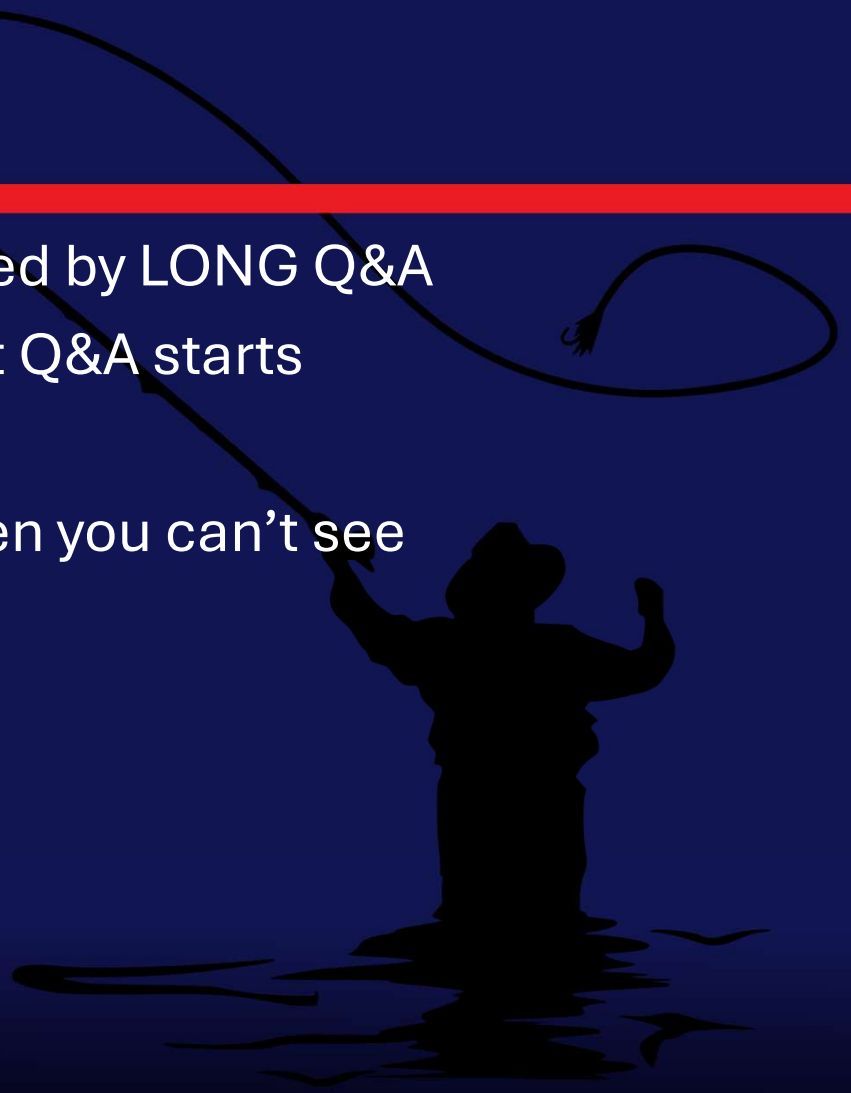
Achieve Zero Trust Objectives with Defender for Cloud and EASM Integrated with Defender XDR

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@corsicatech.com

in/johnjoyner

Morten Knudsen

CONSULTANT, ARCHITECT, STRATEGIC ADVISOR

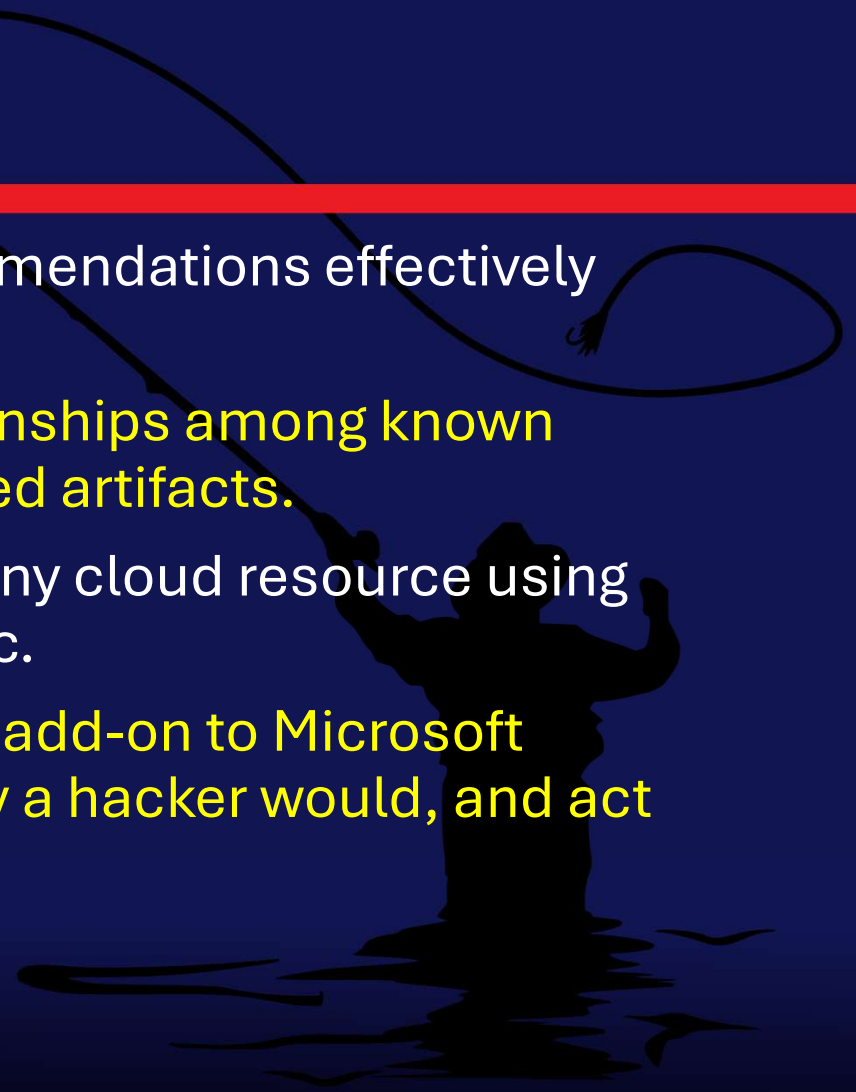
mok@2linkit.net

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.



MMS

The Microsoft Security Stack

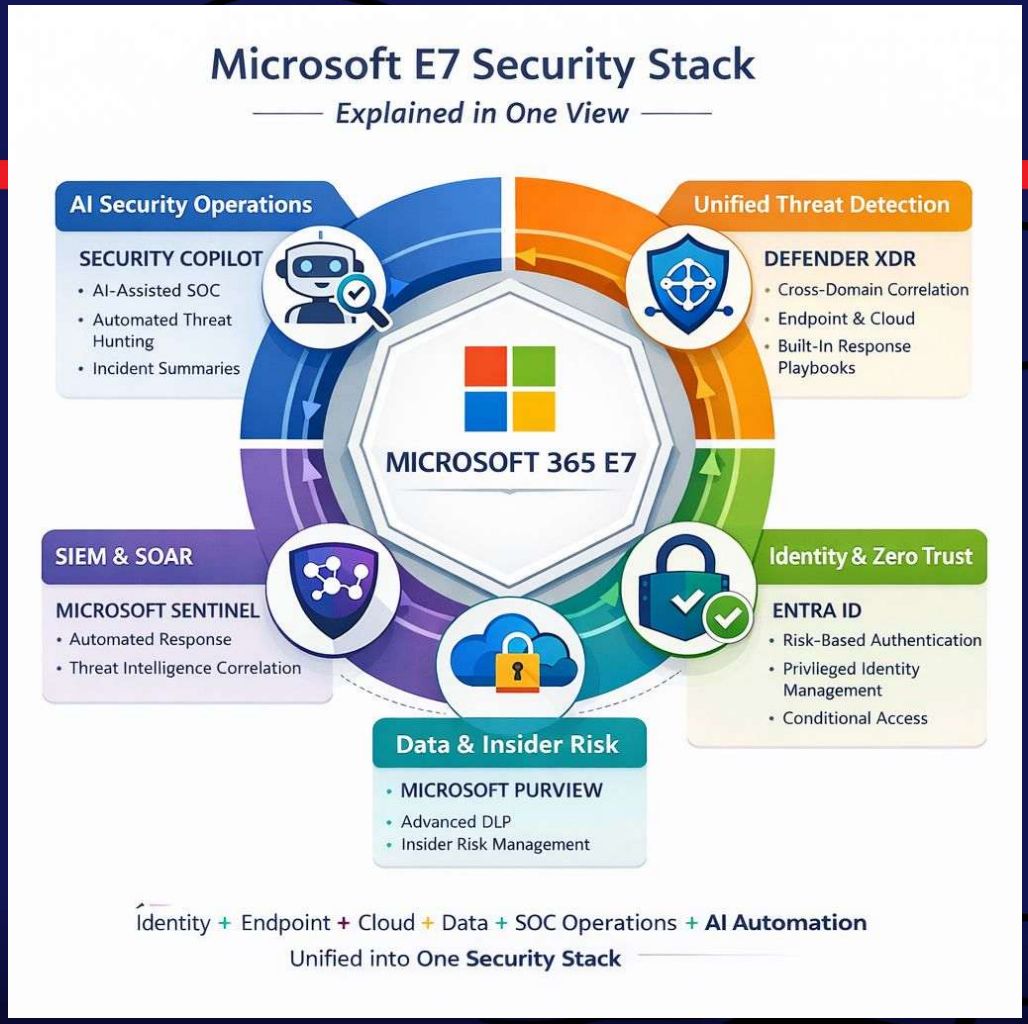
Microsoft’s security product portfolio:
Protecting all your cybersecurity domains.

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

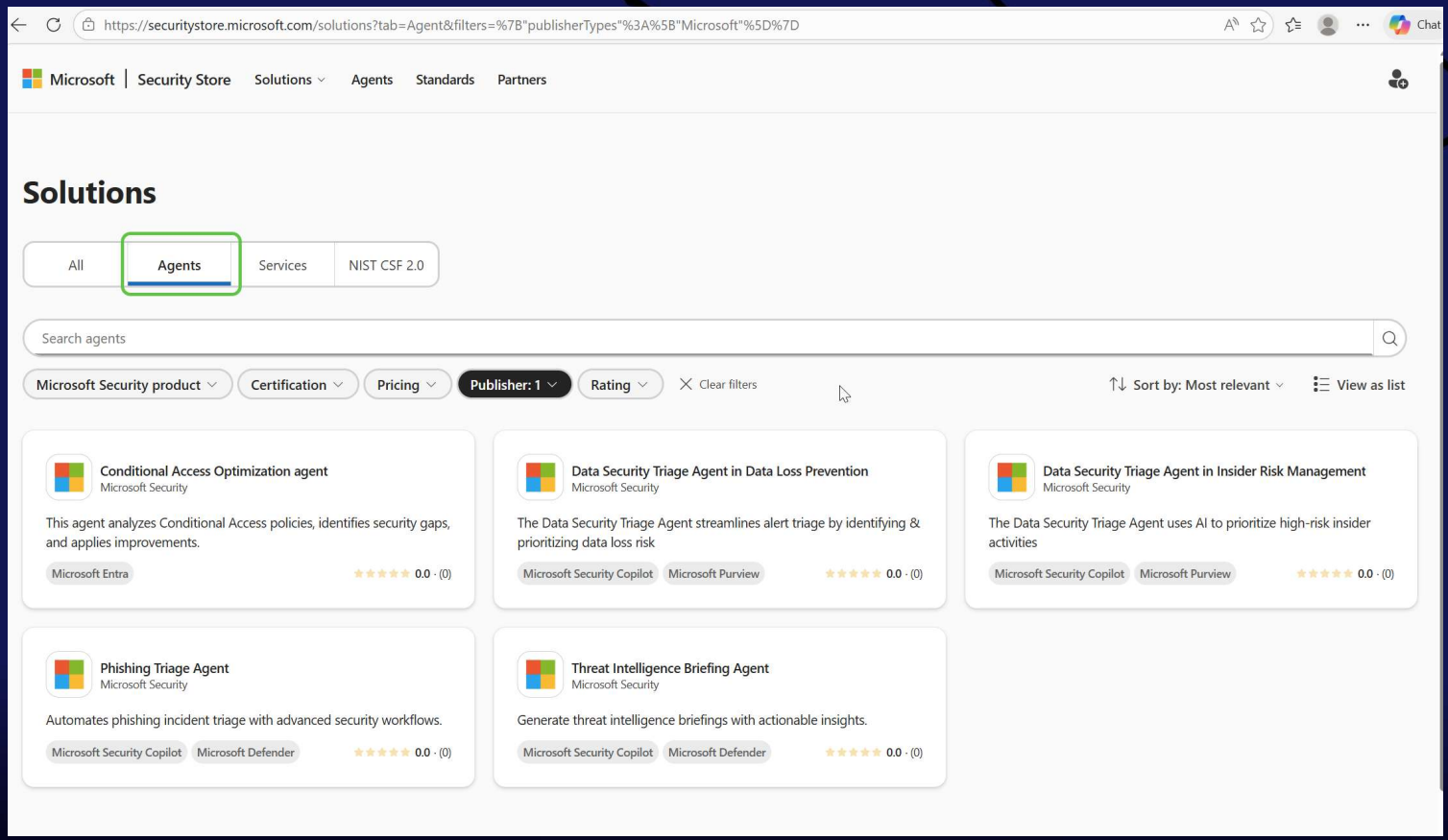
- The “Frontier Suite”
- Includes:
  - Microsoft 365 E5
  - Microsoft Entra Suite
    - Microsoft Entra Private Access
    - Microsoft Entra Internet Access
    - Microsoft Entra ID Protection
    - Microsoft Entra ID Governance
    - Microsoft Entra Verified ID
  - Microsoft 365 Copilot
  - Agent 365



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

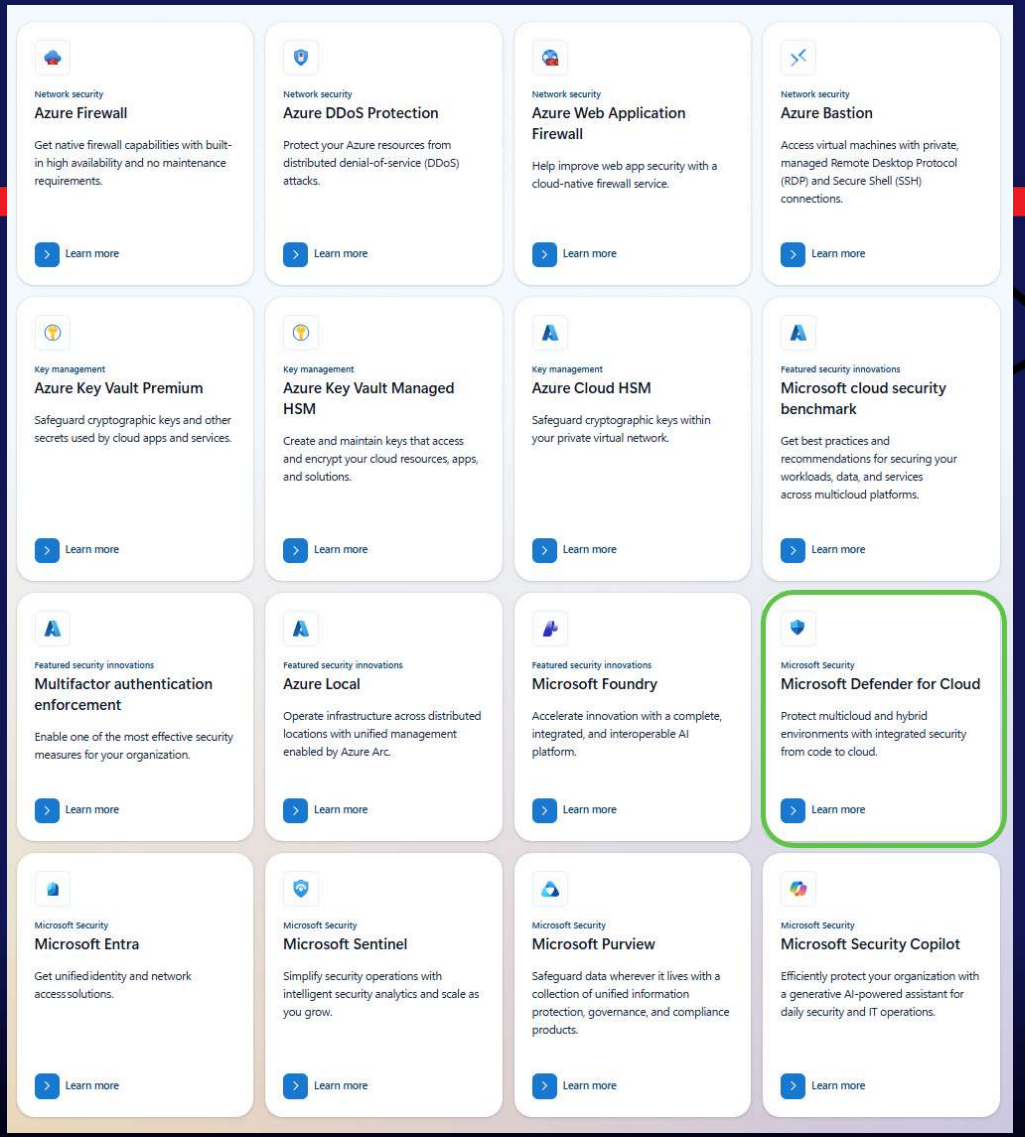


Cloud Security Tools

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



Microsoft Defender for Cloud CSPM and CNAPP

CSPM: Cloud Security Posture Management

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

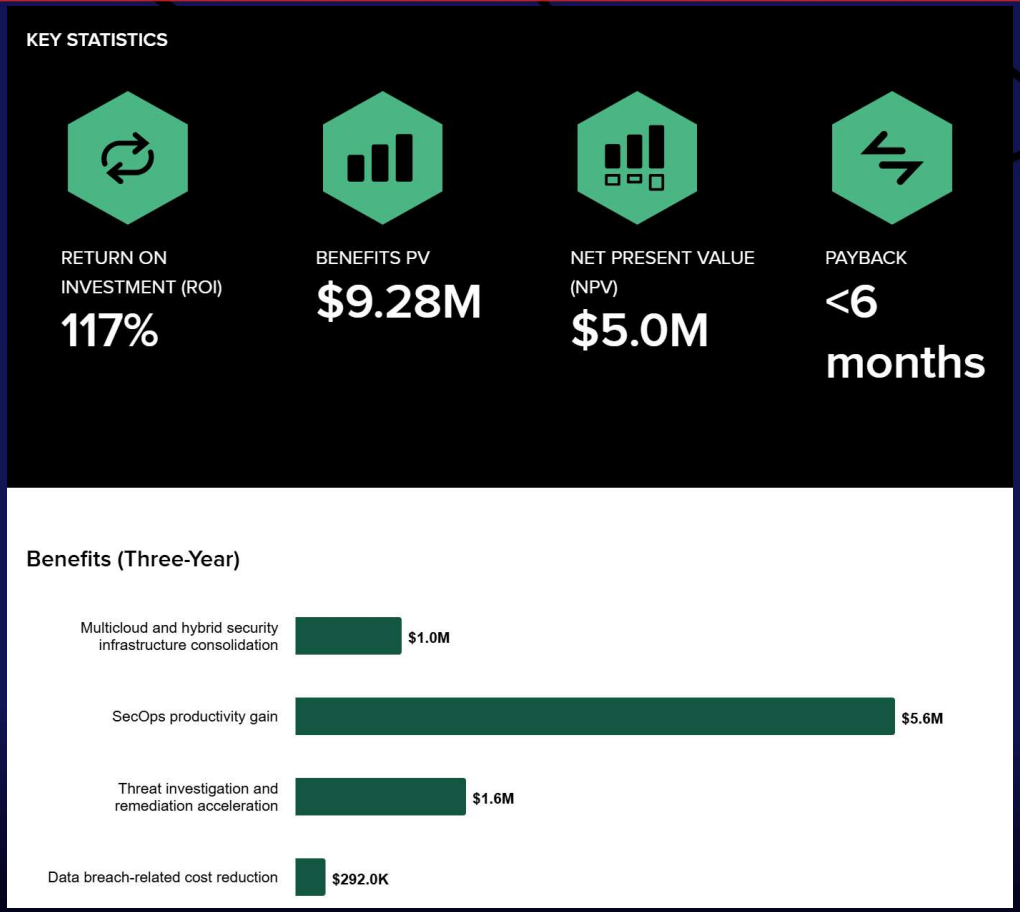
MMS

The Total Economic Impact™ Of Microsoft Defender For Cloud

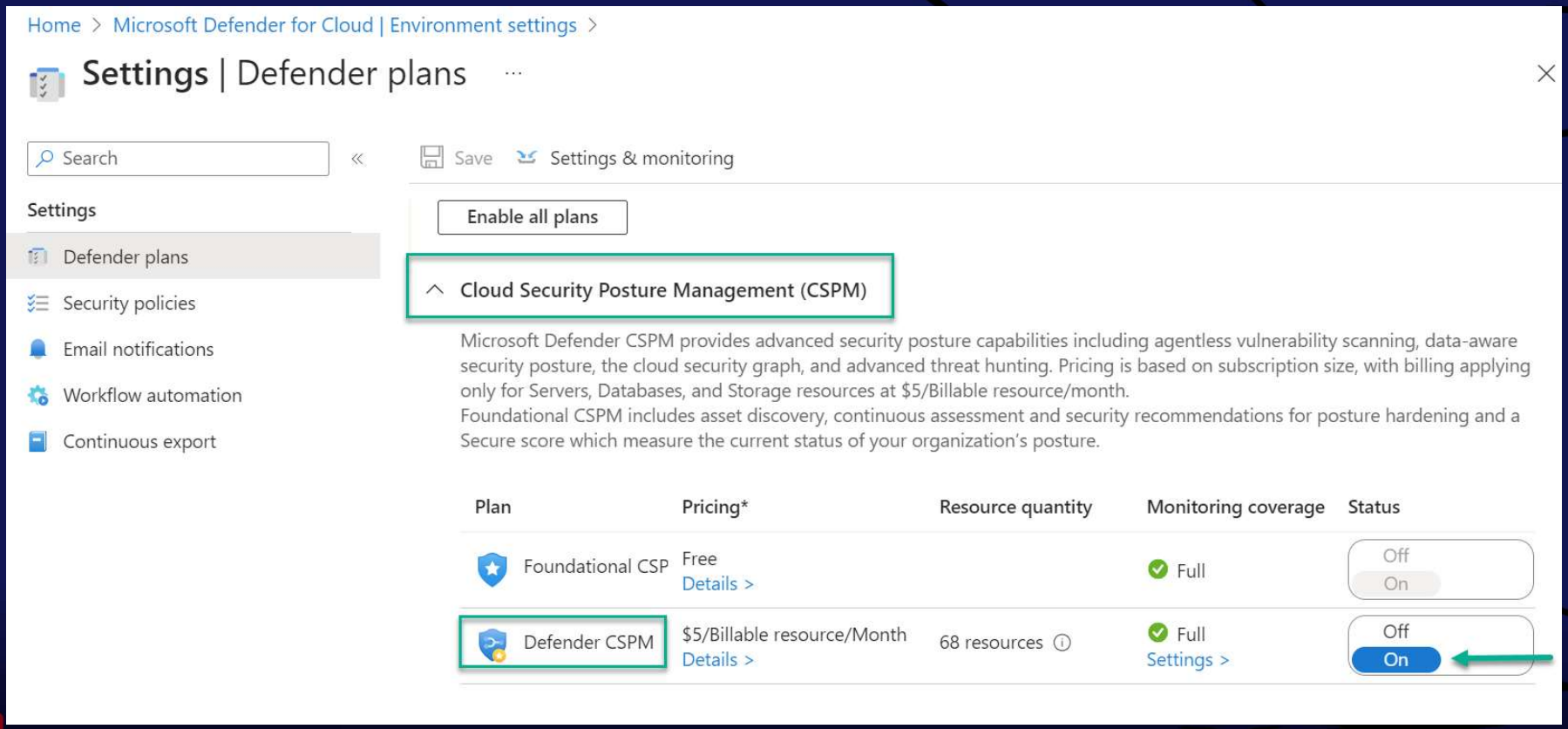
https://tei.forrester.com/go/Microsoft/DefenderForCloud

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.



Enable Defender for Cloud CSPM



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

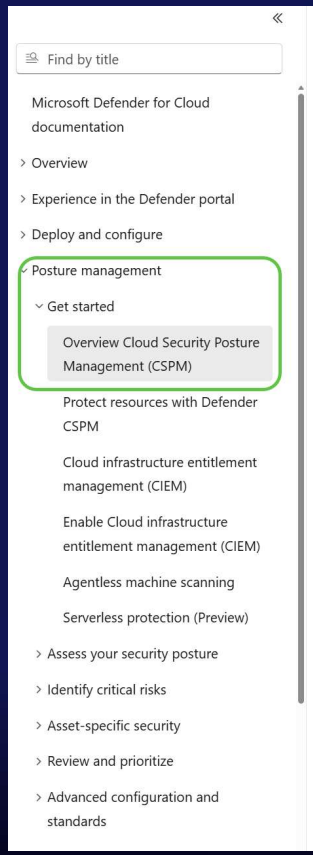
- Regulatory compliance assessments
- ServiceNow Integration
- Critical assets protection
- Governance to drive remediation at-scale
- AI Security Posture Management
- Code-to-cloud mapping for Containers
- Data-aware security posture, Sensitive data scanning
- Kubernetes API access
- Agentless code-to-cloud 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)**



Azure

Expand table

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

Expand table

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

GCP

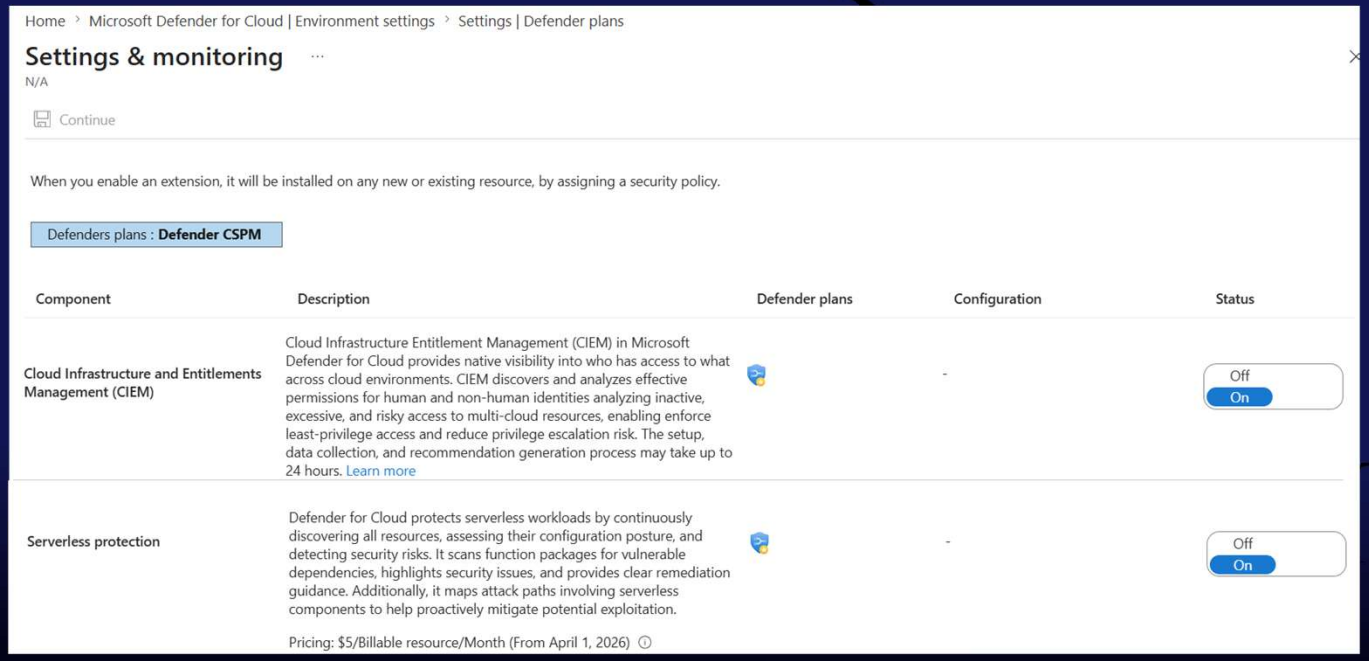
Expand table

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

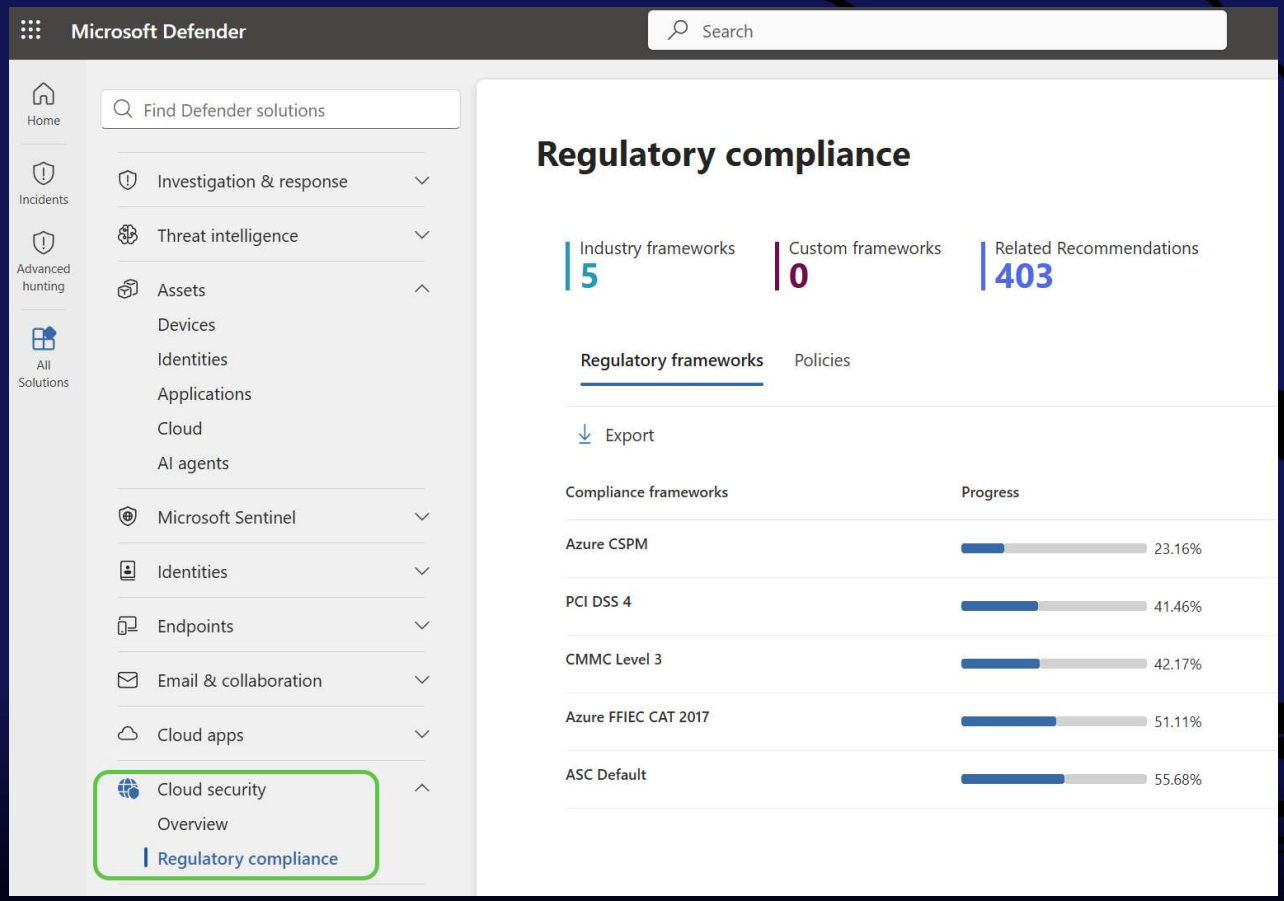
Defender for Cloud CSPM: What's new

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

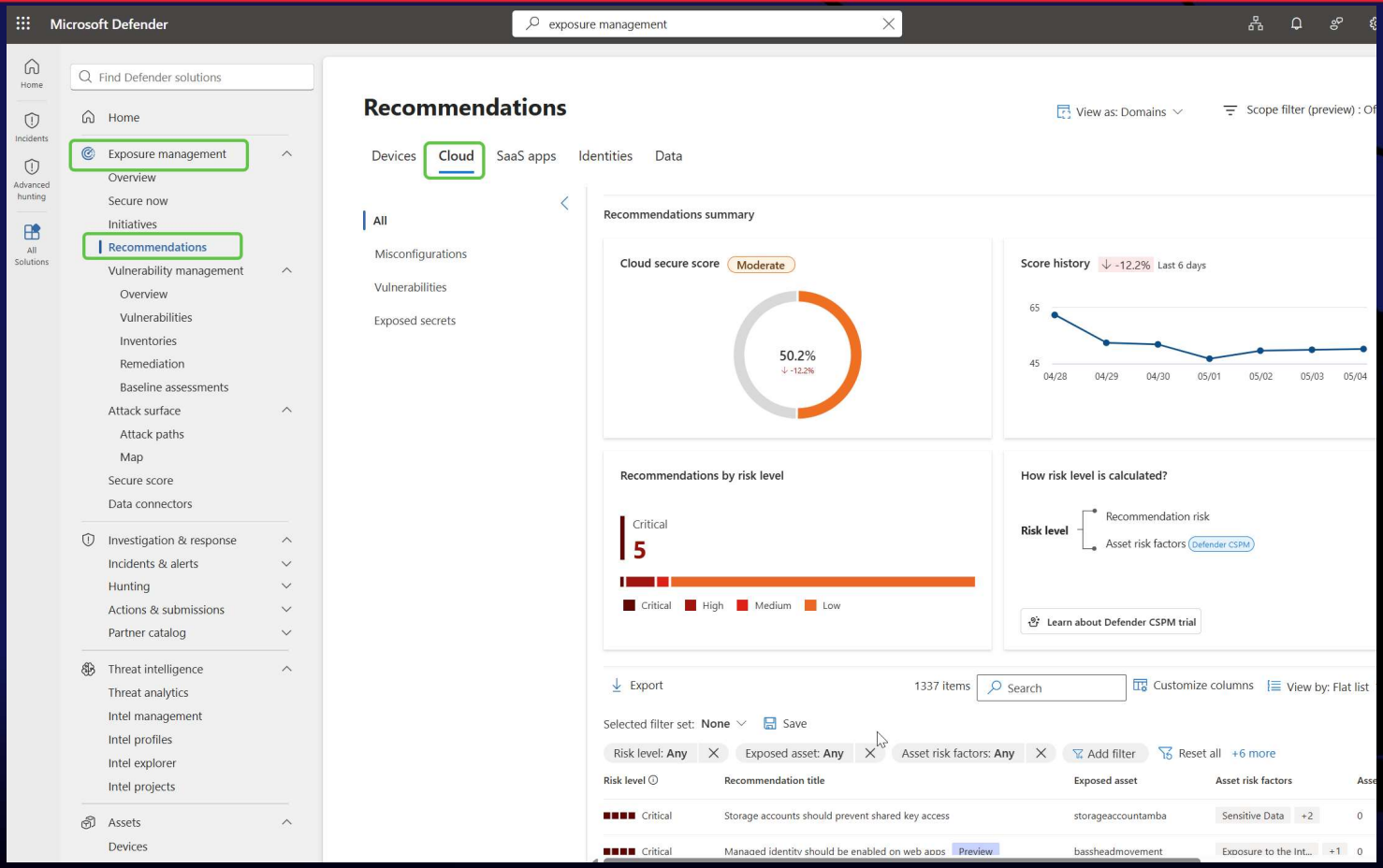
Serverless: https://learn.microsoft.com/en-us/azure/defender-for-cloud/serverless-protection (Azure Web Apps, Azure Functions, and Amazon Web Service (AWS) Lambda)



Use Defender for Cloud CSPM in the Defender XDR Portal



Use Defender for Cloud CSPM in the Defender XDR Portal



DEMO

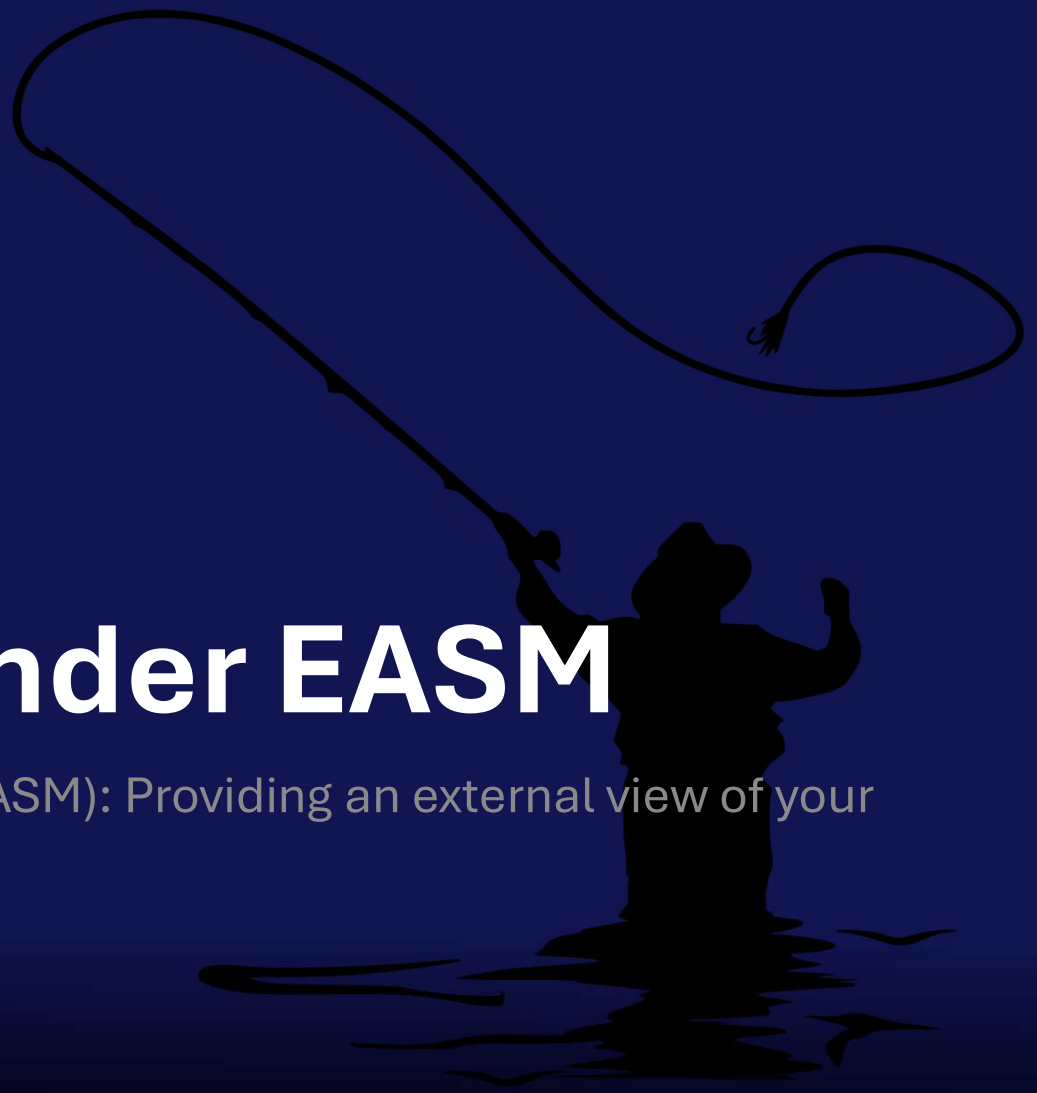
Microsoft Defender for Cloud CSPM

Indispensable tools in a Zero Trust compliance initiative.

MMS

Microsoft Defender EASM

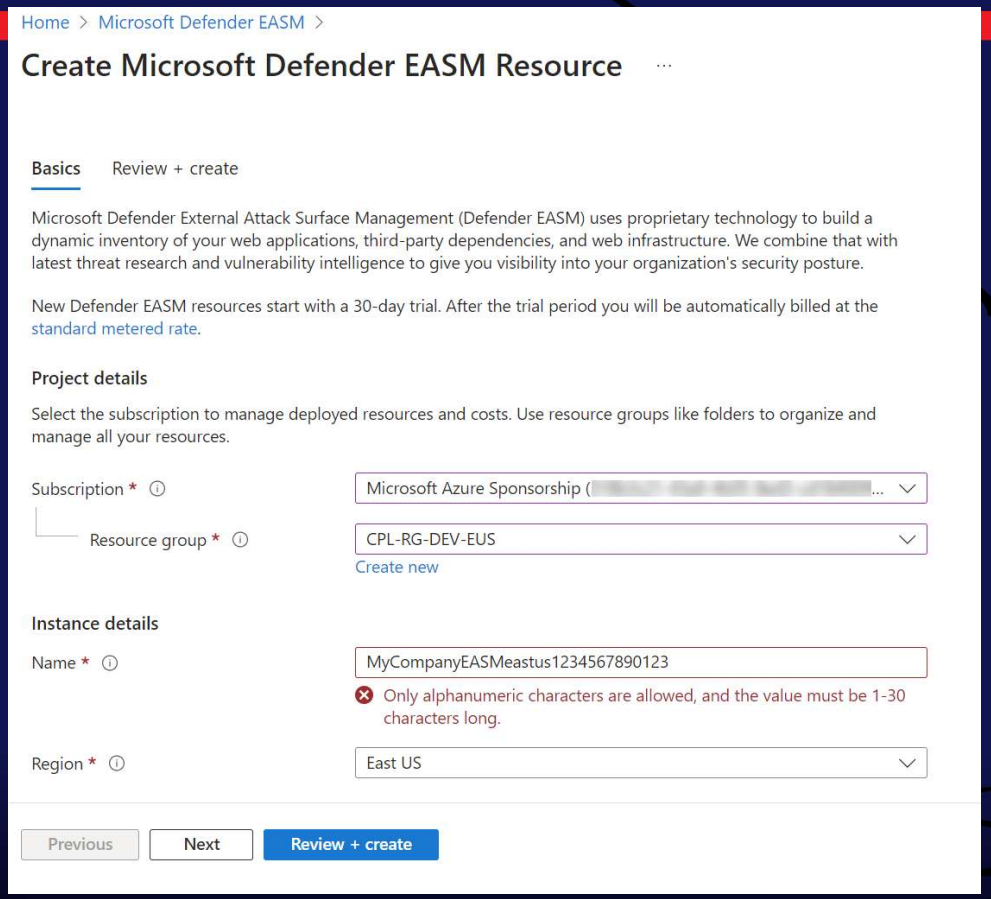
External Attack Surface Management (EASM): Providing an external view of your online infrastructure.



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

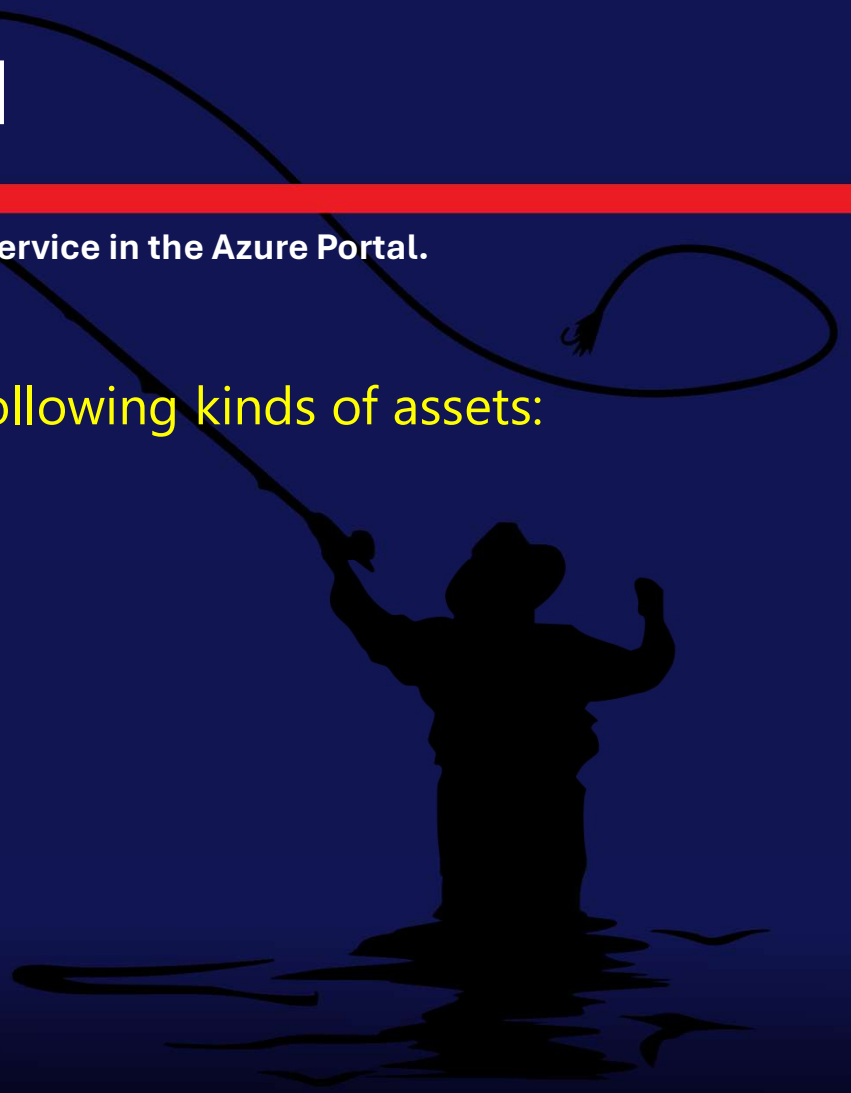


Defender for Cloud EASM

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

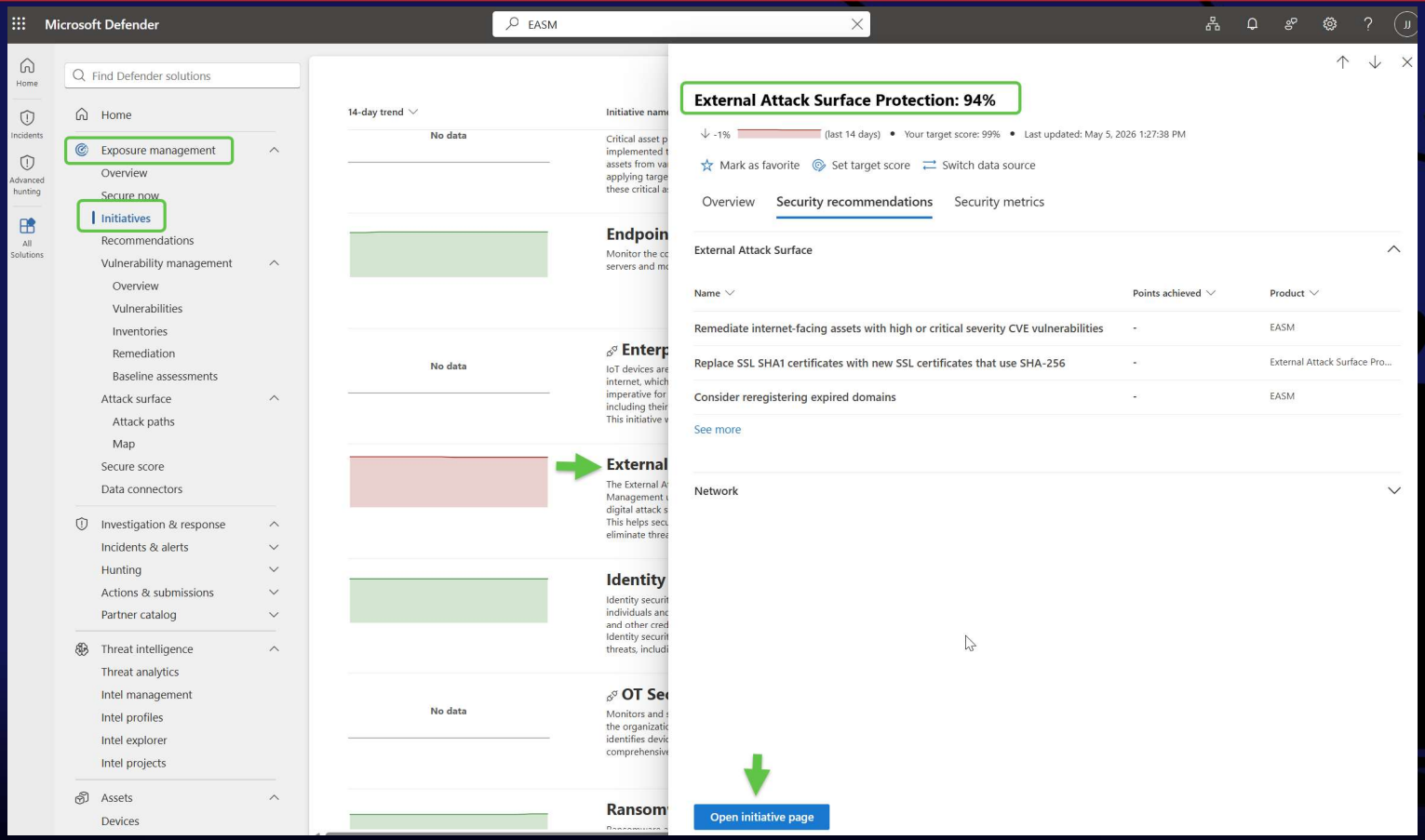
Defender EASM includes the discovery of the following kinds of assets:

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

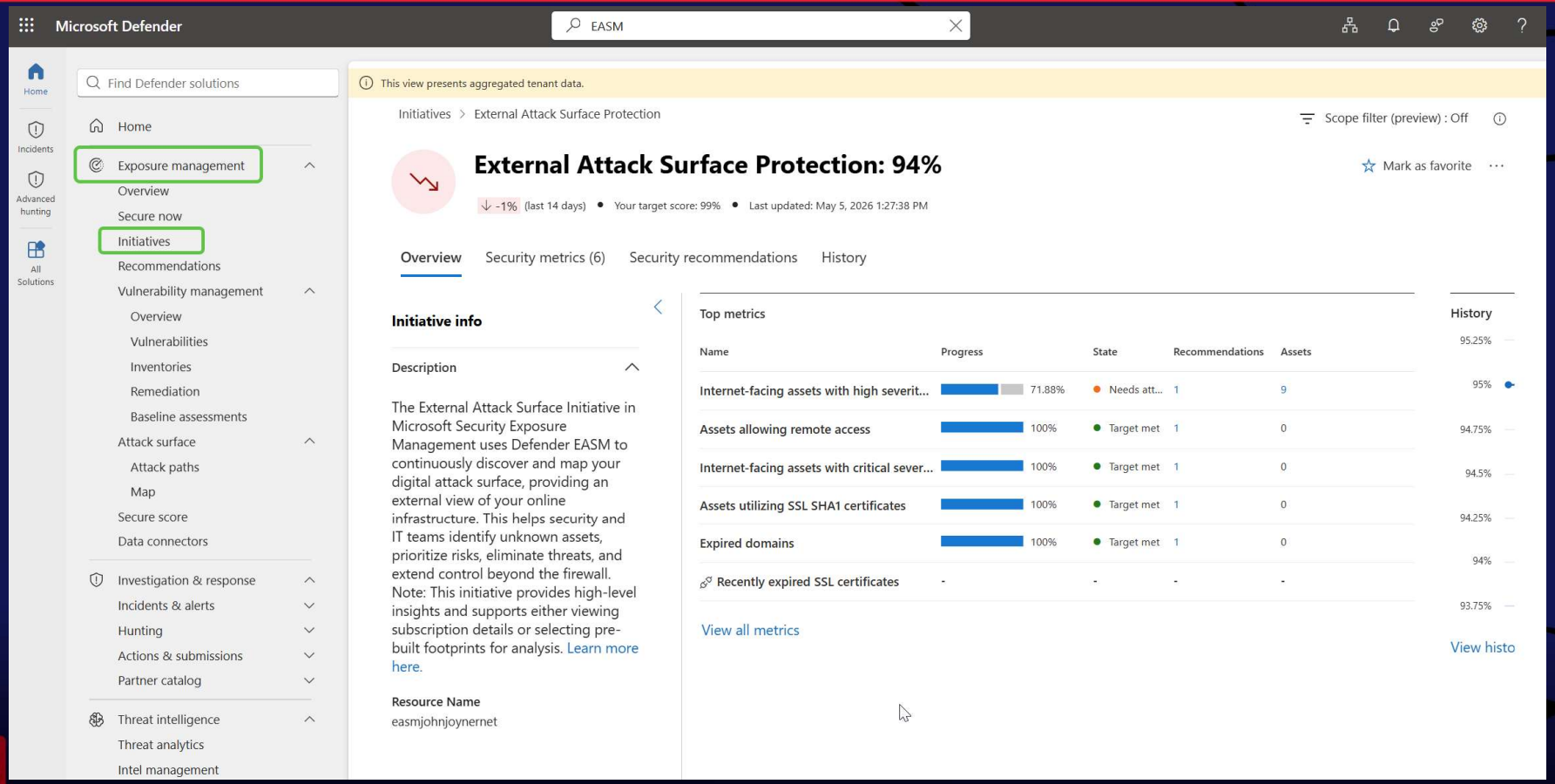


MMS

Use Defender for Cloud EASM in the Defender XDR Portal



Use Defender for Cloud EASM in the Defender XDR Portal



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.

MMS

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

MMS

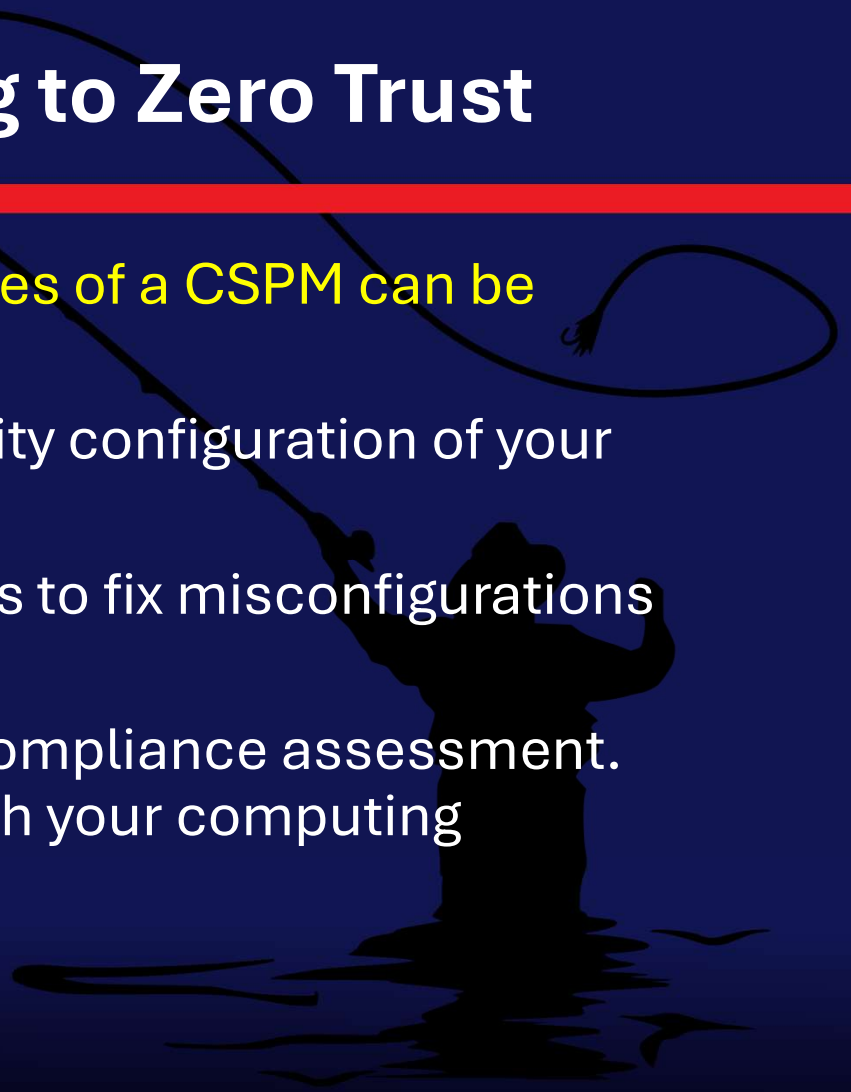
Don’t Trust and Do Verify

- 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:

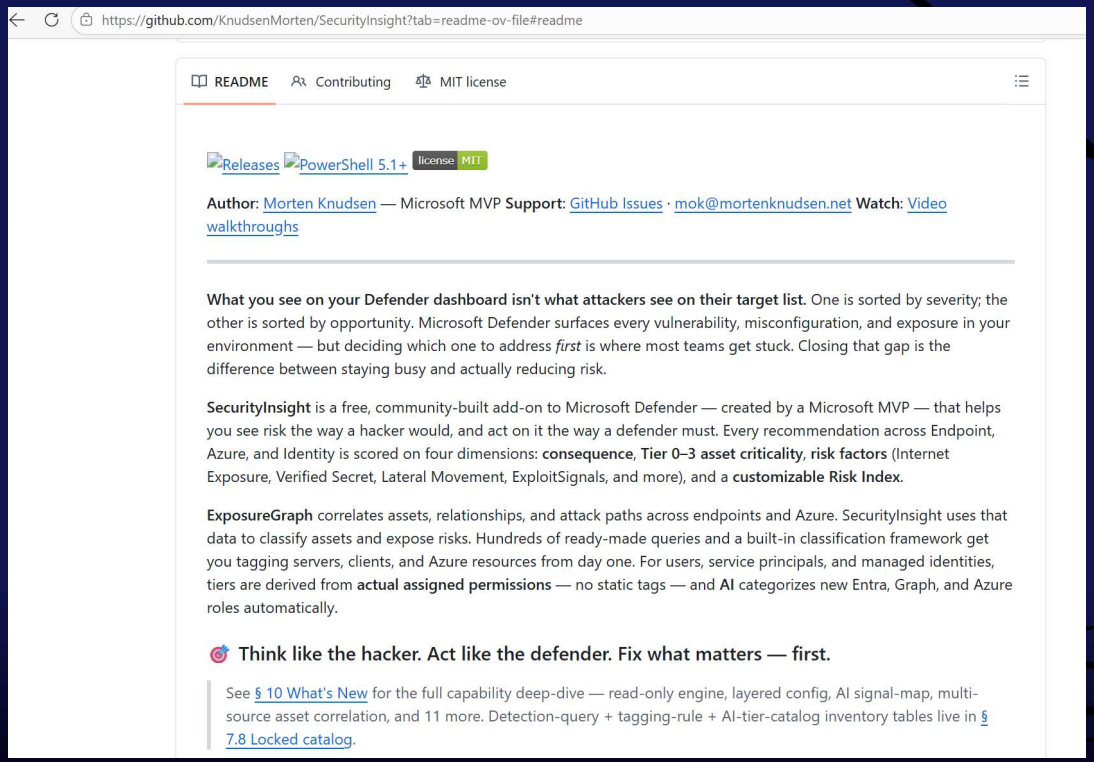
1. Continuous assessment of the security configuration of your cloud resources
2. Delivery of security recommendations to fix misconfigurations and weaknesses
3. A reporting or scoring capability for compliance assessment. This is how you achieve Zero Trust with your computing resources—by inspecting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



MMS

Introducing: SecurityInsight

https://github.com/KnudsenMorten/SecurityInsight



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

MMS

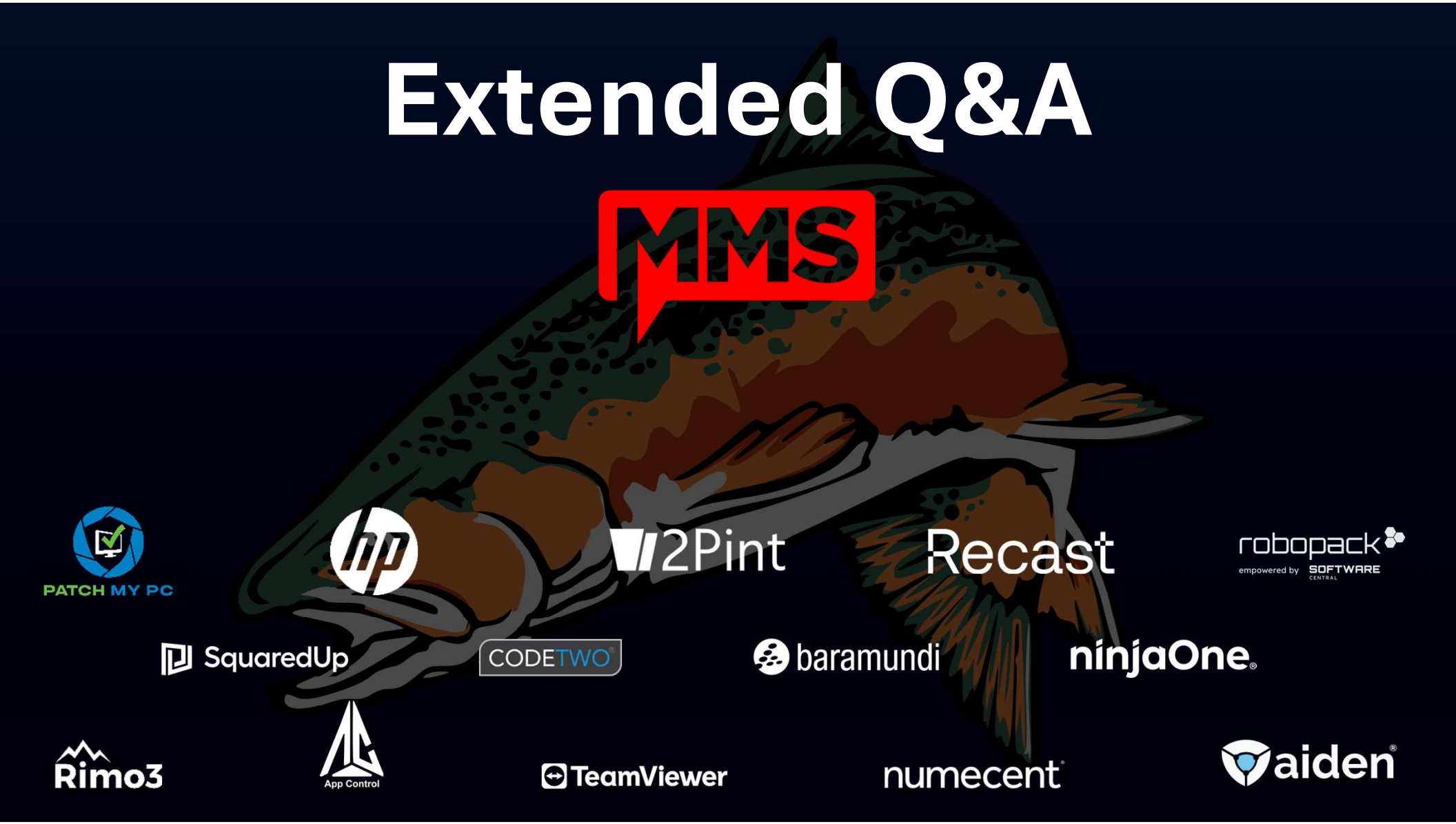
SAVE THE DATES

Oct 25-28, 2026

May 2-6, 2027

Oct 10-13, 2027

Extended Q&A


MMS
PATCH MY PC
hp
2Pint
Recast
robopack
empowered by SOFTWARE CENTRAL
SquaredUp
CODETWO
baramundi
ninjaOne
Rimo3
App Control
TeamViewer
numecent
aiden