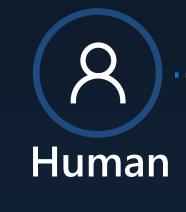
Microsoft Security Copilot Coverage and Capabilities

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



Submit a prompt

Receives response



Security

Orchestrator

Determines initial context and builds available skills

Build context

Executes the plan to get the required data context to

Analyzes all data and patterns to provide intelligent

Plugins

Responding

Copilot a plan using all the answer the prompt insights

Combines all data and context and the model will work out a response

Formats the data

Response

Security Copilot offers Al-driven guidance and analysis across identities, devices, data, clouds, and apps. It helps teams across the entire security stack catch what others miss, respond faster, and strengthen team expertise.

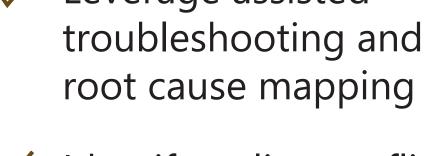
For security analysts



- alerts into concise, actionable summaries Receive actionable step-by-step
- guidance for incident response Analyze malicious scripts
- quickly and translate them to natural language with clear explanations
- Use Al-driven analytics to assess the potential impacts of security incidents

Leverage assisted

For IT admins



- Identify policy conflicts
- Drafting KQL queries to get real time device insights
- Policy creation guidance and summarization
- Optimize cloud PC performance
- Streamline update management

Uncover, manage and act on hidden risk



- Analyze incidents deeper
- and more efficiently Discover protection gaps
- and streamline controls Expedite data security
- investigations
- Explore Al-powered guidance to empower teams



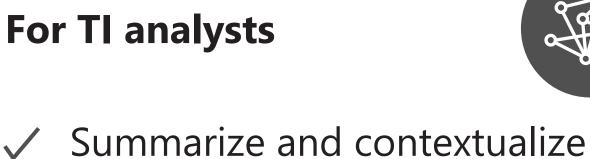
Get Al-driven risk detection,

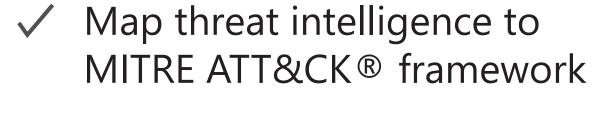
Troubleshoot access failures during critical access attempts

insights, and mitigation

- Manage least-privileged access for enhanced security
- Assisted incident investigation and troubleshooting

threat intelligence





Understand the threats most

- critical to your organization Find all threat intelligence
- related to an indicator or artifact Use promptbooks for a guided
- experience with common investigation workflows

For CISOs



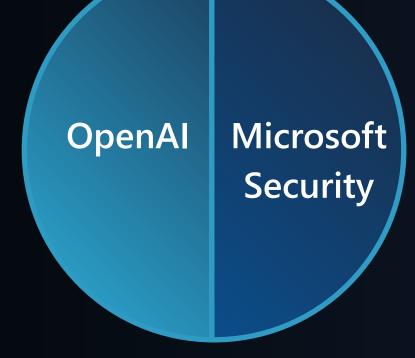
- Summarize and contextualize threat intelligence
- Create a report on the state of your organization's security posture
- optimized for the organization Prioritize critical security

Build custom security plans

- incidents Assess team performance

The Security Copilot advantage

Most advanced general models



infrastructure

Hyperscale

orchestrator

Security-specific

Plugins +

intelligence

Evergreen threat promptbooks

Cyber skills and



Copilot works across the Microsoft Security Microsoft is in a unique position to

transform security for our customers,

not only because of our investments in

Al, 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.

Standalone

Experiences to meet you

where and how you work

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

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already

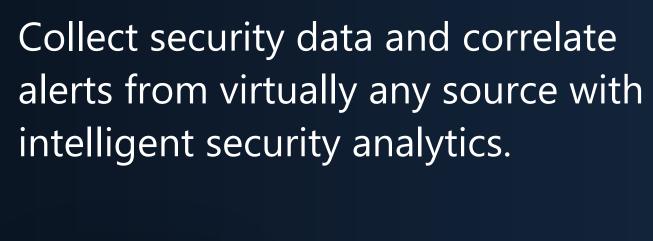
Embedded

work from and are familiar with.

product integrations

Security Copilot





Microsoft Entra

Help protect any identity and

Microsoft Sentinel



Microsoft Intune

Microsoft Purview



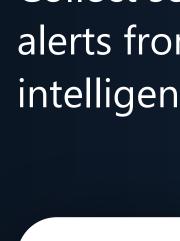
with Copilot.

Microsoft Defender **External Attack**

Surface Management See your rapidly changing, global external cyberattack surface in real time.

Subjects with

Copilot were



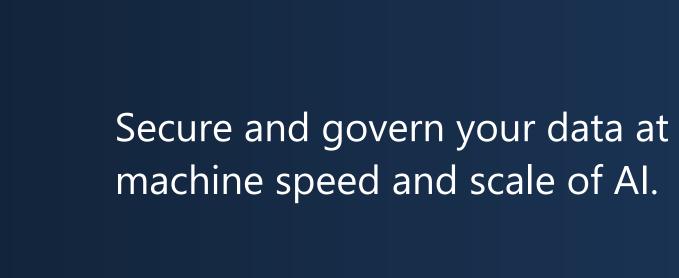
secure access to any resource with one family of solutions.

Microsoft Defender

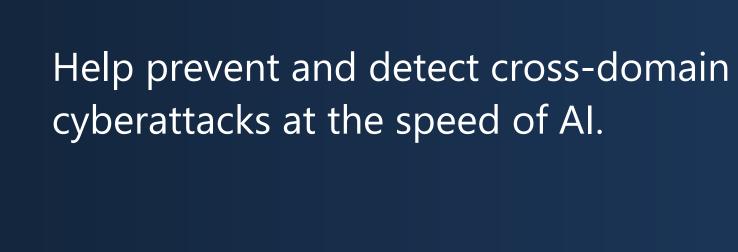
Understand multicloud risk and get

remediation recommendations.

for Cloud



Microsoft Defender



XDR



more accurate across all tasks Security Copilot randomized controlled trial (RCT) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024.

Ideas on how to measure

your own ROI Measure your team metrics for the six months prior to

Top metrics to compare would be: Mean time to respond

using Copilot against the

months of full team usage.

metrics for your first six

• Incidents worked per day ••• Average incident

resolution time

(MTTR)

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.

Analysts using

Security Copilot were

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.

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.

Measuring the quality of work is hard. Are you finding more

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)."