Comm Compliance
Customer Lockbox
Information Barriers
Privileged Access Management
Information Protection & Governance
Endpoint DLP
3x Premium & Custom Compliance Templates
Conditional Access for Sites
Customer Key
Data Lifecycle Management
Double Key Encryption
Exact Data Match
Rules-Based Classification (Client & Scanner)
Trainable Classifiers
Message Encryption (advanced)
Records Management
Rules-Based Classification (Office 365)
Teams Data Loss Prevention
Teams DLP & Export Graph API
App Governance
Defender for Cloud Apps

[Microsoft 365 E5 | M365 Maps]

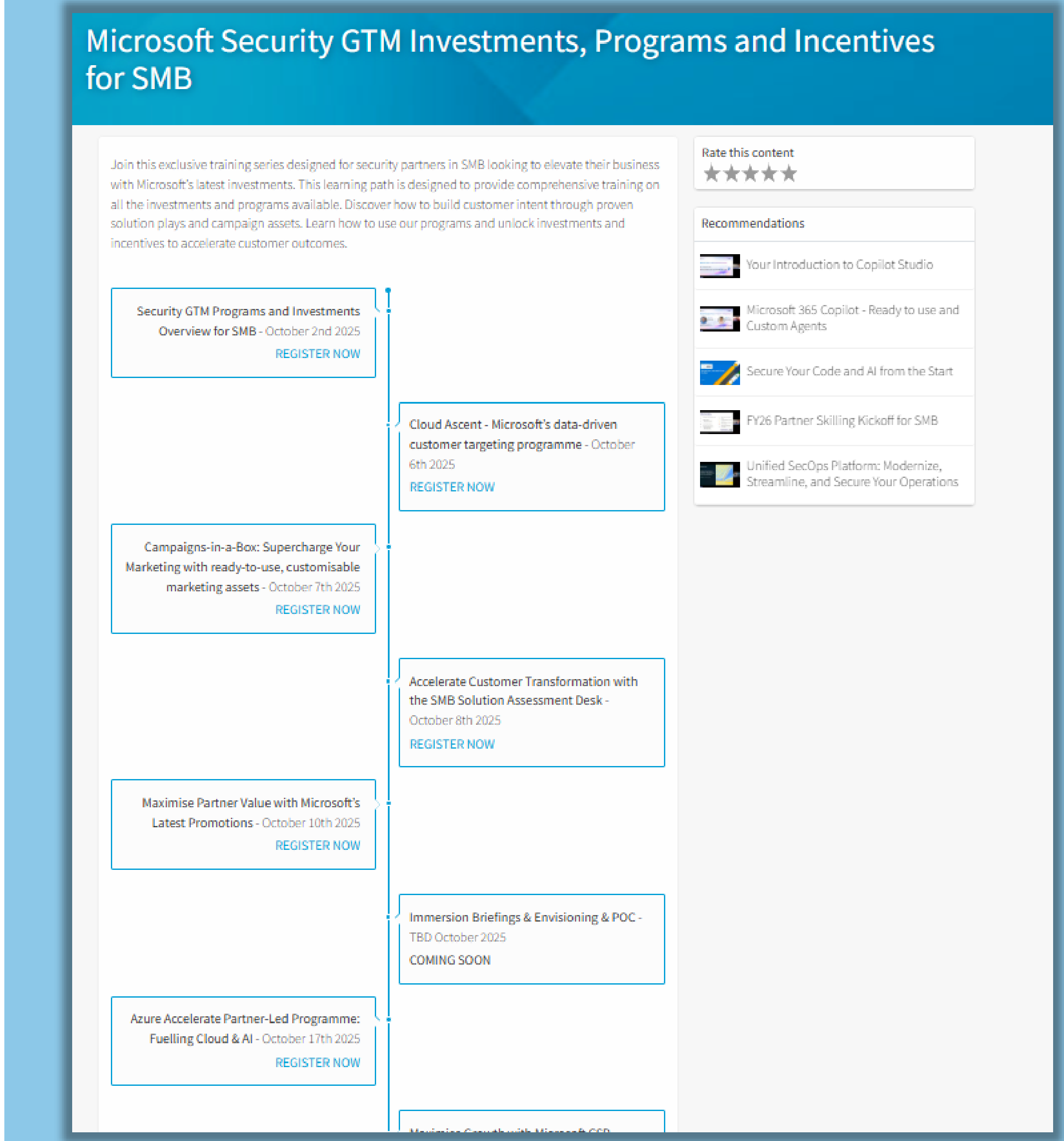
Microsoft Security SMB GTM Learning path

Join us to explore the various Microsoft investments, programs and resources to help you build differentiated practices and deliver impactful customer outcomes.

Register Now!

[Microsoft Security SMB GTM Learning Path](https://www.cloudchampion.co/c/microsoft-security-gtm-investments-programs-and-incentives-for-smb/)

https://www.cloudchampion.co/c/microsoft-security-gtm-investments-programs-and-incentives-for-smb/



Microsoft Security GTM Investments, Programs and Incentives for SMB

Join this exclusive training series designed for security partners in SMB looking to elevate their business with Microsoft's latest investments. This learning path is designed to provide comprehensive training on all the investments and programs available. Discover how to build customer intent through proven solution plays and campaign assets. Learn how to use our programs and unlock investments and incentives to accelerate customer outcomes.

Security GTM Programs and Investments Overview for SMB - October 2nd 2025
REGISTER NOW

Cloud Ascent - Microsoft's data-driven customer targeting programme - October 6th 2025
REGISTER NOW

Campaigns-in-a-Box: Supercharge Your Marketing with ready-to-use, customisable marketing assets - October 7th 2025
REGISTER NOW

Accelerate Customer Transformation with the SMB Solution Assessment Desk - October 8th 2025
REGISTER NOW

Maximise Partner Value with Microsoft's Latest Promotions - October 10th 2025
REGISTER NOW

Immersion Briefings & Envisioning & POC - TBD October 2025
COMING SOON

Azure Accelerate Partner-Led Programme: Fuelling Cloud & AI - October 17th 2025
REGISTER NOW

Maximise Growth with Microsoft CSP

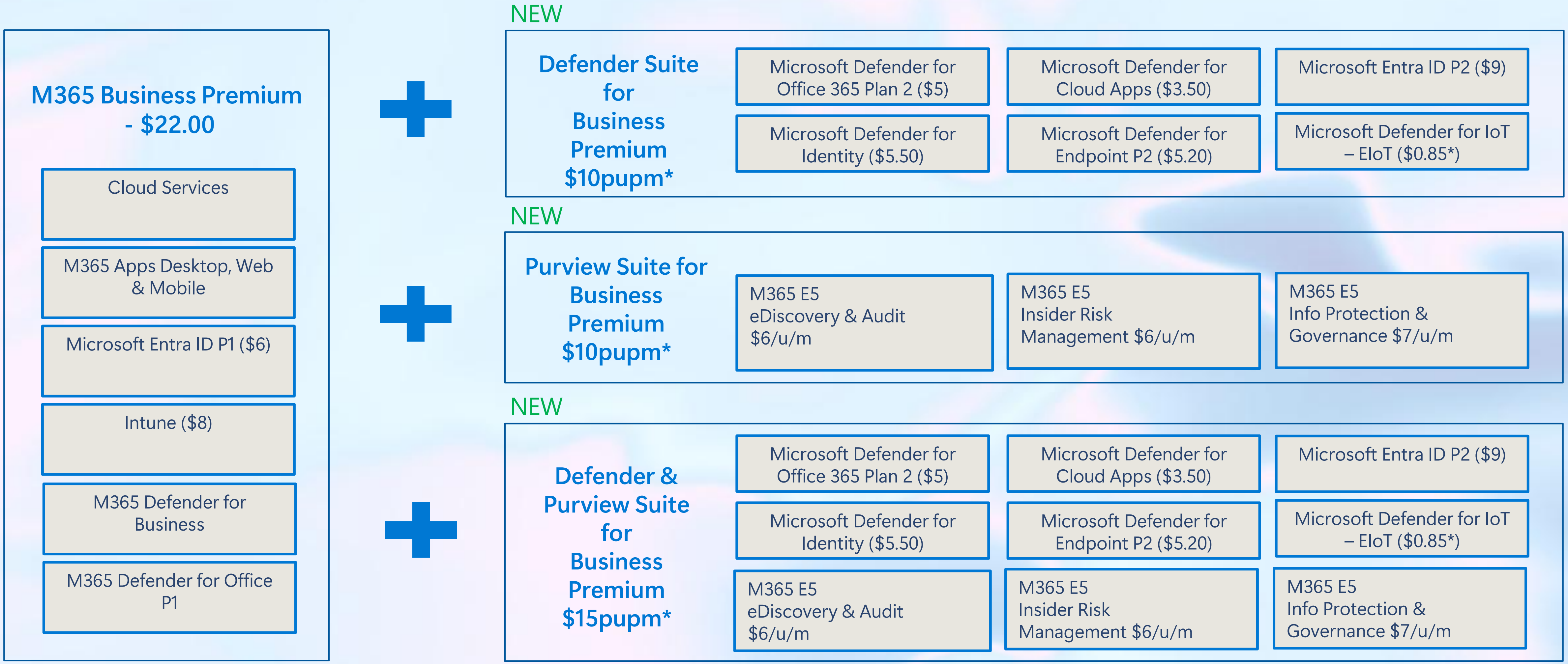
Rate this content
★★★★★

Recommendations

- Your Introduction to Copilot Studio
- Microsoft 365 Copilot - Ready to use and Custom Agents
- Secure Your Code and AI from the Start
- FY26 Partner Skilling Kickoff for SMB
- Unified SecOps Platform: Modernize, Streamline, and Secure Your Operations

Microsoft Security

Defender/Purview Suite for Business Premium



M365 Business Premium - $22.00

- Cloud Services
- M365 Apps Desktop, Web & Mobile
- Microsoft Entra ID P1 ($6)
- Intune ($8)
- M365 Defender for Business
- M365 Defender for Office P1

+

NEW

Defender Suite for Business Premium $10pupm*

- Microsoft Defender for Office 365 Plan 2 ($5)
- Microsoft Defender for Cloud Apps ($3.50)
- Microsoft Entra ID P2 ($9)
- Microsoft Defender for Identity ($5.50)
- Microsoft Defender for Endpoint P2 ($5.20)
- Microsoft Defender for IoT – EIoT ($0.85*)

+

NEW

Purview Suite for Business Premium $10pupm*

- M365 E5 eDiscovery & Audit $6/u/m
- M365 E5 Insider Risk Management $6/u/m
- M365 E5 Info Protection & Governance $7/u/m

+

NEW

Defender & Purview Suite for Business Premium $15pupm*

- Microsoft Defender for Office 365 Plan 2 ($5)
- Microsoft Defender for Cloud Apps ($3.50)
- Microsoft Entra ID P2 ($9)
- Microsoft Defender for Identity ($5.50)
- Microsoft Defender for Endpoint P2 ($5.20)
- Microsoft Defender for IoT – EIoT ($0.85*)
- M365 E5 eDiscovery & Audit $6/u/m
- M365 E5 Insider Risk Management $6/u/m
- M365 E5 Info Protection & Governance $7/u/m

Partner-to-customers OFT https://aka.ms/SMB-SKUs-CustomerOFT
Partner Center Announcement – Partner Center announcements - Partner Center announcements | Microsoft Learn
Tech Community Blog- Introducing new security and compliance add-ons for Microsoft 365 Business Premium | Microsoft Co...

*CSP List Price

Microsoft Security SMB Hero Offerings

SMB MID MARKET

CAPPED AT 300 USERS

BUSINESS PREMIUM

Advanced Endpoint protection | AIR, Endpoint Detection & Response, Attack Surface reduction

Advanced Device Management | Mobile/ App Management and Endpoint Security policies

Identity Protection | SSO, MFA, Conditional Access and Password Reset

Email Security | Anti-Spam/Malware/Phishing protection

Information Protection | Manual sensitivity labelling, DLP for email/files

$22 user/month

DEFENDER SUITE FOR BP

Advanced Endpoint protection (in addition to BP, includes Threat Hunting and Threat Experts)

Advanced Identity Protection | Risk-based Conditional Access, User Risk Detection, PIM

Advanced Email & Collaboration Security | Advanced anti-phishing, AIR, Attack Simulation and Threat Explorer

Advanced Apps & Cloud security | Shadow IT Control & Real-Time Threat Protection

$10 user/month

PURVIEW SUITE FOR BP

Advanced Information Protection & Governance | Automated Sensitivity Labelling, Endpoint & Teams DLP and Data Lifecycle management

Insider Risk Management | Privileged Access Management & information barriers

Advanced eDiscovery | eDiscovery & Audit Premium

$10 user/month

$15 user/month when bundled together

SMB UPPER MEDIUM MARKET

NO USER LIMITATION

M365 E3

Endpoint protection | Antivirus, Device Guard, Credential Guard, basic EDR (no AIR)

Advanced Device Management | Windows Autopilot, Conditional Access, Advanced Policy Controls

Identity Protection | Advanced Identity Gov, SSO, MFA, Conditional Access and Password Reset

Email Security | Anti-Spam/Malware/Phishing protection

Information Protection | Manual sensitivity labelling, DLP for email/files, BYOK

$36 user/month

E5 SECURITY

Advanced Endpoint protection | AIR, Endpoint Detection & Response, Attack Surface reduction, Threat Hunting/Experts

Advanced Identity Protection | Risk-based Conditional Access, User Risk Detection, PIM

Advanced Email & Collaboration Security | Advanced anti-phishing, AIR, Attack Simulation and Threat Explorer

Advanced Apps & Cloud security | Shadow IT Control & Real-Time Threat Protection

$12 user/month

E5 COMPLIANCE

Advanced Information Protection & Governance | Automated Sensitivity Labelling, Endpoint & Teams DLP and Data Lifecycle management

Insider Risk Management | Privileged Access Management & information barriers

Advanced eDiscovery | eDiscovery & Audit Premium

$12 user/month

$57 user/month when bundled together (M365 E5)

Leaves organizations on the back foot to protect data

External risks

User falls prey to phishing attack, compromises user credentials

Data compromise
by external threat

Internal risks

User copies file to a USB, then uploads to a personal Dropbox to take to a competitor

Data theft
by malicious insider

User negligently shares sensitive data in generative AI apps

Data leak
by negligent insider

User deletes sensitive information before leaving the organization

Data sabotage
by disgruntled insider

…and impedes effective compliance practices

I need to **manage…**

…investigations across data silos, tools, and teams.

…privacy with manual tools and solutions.

…compliance at scale with increasing regulatory requirements.

…litigation and privacy with limited staff and resources.

I need to **mitigate risk…**

…related to:

Data protection

Data privacy

Regulatory compliance

Litigation

I need to **transform…**

…how I identify and manage data loss and compliance risks from reactively to proactively.

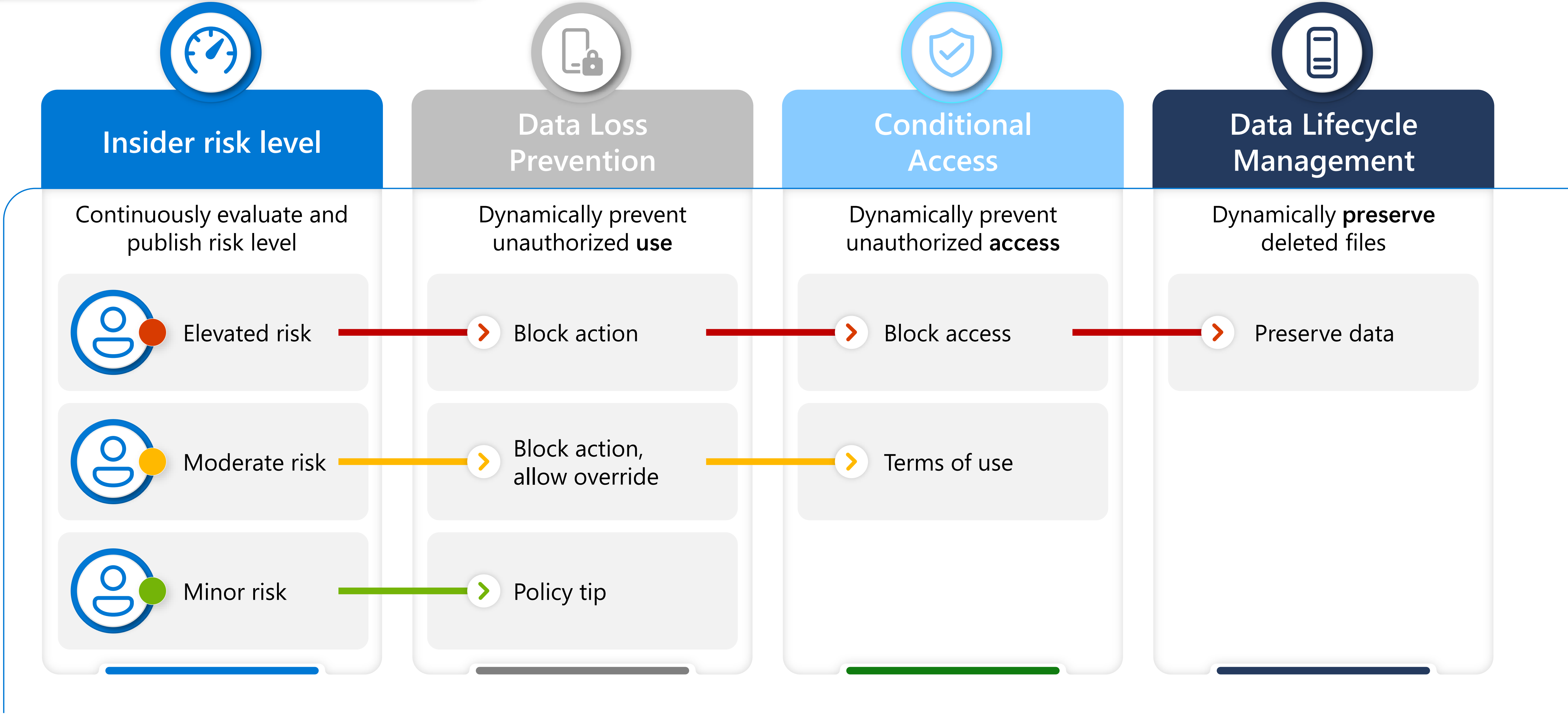
…data discovery from a survey-based approach to AI/ML- powered discovery.

…complex manual workflows to streamline audit compliance.

…Legal, Compliance, and Privacy teams from cost centers to delivering business value.

Effective data protection removes silos + takes action

Microsoft Purview offers...



Insider risk level	Data Loss Prevention	Conditional Access	Data Lifecycle Management
Continuously evaluate and publish risk level	Dynamically prevent unauthorized **use**	Dynamically prevent unauthorized **access**	Dynamically **preserve** deleted files
Elevated risk	Block action	Block access	Preserve data
Moderate risk	Block action, allow override	Terms of use	
Minor risk	Policy tip		

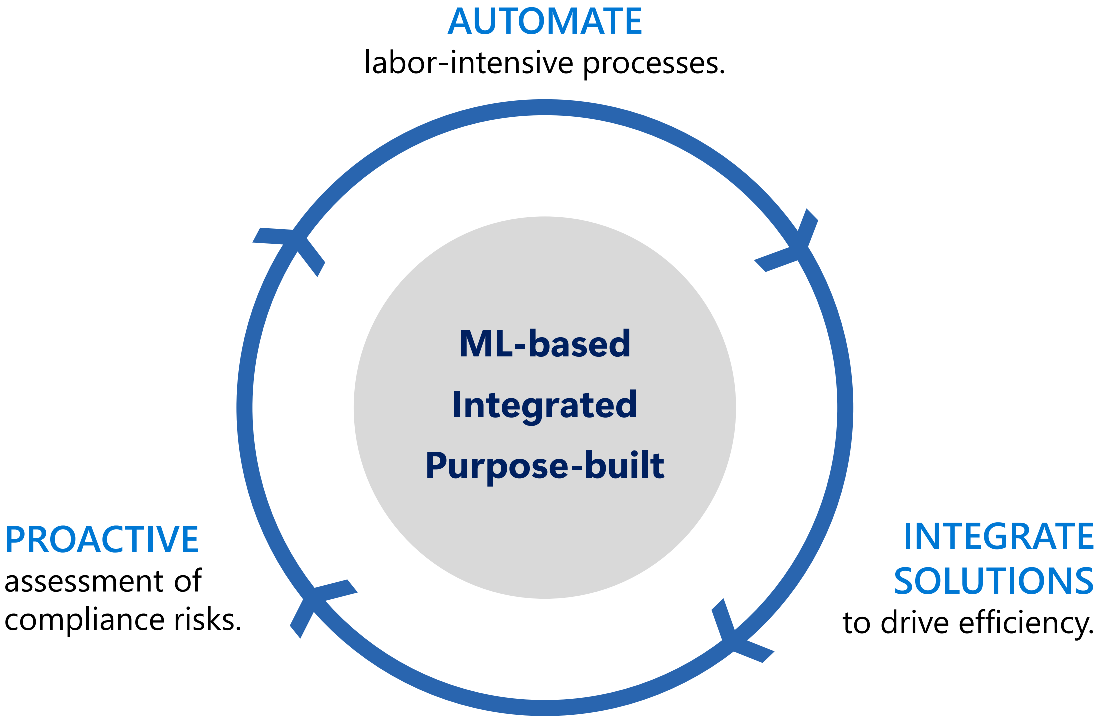
…and overlays with intelligent tooling to support compliance requirements

Your needs…

Data privacy

Regulatory compliance

Litigation



AUTOMATE
labor-intensive processes.

INTEGRATE SOLUTIONS
to drive efficiency.

PROACTIVE
assessment of
compliance risks.

ML-based
Integrated
Purpose-built

Purview solutions…

Data Lifecycle Management

Compliance Manager

Audit + eDiscovery

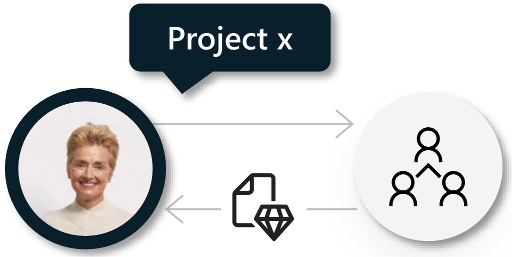
Integrated into Microsoft Purview

Challenges with GenAI proliferation compound risks

1

Data oversharing

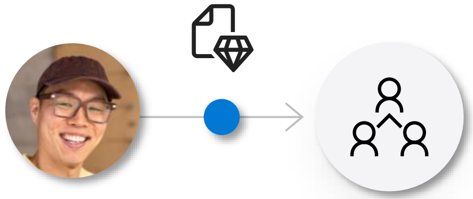
Users might access sensitive data through AI apps without proper authorization



2

Data leak

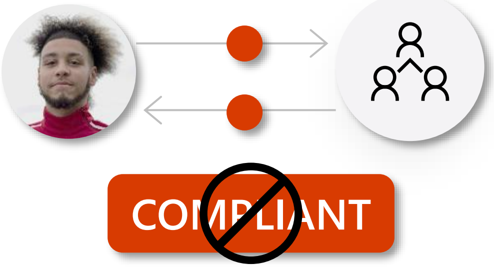
Users may inadvertently leak sensitive data to AI apps



3

Non-compliant usage

Users might use AI apps to generate unethical or other high-risk content



Secure and govern Microsoft 365 Copilot data

Security + Compliance + Privacy + Responsible AI

Discover risks

Identify sensitive data used in Copilot with **Data Security Posture Management for AI**

Get alerted to risky Copilot use with **Communication Compliance**

Detect a sequence of risky user actions with **Insider Risk Management**

Protect data

Detect when content contains sensitive data and auto-apply protections with **Information Protection**

Block Copilot access to sensitive files with **Data Loss Prevention**

Automatically adjust security policies based on a user's risk level with **Adaptive Protection**

Govern usage

Audit Copilot interactions and enforce lifecycle policies with **Audit** and **Data Lifecycle Management**

Assess and track adherence to regulatory frameworks with **Compliance Manager**

Include Copilot interactions in investigations and legal holds with **eDiscovery**

Purpose-built into Microsoft Purview

A tale of corporate espionage

Trusted employee, Jane Doe, used stolen proprietary information to start her own company

Jane Doe

Principal/Manager in two Fortune 500 companies leveraging her privileged title for 5+ years

- Collected proprietary info from multiple companies leveraging her privileged title.
- Attempted to copy the info to an external hard drive but was blocked by the DLP policy at Company A.
- She found a loophole and uploaded sensitive content to her personal cloud storage at both companies.
- She copied those files from the cloud storage to an external hard drive at Company B.
- Had inappropriate conversations and threatened her peers to hide her tracks.
- Suspected that one of her peers would report and tried to delete the sensitive information.
- She was terminated from both companies and her hard drive underwent an authority investigation.

- Companies didn't have visibility into sensitive data
- DLP didn’t flag the repeated offender
- The granted collaboration was abused
- Inappropriate behavior was not flagged
- Sensitive data was not preserved

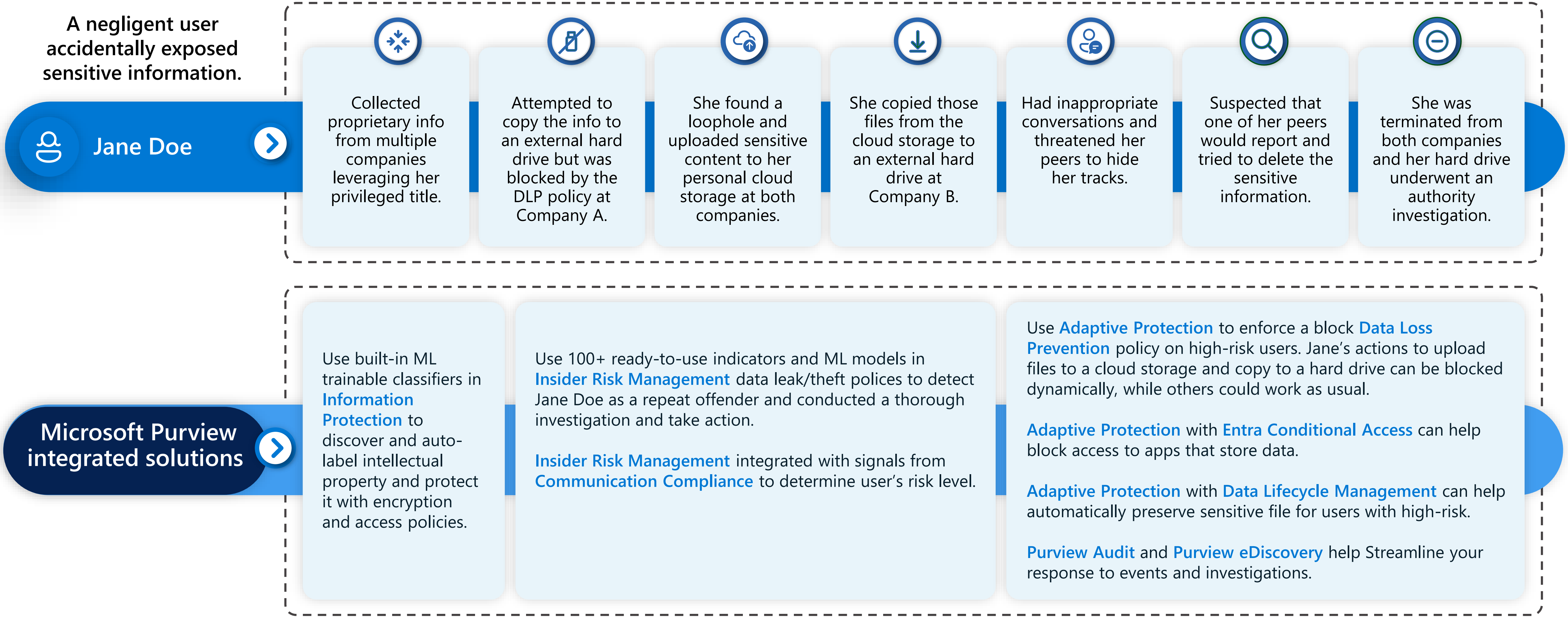
Outcome

Convicted felon

Jane was convicted and charged with wire fraud, economic espionage, and trade secret theft for collecting trade secret information to apply for foreign government funds and attempting to start her own company.

The intellectual property **cost companies over $100 million** to develop.

How Purview delivers actionable protection



A negligent user accidentally exposed sensitive information.

Jane Doe

Collected proprietary info from multiple companies leveraging her privileged title.

Attempted to copy the info to an external hard drive but was blocked by the DLP policy at Company A.

She found a loophole and uploaded sensitive content to her personal cloud storage at both companies.

She copied those files from the cloud storage to an external hard drive at Company B.

Had inappropriate conversations and threatened her peers to hide her tracks.

Suspected that one of her peers would report and tried to delete the sensitive information.

She was terminated from both companies and her hard drive underwent an authority investigation.

Microsoft Purview integrated solutions

Use built-in ML trainable classifiers in Information Protection to discover and auto-label intellectual property and protect it with encryption and access policies.

Use 100+ ready-to-use indicators and ML models in Insider Risk Management data leak/theft polices to detect Jane Doe as a repeat offender and conducted a thorough investigation and take action.

Insider Risk Management integrated with signals from Communication Compliance to determine user's risk level.

Use Adaptive Protection to enforce a block Data Loss Prevention policy on high-risk users. Jane's actions to upload files to a cloud storage and copy to a hard drive can be blocked dynamically, while others could work as usual.

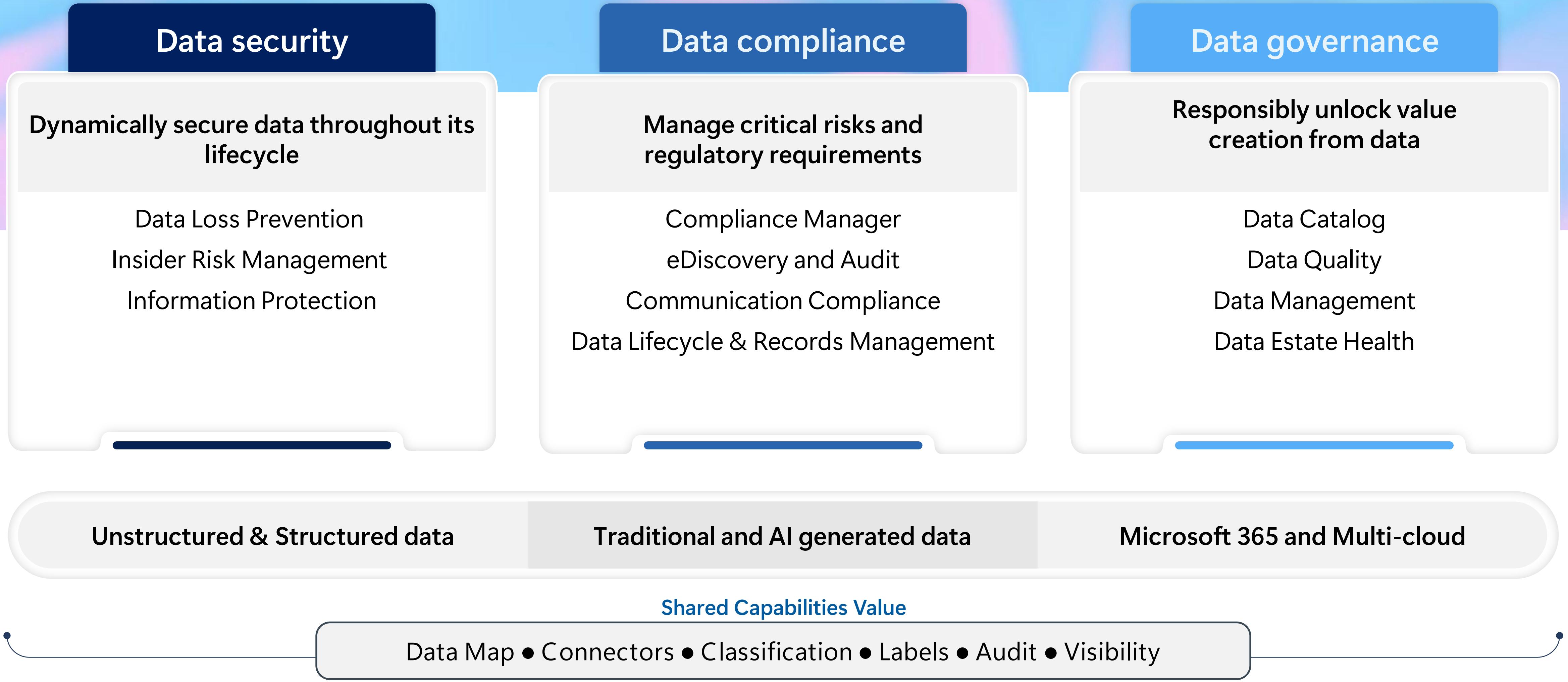
Adaptive Protection with Entra Conditional Access can help block access to apps that store data.

Adaptive Protection with Data Lifecycle Management can help automatically preserve sensitive file for users with high-risk.

Purview Audit and Purview eDiscovery help Streamline your response to events and investigations.

Microsoft Purview

Secure and govern data for the era of AI



Data security

Dynamically secure data throughout its lifecycle

Data Loss Prevention

Insider Risk Management

Information Protection

Data compliance

Manage critical risks and regulatory requirements

Compliance Manager

eDiscovery and Audit

Communication Compliance

Data Lifecycle & Records Management

Data governance

Responsibly unlock value creation from data

Data Catalog

Data Quality

Data Management

Data Estate Health

Unstructured & Structured data | **Traditional and AI generated data** | **Microsoft 365 and Multi-cloud**

Shared Capabilities Value

Data Map ● Connectors ● Classification ● Labels ● Audit ● Visibility

Microsoft Purview

Secure and govern data for the era of AI

Available for M365 data in a single offer

Data security

Dynamically secure data throughout its lifecycle

Data Loss Prevention

Insider Risk Management

Information Protection

Data compliance

Manage critical risks and regulatory requirements

Compliance Manager

eDiscovery and Audit

Communication Compliance

Data Lifecycle & Records Management

Data governance

Responsibly unlock value creation from data

Data Catalog

Data Quality

Data Management

Data Estate Health

Unstructured & Structured data | **Traditional and AI generated data** | **Microsoft 365 and Multi-cloud**

Shared Capabilities Value

Data Map ● Connectors ● Classification ● Labels ● Audit ● Visibility

Microsoft Purview via M365 Purview Suite

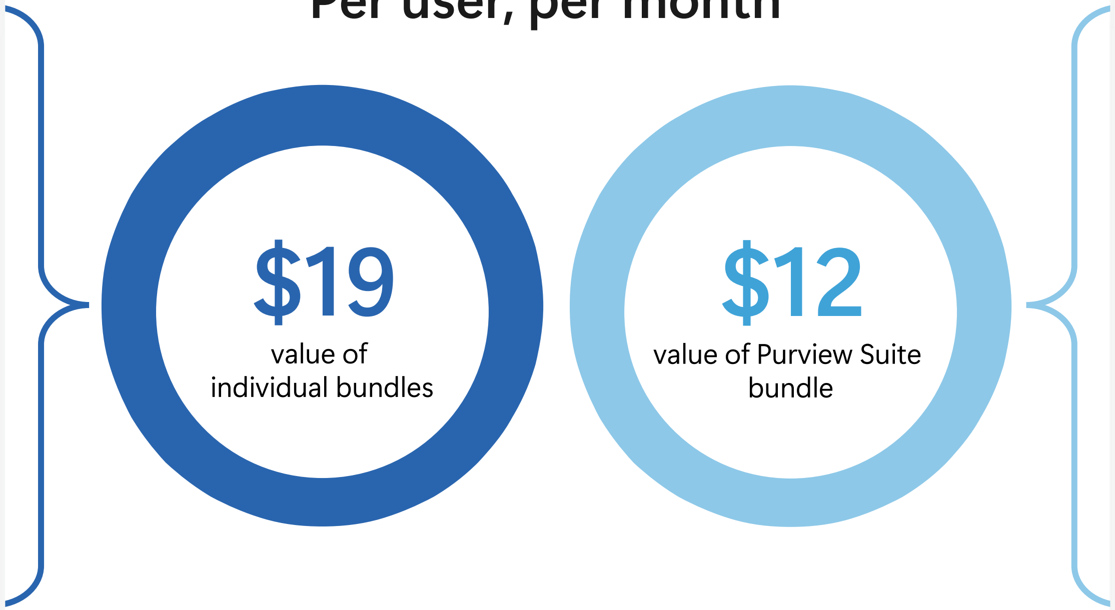
- Effective data protection that removes silos and takes action to ensure data security
- Intelligent tooling supports more efficient data and regulatory compliance
- Purpose-built innovation helps safeguard Microsoft 365 Copilot data

Microsoft Purview

Standalone bundles

Information Protection + Governance Data Loss Prevention Information Protection Data Lifecycle Management ...and more	$7
Insider Risk Mgmt. Insider Risk Management Communication Compliance Privileged Access Management ...and more	$6
eDiscovery + Audit eDiscovery (Premium) Audit (Premium)	$6
Add on Compliance Manager	$8,500 per template

Per user, per month



$19

value of individual bundles

$12

value of Purview Suite bundle

Microsoft 365 Purview Suite

Save ~36% per license

- Enable end-to-end data security + compliance
- Prepare for GenAI + regulatory requirements

*Prices are USD list and per user, per month. Prices may vary by region, currency, and customer pricing agreements.

Prepare for AI with O365 E3 + EMS E3 + Purview Suite

Office 365 E3 + EMS E3

Data Security + Compliance

Built for organizations **with low data risk** and regulatory requirements and **unlikely to activate GenAI** apps

Microsoft 365 Purview Suite

Data Security + Compliance

Built for organizations subject to **higher data risk** and regulatory requirements and **activating GenAI** apps

Prepare for AI with O365 E3 + EMS E3 + Purview

Office 365 E3 + EMS E3

Data Security + Compliance

Built for organizations with low data risk and regulatory requirements and unlikely to activate GenAI apps

- Standard **Conditional Access** based on predefined conditions like device compliance, location, and app sensitivity.
- Basic **endpoint security**, including anti-virus and firewall features, and device compliance policies
- Manual **Information Protection** to classify, label, and protect sensitive data, **lacks automated discovery + protection**
- **Data Loss Prevention (DLP)** policies to monitor and protect how information is shared, **limited to M365 emails + files**.
- **Manual data lifecycle management** retention labels and basic org-wide or location-wide retention policies
- eDiscovery basic search and export and ability to create a case and limited Audit with **180-day maximum retention** and **no ability to apply retention policies**.
- **No customer key which is required for most regulatory** and compliance requirements.

+

Microsoft 365 Purview Suite

Data Security + Compliance

Built for organizations subject to higher data risk and regulatory requirements and activating GenAI apps

- **Protect Microsoft 365 Copilot data** from accidental oversharing, data leaks, or non-compliance usage.
- **Get visibility into critical data security risks and recommended protection controls** with Data Security Posture Management (DSPM) and DSPM for AI.
- **Automatically discover, classify and label sensitive data**, and **prevent its unauthorized use** across apps, services, and devices with integrated Information Protection and DLP
- **Understand user intent** around use of sensitive data and **defend against insider risks** with Insider Risk Management and Adaptive Protection to automatically adapt policies based on risk level.
- Drive **adherence to common industry and regional regs** (eg EU AI Act, ISO, etc) with pre-built templates in Compliance Manager
- Streamline your response to events and investigations with **Audit retention policies, up to 10-years retention**, and Audit insights while **eDiscovery** workflows, export, custodian mgmt., tagging, ML-based capabilities and analytics **drive investigation efficiencies**.

Together, AI-ready

Value Comparison

O365 E3 + EMS vs Purview Suite

Customer value	O365 E3 + EMS E3	Purview Suite
Access and Endpoints		
Standard conditional access, multi-factor authentication, Entra ID Plan1, and endpoint security basics	✓	-
Data Security		
Data Loss Prevention (DLP) to monitor and protect sensitive information	O365 Emails + files	M365 Emails, files, Teams chat, endpoints
Information Protection for manual, default, and mandatory sensitivity labeling in M365 apps	✓	✓
Automatically discover, classify and label sensitive data, and prevent its unauthorized use across apps, services, and devices with integrated Information Protection and DLP	-	✓
Understand the user intent and context around the use of sensitive data to identify the most critical risks w/ Insider Risk Management which provides 100+ ready-to-use indicators and ML models	-	✓
Enable Adaptive Protection which automatically learns and assigns high-risk users appropriate DLP, DLM, and Entra Conditional Access policies to prevent loss as risky behaviors rise.	-	✓
Data Compliance		
Manual Data Lifecycle Management (DLM) retention labels and policies	✓	✓
Support regulatory requirements with Rules- and ML-based DLM retention policies and Records Mgmt.	-	✓
eDiscovery basic search and export and ability to create a case.	✓	✓
eDiscovery premium workflows, export, custodian mgmt., tagging, ML-based models to drive investigation efficiencies, and analytics.	-	✓
Audit default enabled, search UX/APIs, export	✓	✓
Effectively respond to security events and investigations with Audit, incl log retention + retention policies	180-days, no policies	180-d, 1-yr, 10-yr, policies
Communication Compliance automatically flags non-compliant employee comms	-	✓
Compliance Manager streamlines adherence to common industry and regional regs (eg EU AI Act, ISO, etc)	$8500 / template	3 templates
Privileged Access Management	-	✓

APPENDIX

Reduce costs while reducing risks

Up to **60%** savings[1]

46% ROI over three years[2]

Protect sensitive data throughout its lifecycle

85%

Less time spent identifying, classifying and labeling sensitive data with automation and AI

Understand user activity context around the data and identify risks

96%

Less time spent detecting potential suspicious activity

Prevent data from unauthorized use across apps, services, and devices

30-40%

Reduced risk of breach reduced costs by

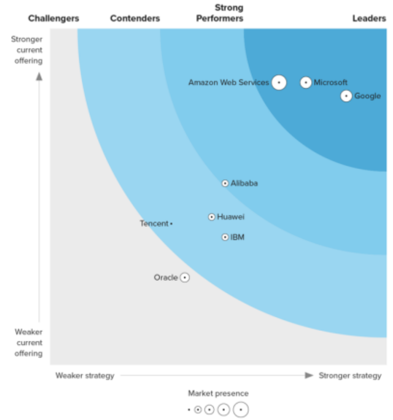
40-50%

Savings based on publicly available estimated pricing for other vendor solutions and Web Direct/Base Price shown for Microsoft offerings, comparing the cost of comparable third-party solutions to the cost of moving from Microsoft 365 E3 to Microsoft 365 Purview Suite.

Forrester Consulting, "The Total Economic Impact Of Microsoft 365 E5 Compliance," June, 2021, commissioned by Microsoft

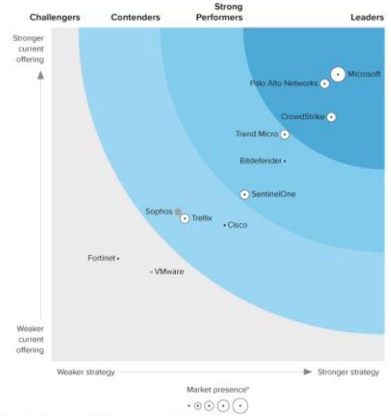
Microsoft – a leader in nine Forrester Wave™ reports

THE FORRESTER WAVE™
Infrastructure-As-A-Service Platform Native Security
Q2 2023



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

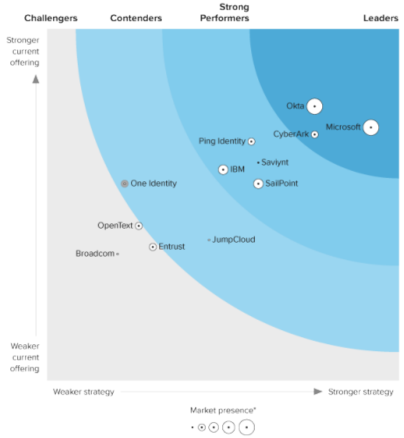
THE FORRESTER WAVE™
Extended Detection And Response Platforms
Q2 2024



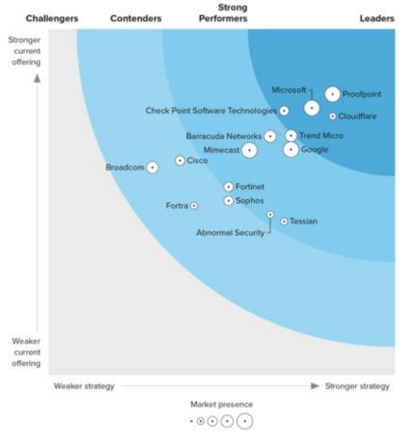
*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

THE FORRESTER WAVE™
Workforce Identity Platforms
Q1 2024

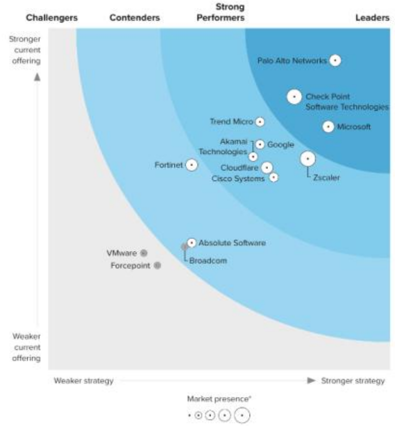


THE FORRESTER WAVE™
Enterprise Email Security
Q2 2023

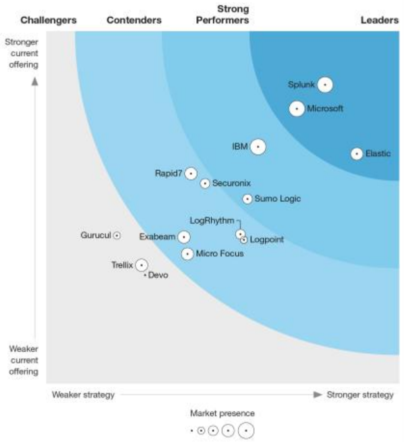


Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

THE FORRESTER WAVE™
Zero Trust Platforms
Q3 2023

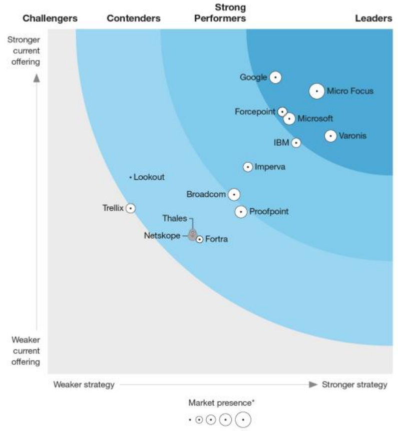


THE FORRESTER WAVE™
Security Analytics Platforms
Q4 2022



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

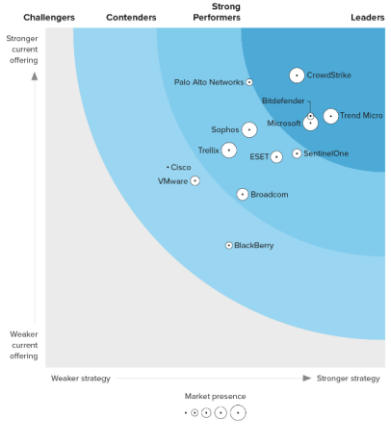
THE FORRESTER WAVE™
Data Security Platforms
Q1 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

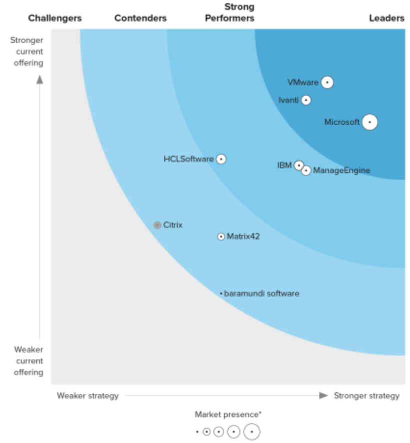
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

THE FORRESTER WAVE™
Endpoint Security
Q4 2023



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

THE FORRESTER WAVE™
Unified Endpoint Management
Q4 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

The Forrester New Wave™: Extended Detection And Response Platforms,

The Forrester Wave™: Workforce Identity Platforms,

The Forrester Wave™: Enterprise Email Security,

The Forrester Wave™: Security Analytics Platforms,

The Forrester Wave™: Infrastructure-As-A-Service Platform Native Security,

The Forrester Wave™: Data Security Platforms,

The Forrester Wave™: Zero Trust Platform Providers,

The Forrester Wave™: Endpoint Security,

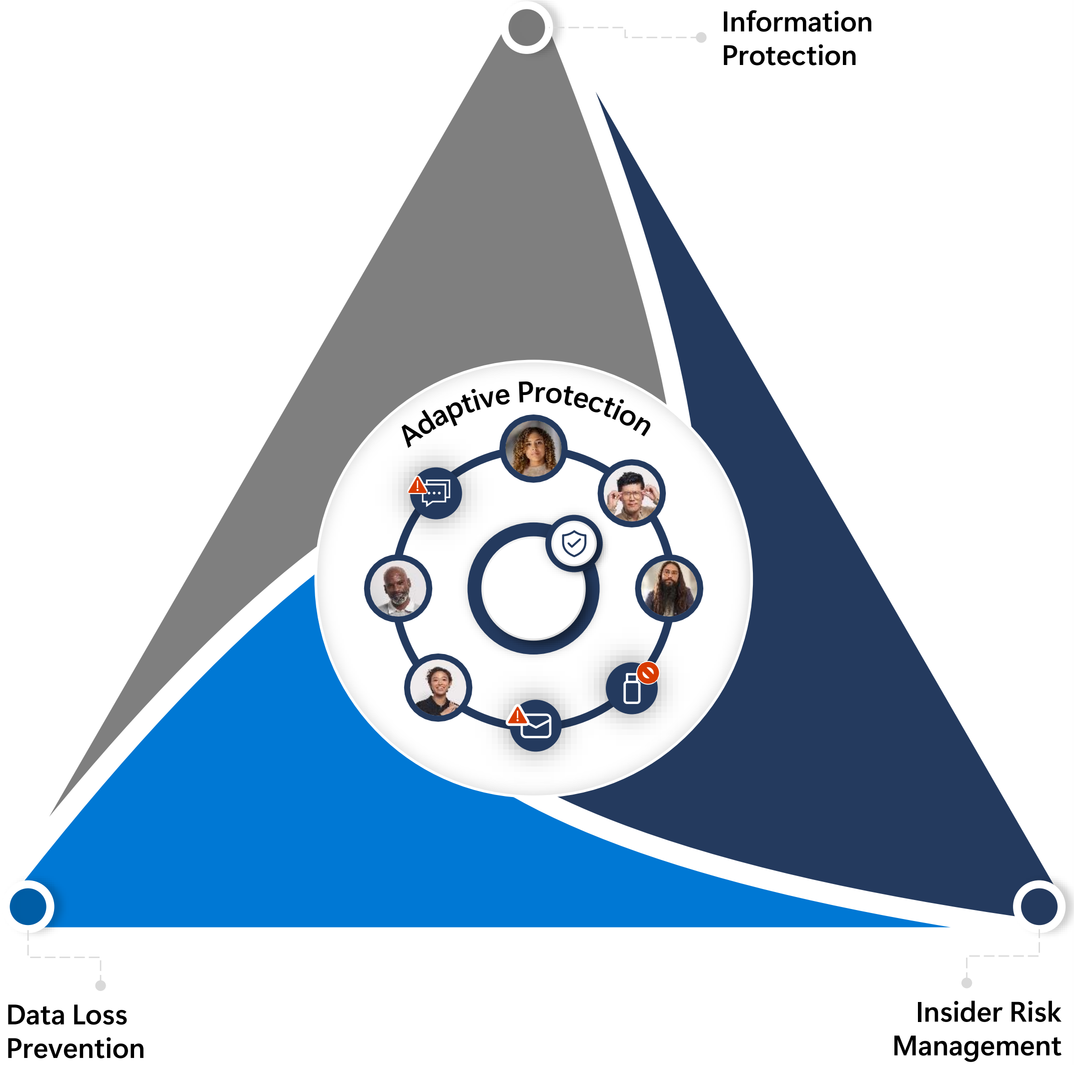
The Forrester Wave™: Unified Endpoint Management,

Fortify data security with an integrated approach

Automatically **discover, classify and label sensitive** data, and **prevent its unauthorized use** across apps, services, and devices.

Understand the **user intent and context around the use of sensitive data** to identify the most critical risks

Enable **Adaptive Protection** to assign high-risk users to appropriate DLP, Data Lifecycle Management, and Entra Conditional Access policies



Support for all data – hybrid, Cloud, SaaS, and devices | Partner ecosystem