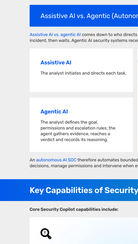
paramount

How Security Copilot Is Transforming Security Operations



Microsoft Security Copilot uses AI to investigate threats, generate queries, and automate security workflows with human oversight.

Microsoft Security Copilot is Microsoft's generative AI security platform for incident investigation, KQL query generation, threat intelligence and agent-led automation. It works across Microsoft Defender, Sentinel, Intune, Entra and Purview, combining organizational data with Microsoft's global threat signals. Analysts can use it interactively, while specialized agents handle defined tasks under human oversight across everyday enterprise security operations workflows today.

What Is Microsoft Security Copilot?

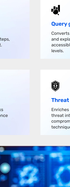
Security Copilot combines foundation models, security-specific orchestration and Microsoft threat intelligence, which now processes 100 trillion signals daily. It acts as an AI layer across Microsoft security products, not a replacement. A security operations center (SOC) is the team that monitors and responds to threats.

Assistive AI vs. Agentic (Autonomous) AI

Assistive AI vs. agentic AI comes down to who directs the workflow. Assistive AI completes a requested task, such as summarizing an incident, then waits. Agentic AI security systems receive an objective and decide which permitted steps to take towards it.

Assistive AI

The analyst initiates and directs each task.



Agentic AI

The analyst defines the goal, permissions and escalation rules; the agent gathers evidence, reaches a verdict and records its reasoning.

An autonomous AI SOC therefore automates bounded workflows, not the entire security function. Analysts still review consequential decisions, manage permissions and intervene when evidence is ambiguous.

Key Capabilities of Security Copilot

Core Security Copilot capabilities include:

Incident response

Correlates security signals into clear incident summaries, timelines and recommended next steps, helping analysts decide what to investigate first.

Query generation

Converts natural-language questions into KQL queries and explains existing queries, making threat hunting accessible to analysts with different technical skill levels.

Agentic automation

Uses specialized agents to perform defined tasks such as alert triage, threat hunting and intelligence briefings with analyst oversight.

Threat intelligence

Enriches organizational security data with Microsoft threat intelligence, connecting indicators of compromise to relevant actors, infrastructure, tools and techniques.

Incident Response & Summarization

Security Copilot incident response turns multi-signal Defender or Sentinel alerts into a readable timeline, affected assets, and recommended next steps. This AI incident summarization accelerates incident triage, which means determining what happened, how serious it is, and what needs attention first.

Natural-Language to KQL Query Generation

Natural language to KQL lets analysts describe a hunting question in plain English. Security Copilot KQL capabilities generate or explain the Kusto Query Language script used to search telemetry. This Security Copilot query generation lowers the technical barrier to threat hunting.

Agentic Automation (Security Copilot Agents)

Current Security Copilot agents in Defender cover alert triage, threat-intelligence briefings, threat hunting, security analysis, and dynamic threat detection. This Security Copilot agentic AI operates within assigned permissions. The Security Store provides Microsoft- and partner-built Security Store agents; some capabilities require SCUs.

Threat Intelligence Integration

Security Copilot threat intelligence combines Microsoft Defender Threat Intelligence with authorized organizational data. Analysts can connect indicators of compromise to threat actors, infrastructure, tools, and techniques without leaving the investigation workflow.

How Security Copilot Works

The Security Copilot architecture, which is increasingly being used to both in-house SOC teams and managed security services providers, typically follows a grounded response cycle:

1. A user submits a prompt.
2. The orchestrator selects relevant plugins and skills.
3. Those sources retrieve authorized organizational telemetry and threat context.
4. The model processes the grounded prompt.
5. Copilot applies safeguards and returns a plain-English answer with source references for review.

Where Security Copilot Fits: Standalone vs. Embedded

The standalone portal supports investigations across sources. Embedded experiences, including Security Copilot in Defender, place Copilot beside workflows in Defender, Sentinel, Entra, Intune, and Purview, although capabilities vary by product.

Security Copilot Licensing, Access & Pricing

Security Copilot pricing has three access paths:

ACCESS PATH	WHAT'S INCLUDED	TYPICAL COST	BEST FOR
E5/E7	400 SCUs per 1,000 paid licenses monthly, 10,000 cap	Included	Eligible tenants
Provisioned SCUs	Identity and Access Management	About US$4/SCU/hour	Predictable workloads
Overage	On-demand SCUs	About US$6/raised SCU	Unexpected spikes

E5/E7 inclusion depends on tenant rollout. Check Microsoft's pricing page for current regional rates and eligibility.

What Is a Security Compute Unit (SCU)?

A Security Compute Unit meters Copilot processing, like a compute allowance. Simple prompts may use part of an SCU; complex investigations and agents use more. Monitor consumption by workload.

How Security Copilot Is Transforming Day-to-Day Security Operations

The Microsoft Security Copilot benefits change how teams use AI in security operations:

- Automated alert triage
- Faster mean time to respond (MTTR)
- Wider access to KQL-led hunting
- More senior-analyst time for strategic investigations

1 Reducing Alert Fatigue and Analyst Burnout

Autonomous triage filters repetitive alerts and records its reasoning. Analysts can concentrate on credible threats instead of repeatedly proving low-severity activity harmless, reducing a persistent source of SOC workload and burnout.

2 Faster Incident Response Times

Copilot correlates alerts, entities, indicators and timelines that analysts otherwise gather manually. Suitable investigations can move from hours to minutes, although analysts must still validate the underlying evidence and recommended actions.

3 Upskilling Analysts and Closing the Skills Gap

Natural-language KQL and guided investigations let junior analysts attempt work once reserved for experienced query writers. Senior staff retain review authority while the wider team gains access to advanced hunting methods.

Security Copilot Use Cases by Role

Security Copilot use cases vary by role, from SOC triage to CISO reporting, and it is typically deployed alongside an organization's existing cloud security solutions rather than as a replacement for them.

ROLE	TYPICAL USE
SOC analyst	Incident triage and response
Threat-intelligence analyst	Hunting and KQL generation
Identity administrator	Entra and Conditional Access reviews
Cloud security administrator	Posture and infrastructure-as-code (IaC) remediation
Data security administrator	Purview and eDiscovery
CISO	Posture visibility and executive reporting

Getting Started with Security Copilot

A disciplined Security Copilot setup also makes later Security Copilot onboarding easier and follows six steps:

1. Confirm E5/E7 inclusion or provision SCUs.
2. Assign least-privileged roles.
3. Connect Defender, Sentinel, Entra, and Purview data.
4. Pilot one workflow, such as phishing triage.
5. Add suitable Security Store agents.
6. Monitor SCU consumption before expanding.

Organizations without in-house Copilot expertise often bring in implementation partners for tenant setup, RBAC design, role scoping and data connector setup carry the most risk of misconfiguration.

Key Considerations Before Adopting Security Copilot

Key Security Copilot limitations are operational in nature; keep these in mind when adopting Security Copilot:

- Consumption spikes can increase Security Copilot cost.
- Large prompts and promptbooks face context limits.
- Poorly connected or stale data weakens answers.
- Agents need scoped permissions and human oversight.
- Preview capabilities can change.

Why Partner with Paramount Assure to Deploy Security Copilot

A Security Copilot implementation partner should connect technology decisions to operational risk. Paramount combines cloud and threat-detection expertise with managed security services for AI (managed security services AI). Our Security Copilot consulting helps organizations size SCUs, connect useful data, configure least-privileged agents, and govern AI-led security actions.

Frequently Asked Questions

Q What is Microsoft Security Copilot used for?

A Microsoft Security Copilot supports incident response, KQL generation, agentic automation, and threat-intelligence enrichment across connected security tools. It works across connected security tools.

Q How much does Microsoft Security Copilot cost?

A Security Copilot pricing includes SCUs for eligible E5/E7 tenants. Other customers buy provisioned capacity and overage, so the Security Compute Unit price determines their Security Copilot cost. Verify Microsoft's current pricing.

Q Does my organization need Microsoft 365 E5 to use Security Copilot?

A No. Organizations without E5 or E7 can provision SCUs through Azure. Eligible E5/E7 tenants receive included capacity.

Q What is a Security Compute Unit (SCU)?

A An SCU meters Security Copilot compute, like a prepaid allowance. Consumption varies with each prompt, workflow or agent.

Q Is Security Copilot the same as Microsoft Copilot for Microsoft 365?

A No. Security Copilot serves security and IT teams. Microsoft 365 Copilot supports productivity applications such as Word and Teams.

Q Which Microsoft security products does Security Copilot integrate with?

A Security Copilot integrates with Defender, Sentinel, Intune, Entra and Purview. Access can be standalone or embedded.

Q Can Security Copilot act autonomously without an analyst?

A Agents can complete defined tasks autonomously. Analysts must govern permissions, monitor activity and validate consequential outputs.

Q How do I get started with Security Copilot for my organization?

A Confirm access, roles and data, then pilot one workflow. A guided Security Copilot onboarding program with Paramount can then expand agents and capacity safely.

Talk to a security specialist Plan a controlled Security Copilot deployment with Paramount Assure.