

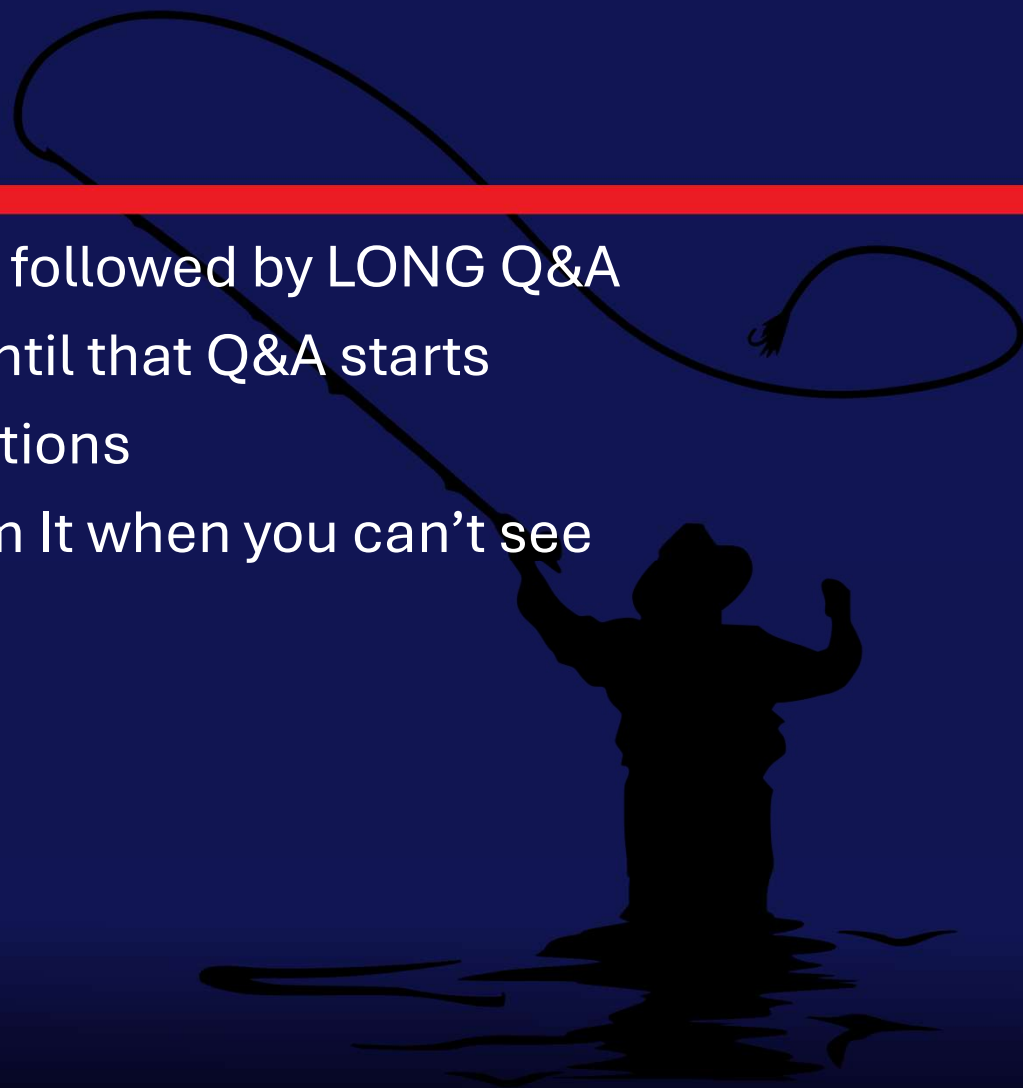
Achieve Zero Trust Objectives with Defender for Cloud and EASM Integrated with Defender XDR

Proactive protection pillars in the Microsoft Security stack



Attention

- ◆ MMS sessions are 60-75 minutes followed by LONG Q&A
- ◆ Please hold detailed questions until that Q&A starts
- ◆ Feel free to ask clarification questions
- ◆ Remind the speakers to use Zoom It when you can't see



Speakers



John Joyner

Senior Director, Technology @ Corsica Technologies

 john.joyner@corsicotech.com

 [in/johnjoyner](https://www.linkedin.com/in/johnjoyner)



Morten Knudsen

CONSULTANT, ARCHITECT, STRATEGIC ADVISOR

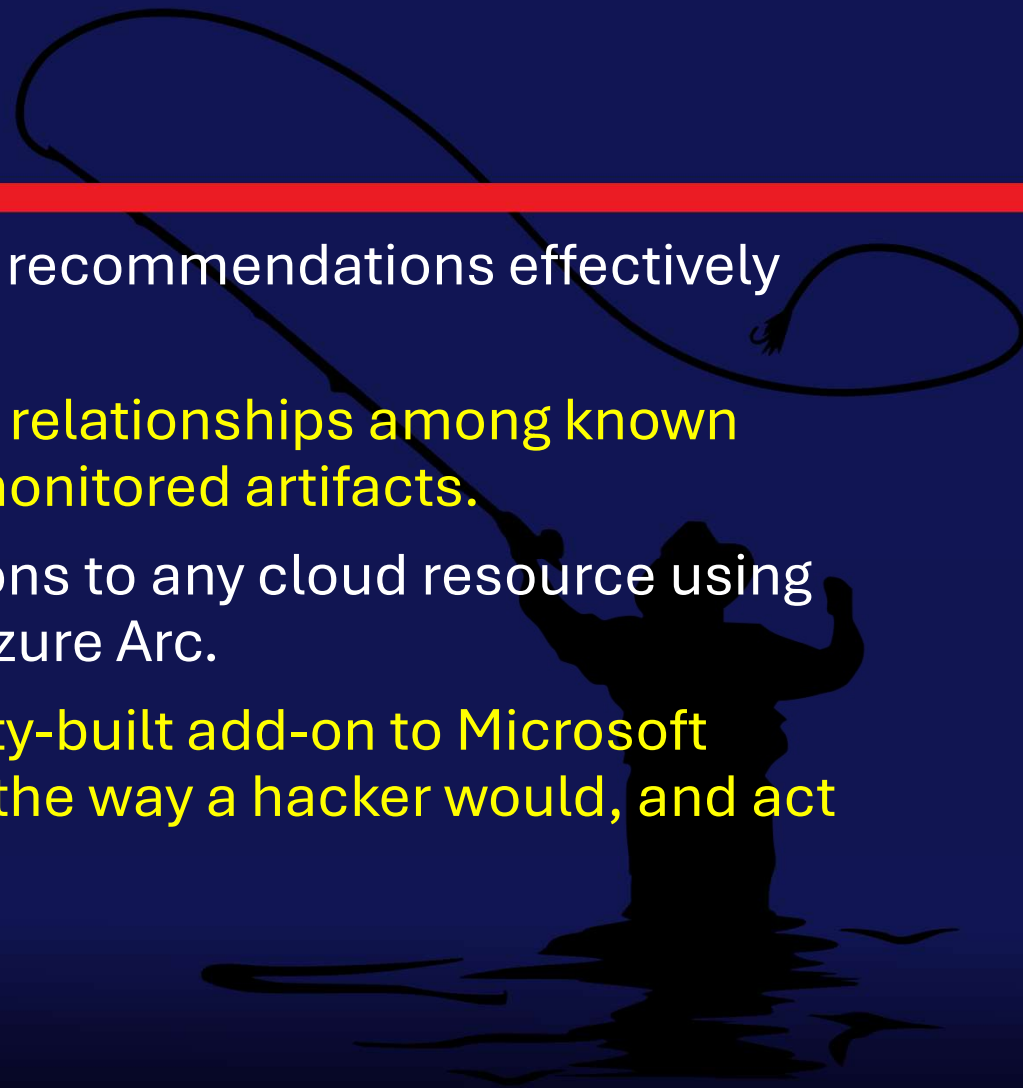
 mok@2linkit.net

 [in/knudsenmorten/](https://www.linkedin.com/in/knudsenmorten/)

Can't see our slides? Can't hear? Need to repeat the question? Call us out!

What you will learn

- ◆ Prioritize cross-platform security recommendations effectively using the Defender XDR portal.
- ◆ Utilize Defender EASM to identify relationships among known assets and reveal previously unmonitored artifacts.
- ◆ Extend CSPM and CIEM protections to any cloud resource using multi-cloud connectors and/or Azure Arc.
- ◆ SecurityInsight: a free, community-built add-on to Microsoft Defender that helps you see risk the way a hacker would, and act on it the way a defender must.



A silhouette of a cowboy in a hat, standing in water and swinging a lasso. The lasso is captured in mid-air, forming a large loop. The background is a solid dark blue.

The Microsoft Security Stack

Microsoft's security product portfolio:
Protecting all your cybersecurity domains.



The Microsoft Security Stack

◆ Microsoft 365 Client license bundles:

- ◆ Microsoft 365 E5/A5/G5 (or Microsoft 365 E7 which includes Microsoft 365 Agent)
- ◆ Microsoft 365 E3/A3/G3 + Microsoft Defender Suite
- ◆ Microsoft 365 Business Premium + Microsoft Defender Suite for Microsoft 365 Business Premium

◆ Defender for Cloud

- ◆ Cloud Workload Protection (CWP) plan 2 for servers, on for all workloads
- ◆ Cloud Security Posture Management (CSPM) for regulatory compliance

◆ Defender External Attack Surface Management (EASM)

- ◆ Microsoft Sentinel SIEM, Log Analytics Workspace, Logic Apps for automation, Azure Policy for governance
- ◆ Azure Update Manager (AUM), Change Tracking and Inventory
- ◆ Azure Arc for non-Azure servers and resources in any cloud
- ◆ Microsoft Security Copilot: Standalone, Embedded, and Agentic models



M365 E7

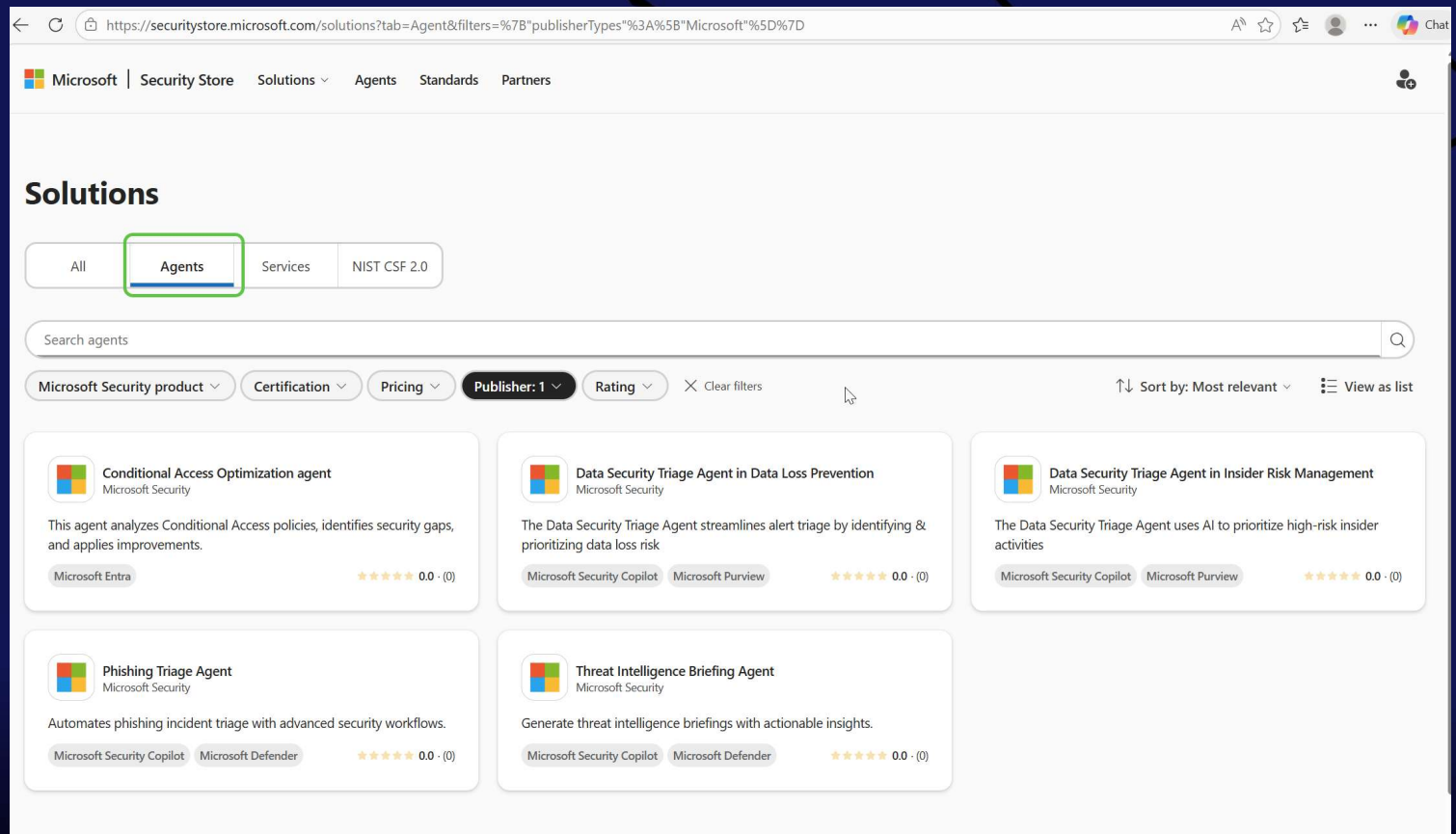
- ◆ The “Frontier Suite”
- ◆ Includes:
 - ◆ Microsoft 365 E5
 - ◆ Microsoft Entra Suite
 - ◆ Microsoft Entra Private Access
 - ◆ Microsoft Entra Internet Access
 - ◆ Microsoft Entra ID Protection
 - ◆ Microsoft Entra ID Governance
 - ◆ Microsoft Entra Verified ID
 - ◆ Microsoft 365 Copilot
 - ◆ Agent 365



Available May 1, 2026 for \$99 per user per month

The Microsoft Security Store

- ◆ Agentic solutions from Microsoft and partners
- ◆ Fractional SCU spend
- ◆ Fund with M365 E5 entitlement



The screenshot displays the Microsoft Security Store interface. The URL in the browser is <https://securitystore.microsoft.com/solutions?tab=Agent&filters=%7B%22publisherTypes%3A%5B%22Microsoft%22%7D>. The page features a navigation bar with 'Microsoft | Security Store | Solutions | Agents | Standards | Partners'. Below this, a 'Solutions' section has tabs for 'All', 'Agents' (highlighted with a green box), 'Services', and 'NIST CSF 2.0'. A search bar is present with the text 'Search agents'. Filter options include 'Microsoft Security product', 'Certification', 'Pricing', 'Publisher: 1', and 'Rating'. The results are sorted by 'Most relevant' and can be viewed as a list. Five security agents are displayed in a grid:

- Conditional Access Optimization agent** (Microsoft Security): This agent analyzes Conditional Access policies, identifies security gaps, and applies improvements. It is available for Microsoft Entra and has a rating of 0.0 (0).
- Data Security Triage Agent in Data Loss Prevention** (Microsoft Security): The Data Security Triage Agent streamlines alert triage by identifying & prioritizing data loss risk. It is available for Microsoft Security Copilot and Microsoft Purview and has a rating of 0.0 (0).
- Data Security Triage Agent in Insider Risk Management** (Microsoft Security): The Data Security Triage Agent uses AI to prioritize high-risk insider activities. It is available for Microsoft Security Copilot and Microsoft Purview and has a rating of 0.0 (0).
- Phishing Triage Agent** (Microsoft Security): Automates phishing incident triage with advanced security workflows. It is available for Microsoft Security Copilot and Microsoft Defender and has a rating of 0.0 (0).
- Threat Intelligence Briefing Agent** (Microsoft Security): Generate threat intelligence briefings with actionable insights. It is available for Microsoft Security Copilot and Microsoft Defender and has a rating of 0.0 (0).

Cloud Security Tools

Improve your security posture

- ◆ Unified security designed to scale with your business
- ◆ Help secure hybrid, multicloud, and AI workloads with premium integrated tools that streamline operations, strengthen compliance, and respond faster to threats.

<https://azure.microsoft.com/en-us/products/category/security>

<p>Network security Azure Firewall</p> <p>Get native firewall capabilities with built-in high availability and no maintenance requirements.</p> <p>Learn more</p>	<p>Network security Azure DDoS Protection</p> <p>Protect your Azure resources from distributed denial-of-service (DDoS) attacks.</p> <p>Learn more</p>	<p>Network security Azure Web Application Firewall</p> <p>Help improve web app security with a cloud-native firewall service.</p> <p>Learn more</p>	<p>Network security Azure Bastion</p> <p>Access virtual machines with private, managed Remote Desktop Protocol (RDP) and Secure Shell (SSH) connections.</p> <p>Learn more</p>
<p>Key management Azure Key Vault Premium</p> <p>Safeguard cryptographic keys and other secrets used by cloud apps and services.</p> <p>Learn more</p>	<p>Key management Azure Key Vault Managed HSM</p> <p>Create and maintain keys that access and encrypt your cloud resources, apps, and solutions.</p> <p>Learn more</p>	<p>Key management Azure Cloud HSM</p> <p>Safeguard cryptographic keys within your private virtual network.</p> <p>Learn more</p>	<p>Featured security innovations Microsoft cloud security benchmark</p> <p>Get best practices and recommendations for securing your workloads, data, and services across multicloud platforms.</p> <p>Learn more</p>
<p>Featured security innovations Multifactor authentication enforcement</p> <p>Enable one of the most effective security measures for your organization.</p> <p>Learn more</p>	<p>Featured security innovations Azure Local</p> <p>Operate infrastructure across distributed locations with unified management enabled by Azure Arc.</p> <p>Learn more</p>	<p>Featured security innovations Microsoft Foundry</p> <p>Accelerate innovation with a complete, integrated, and interoperable AI platform.</p> <p>Learn more</p>	<p>Microsoft Security Microsoft Defender for Cloud</p> <p>Protect multicloud and hybrid environments with integrated security from code to cloud.</p> <p>Learn more</p>
<p>Microsoft Security Microsoft Entra</p> <p>Get unified identity and network access solutions.</p> <p>Learn more</p>	<p>Microsoft Security Microsoft Sentinel</p> <p>Simplify security operations with intelligent security analytics and scale as you grow.</p> <p>Learn more</p>	<p>Microsoft Security Microsoft Purview</p> <p>Safeguard data wherever it lives with a collection of unified information protection, governance, and compliance products.</p> <p>Learn more</p>	<p>Microsoft Security Microsoft Security Copilot</p> <p>Efficiently protect your organization with a generative AI-powered assistant for daily security and IT operations.</p> <p>Learn more</p>

A silhouette of a person standing in water, holding a lasso that is looped in the air. The background is a dark blue gradient.

Microsoft Defender for Cloud CSPM and CNAPP

CSPM: Cloud Security Posture Management

CNAPP: Cloud Native Application Protection Platform
(superset of CWP, Cloud Workload Protection)

The Total Economic Impact™ Of Microsoft Defender For Cloud

<https://tei.forrester.com/go/Microsoft/DefenderForCloud>

Cost Savings And Business Benefits Enabled By Defender For Cloud

- ◆ 10% license savings compared to legacy security infrastructure tools
- ◆ 30% percent improvement in SecOps productivity from expanded visibility, context, and automations.
- ◆ 50% percent reduction in false positives and 30% decrease in the time to investigate and remediate threats.
- ◆ 10% percent reduction in incidents needing response that would not have been caught in the prior environment.
- ◆ 15% reduction in audit compliance overhead and lower reliance on auditing services.

KEY STATISTICS



RETURN ON INVESTMENT (ROI)
117%



BENEFITS PV
\$9.28M

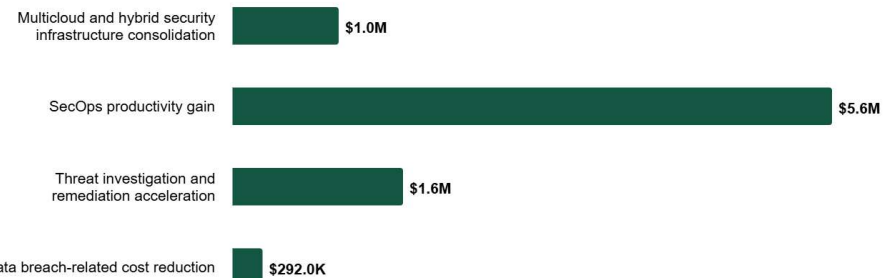


NET PRESENT VALUE (NPV)
\$5.0M



PAYBACK
<6 months

Benefits (Three-Year)



Enable Defender for Cloud CSPM

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

Search << Save Settings & monitoring





Settings

- Defender plans
- Security policies
- Email notifications
- Workflow automation
- Continuous export

Enable all plans

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
 Foundational CSPM	Free Details >		 Full	Off On
 Defender CSPM	\$5/Billable resource/Month Details >	68 resources ⓘ	 Full Settings >	Off On

Defender for Cloud CSPM

- ◆ Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.
- ◆ Pricing: \$5 per billable resource per month
- Agentless VM vulnerability scanning
- Agentless VM secrets scanning
- Attack path analysis
- Risk Prioritization
- Risk hunting with Security Explorer
- Code-to-cloud mapping for IaC
- PR annotations
- Internet exposure analysis
- External attack surface management (EASM)
- Permissions Management (CIEM)
- Regulatory compliance assessments
- Regulatory compliance assessments
- ServiceNow Integration
- Critical assets protection
- Governance to drive remediation at-scale
- AI Security Posture Management
- Code-to-cloud mapping for Containers
- Data-aware security posture, Sensitive data scanning
- Kubernetes API access
- Agentless code-to-cloud containers vulnerability assessment
- API Security Posture Management

Free foundational security posture capabilities

- Continuous assessment of the security configuration of your cloud resources
- Security recommendations to fix misconfigurations and weaknesses
- Secure score summarizing your current security situation

Defender for Cloud CSPM: What's included

- ◆ In-Azure, AWS, and GCP platform-only
- ◆ **Universally: compute, storage, and database**
- ◆ No Azure Arc support
- ◆ **CIEM & Serverless (new)**

The screenshot displays the Microsoft Defender for Cloud console interface. On the left is a navigation pane with a search bar and a list of menu items. The 'Posture management' section is highlighted with a green box, and 'Overview Cloud Security Posture Management (CSPM)' is selected. On the right, three tables are shown, each with a green arrow pointing to it from a platform label (Azure, AWS, GCP) in a green box. Each table lists supported services, resource types, and exclusions.

Azure

Service	Resource Types	Exclusions
Compute	Virtual machines, VM scale sets, classic VMs	Deallocated VMs, Databricks VMs
Storage	Storage accounts	Accounts without blob containers or file shares
Databases	SQL servers, PostgreSQL/MySQL servers, Synapse workspaces	-

AWS

Service	Resource Types	Exclusions
Compute	EC2 instances	Deallocated VMs
Storage	S3 buckets	-
Databases	RDS instances	-

GCP

Service	Resource Types	Exclusions
Compute	Compute instances, Instance Groups	Nonrunning instances
Storage	Storage buckets	Nearline/coldline/archive classes, unsupported regions
Databases	Cloud SQL instances	-

Defender for Cloud CSPM: What's new

CIEM: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-permissions-management> (Azure CIEM, AWS CIEM, GCP CIEM)

Serverless: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/serverless-protection> (Azure Web Apps, Azure Functions, and Amazon Web Service (AWS Lambda))

Home > Microsoft Defender for Cloud | Environment settings > Settings | Defender plans

Settings & monitoring

N/A

Continue

When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy.

Defenders plans: **Defender CSPM**

Component	Description	Defender plans	Configuration	Status
Cloud Infrastructure and Entitlements Management (CIEM)	Cloud Infrastructure Entitlement Management (CIEM) in Microsoft Defender for Cloud provides native visibility into who has access to what across cloud environments. CIEM discovers and analyzes effective permissions for human and non-human identities analyzing inactive, excessive, and risky access to multi-cloud resources, enabling enforce least-privilege access and reduce privilege escalation risk. The setup, data collection, and recommendation generation process may take up to 24 hours. Learn more		-	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On
Serverless protection	Defender for Cloud protects serverless workloads by continuously discovering all resources, assessing their configuration posture, and detecting security risks. It scans function packages for vulnerable dependencies, highlights security issues, and provides clear remediation guidance. Additionally, it maps attack paths involving serverless components to help proactively mitigate potential exploitation.		-	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On

Pricing: \$5/Billable resource/Month (From April 1, 2026) ⓘ

Use Defender for Cloud CSPM in the Defender XDR Portal

The screenshot displays the Microsoft Defender XDR Portal interface. The left-hand navigation pane includes a search bar for 'Find Defender solutions' and a list of solution categories: Home, Incidents, Advanced hunting, All Solutions, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, and Cloud security. The 'Cloud security' category is expanded, showing 'Overview' and 'Regulatory compliance', with the latter highlighted by a green box. The main content area is titled 'Regulatory compliance' and features a summary of 5 industry frameworks, 0 custom frameworks, and 403 related recommendations. Below this, there are tabs for 'Regulatory frameworks' and 'Policies', an 'Export' button, and a table of compliance frameworks with their respective progress percentages.

Compliance frameworks	Progress
Azure CSPM	23.16%
PCI DSS 4	41.46%
CMMC Level 3	42.17%
Azure FFIEC CAT 2017	51.11%
ASC Default	55.68%

Use Defender for Cloud CSPM in the Defender XDR Portal

The screenshot displays the Microsoft Defender XDR Portal interface. The left-hand navigation pane includes sections for Home, Incidents, Advanced hunting, All Solutions, Investigation & response, Threat intelligence, and Assets. The 'Recommendations' section is highlighted in the navigation pane. The main content area is titled 'Recommendations' and is filtered to show 'Cloud' recommendations. It features a 'Recommendations summary' section with a 'Cloud secure score' of 50.2% (Moderate) and a 'Score history' line chart showing a decrease of -12.2% over the last 6 days. Below this, there is a 'Recommendations by risk level' bar chart showing 5 Critical items. A 'How risk level is calculated?' section explains that risk level is determined by Recommendation risk and Asset risk factors (Defender CSPM). At the bottom, there is an 'Export' button, a search bar, and a table of recommendations. The table has columns for Risk level, Recommendation title, Exposed asset, and Asset risk factors. Two recommendations are visible, both marked as Critical.

Risk level	Recommendation title	Exposed asset	Asset risk factors
Critical	Storage accounts should prevent shared key access	storageaccounttamba	Sensitive Data +2 0
Critical	Managed identitv should be enabled on web apps	basheadmovement	Exposure to the Int... +1 0

DEMO

Microsoft Defender for Cloud CSPM

Indispensable tools in a Zero Trust compliance initiative.



A silhouette of a cowboy in a hat, standing in water and holding a lasso that is looping through the air. The background is a dark blue gradient.

Microsoft Defender EASM

External Attack Surface Management (EASM): Providing an external view of your online infrastructure.

Microsoft Defender EASM

- ◆ Continuously discovers and maps an organization's digital attack surface to provide an external view of their online infrastructure. This visibility enables security and IT teams to identify unknowns, prioritize risk, eliminate threats, and extend vulnerability and exposure control beyond the firewall.
- ◆ Leverages Microsoft's crawling technology to discover assets that are related to an organization's known online infrastructure, and actively scans these assets to discover new connections over time.
- ◆ Attack Surface Insights are generated by leveraging vulnerability and infrastructure data to showcase the key areas of concern for an organization.

Enable Defender for Cloud EASM

Home > Microsoft Defender EASM >

Create Microsoft Defender EASM Resource

Basics Review + create

Microsoft Defender External Attack Surface Management (Defender EASM) uses proprietary technology to build a dynamic inventory of your web applications, third-party dependencies, and web infrastructure. We combine that with latest threat research and vulnerability intelligence to give you visibility into your organization's security posture.

New Defender EASM resources start with a 30-day trial. After the trial period you will be automatically billed at the standard metered rate.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name * ⓘ
 ❌ Only alphanumeric characters are allowed, and the value must be 1-30 characters long.

Region * ⓘ

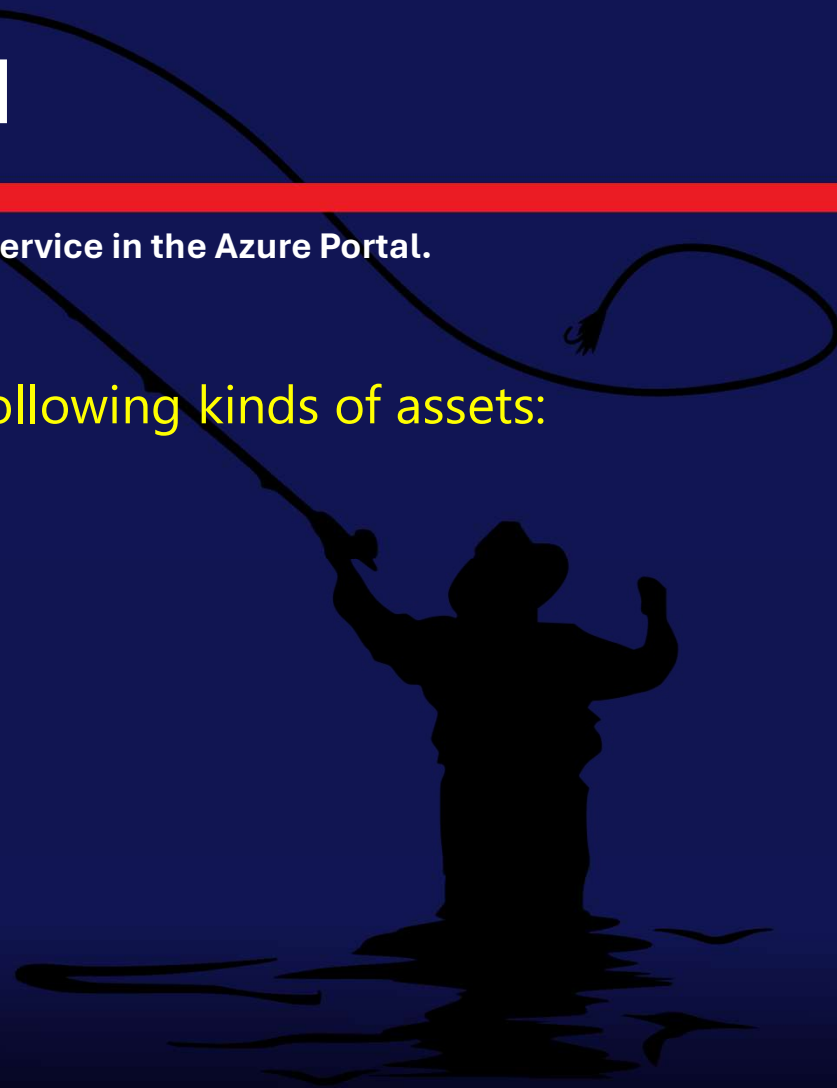


Defender for Cloud EASM

- ◆ Defender for Cloud EASM is available as an on-demand microservice in the Azure Portal.
- ◆ Pricing: \$0.011 asset/day

Defender EASM includes the discovery of the following kinds of assets:

Domains
Hostnames
Web Pages
IP Blocks
IP Addresses
ASNs
SSL Certificates
WHOIS Contacts



Use Defender for Cloud EASM in the Defender XDR Portal

The screenshot shows the Microsoft Defender XDR Portal interface. The left sidebar contains navigation options such as Home, Incidents, Advanced hunting, All Solutions, Investigation & response, Threat intelligence, and Assets. The main content area is divided into several sections:

- 14-day trend:** A bar chart showing a downward trend in protection score over the last 14 days.
- External Attack Surface Protection: 94%**: A prominent green box highlighting the current protection score. Below it, a progress bar shows a -1% change (last 14 days), a target score of 99%, and the last update time: May 5, 2026 1:27:38 PM.
- Security recommendations:** A table listing various recommendations with their status and the product used for remediation.

Name	Points achieved	Product
Remediate internet-facing assets with high or critical severity CVE vulnerabilities	-	EASM
Replace SSL SHA1 certificates with new SSL certificates that use SHA-256	-	External Attack Surface Pro...
Consider reregistering expired domains	-	EASM

At the bottom of the page, there is a blue button labeled "Open initiative page" with a green arrow pointing to it.

Use Defender for Cloud EASM in the Defender XDR Portal

The screenshot shows the Microsoft Defender XDR Portal interface. The left sidebar contains navigation options: Home, Incidents, Advanced hunting, All Solutions, Exposure management (highlighted), Initiatives (highlighted), Vulnerability management, Attack surface, Investigation & response, Threat intelligence, and Intel management. The main content area displays the External Attack Surface Protection (EASM) dashboard. The dashboard shows a score of 94% with a downward trend arrow, indicating a decrease of 1% over the last 14 days. The target score is 99%. The dashboard includes tabs for Overview, Security metrics (6), Security recommendations, and History. The Overview tab is active, showing a description of the EASM initiative and a table of top metrics.

External Attack Surface Protection: 94%

↓ -1% (last 14 days) • Your target score: 99% • Last updated: May 5, 2026 1:27:38 PM

Initiative info

Description

The External Attack Surface Initiative in Microsoft Security Exposure Management uses Defender EASM to continuously discover and map your digital attack surface, providing an external view of your online infrastructure. This helps security and IT teams identify unknown assets, prioritize risks, eliminate threats, and extend control beyond the firewall. Note: This initiative provides high-level insights and supports either viewing subscription details or selecting pre-built footprints for analysis. [Learn more here.](#)

Resource Name
easmjohnjoynet

Top metrics

Name	Progress	State	Recommendations	Assets	History
Internet-facing assets with high severit...	71.88%	Needs att...	1	9	95%
Assets allowing remote access	100%	Target met	1	0	94.75%
Internet-facing assets with critical sever...	100%	Target met	1	0	94.5%
Assets utilizing SSL SHA1 certificates	100%	Target met	1	0	94.25%
Expired domains	100%	Target met	1	0	94%
Recently expired SSL certificates	-	-	-	-	93.75%

[View all metrics](#)

[View histo](#)

Copilot for Security and Defender EASM

◆ **Defender for Cloud EASM is installed by default as a Security Copilot plug-in**



Sample prompts:

- What are the high priority attack surface insights for my organization?
- **Get assets affected by high priority CVSS's in my attack surface.**
- How many assets are using SSL SHA1 for my organization?
- **Get list of expired SSL certificates.**



DEMO

Microsoft Defender EASM

Indispensable tools in a Zero Trust compliance initiative.



A silhouette of a cowboy on a horse, holding a lasso that is looped in the air. The scene is set against a dark blue background.

Zero Trust and Cloud Security Posture Management (CSPM)

How Defender for Cloud CSPM and EASM features help an organization get closer to a Zero Trust model

Don't Trust and Do Verify

- ◆ At the essence of a Zero Trust strategy is the mindset that all entities and processes are assumed to be untrustworthy until found otherwise. That means for every IT activity we need to implement a verification process to validate the trust for the activity.
- ◆ We don't trust a user login until multi-factor authentication (MFA) has been completed. Likewise, we don't trust a user to safely operate their corporate computing device without endpoint detection and response (EDR) in place.
- ◆ MFA and EDR are well accepted solutions for organizations seeking a Zero Trust model. For the security team wanting to assure their due diligence in cybersecurity architecture, another front-line Zero Trust resource is a Cloud Security Posture Management (CSPM) solution.

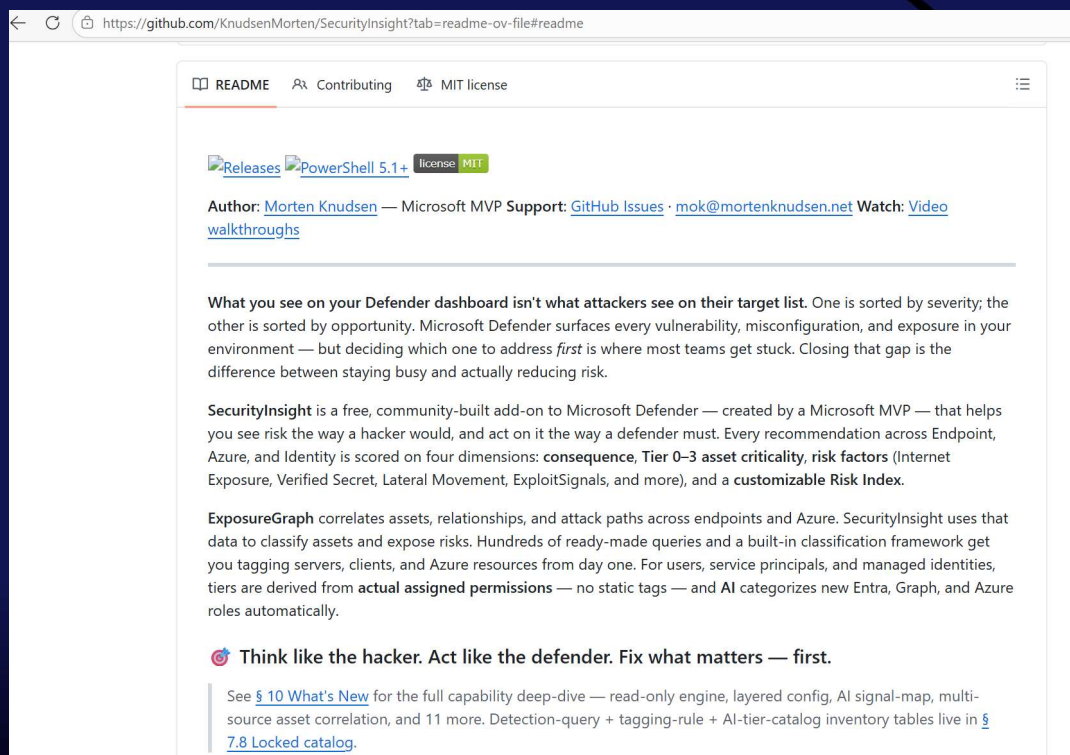
CSPM Features contributing to Zero Trust

The core posture management capabilities of a CSPM can be considered:

1. Continuous assessment of the security configuration of your cloud resources
2. Delivery of security recommendations to fix misconfigurations and weaknesses
3. A reporting or scoring capability for compliance assessment. This is how you achieve Zero Trust with your computing resources—by inspecting them.

Introducing: SecurityInsight

<https://github.com/KnudsenMorten/SecurityInsight>



The screenshot shows the GitHub repository page for SecurityInsight. At the top, there are navigation links for README, Contributing, and MIT license. Below that, there are links for Releases, PowerShell 5.1+, and a license badge for MIT. The author information is listed as Morten Knudsen, a Microsoft MVP, with links to GitHub Issues, an email address (mok@mortenknudsen.net), and video walkthroughs. The main text of the README describes the tool's purpose: to help users understand risk from a hacker's perspective. It explains that while Microsoft Defender shows vulnerabilities, SecurityInsight helps prioritize them based on severity and opportunity. The tool is a free, community-built add-on to Microsoft Defender, created by a Microsoft MVP. It helps users see risk the way a hacker would and act on it the way a defender must. Every recommendation across Endpoint, Azure, and Identity is scored on four dimensions: consequence, Tier 0-3 asset criticality, risk factors (Internet Exposure, Verified Secret, Lateral Movement, ExploitSignals, and more), and a customizable Risk Index. ExposureGraph is also mentioned, which correlates assets, relationships, and attack paths across endpoints and Azure. SecurityInsight uses this data to classify assets and expose risks. The README concludes with the motto: 'Think like the hacker. Act like the defender. Fix what matters — first.' and provides a link to a 'What's New' section for a full capability deep-dive.

← <https://github.com/KnudsenMorten/SecurityInsight?tab=readme-ov-file#readme>

README Contributing MIT license

Releases PowerShell 5.1+ license MIT

Author: [Morten Knudsen](#) — Microsoft MVP Support: [GitHub Issues](#) · mok@mortenknudsen.net Watch: [Video walkthroughs](#)

What you see on your Defender dashboard isn't what attackers see on their target list. One is sorted by severity; the other is sorted by opportunity. Microsoft Defender surfaces every vulnerability, misconfiguration, and exposure in your environment — but deciding which one to address *first* is where most teams get stuck. Closing that gap is the difference between staying busy and actually reducing risk.

SecurityInsight is a free, community-built add-on to Microsoft Defender — created by a Microsoft MVP — that helps you see risk the way a hacker would, and act on it the way a defender must. Every recommendation across Endpoint, Azure, and Identity is scored on four dimensions: **consequence**, **Tier 0-3 asset criticality**, **risk factors** (Internet Exposure, Verified Secret, Lateral Movement, ExploitSignals, and more), and a **customizable Risk Index**.

ExposureGraph correlates assets, relationships, and attack paths across endpoints and Azure. SecurityInsight uses that data to classify assets and expose risks. Hundreds of ready-made queries and a built-in classification framework get you tagging servers, clients, and Azure resources from day one. For users, service principals, and managed identities, tiers are derived from **actual assigned permissions** — no static tags — and AI categorizes new Entra, Graph, and Azure roles automatically.

🔒 Think like the hacker. Act like the defender. Fix what matters — first.

See [§ 10 What's New](#) for the full capability deep-dive — read-only engine, layered config, AI signal-map, multi-source asset correlation, and 11 more. Detection-query + tagging-rule + AI-tier-catalog inventory tables live in [§ 7.8 Locked catalog](#).



DEMO

SecurityInsight

Rethink Secure Score into a new risk-based security risk score, based on consequence, probability and risk factors. Solution includes critical asset tagging, ready-to-use reports (based on Defender Exposure Graph and Azure Resource Graphs), automation-scripts, risk index and more



SAVE THE DATES

Oct 25-28, 2026

May 2-6, 2027

Oct 10-13, 2027



Extended Q&A

