Proactive Protection for Multi-cloud Environments

SYNERGY ADVISORS

Assess, monitor, and protect your on-premises and cloud-based resources

Cloud security landscape

As organizations continue their journey to the cloud and adopt multi-cloud infrastructures, the threats to these environments are also growing in number and complexity.
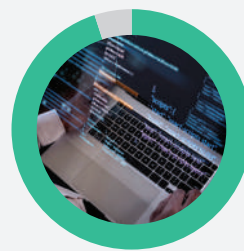
45%
... of security breaches are cloud-based

80%
... of companies experienced at least one cloud security incident in 2022.

99%
... of cloud security breaches are due to misconfigured resources.

59%
... of cloud professionals experienced an increase in complexity of attacks.

Secure your multi-cloud environments with Microsoft Defender for Cloud

Microsoft Defender for Cloud is a security platform designed to protect your on-premises and cloud-based resources for Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). Microsoft Defender for Cloud collects and processes data and evaluates your resources to provide you with a Secure Score, this way you can have a broad understanding of your current security posture.

Microsoft Defender for Cloud combines the **best practices** in security designed to protect cloud-based applications from various **cyberthreats and vulnerabilities**.

CSPM

CLOUD SECURITY POSTURE MANAGEMENT

Surfaces actions that you can take to prevent breaches
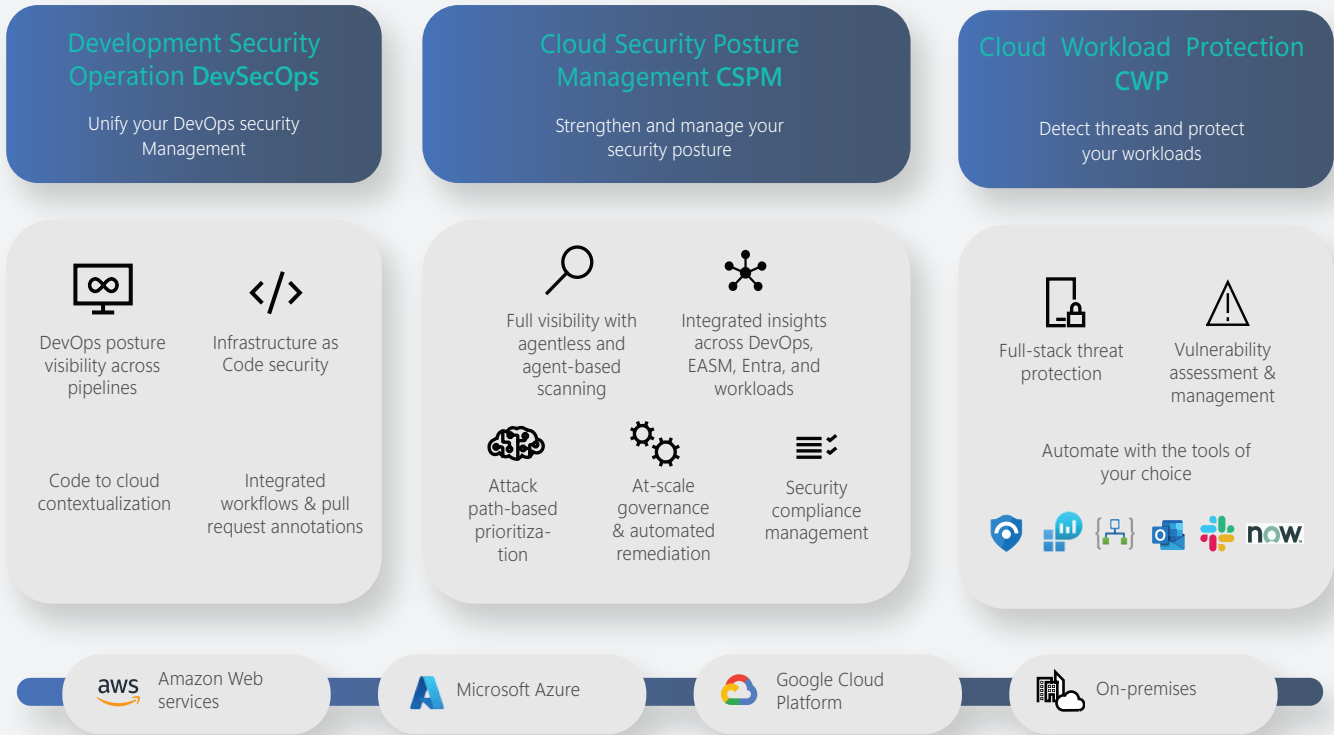
CWP

CLOUD WORKLOAD PROTECTION

Specific protections for servers, containers, storage, databases, and other workloads.

DevSecOps

DEVELOPMENT SECURITY OPERATIONS

Specific protections for servers, containers, storage, databases, and other workloads.

Microsoft Defender for Cloud's protection diagram

Development Security Operation **DevSecOps**
Unify your DevOps security Management

Cloud Security Posture Management **CSPM**
Strengthen and manage your security posture

Cloud Workload Protection **CWP**
Detect threats and protect your workloads

DevOps posture visibility across pipelines

Infrastructure as Code security

Code to cloud contextualization

Integrated workflows & pull request annotations

Full visibility with agentless and agent-based scanning

Integrated insights across DevOps, EASM, Entra, and workloads

Attack path-based prioritiza- tion

At-scale governance & automated remediation

Security compliance management

Full-stack threat protection

Vulnerability assessment & management

Automate with the tools of your choice

aws Amazon Web services

Microsoft Azure

Google Cloud Platform

On-premises

Advanced **features to protect** your cloud workloads from **cyberattacks** and meet **compliance** requirements, all while gaining **insights and visibility into your cloud environment**.

STRENGTHEN & MANAGE SECURITY POSTURE

Combination of agentless and agent-based scanning for full visibility and protection, while featuring attack path-based prior- itization to identify critical threats, and at-scale governance and automated remediation for easier compliance management.

DETECT THREATS AND PROTECT WORKLOADS

Microsoft Defender for Cloud uses full-stack threat protection and vulnerability assessment manage- ment. The platform is designed to provide continuous monitoring of your workloads, detecting, and responding to threats in real-time.

SECURITY COMPLIANCE MANAGEMENT

The platform offers compliance assessment reports that identify potential compliance gaps and provides remediation recommen- dations. It also includes built-in compliance controls for regula- tions such as GDPR, HIPAA, and ISO 27001.

Unified management console for multi-cloud enviroments

Manage and monitor your cloud security from a single pane of glass!
Configure **policies**, **alerts**, and **automate** responses across multiple cloud platforms, **all from one location**

Get started on your multi-cloud protection strategy with the
'Secure Multi-Cloud Environments' Workshop

'Secure Multi-Cloud Environments' Workshop is designed to get a customized threat and vulnerability analysis of your hybrid and multi-cloud environment and learn how to build a more robust cloud security system.

This workshop focuses on multi-cloud environments, which is why **we highly recommend enabling Microsoft Defender for Cloud** not only for your Azure subscriptions, but also creating connectors to your Amazon Web Services (AWS) accounts and Google Cloud Platform (GCP) projects. By doing so, you can fully leverage the capabilities of this powerful tool and experience its comprehensive value across multiple cloud platforms.

What can you get from this workshop?

Analyze threats and vulnerabilities of your multi-cloud environment.at-tacks.	Discover how to efficiently build a more robust and strong cloud security system.	Prioritize and mitigate potential threats, while reducing the attack surface area.	Develop defined next steps based on your business needs and objectives.

Workshop phases

|			
Validate MDC trial	Turn on MDC	Collect data	Turn off MDC

E-Visor post-workshop results report

Complement your multi-cloud protection experience with rich analytics from Synergy Advisors' E-Visor, an analytics solution that enables you to have control of what happens in your multi-cloud environment through the correlation of data resulting from the discoveries made by Microsoft Defender for Cloud, through holistic and security-driven integration between both technologies.
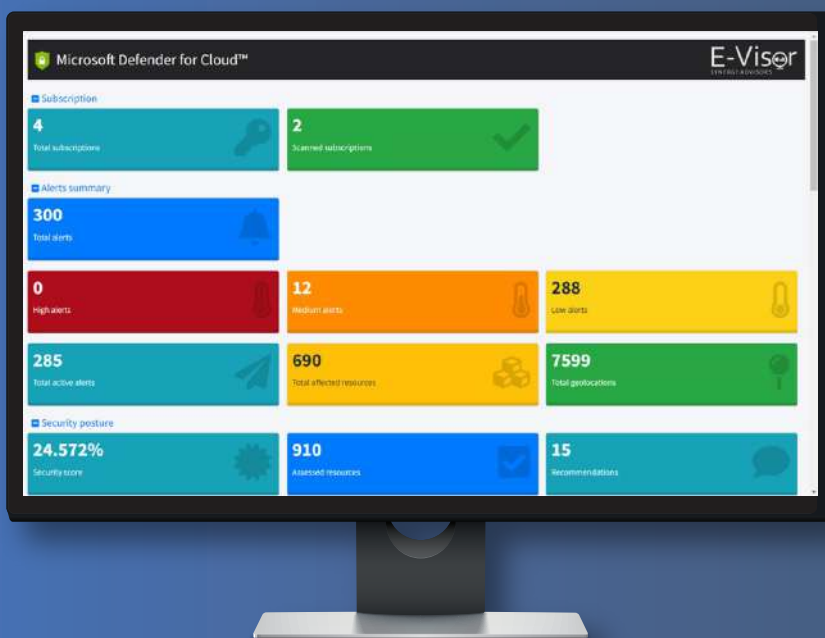
What can you find in the E-Visor for MDC reports?

• Active and scanned subscriptions.

• Active alerts in the Microsoft Defender for Cloud portal.

• Active alerts categorized by high, low, and medium severity levels.

• Affected resources and locations.

Security and Compliance posture, alerts, assessments, recommendations, and more!
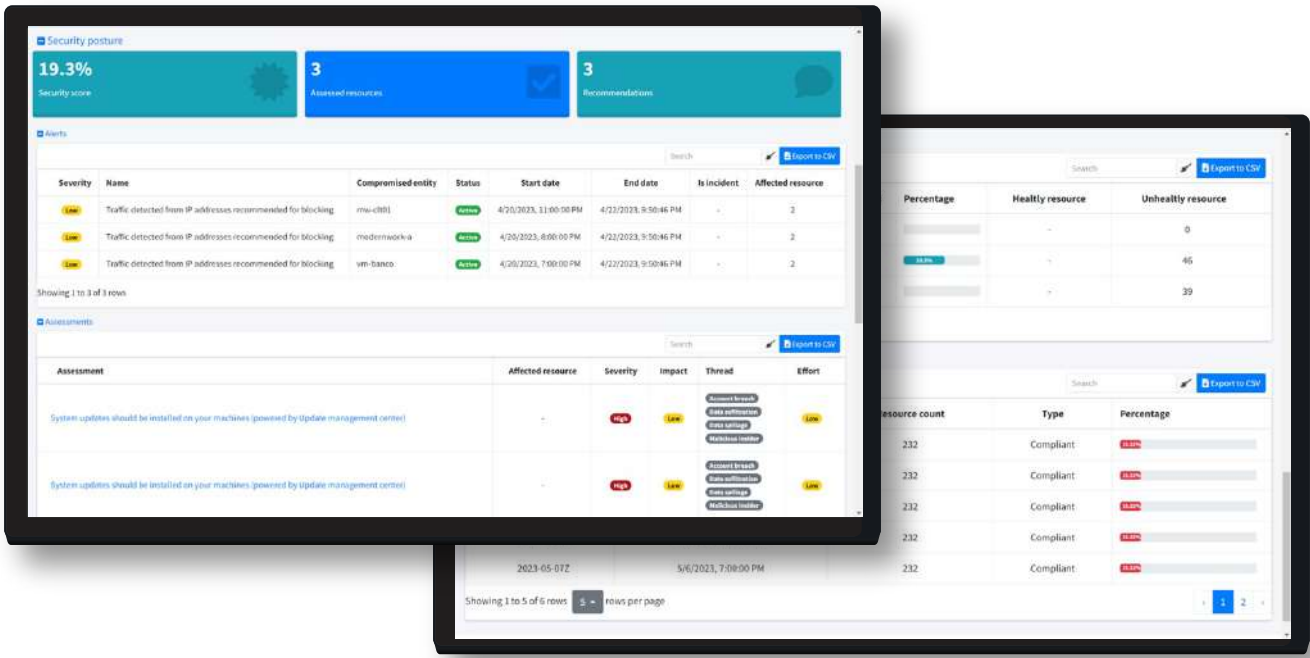
• Secure Score to help you improve the security posture of Azure resources, hybrid workloads, and multi-cloud environments.

• Total evaluated resources.

• Total recommendations provided by Microsoft Defender for Cloud to enhance the security of affected resources.

• Detailed information about the generated alerts.

• Table of global recommendations from Microsoft Defender for Cloud for the entire tenant.

• Number of recommendations that can be implemented on the affected resources to enhance their security.

• Insights into your compliance posture based on how you are meeting specific compliance requirements.

Contac us to get more information on the
**'Secure Multi-cloud Environments' Workshop,
or our Consulting Services**:

≫ **LEARN MORE**

About Synergy Advisors

Premier Microsoft Certified Partner specialized in Microsoft 365, identity, Azure B2C and B2B collaboration, security, Modern Work, and cloud technologies. We help you digitally transform and implement a more secure collaborative infrastructure, reduce IT costs, and meet regulatory requirements through our portfolio, and experience in consulting and managed services.

Secure E-mail	Secure Collaboration	Device Protection	Information Protection and compliance	Threat Protection	Platform Protection
• Users	• Users (internal / external)	• Applications security	• Data in use	• Users (internal / external)	• Monitoring / Services analysis/ Alerts and notifications
• Apps	• Apps	• O.S. security	• Data at rest	• Devices	• Security baseline
• Services	• Services	• Security baseline	• Data in transit	• Identities	
• Hygiene	• Hygiene	• Threats	• Application integration	• Endpoints	
• Threats	• Threats	• Data Leak Mitigation	• Data Leak Mitigation	• Cloud	
• Data Leak Mitigation	• Data Leak Mitigation		• Structured and unstructured data protection	• Monitoring	
				• Infrastructure	
				• Security baseline	