Synergy Advisors - Copilot for Security Architecture Design Sessions [ADS]

A Next-Gen AI-Powered Security Solution for Enhanced Efficiency and Capabilities of defenders to improve security outcomes at machine speed and scale.

Synergy Advisors' Copilot for Security Architecture Design Sessions [ADS] offers a high-level engagement tailored to empower organizations with the knowledge and skills required for a Copilot for Security implementation and optimization. Through a collaborative approach and in-depth design sessions, stakeholders gain valuable insights and recommendations to effectively leverage Copilot for Security in their security operations.

Architecture Design Sessions Overview

The Copilot for Security ADS encompasses a [1.5 – 2 days] architecture design workshop involving key stakeholders responsible for the design, operation, and implementation of Copilot for Security. This session includes knowledge transfer, focusing on recommended practices, lessons learned, and understanding your current environment to identify requirements. Additionally, it offers insights into common scenarios, unique use cases, and leveling up technology understanding.

Scope

The scope of this engagement includes the review and evaluation of your organization's readiness for Copilot for Security deployment. It covers assessing your current usage and configuration within the Microsoft security solutions, evaluating up to two use case scenarios, discussing granular security roles (RBAC controls), and exploring automation capabilities. Furthermore, it addresses capacity planning, usage monitoring, and cost optimization strategies.

Deliverables

Upon completion of the Copilot for Security ADS, the following deliverables will be provided:

- Business requirements document
- Solution design presentation, focusing on how Copilot for Security can help your organization's security needs, with recommendations from Synergy Advisors and with focus on specific use cases.

What's included in this engagement

The engagement includes:

- Copilot for Security Readiness: We assess the prerequisites and evaluate your tenant readiness level within the Microsoft security suite and its integration with Copilot for Security, including providing findings and recommendations to enhance readiness.
- Copilot for Security Use Case Scenarios: Evaluate up to two Copilot for Security use case scenarios.
- Granular Security Roles Configuration: Discuss security roles (RBAC) following industry best practices.
- Automation Capabilities: Understand Copilot's automation capabilities like promptbooks and logic apps to streamline their security processes.
- Capacity Planning and Usage Monitoring: Help you understand your needs and how to monitor usage to ensure optimal performance and cost optimization.

ADS – Key scenarios (Up to two)

1. Script Analysis with Microsoft Copilot for Security

Analyzing complex scripts demands a sophisticated level of technical expertise and experience to comprehend their functionality and ascertain their malicious intent. By harnessing Copilot for Security, we can demonstrate how it aids individuals lacking extensive experience or expertise in script analysis to effectively investigate potentially harmful scripts. This capability not only helps upskill SOC or security teams but also enhances their efficiency in threat detection and response.

Problem	Risk	Solution
- Threat actors deploy ever more complex scripts with sophisticated evasion techniques - There is a lack of expertise and experienced security professionals - Script analysis can be complex and time consuming	- Malicious scripts go unnoticed - Teams may be unable to determine if a script is malicious or not - Cybersecurity breaches from unnoticed malicious script execution - Data exfiltration	- Leverage Copilot for Security's capabilities to analyze scripts - Save time by running promptbooks for script investigation - Help upskill security professionals by leveraging Copilot for Security

2. Mitigating False Positive Sentinel Alerts with Copilot for Security

SOC efficiency and alert fatigue can have adverse effects on SOC teams. Copilot for Security offers analysts the opportunity to collaboratively brainstorm strategies for enhancing the quality of security alerts and mitigating the generation of false positive incidents.

Problem	Risk	Solution
- Alert fatigue - Security teams are unable to focus or prioritize the right incidents - There is a lack of quality check process	- Burnout among security personnel - Increased difficulty to prioritize incidents	- Use Copilot for Security's analysis capabilities to help investigate false positive incidents/alerts - Copilot can help find ways to improve the quality of security alerts and prevent false positive incidents from being generated - KQL generation to fine tune analytics rules and mitigate false positive alerts

3. Enhancing Security Analysis: Leveraging Copilot for Investigating and Remediating User Risks

The objective of this use case is to showcase Copilot for Security's role in aiding security analysts to detect and address user-associated risks within a cybersecurity landscape. It offers actionable recommendations and facilitates streamlined information retrieval through intuitive natural language queries.

Problem	Risk	Solution
- User behavior can often be a significant source of security risk. This can include risky actions such as clicking on phishing links, using weak passwords, or accessing sensitive data without proper authorization. - User actions can lead to security breaches ir data loss	- User account compromise - Unauthorized access to corporate resources - Lateral movement from adversaries	- Copilot for Security can help security tams analyze user activity logs, and recommending appropriate remediation actions for risky users

4. Copilot for Security: Streamlining Device Compliance Troubleshooting

The objective of this scenario is to illustrate how Copilot for Security offers comprehensive insights into individual device details and their compliance status. This encompasses the capability to diagnose policies, evaluate device compliance, and recommend potential remediation measures.

Problem	Risk	Solution
- Teams often struggle with managing and troubleshooting security policies and device compliance. - Not remediating device compliance can lead to potential security risks if devices are not compliant with the organization's security policies. - Non-compliant devices may conflict or cause issues with conditional access policies	- Non-compliant devices can become potential entry points for cyber threats - Troubleshooting policies and device compliance can be time-consuming and complex, potentially leading to oversight and errors	- Copilot for Security can help teams by providing detailed information about a specific device and its compliance status - Copilot can assist in troubleshooting policies, assessing device compliance, and suggesting possible remediation actions

Additional information

• This ADS is tailored for technical decision makers, and IT professionals.

• Experience in managing Microsoft 365/Azure Security solutions for cybersecurity incident management scenarios.

• Technical support and guidance will be provided throughout the ADS session.

Contact Us for more information about the '**Synergy Advisors' Copilot for Security ADS**' or our **Consulting Services**:

LEARN MORE

If you want to take your organization's security and compliance posture to the next level, if you are taking your first steps and want to quickly assess this technology as you progress along your path, **we offer the following options**:

Hands-On-Lab [HOL]

Step into the realm of advanced cybersecurity with our hybrid **Hands-On-Lab [HOL]** experience, where we delve deep into the transformative capabilities of Microsoft Copilot for Security. Join us as we embark on a journey to revolutionize your SecOps strategy through the power of AI-driven insights and recommendations. LEARN MORE

Proof of Concept [PoC]

The Copilot for Security PoC provides a streamlined approach to evaluating and demonstrating the capabilities of the solution within your organization. This (PoC) includes all necessary components, tools, and resources required to conduct a comprehensive assessment and showcase the functionality of Copilot for Security. LEARN MORE

Pilot

The Copilot for Security Engagement is a high-level session to prepare your organization for Copilot deployment. It involves evaluating readiness, reviewing usage and integration, validating use cases, implementing scenarios, configuring plug-ins, and providing knowledge transfer sessions on best practices. LEARN MORE

Why choose Synergy Advisors as your strategic partner?

At Synergy Advisors, we not only provide consulting and managed services but also accompany you every step of the way on your journey to digital excellence across Microsoft products and our solutions **(E-Suite)**, which amplify the power of your existing M365 and Azure investments. We are dedicated to driving your digital transformation, creating a more secure and efficient collaborative infrastructure. How do we achieve this? Through a unique blend of consulting expertise and managed services, we focus on your specific needs, offering comprehensive solutions that address both your security concerns and regulatory requirements.

Consulting Services

+12 years, +100 Top customers, and, with specializations in Security, Modern Work, Azure Data & AI, and Azure Infrastructure

We support our customers in the correct implementation of Microsoft solutions, aimed at improving their security postures and Modern Work, accompanied by a strategy that seeks to increase the adoption of these technologies and generate more upsell and cross-sell projects.

Managed Services

Leverage cybersecurity experts to review and monitor organizations' Microsoft 365 and Azure infrastructure and security. In-depth assessments of cloud applications, deployments as we help draft prioritized plans for improvements based on organizations unique security goals. Highly trained staff who monitor end-user activity through robust log analysis to provide you reliable monitoring, proactive and reactive incident response, and troubleshooting

Solutions (E-Suite)

Synergy Advisors' E-Suite seamlessly integrates various products with Microsoft 365, extending its features to address common advanced use cases encountered in organizations we've partnered with.

- E-Visor
- E-Visor Teams App
- E-Inspector
- E-Cryptor
- E-Vigilant
- E-Migrator