Enabling a whole new way to work

Build a foundation of secure productivity to get AI-ready

Μπότας Ανδρέας
Σύμβουλος στρατηγικής τεχνολογίας
&
Δημήτρης Πατσός
Ειδικός Κυβερνοασφάλειας

Three steps to achieve foundational productivity with Microsoft 365

Cut through complexity and get to the new era of work

With Microsoft 365

1 **Set up a strong Zero Trust foundation**
Verify explicitly, use least privilege access, and assume breach

2 **Streamline endpoint management**
Protect, manage and support all endpoints and apps

3 **Drive productivity and collaboration**
Improve productivity and foster a culture of collaboration with connected experiences

Three steps and products to achieve foundational productivity with Microsoft 365 and Copilot

Cut through complexity and get to the new era of work

With Microsoft 365

1 **Set up a strong Zero Trust foundation**
Microsoft Entra ID | Microsoft Defender | Microsoft Purview Information Protection

2 **Streamline endpoint management**
Windows 11 Enterprise | Microsoft Intune | Windows Autopatch | Universal Print

3 **Drive productivity and collaboration**
Microsoft Teams | Word | Excel | PowerPoint | Loop | Outlook | Planner
Exchange Online | SharePoint Online | Microsoft Viva

Elevate productivity with Microsoft 365 Copilot

Microsoft 365
The journey to a new way of working

Set Up a Strong Zero Trust Foundation

Secure and manage identities

Defend against threats on multi platforms

Protect sensitive information across data estate

Streamline Endpoint Management

Improve IT efficiency

Manage and protect any endpoint

Deliver the best experience with Windows 11

Drive Productivity and Collaboration

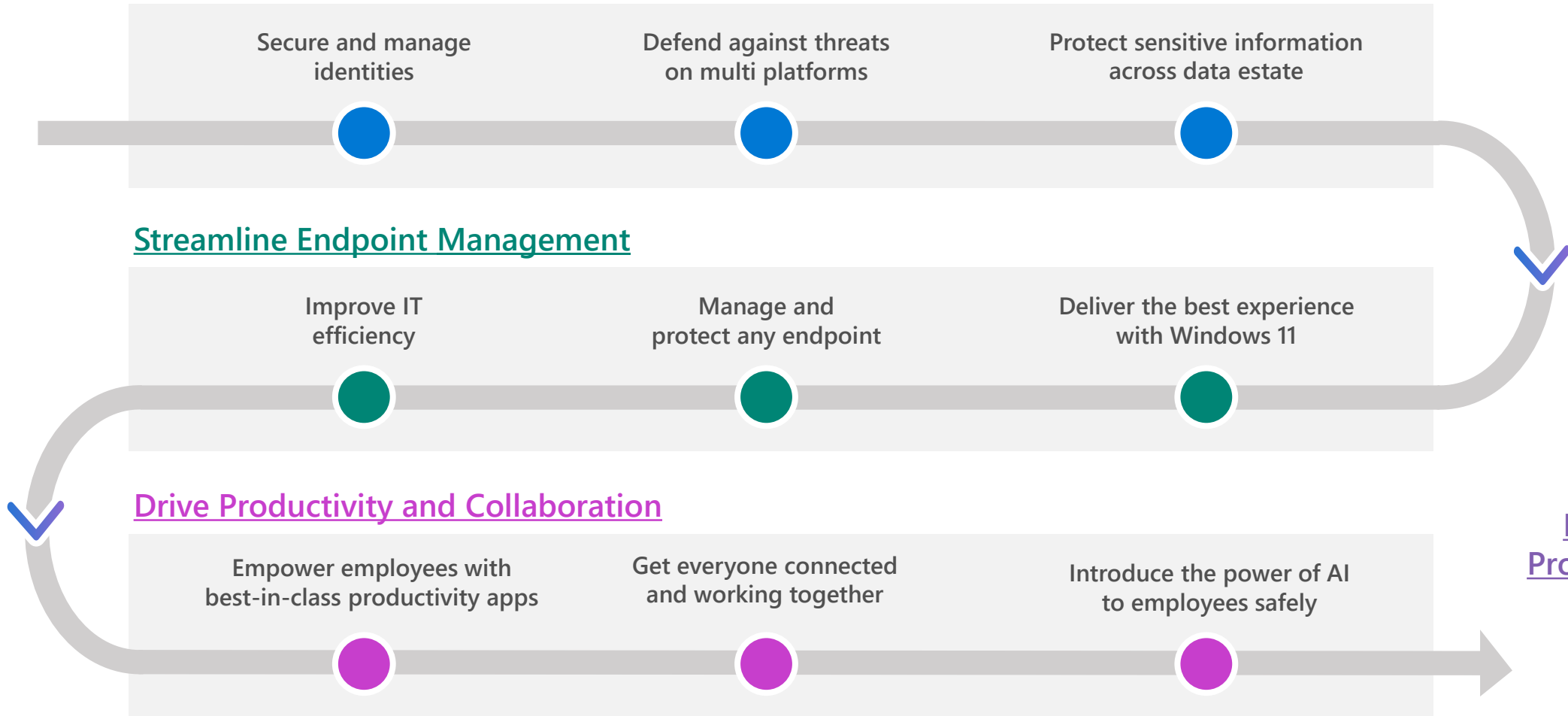Empower employees with best-in-class productivity apps

Get everyone connected and working together

Introduce the power of AI to employees safely

Elevate Productivity with

Copilot for Microsoft 365

Productivity and Collaboration
for today's digitally connected and distributed workforce

Get everyone connected and working together

Enable new patterns of work

Engage and empower your employees

Microsoft Teams, Exchange Online, Sharepoint Online, OneDrive for Business

Word, Excel, PowerPoint, Outlook

**Viva Insights in Teams
Viva Learning in Teams**

Get everyone connected and working together

1 **Connect and empower everyone** wherever, whenever they are

2 **Designed for all types of workers** from information workers to the frontline

3 **Chat, meet, collaborate, brainstorm** in one place without context switching

4 **Help ensure participants can be seen**, heard, and participate from anywhere

Microsoft Teams
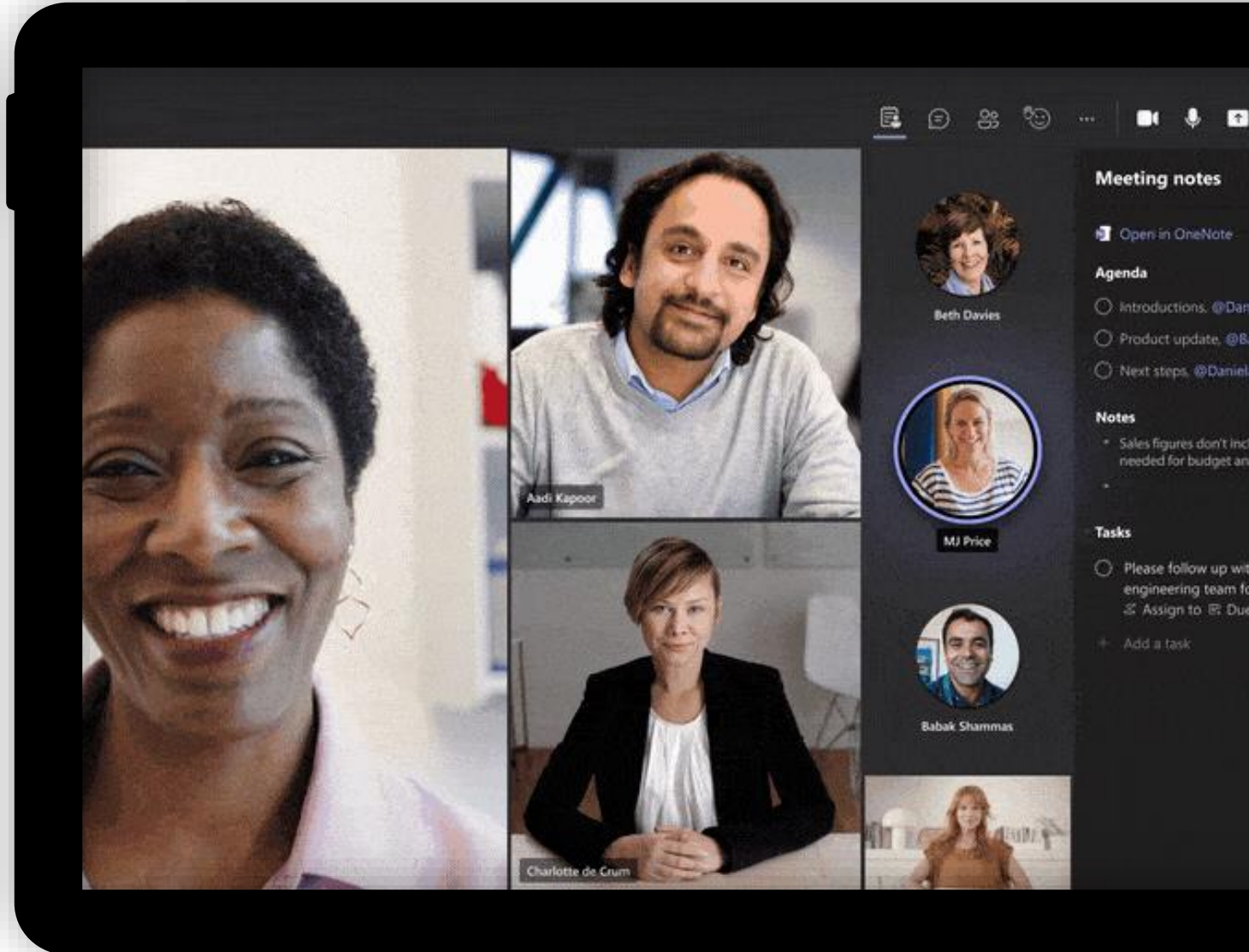
Empower Employees with best-in-class productivity apps

1 **Attend fewer meetings with** automatic meeting summaries, transcripts, and video

2 **Rewire creative workflows** with always up-to-date Loop components

3 **Get real-time translation** of a meeting into 40 languages with Live Captions

4 **Streamline business workflows** in the flow of work with collab apps
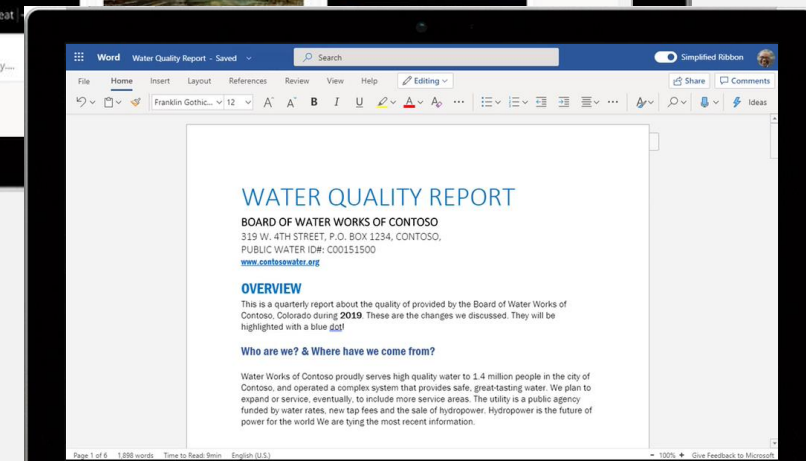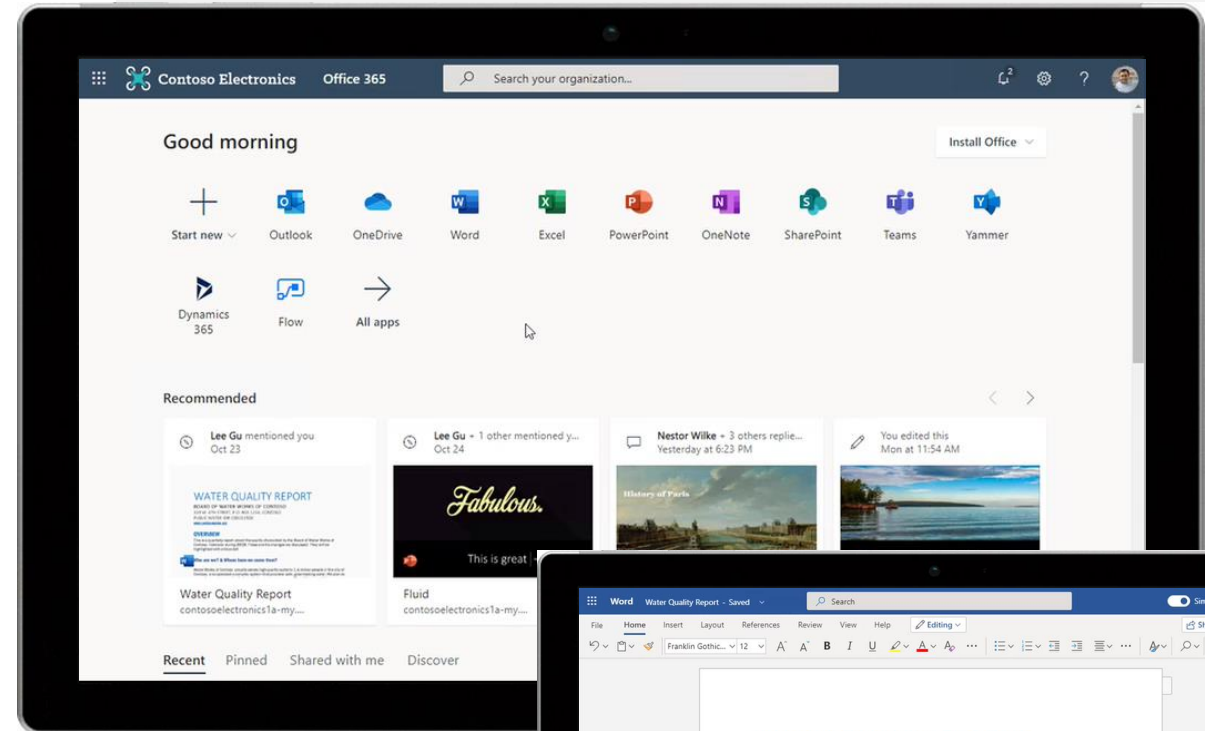
Teams, Word, Excel, PowerPoint, Outlook, Loop

Introduce the power of AI to employees safely

① **Draft content** including emails and social content

② **Get answers to complex questions** including questions with multiple data points

③ **Summarize PDFs** by using Copilot in Edge

④ **Generate new custom images** instead of stock and text only
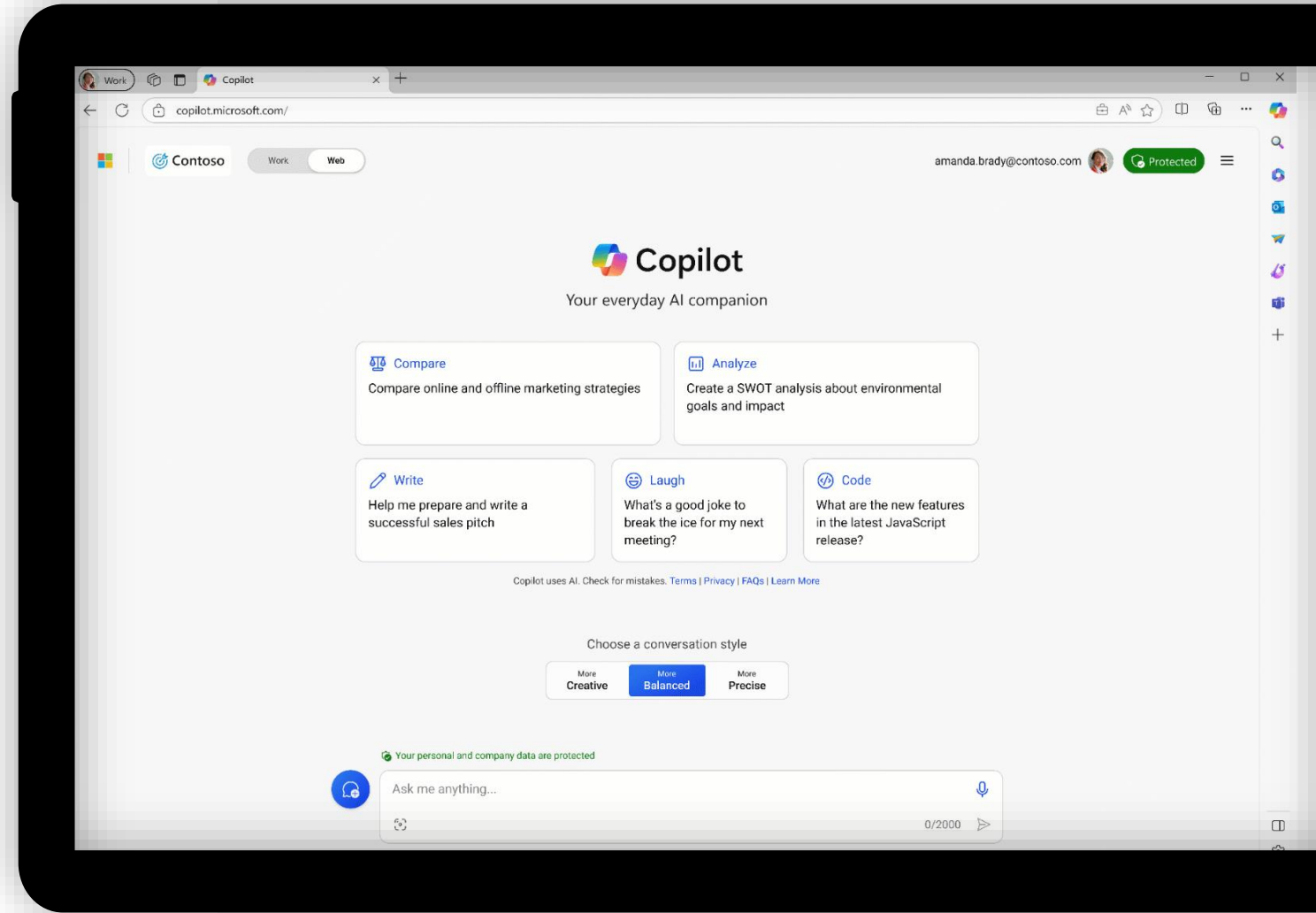
Copilot (with enterprise data protection)

Streamlined endpoint management

Manage company owned and BYO devices

Deliver the best experience
with Windows 11

Deploy any endpoint
from the cloud

Improve support and
reduce incidents

Windows 11 Enterprise

Microsoft Intune
Windows Autopilot

Endpoint Analytics
Universal Print
Organizational Messages

Deliver the best experience with Windows 11

① **Keep people, data, & devices protected** and private through hardware and software security designed to work together

② **Upgrade to Windows 11 with confidence,** with over 99% app compatibility and App Assure [1]

③ **Empower flexible workstyles and smarter work** with snap assist, Microsoft Teams controls from the Task Bar, focus time controls, and more

④ **Use enhanced accessibility features,** e.g., system-wide live captions, natural voice access

Windows 11 Enterprise

[1] Based on Microsoft AppAssure data 2018-2021.

Deploy to virtually any endpoint from the cloud

1 **Ship new devices directly to employees** with zero-touch IT endpoint provisioning; enable mobile, BYOD, and personal devices

2 **Determine upgrade readiness** through endpoint analytics and machine learning

3 **Automate quality and feature updates** using Windows Autopatch

4 **Control quality, driver, feature updates,** tailored to your custom compliance policies

Microsoft Intune
Windows Autopilot
Windows Autopatch

Zero Trust is foundational to great security

Secure & manage identities

Defend against threats on multi platforms

Protect sensitive information across data estate

Microsoft Entra ID

Microsoft Defender for Endpoint
Microsoft Defender for O365
Microsoft Intune

Microsoft Purview
Information Protection
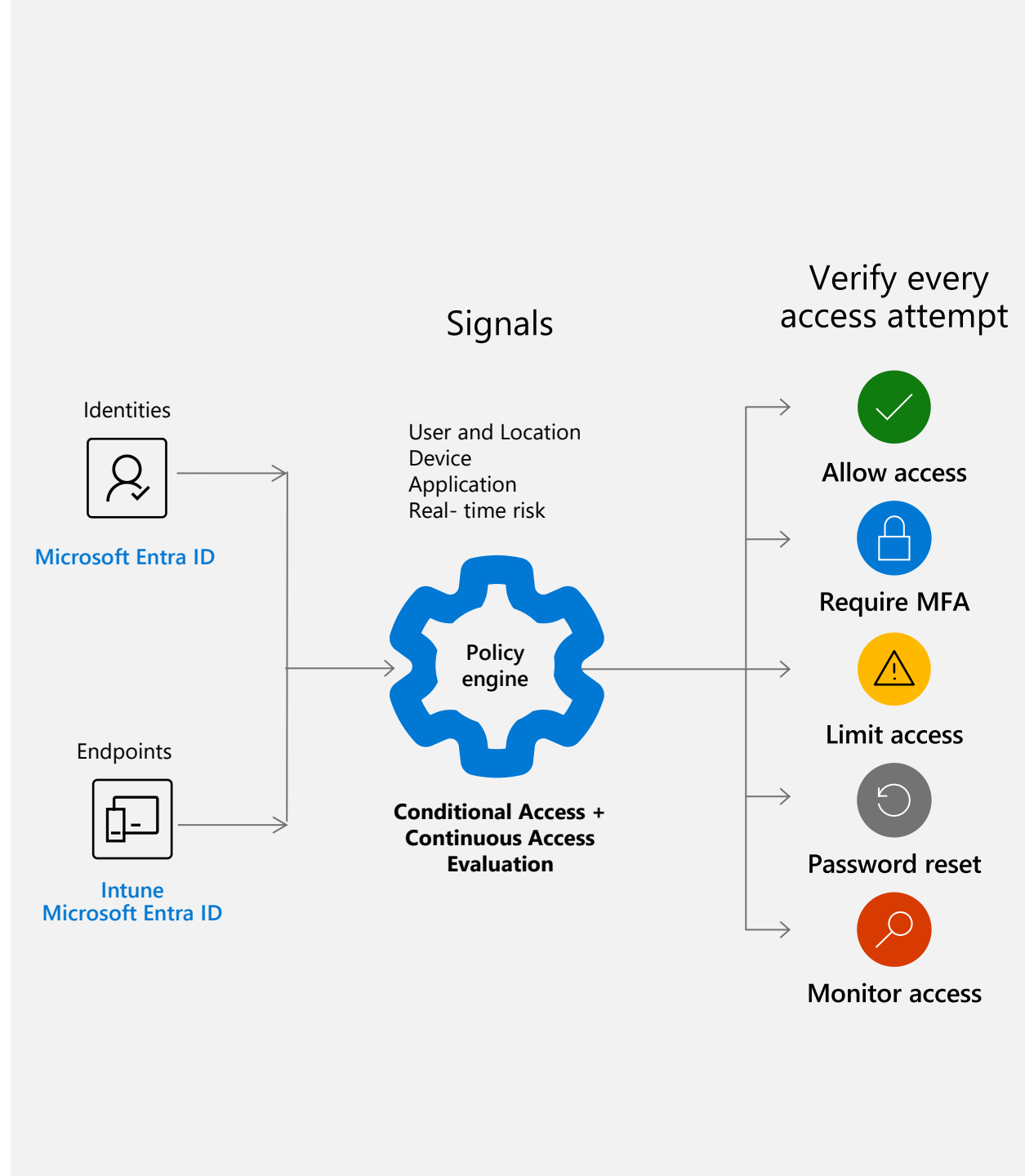
Defend against threats on multi platforms

(1) **Help reduce risks** with threat detection and remediation

(2) **Assess security posture,** isolate threats, and proactively block malware

(3) **Help keep software current** with automated updates and ensure patches are deployed in a timely and efficient manner

(4) **Enable device-based conditional access** for added data protection and breach prevention

Microsoft Defender for Endpoint

Microsoft Defender for O365

Secure Score

Microsoft Intune
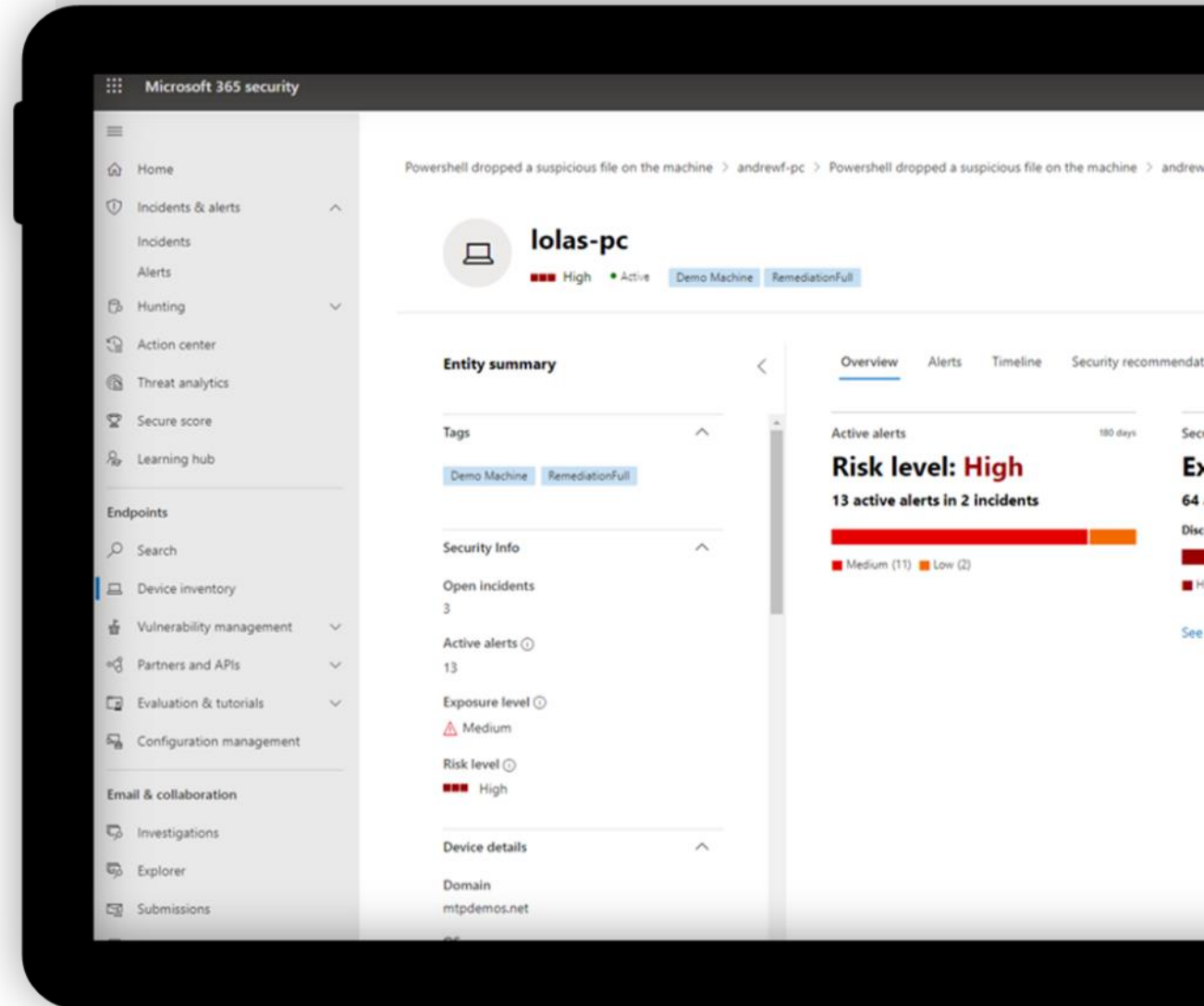
Protect sensitive information across your data estate

1. **Encrypt data** at rest, in transit, and in use

2. **Discover and classify sensitive** content at scale and extend protection to Microsoft and non-Microsoft apps

3. **Address threat of data theft or exposure** from lost, stolen, or inappropriately decommissioned computers

4. **Preserve content** by custodian and send hold notifications

BitLocker

Microsoft Purview Information Protection
part of Microsoft Purview

Cloud

On-premises
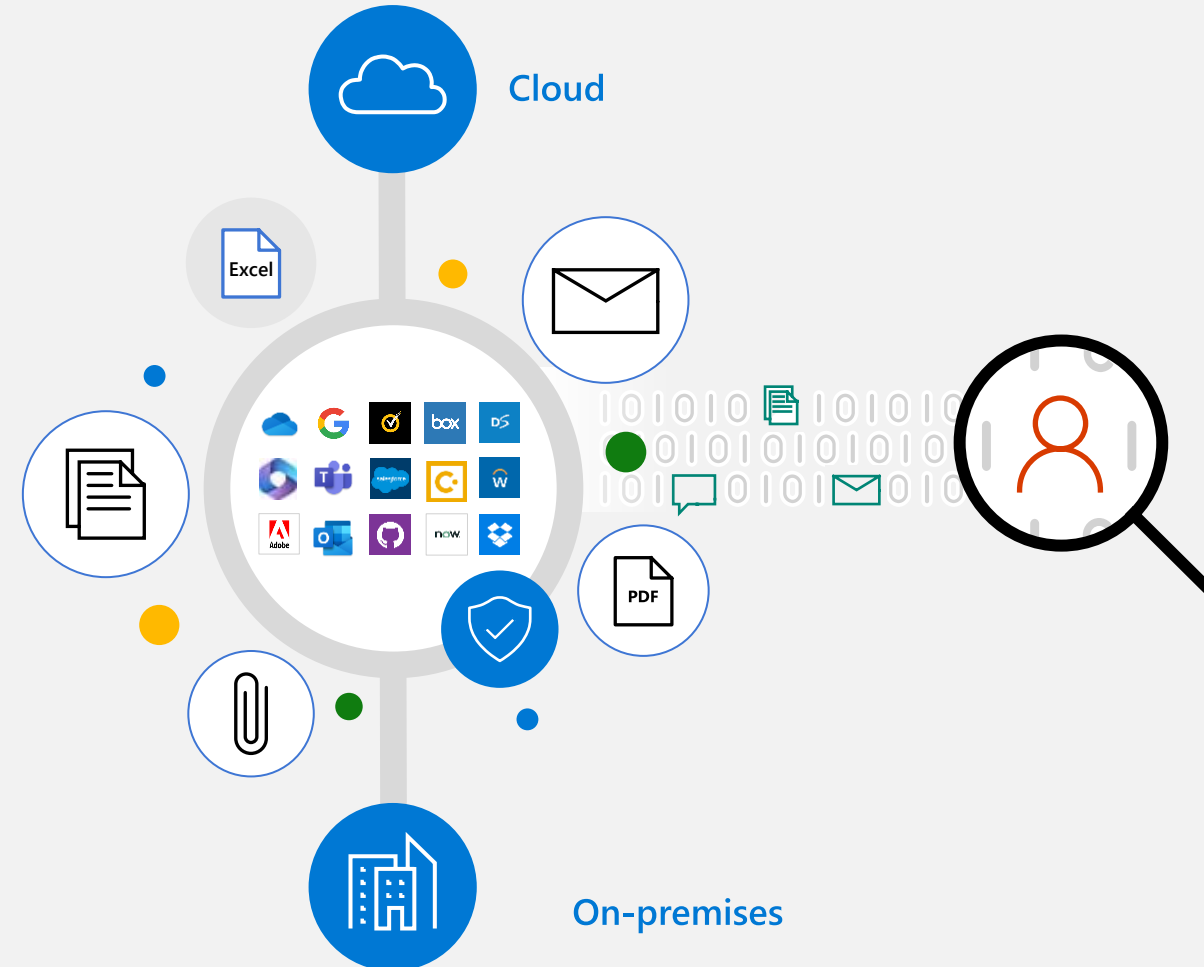
Core security controls for a secure user journey from login to using Copilot

Manage overprivileged and risky users — Protect business information and restrict actions

Microsoft Entra ID

✓ Login to Microsoft 365 with a single & managed corporate identity.

✓ Evaluate login attempts based on user or group membership, IP location, device state, application, risk detection.

✓ Decide access level with Conditional Access policies.

✓ Monitor critical events and issue access tokens that can be revoked immediately.

Microsoft Purview Information Protection

✓ Data consumption and processing with Copilot is limited to the user's permissions.

✓ Copilot inherits sensitive documents' sensitivity labels and applies them to its output and references.

✓ If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply.

✓ Interactions with Copilot are retained and logged for audits or search purposes. Detect business, or code of conduct violations.

✓ Remove inactive data to reduce obsolete insights

End-to-end threat intelligence and protection all in one

For keeping the lights on

And for when things go wrong

Microsoft 365 E5 Security

Microsoft 365 E5 Compliance

Identity management

Device management

Compliance management

AI governance

Phishing mail

Click a URL

Email

Device is exploited, malware is installed

Remote command and control of the system

Endpoints

User account is **compromised**

Attacker **compromises** an admin account

Domain is **compromised**

Identities

Applications

Attacker **exfiltrates sensitive data**

Services stopped and backups deleted

Files encrypted on additional devices

Workloads

Smarter and faster tools for effective detection, response, and remediation

Microsoft 365 E5 Security

Security

Microsoft Defender for Office 365 Plan 2

Microsoft Defender for Cloud Apps

Microsoft Entra ID P2

Microsoft Defender for Identity

Microsoft Defender for Endpoint P2

Microsoft Defender for IoT – EIoT

Microsoft 365 E5 Security

M365 E5 Security

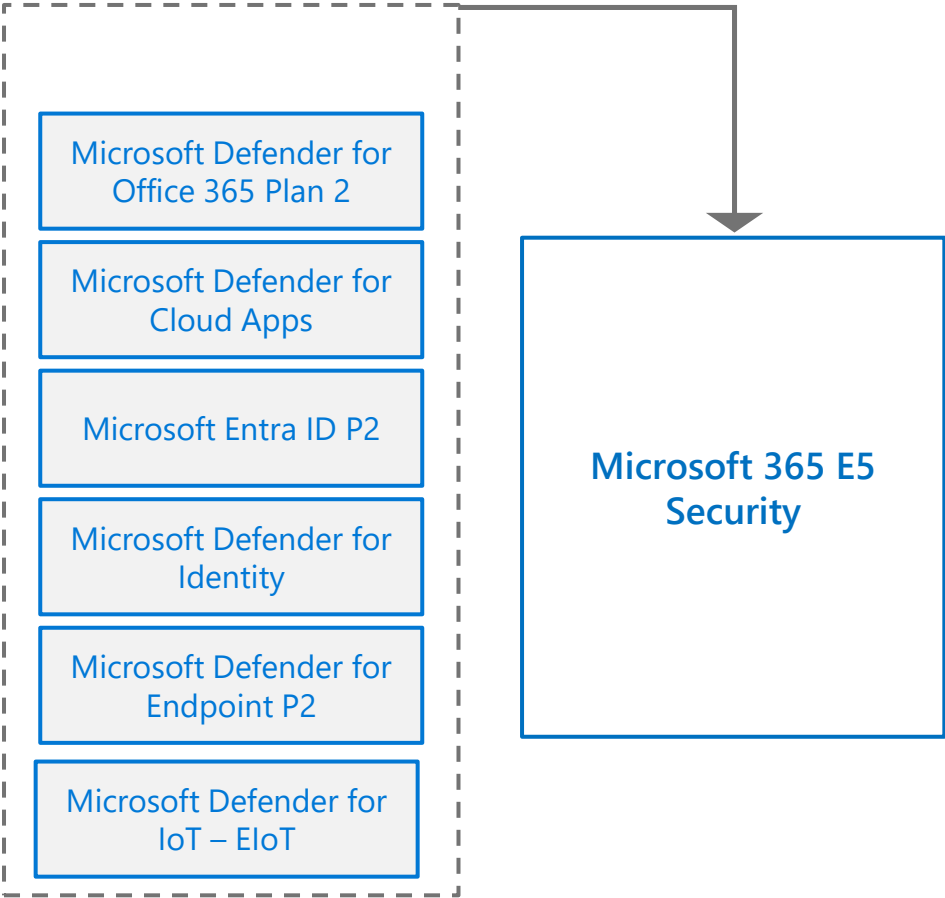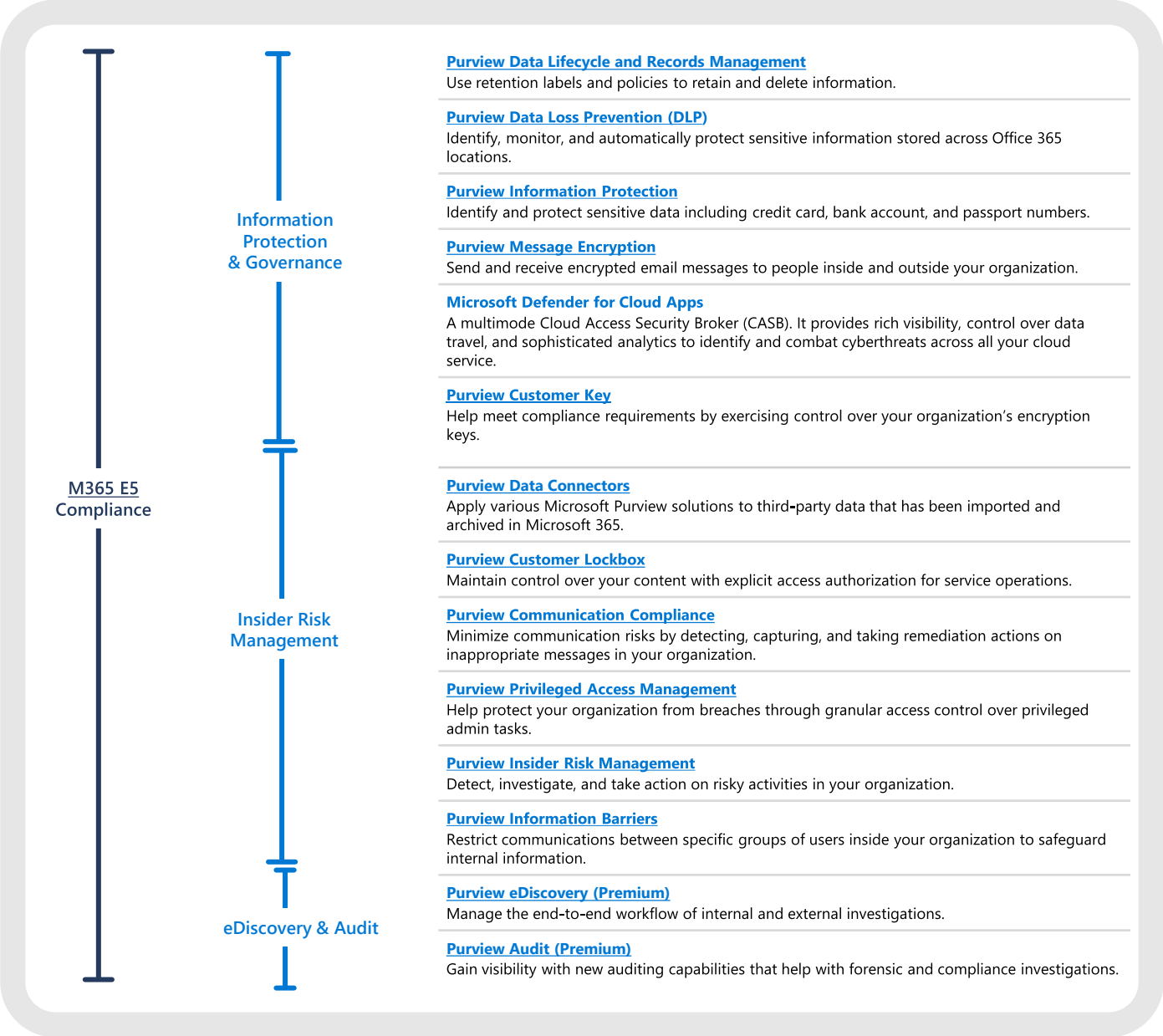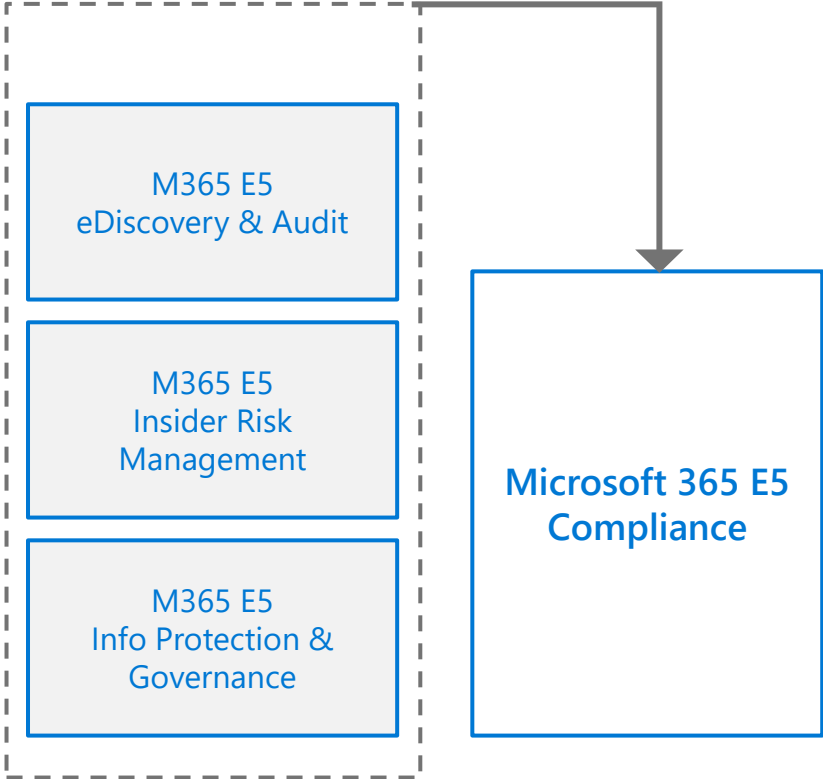|		
Microsoft Defender for Office 365 P2		A cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection and includes features to safeguard your organization from harmful links in real time. In addition to Plan1, Plan 2 also offers automated investigation & response, threat trackers, and an attack simulator
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 services.
Microsoft Entra ID P2		Microsoft's cloud-based identity and access management service, which helps employees sign in and access resources. In addition to Free and P1 features, P2 also offers Identity Protection to help provide risk-based Conditional Access to apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
Microsoft Defender for Identity		A cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Defender for Endpoint P2		A unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. The product offers Threat and Vulnerability Management, tools to surgically reduce the attack surface, next-generation protection to block threats and malware, Endpoint detection and response to detect advanced attacks, automated investigation and remediation of threats and Managed threat-hunting service.
Safe Documents[1]	*	Uses Microsoft Defender for Endpoint to scan documents and files that are opened in Protected View or Application Guard to automatically check Office documents (Excel, PowerPoint, Word etc.) "against known risks and threat profiles" before users open them.
Application Guard for Office 365[1]	*	Isolates untrusted documents to protect users against malicious and potentially harmful threats. at risk. When a user encounters a malicious document, it is safely isolated.
Microsoft Defender for IoT – EIoT[2]	*	Includes coverage of 5 EIoT devices for each M365 E5 license; additional device coverage is $0.85 per device per month. Provides discovery of network devices, vulnerability management, and threat detection and response.

Microsoft 365 E5 Compliance

ME5 Compliance

M365 E5
eDiscovery & Audit

M365 E5
Insider Risk
Management

M365 E5
Info Protection &
Governance

Microsoft 365 E5 Compliance

M365 E5 Compliance

Information Protection & Governance

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 Office 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.

Insider Risk Management

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.

eDiscovery & Audit

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.

Stay compliant

Secure and govern your organization's data across your entire digital estate.

Accelerate the secure adoption of AI with ready-to-go data security and governance tools purpose-built for generative AI.

90+
Global certifications and attestations, including GDPR, ISO 27001, and SOC 1/2/3

400+
GenAI app risk assessments ready for use by your team

320+
Ready-to-use and customizable regulatory assessment templates to meet multicloud compliance requirements, incl. **NIS2**

Supports AI compliance with the EU AI Act, NIST AI Risk Management Framework, ISO 42001, ISO 23894, code-of-conduct policies, and more

99.9%
Uptime commitment for Microsoft 365 ensures continuous compliance management

Discover, protect, and govern the use of generative AI for Copilot, ChatGPT, Claude, Gemini, private LLMs, and more

Microsoft's AI principles

Fairness

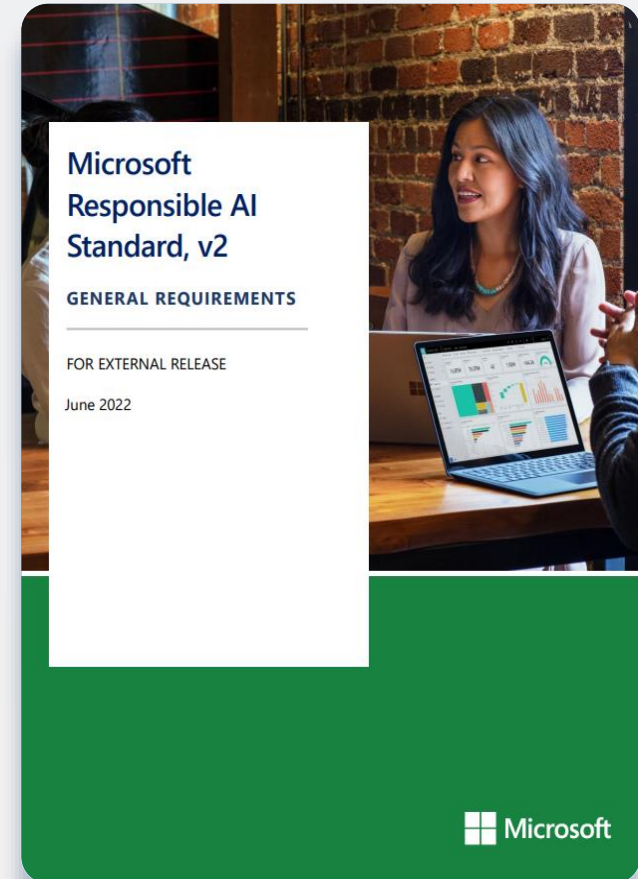Reliability & Safety

Privacy & Security

Inclusiveness

Transparency

Accountability

Microsoft Responsible AI Standard, v2

GENERAL REQUIREMENTS

FOR EXTERNAL RELEASE

June 2022

Microsoft

Microsoft's data commitments

Microsoft's privacy commitments apply to AI

We will keep your organization's data private

Your organization's data is not shared

You are in control of your organization's data

Your organization's data security and privacy are protected by design

Your access control and enterprise policies are maintained

Your organization's data is not used to train foundation models

Our products and solutions comply with global data protection regulations

Our commitments are outlined

Data Protection Addendum

Product Terms

Microsoft's Privacy Statement

Committed leadership in data residency

Spotlight | **EUDB**

European Union Data Boundary (EUDB) enables customers in EU and EFTA countries to process and store their customer data in the EU.

Promises

- Store and process data in the EU
- Expand data centers in the EU
- Provide for global security
- Provide in-region support model

Additional Information: aka.ms/EUDataBoundary

Microsoft

Thank you!