Microsoft Copilot Guidebook

FIRST DISTRIBUTION™
Epsidon Technology Holdings

Microsoft

How to position Microsoft 365 Copilot with the 7 step program powered by First Distribution

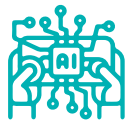
A guide for partners who want to leverage AI and offer value to their customers

1 Define intent

DISCOVERY WORKSHOP

Tasks: Assemble stakeholders and business requirements.

Milestones: Business model designed around AI, prioritized use cases, environmental assessment, and strategic roadmap.

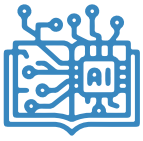


2 Migrate

CLOUD ENABLEMENT

Tasks: Migrate and integrate data into the Microsoft Modern Workplace.

Milestones: Centralized management and search capabilities across Microsoft Teams and SharePoint



3 Secure

DATA PROTECTION

Tasks: Implement Identity & Access Management, Microsoft Defender, Data Loss Prevention, and Collaboration and Sharing Insights.

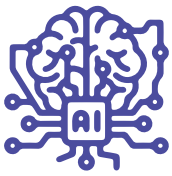
Milestone: Comprehensive security.

4 Control

DATA GOVERNANCE

Tasks: Apply data policies and requirements with Microsoft Purview and SharePoint Premium.

Milestones: Consistent policy application, data classification, retention, and content management to ensure compliance.



5 Enable Change

EMPLOYEE EXPERIENCE

Tasks: Implement Microsoft Viva Connections, Topics, and Goals.

Milestones: Employee engagement, knowledge management, and aligned objectives for a high-performance organization.

6 Refine Intent

COPILOT READINESS

Tasks: Organize champions and test AI business cases.

Milestones: Copilot Center of Excellence, Copilot Dashboard powered by Viva, and success stories.

7 Realize

COPILOT INTEGRATION

Tasks: Apply organizational change framework to integrate humans and their domain expertise.

Milestones: Improved employee productivity, customer satisfaction, and market share.

How to sign up or next steps:

Contact us: Sahil.Kassie@firstdistribution.com

Microsoft

Secure your email and collaboration tools with Microsoft Defender for Office 365 and Business Premium

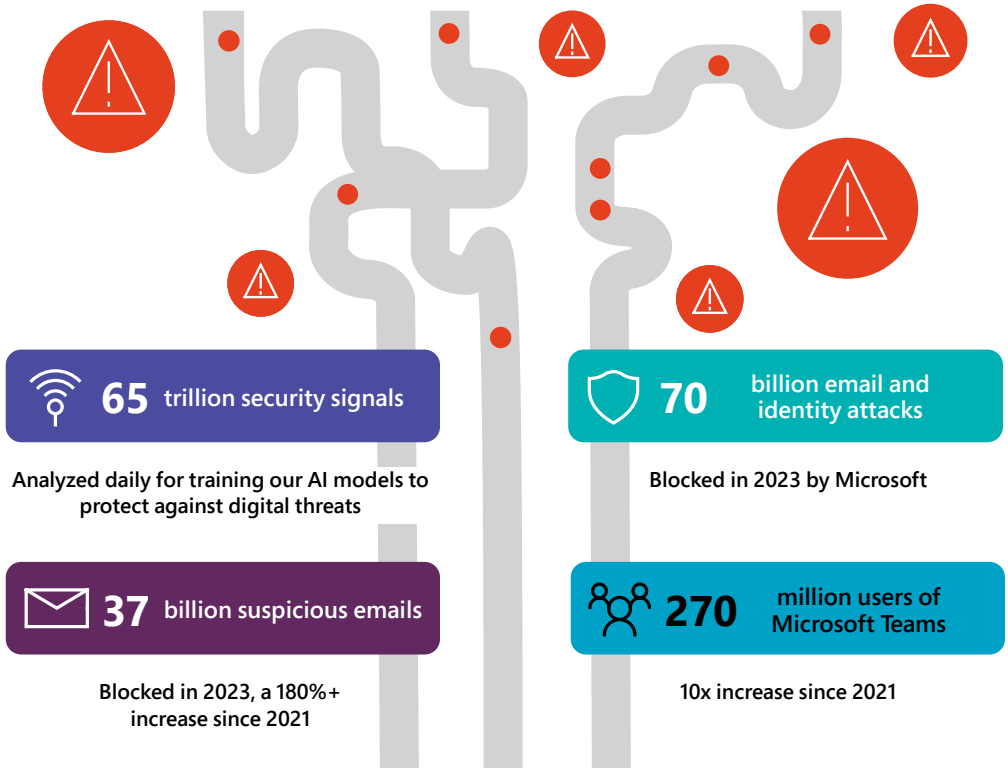
Organizations rely on email and Microsoft Teams now more than ever for productivity... but keeping these tools secure is a constantly evolving challenge:

Email is the top target for cyber attacks

Over 90% of cyber attacks start with email. Defending email is critical to stopping. threats throughout your entire organization.

The threat landscape continues to evolve

With hybrid work on the rise, attackers now target other collaboration platforms as entry points to compromise sensitive information.



65 trillion security signals

Analyzed daily for training our AI models to protect against digital threats

70 billion email and identity attacks

Blocked in 2023 by Microsoft

37 billion suspicious emails

Blocked in 2023, a 180%+ increase since 2021

270 million users of Microsoft Teams

10x increase since 2021

Nearly 2 billion threats are filtered before they reach the inbox each month.

Prevention

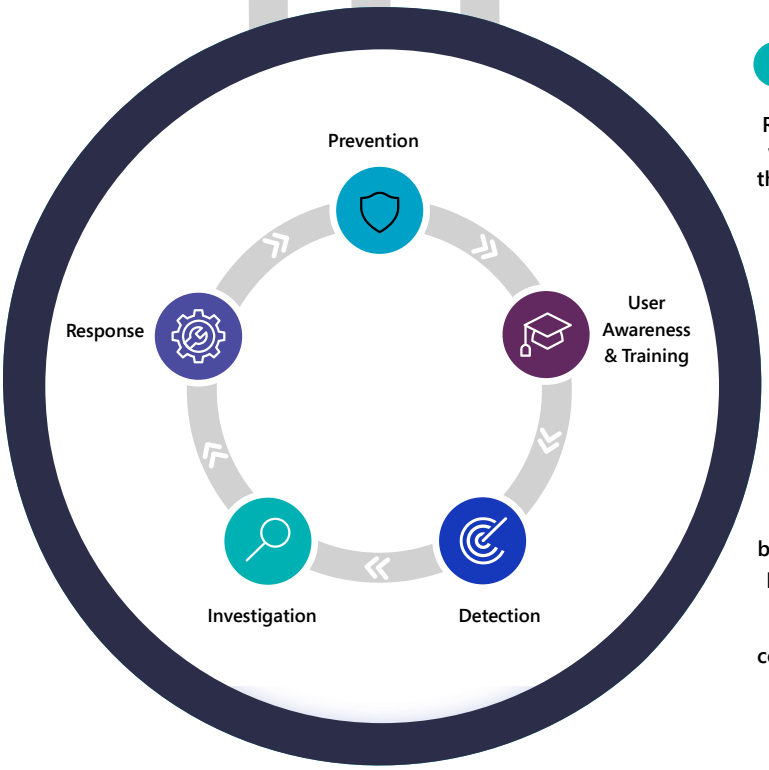
Easily assess, configure and continuously tune your security posture with prioritized recommendations

User Awareness & Training

Educate users with built-in tools to run phishing simulations and manage training assignments based on individual user results.

Detection

Proactively block threats with a comprehensive protection stack, driven by AI and automation based on 65 trillion signals analyzed daily.



Investigation

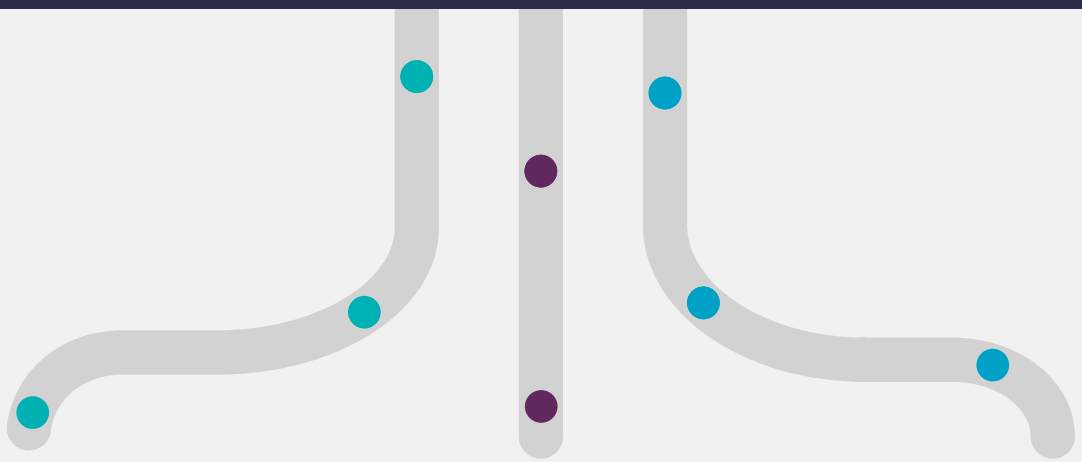
Reduce investigation time by 92% with advanced analytics tools for the full spectrum of threats. Extend investigations to endpoints, identity, and more with XDR.

Response

Minimize response time with built-in automation and integrated playbooks that remove malicious emails, even post-delivery. Get further transparency with a comprehensive incidentbased view of threats.

Microsoft

Microsoft Defender for Office 365 includes:



Deeply integrated email protection

Seamlessly integrated threat protection with Microsoft 365 Defender enables email security that automatically stops attack progression and boost SecOps productivity, with lower cost of ownership.

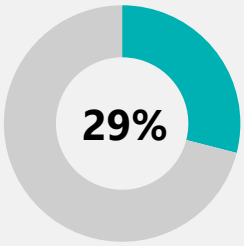
Industry-leading AI and automation

Leveraging the full breadth of our XDR signals database and research, our AI-driven detection capabilities set a new standard in accuracy and automation throughout the security lifecycle.

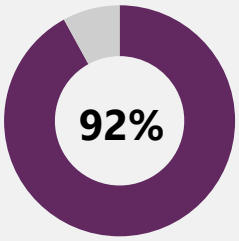
Unified XDR-level investigation and response

Using email and collaboration signals in Microsoft 365 Defender can help combat advanced attacks, while incident-based detection empowers SecOps to hunt across the entire kill chain.

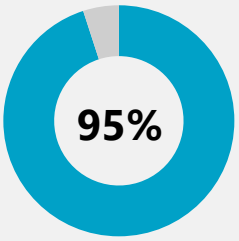
A safer organization and empowered SecOps team



Reduced risk of an email breach when moving from a competitive tool.



Average investigation time reduced from 12 hours to 1 hour.



Time reduced to block malicious links.

To go beyond email security, Microsoft 365 Defender delivers industry leading XDR, spanning security for multiplatform endpoints, identities, email, and SaaS apps

Ready to learn more?

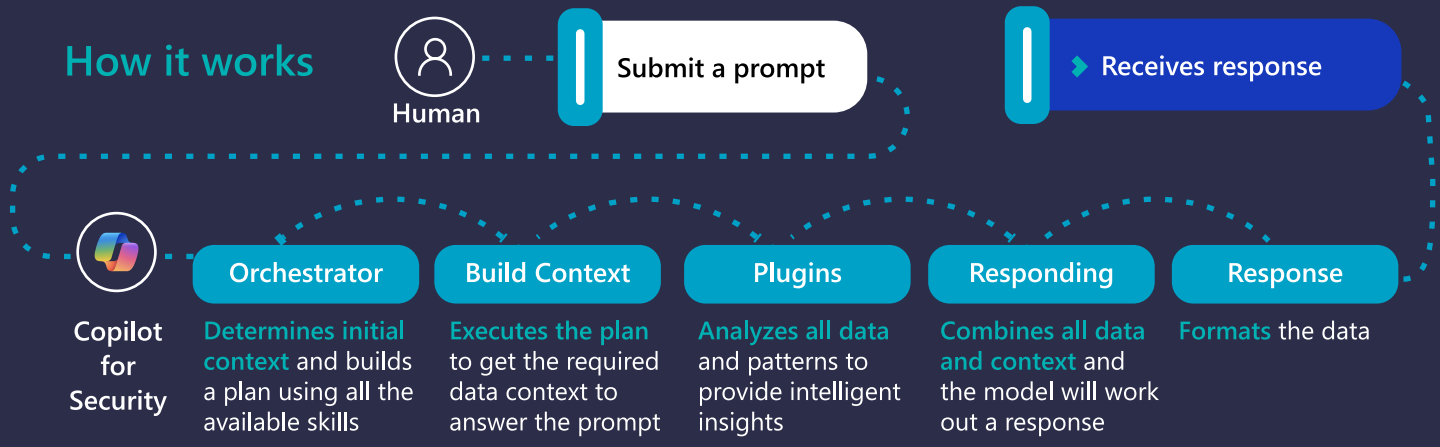
Contact us: Sahil.Kassie@firstdistribution.com

Microsoft

Copilot and Security Coverage and Capabilities

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI, while remaining compliant to responsible AI principles.

How it works



Human ingenuity and expertise will always be an irreplaceable component of defense. So we need technology that can augment these unique capabilities with the skill sets, processing speeds, and rapid learning of AI.

For Security Analysts

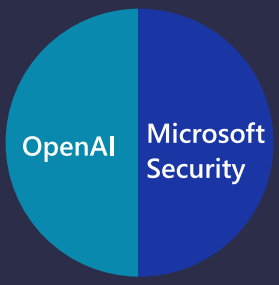
- ✓ Build hunting queries from natural language
- ✓ Get threat intel insights related to specific incidents
- ✓ Analyze malicious scripts with one button click
- ✓ Get remediation guidance
- ✓ Create comprehensive incident reports for leadership

For IT admins

- ✓ Determine if a device is compliant with company□s policies
- ✓ Get advice on configuring and managing new platforms
- ✓ Build new policies and test them to see how they would impact users
- ✓ Proactively identify devices that are not up to date
- ✓ Understand why MFA was triggered for a user

The Microsoft Copilot for Security Advantage

Most advanced general models



Hyperscale infrastructure + Security-specific orchestrator + Evergreen threat intelligence + Cyber skills and promptbooks

Copilot works across the Microsoft Security Stack

Microsoft is in a unique position to transform security for our customers, not only because of our investments in AI, but also because we offer end-to-end security, identity, compliance, and more across our portfolio. We can cover more threat vectors and deliver value with a coordinated experience.

Experiences to meet you where and how you work

Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot for Security itself, with all use cases in one place, enabling enriched cross-product guidance.

Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with.

Copilot in

Microsoft Defender XDR

Investigate and respond to threats in a guided experience

Summarize an incident, assess its impact, provide actionable recommendations for faster investigation and remediation, and, lastly, generate a post-response activity report.

Upskill security talent

Unlock new skills that allow analysts at all levels to complete complex tasks like threat hunting, reverse engineering of malware, and more.

Assess risks with AI-driven threat intelligence

Inquire in natural language about emerging threats and your organization's exposure and gain contextualized insights for rapid response to new and evolving threats.

Copilot in

Unified SOC Platform

Intelligent context for alerts and incidents

Quickly assess emerging threats and your organization's exposure. Respond with enriched, AI-driven insights.

Rapid investigation and response

Security Copilot provides end-to-end support of analysts. From summaries of incidents and response, to assessment of incident impact, to actionable recommendations for faster investigation and remediation.

Unlock advanced SOC skills

Unlock new skills that allow analysts at all levels to complete complex tasks translating natural language to KQL or analyzing malicious scripts.

Copilot in

Microsoft Purview

Scaled visibility

Gain comprehensive, integrated visibility across solutions and insight into relevant compliance regulatory requirements.

Summarization for speed

Quickly summarize alerts containing a breadth of signals and lengthy content to review in the lens of data security and compliance policies.

Unlock expert skills

Receive step-by-step guidance, conduct searches in natural language, and conduct advanced investigations without keyword query language.

Copilot in

Microsoft Entra

Rapid identity risk investigation

Explore sign-ins and risky users, understand the why and get contextualized insights on what to do to protect the accounts, all in natural language.

Faster troubleshooting

With context at your fingertips, find gaps in access policies, generate identity workflows, and get to the root of the problem faster.

New levels of efficiency

Guided recommendations allow admins at all levels to complete complex tasks such as incident investigations. Sign-in log analysis eliminates the need for manual inspection.

Copilot in

Microsoft Intune

Faster response

Swiftly respond to threats, incidents and vulnerabilities with full device context and AI assisted insights and actions.

More informed outcomes

Proactively apply targeted policies and remediate endpoint issues with what-if analysis, actionable guidance and deep understanding of device, user and app status.

Simplified posture management

Quickly translate business intent into recommended and compliant configurations and policies using natural language.

Microsoft

Ideas on how to measure your own ROI

Measure your team metrics for the 6 months prior to using Copilot against the metrics for your first 6 months of full team usage. Top metrics to Compare would be:

- Mean time to respond (MTTR)
- Incidents worked per day
- Average incident resolution time

Do a side by side challenge with your two best analysts. Give one of them Copilot and compare results for time and accuracy to get a quick snapshot of Copilot gains.

Ask a new hire to use copilot and your integrated knowledge base to ramp up and provide an assessment of value at 90 days on the job.

Measuring the quality of work is hard. Are you finding more attack details and documenting them more accurately in the incident? You can sample work output on similar cases with/without Copilot and score them for quality. If the sample size is big enough, you can start to look at trends.

Measure the joy Copilot gives your analysts and admins. It won't have an immediate effect on your ROI, but if they like using Copilot better and are more satisfied with their work experience, the long-term benefits to your team can be considerable (Happy analysts=better work environment=less attrition and better long-term success)."

Ready to learn more?

Contact us: Sahil.Kassie@firstdistribution.com