

Understanding the top cybersecurity threats to your organization

Javier Nevarez

Technical Support Supervisor
Inova Solutions Puerto Rico

Top Breach Types in 2023

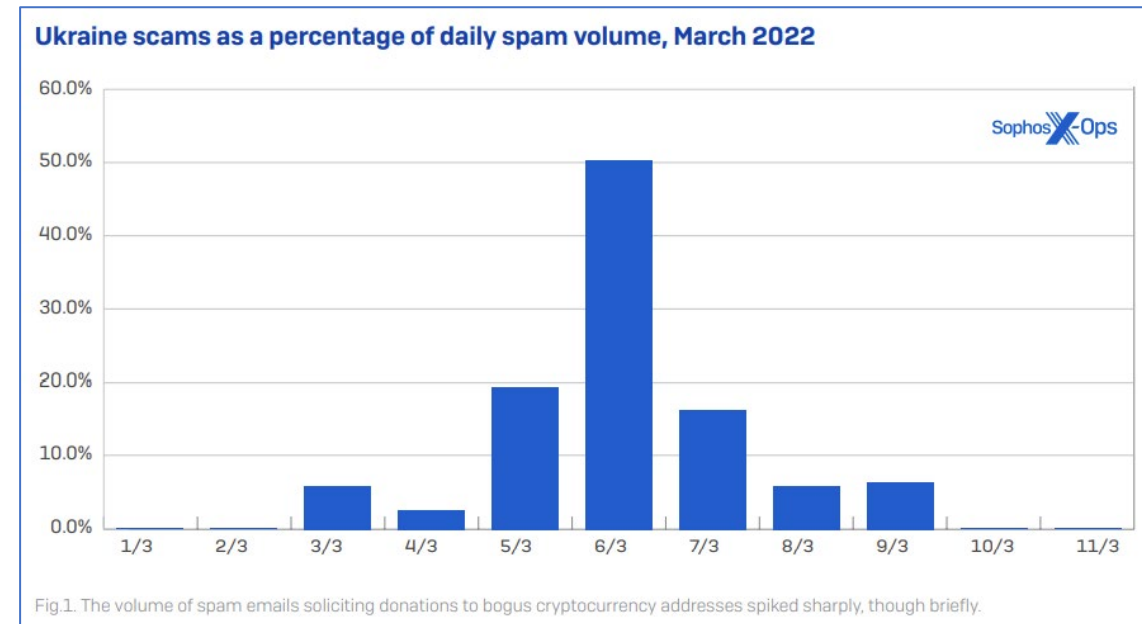


Ransomware

- Malicious software that encrypts your data.
- A type of Extortion.
- Often requires a very large payment.
- Payments are **never** guaranteed to result in release of your data.
- Mostly sent via simple email.

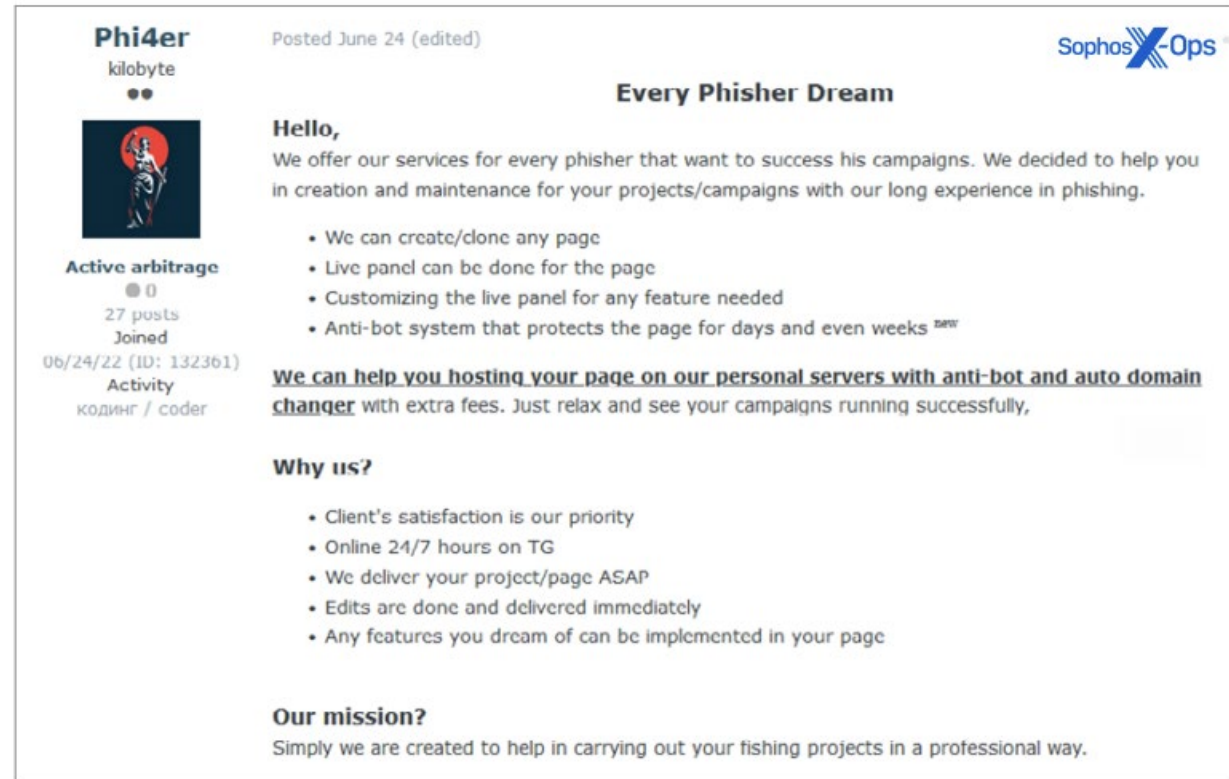
Phishing

- Emails asking for information or credentials to be used maliciously later on commonly disguised as:
 - Invoices
 - Business partners
 - Telephone calls
 - Criminal call centers
 - Social Engineering



Phishing (cont.)

- Guaranteed!
- 24/7 Service
- Expedited
- “Any features you dream”



Phi4er
kilobyte

Posted June 24 (edited)

Every Phisher Dream

Hello,
We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks ^{new}

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?
Simply we are created to help in carrying out your fishing projects in a professional way.

Fig. 6. A suite of phishing services comes with customer-service guarantees.

Social Engineering

- The “human version” of phishing
- Mostly done by impersonating:
 - Partners
 - Bank employees
 - A superior in your own organization



Social Engineering (cont.)

- Art of Manipulation
- Pretexting
- Baiting
- Tailgating

Use of Stolen Credentials

- Via Brute-force attacks
- Via Malware
- Reused passwords from other sites
- Social attacks (phishing and pretexting)

Supply Chain Attack

- Use of a service provider to target their customers
 - Distribute malware
 - Conduct espionage
- Most common in financial, oil industry, and government sectors.

Misconfigurations

- Firewall Rules
- Unpatched Systems (Windows/Linux/Mobile Device OS Updates)
- Antivirus without updates
- Devices Exposed to:
 - Trojans
 - Exploits

Remote Services exploits

- VPN vulnerabilities
 - Bypass security (like conditional access policies)
 - Access sensitive data

How do you know you're compromised

- Watch for anything out of the ordinary
 - Bank Statements
 - Phone Bills
 - Credit Card Statements
 - Email requests
 - Calls

How to avoid being a target

- **Use MFA**
- Do not reuse passwords
- Use complex password generators
- Do not click email links quickly
- Keep work and personal data/devices separate

How to avoid being a target

- Change default passwords
- Use endpoint protection
- Install software updates
- Keep backups

How to avoid being a target

- Configure the security tools at your disposal:
 - Identity management
 - Data classification and data loss prevention
 - Anti Spam, Anti Phishing, Anti Malware
 - Spoofing Protection
 - Mail tips
 - Device and app management



Security Quick Wins

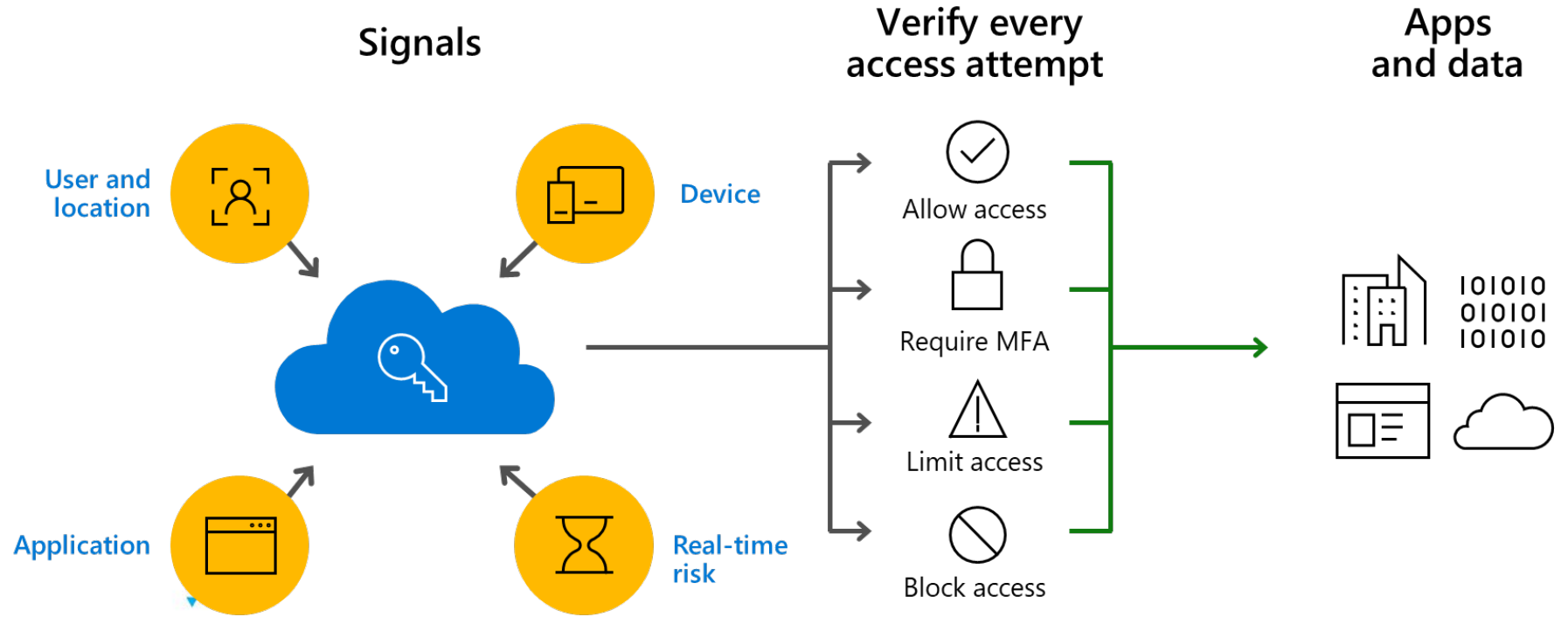
- Configure MFA
- Perform Access Reviews

Security Quick Wins

- Configure MFA
- Perform Access Reviews
- Configure Security in Microsoft 365 / Azure (Not on by default)
 - Review Secure Score
 - Defender for Office 365
 - Conditional Access Policies (location)



Conditional Access Policies



Deploying Copilot Securely





Copilot for Microsoft 365

Built on Microsoft's comprehensive approach



Security



Compliance



Privacy



Responsible AI

Govern access to Copilot

Microsoft Entra ID

Users and Devices

1 Manage overprivileged and risky users with Identity and access management

 Microsoft Entra ID

2 Mitigate Device Risk with Endpoint management

 Microsoft Intune



Copilot for Microsoft 365



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



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



Decide access level with Conditional Access policies.



Allow access



Require MFA



Limit access



Password reset



Monitor access



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

Manage device real-estate

Microsoft Intune

Users and Devices

1 Manage overprivileged and risky users with Identity and access management

 Microsoft Entra ID

2 Mitigate Device Risk with Endpoint management

 Microsoft Intune



Copilot for Microsoft 365



Ensure the Microsoft 365 apps are securely installed on the user's device and kept up to date.



Limit the use of work apps, including Copilot, on personal devices



Implement App protection policies to limit the actions users can take on devices:

- Save generated files to unsecured apps
- Restrict copying and pasting to non-work apps



Wipe all work content if the device is lost or disassociated with the company or the user.

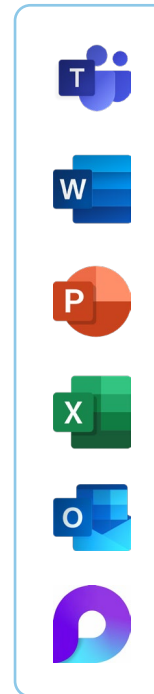
Protect business information and restrict actions

Microsoft Purview Information Protection

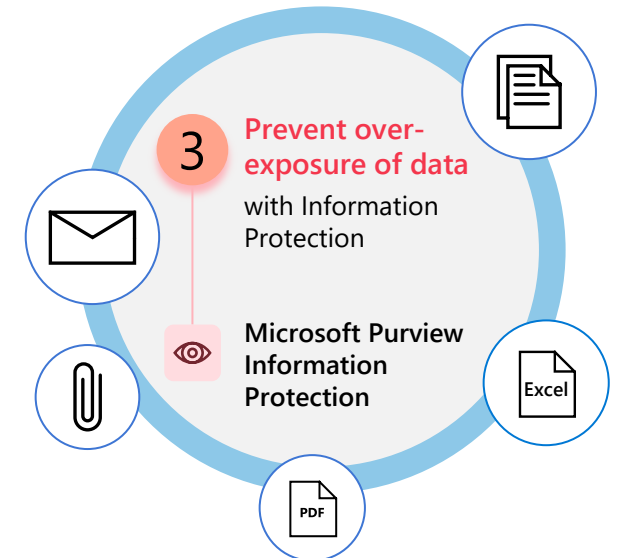
- ✓ Data consumption and processing with Copilot is limited to the user's permissions.
- ✓ Copilot inherits sensitive documents' sensitivity labels and applies them to its output and references.
- ✓ If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply.
- ✓ Interactions with Copilot are logged for auditing purposes and business, or code of conduct violations can be detected.



Copilot for Microsoft 365

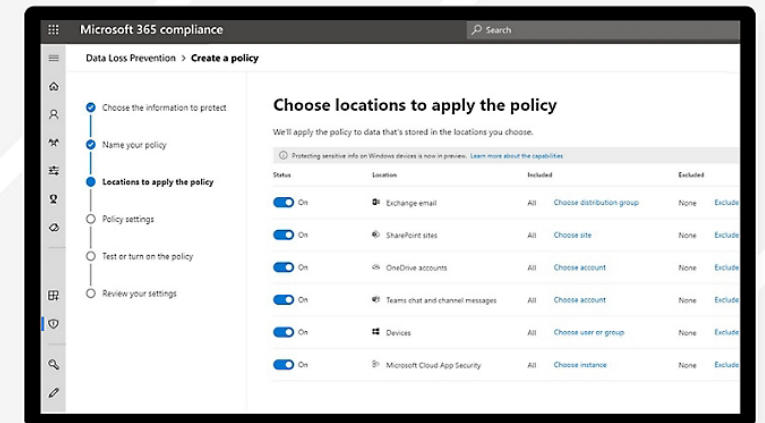


Your Organization Data



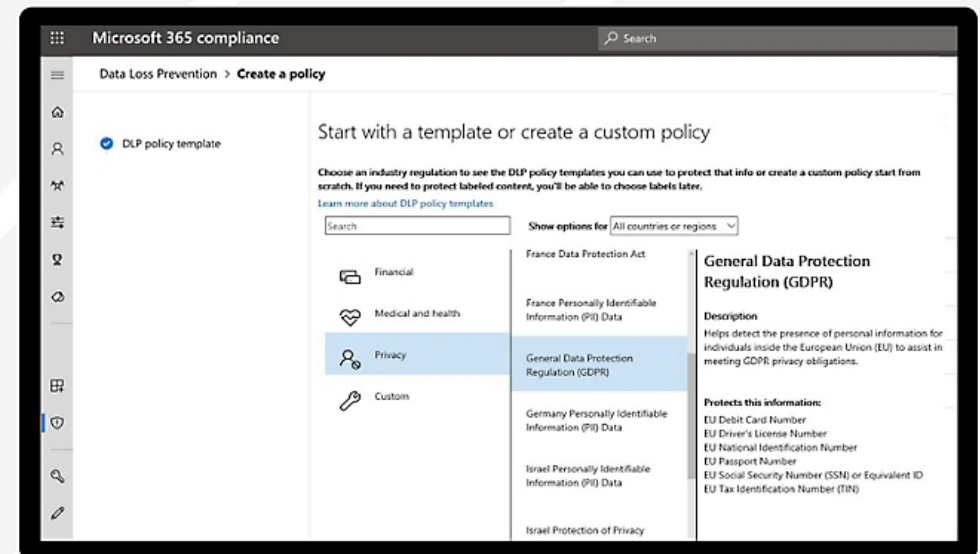
Data Loss Prevention

- Protects sensitive information
- Prevents data leakage
- Helps comply with data protection regulations



DLP: Data types

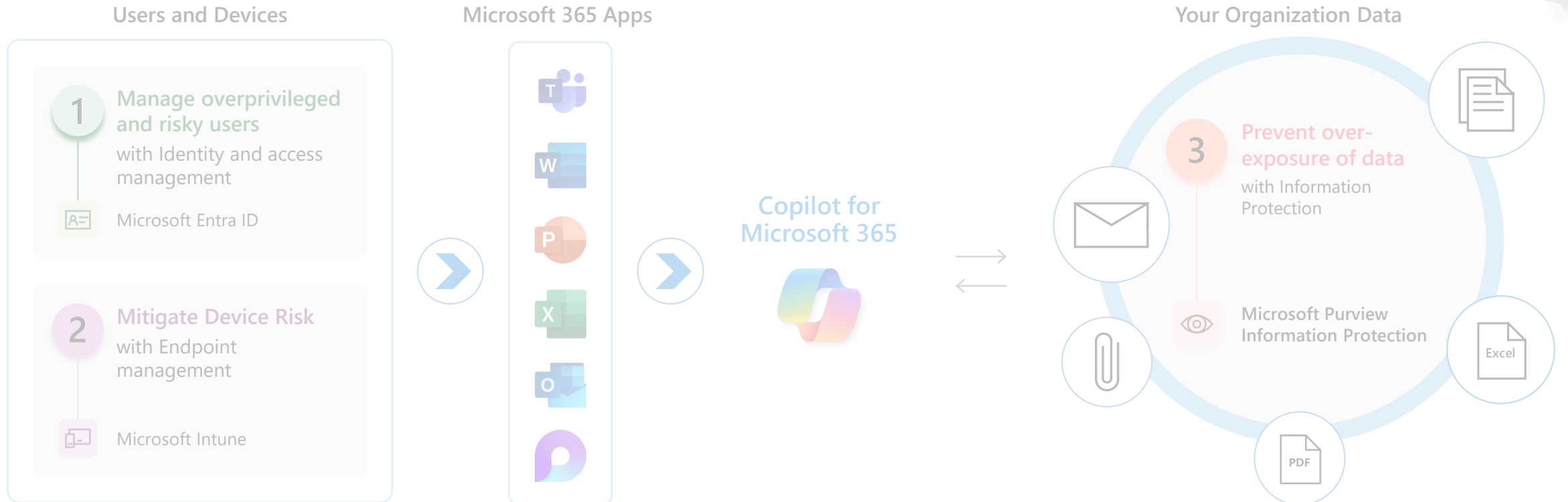
- Financial data
- Personally identifiable information (PII)
- Health information
- Intellectual property





Discover and control the use of AI apps

Microsoft Defender for Cloud Apps



Discover and control the use of AI apps

4



Microsoft Defender for Cloud Apps



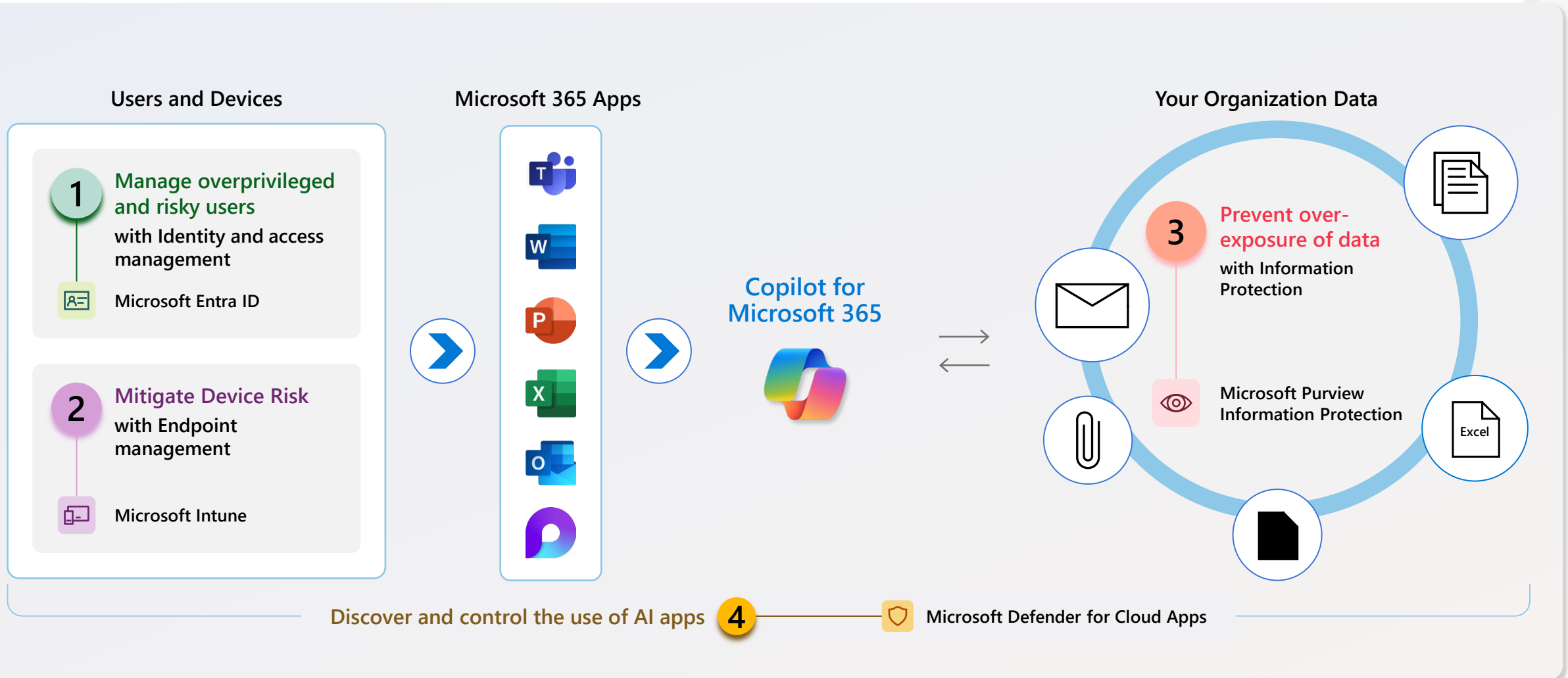
Discover & assess the risk across 400+ AI apps in an organization



Block or approve the use of discovered AI apps in the organization



Security and compliance controls for Copilot for Microsoft 365

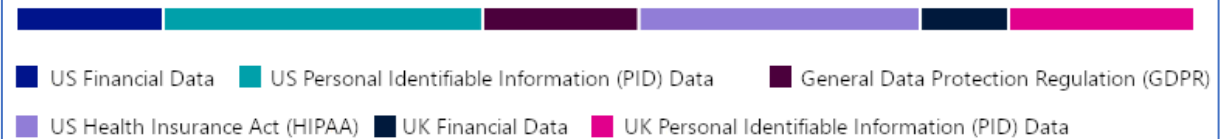


Data Classification

- Create custom labels
- Classify data automatically
- Persistent labelling
- Apply labels automatically
- Track data usage

Top sensitive info types

Sensitive info types used most in your content



[View all sensitive info types](#)

Top activities detected

**115K sensitive files had
2,385 activities recently**

220 Copied to USB

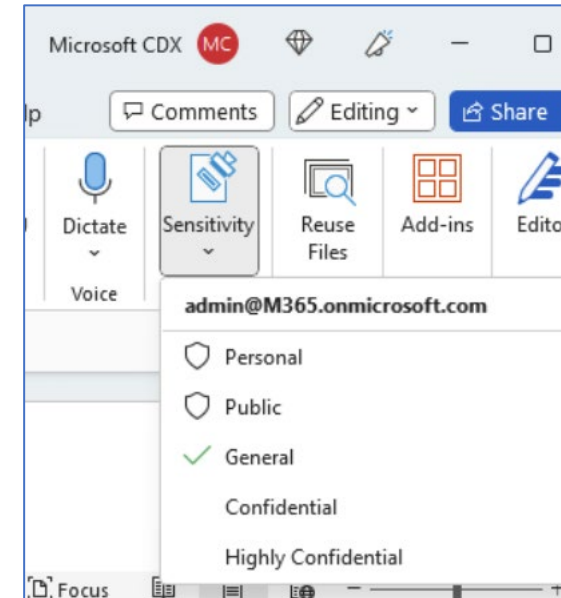
422 Change a label

750 Shared externally

Data Classification

- Secure collaboration
- External sharing
- Collaboration with partners

- Email, Teams, Sharepoint, Onedrive



Before Copilot

- Basic Security (MFA, Conditional Access Policies)
- Data Loss Prevention (DLP)
- Data Classification



How can Inova Solutions help?



Guardian 360

- Adaptive Security & Monitoring
- Automatic Remediation
- Audits and reports
- Backups



Guardian 360

- Security baselines based on CIS best practices
- Establish custom baselines based on your orgs needs



Feature	Guardian 360	Microsoft 365
Multi-tenant, complete posture control	✓	X
Customizable best practices	✓	X
Posture alerts (8x5, 24x7)	✓	X
Posture remediation (8x5, 24x7)	✓	X
Unified visibility of posture gaps and threats	✓	X
Breach detection, triage and remediation	✓	X
Breach monitoring	✓	Requires Azure Sentinel + Cloud App Security

What are your next steps?



1 Do a Copilot Optimization Workshop with us

Learn how to efficiently and securely implement and leverage the features of Copilot for Microsoft 365. Here's what we will do in this workshop:

- **Assess:** We will deep dive deep into your business landscape. Let's define the scope together, pinpoint key stakeholders, and uncover invaluable insights into your business scenarios.
- **Art of the Possible:** Get an in-depth view of how intelligence impacts employee experiences by unleashing creativity, unlocking productivity, and leveling up skills.
- **Build the Plan:** We will create a tailor-made roadmap, prioritizing scenarios that align perfectly with your goals. Together, we'll chart out the next steps and set a timeline to seamlessly implement and revolutionize your solution.

Starting at

USD \$3,499⁰⁰

2 We implement your Copilot Optimization Plan

Give the reins to Inova Solutions and let us efficiently and securely optimize your business for Copilot for Microsoft 365. We will:

- Define the scope of the plan
- Pinpoint key stakeholders
- Identify your business scenario's
- Create a customized optimization roadmap including a timeline

Starting at

USD \$4,999⁰⁰

FOR SMB

Starting at

USD \$9,999⁰⁰

FOR ENTERPRISE



Thank you

▶ Any questions?

