SYNERGY ADVISORS

Secure Multicloud Environments

WORKSHOP

SYNERGY ADVISORS

- END-TO-END SECURE PRODUCTIVITY
- IT AUTOMATION
- CYBERSECURITY
- CONTINUOUS OPTIMIZATION
- PRODUCTIVITY
- ALERTS AND NOTIFICATIONS

MANAGED | SOC *services*

- CYBERSECURITY MONITORING
- NETWORK SECURITY
- CORRELATED INCIDENT MGMT.
- APPLICATIONS SECURITY
- THREAT DETECTION AND INTELLIGENCE
- MGED. DETECTION AND RESPONSE

CONSULTING *services*

- ARCHITECTURE DESIGN SESSIONS [ADS]
- POC IN A BOX
- SECURITY AND COMP. ASSESSMENT
- PRODUCTION PILOT
- END-TO-END DEPLOYMENT
- ADOPTION AND CHANGE MGMT
- WORKSHOPS AND TRAININGS

SYNERGY ADVISORS

Security, Data Governance,
Modern Work, and Analytics
+12 Years
+6.5M End Users

E–SUITE *(and other) solutions*

- E-VISOR
- E-CRYPTOR
- E-INSPECTOR
- E-VIGILANT
- E-MIGRATOR
- YUBICO | THALES SECUDE | ENTRUST DARKTRACE | Others

SOLUTIONS

- SECURE E-MAIL
- SECURE COLLABORATION
- DEVICE PROTECTION
- INFO PROTECTION AND COMPLIANCE
- THREAT PROTECTION
- PLATFORM ´PROTECTION

E-Suite
SYNERGY ADVISORS

E-Visor

Enterprise-wide analytics

- Adoption and security correlated insights
- Configuration best practices
- Licensing usage and activity

E-Cryptor

- Document lifecycle management
- Self-service document access request
- Advanced collaboration
- Application integration

E-Inspector

- Data at rest content inventory and inspection
- Business and compliance driven data labeling and protection
- General alerts

E-Vigilant

- Advanced security and usage alerts and notifications
- Workflow based + E-Bot
- Business and technical incident management

E-Migrator

- Assess, discover, and analyze past and future meetings
- Zoom to Teams [Z2T] phased migration

Solutions

Secure E-mail

- Users
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation

Secure Collaboration

- Users (internal / external)
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation

Device Protection

- Applications security
- O.S. security
- Security baseline
- Threats
- Data Leak Mitigation

Information Protection and Compliance

- Data in use
- Data at rest
- Data in transit
- Application integration
- Data Leak Mitigation
- Structured and unstructured data protection

Threat Protection

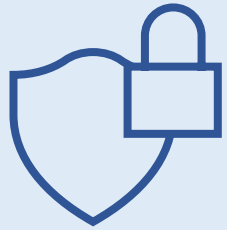
- Users (internal / external)
- Devices
- Identities
- Endpoints
- Cloud
- Monitoring
- Infrastructure
- Security baseline

Platform Protection

- Monitoring / Services analysis/ Alerts and notifications
- Security baseline

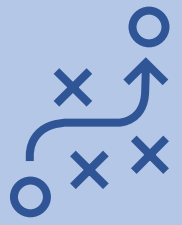
Microsoft Defender for Cloud

Multi-cloud Cybersecurity Challenges



Visibility into security and compliance

- **52%** of organizations cite secure configuration of cloud resources as a top priority.[1]



Increase in number and sophistication of attacks

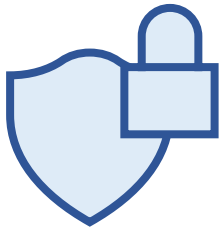
- In 2021, the average cost of a breach was **$4.24M**.[2]

Complexity managing multi-cloud environments

- **92%** of organizations are embracing a multi-cloud strategy

[1]Source: 451 Research
[2]Source: Ponemon Institute, Cost of a Breach Report

Microsoft Defender for Cloud - Benefits



Visibility into security and compliance

Constant monitoring
Identity and access management
Data encryption
Security analytics
Regular audits
Education and awareness
Trusted cloud service providers

Increase in number and sophistication of attacks

Threat Intelligence
Machine Learning and Behavioral Analytics
Integration with Security Ecosystem
Continuous Updates and Enhancements

Complexity managing multi-cloud environments

Centralized Security Management
Cross-Cloud Coverage
Unified Threat Detection and Response
Automated Security Policies
Integration with Cloud Provider Services

Secure Multi-Cloud Environments Workshop

Leveraging Microsoft Defender for Cloud security features

SYNERGY ADVISORS

Secure Multi-Cloud Environments Workshop

Threat and vulnerability analysis of your hybrid and multi-cloud environment

Learn how to build a more robust cloud security system with Microsoft Defender for Cloud.

What will you learn about?

- MDC benefits and capabilities
- Discover threats and vulnerabilities
- Prioritize and mitigate potential threats
- Reduce the attack surface area
- Define next steps based on your needs

Microsoft defender for Cloud

Security Hub that extends capabilities beyond your Azure resources to enhance your security posture across a Hybrid Cloud Environment, all managed through a single console.

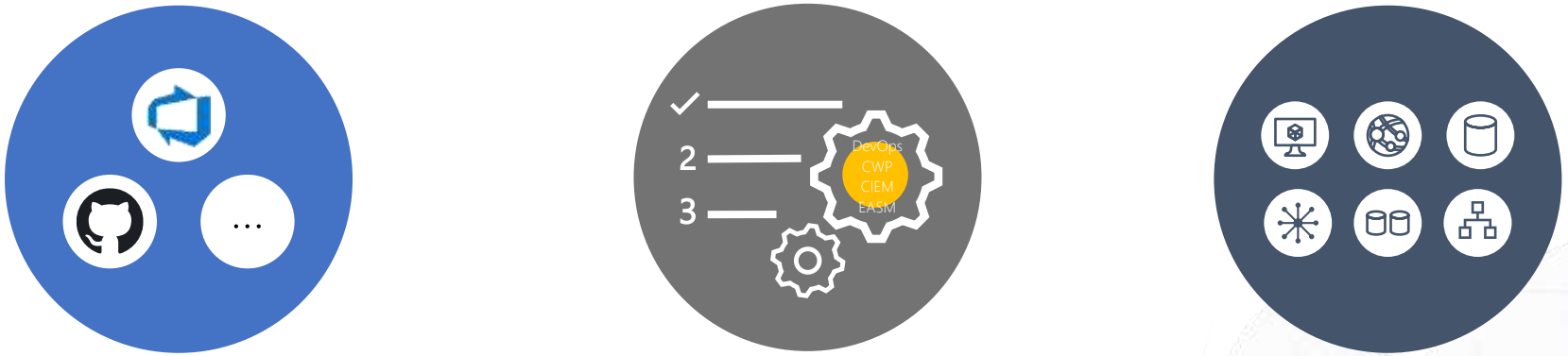
- **CSPM:** Visibility on security posture via the secure score, detection of security misconfigurations, asset inventory, and more.
- **CWPP:** Uses advanced AI and ML based intelligent protection and detection capabilities for Azure and hybrid cloud workloads, and helps to track compliance with regulatory frameworks and standards.

What is Microsoft Defender for Cloud (MDC)?

Unify your DevOps Security Management

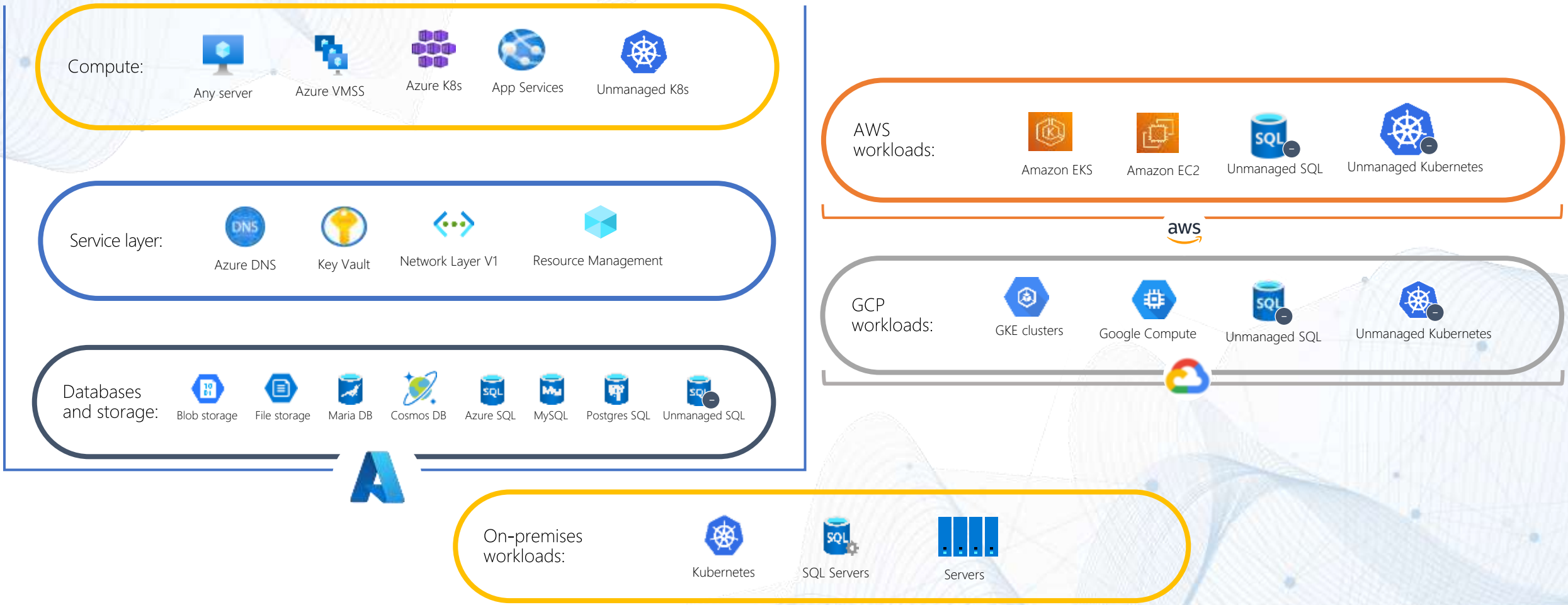
Strengthen and manage your cloud security posture

Protect your cloud workloads



aws

Full-stack coverage with dedicated detections



Secure Multi-Cloud Environments Workshop | Details

IN SCOPE

Work Product
- Overview session.
- Enable MDC security features enablement.
  - AWS and GCP enablement **[Optional]**
- Enable MDC features for Azure resources.
- Auto provisioning of:
  - Microsoft Monitoring Agent or Azure Monitoring agent for Azure VMs
  - Vulnerability assessment for machines
  - Guest Configuration agent
- Findings data collection
- Up to 3 Azure high risk events/recommendations.
- Microsoft POE and surveys required for payment.
- OPTIONAL: Manually onboarding of Windows Azure VMs in Microsoft Defender for Endpoint [MDE]

Document Deliverables
- Findings and recommendations presentation

OUT OF SCOPE

Work Product
- Production and pre-production environments modifications
- Additional incidents/recommendations review
- Additional Microsoft Azure and Microsoft 365 integration capabilities
- MDC or other Microsoft Defender trainings
- Non-Azure Arc-enabled Servers
- Onboard Linux Azure VMs
- Uninstall VMs extensions for collect security-related configuration and events logs
- Uninstall 3rd Party AV or EDR Servers solutions

Document Deliverables
- Findings and recommendations presentation

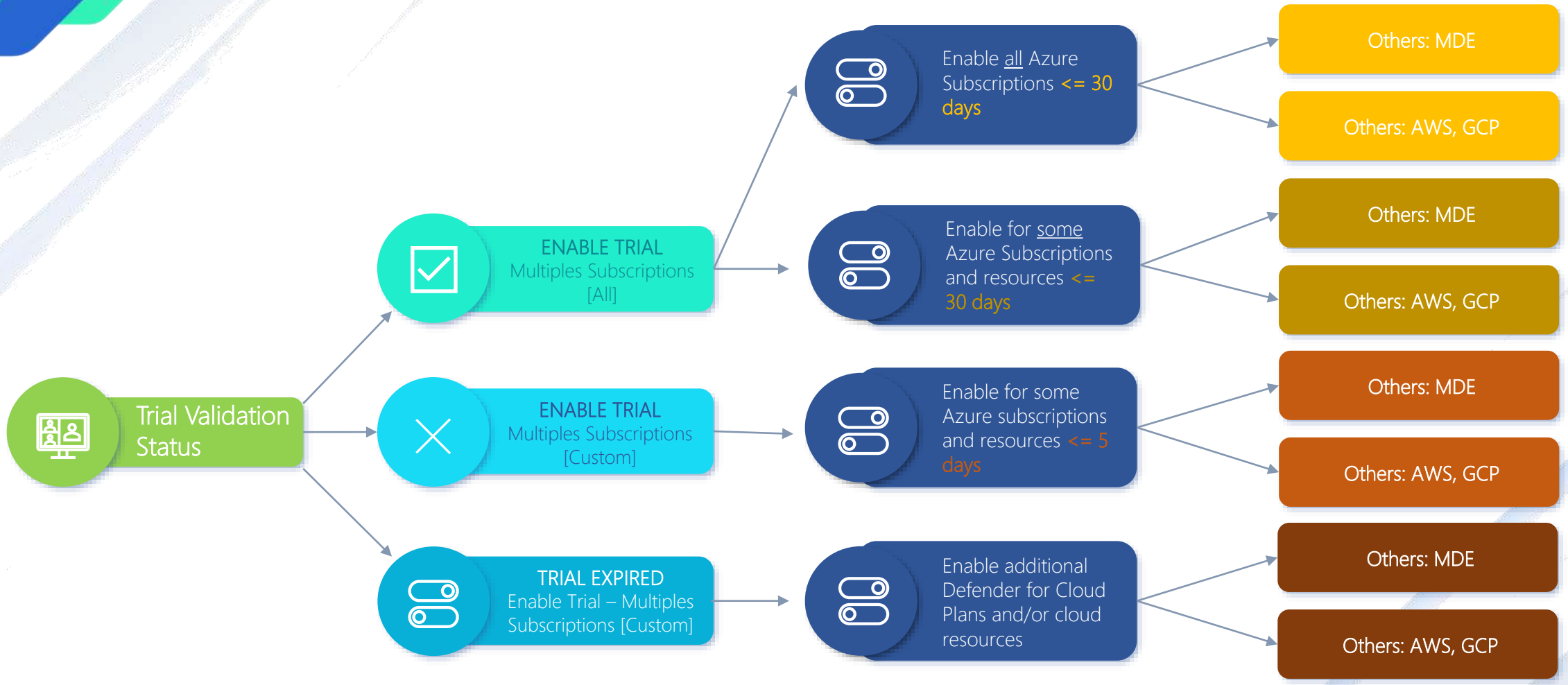
PRE-REQUISITES

Core
- MDC trial available for at least one Production Azure Subscription
- Include the account with the Owner or Security Admin role permissions for Azure subscription(s) in the engagement.

MDC & MDE (Better Together)
- For MDE Onboarded Windows VMs Servers:
  - Windows Server 2016 or later
  - For Windows 2016:
    - SSU from September 14, 2021, or later
    - Microsoft Defender Antivirus feature
    - Latest platform version using Windows Update
  - Internet access
- 3rd Party AV or EDR solution not installed

AWS / GCP
- Owner or Security Admin role permissions
- Administrator on AWS account
- Owner on the GCP organization or project

Microsoft Defender for Cloud implementation scenarios



Workshop phases

Phase 1

Validate MDC Trial

Phase 2

Turn ON Microsoft Defender for Cloud

Phase 3

Collect data

Phase 4

Turn OFF Microsoft Defender for Cloud

SYNERGY ADVISORS

Thanks!

Follow us…

Synergy Advisors | Synergy Advisors | Synergy Advisors LLC | @SynergySEC | @Synergyadvisors

Learn more about us

Consulting services

E-Suite solutions

Managed services

E-Visor

E-Visor Teams App

E-Inspector

E-Cryptor

E-Migrator

E-Vigilant