See your business the way an attacker can with External Attack Surface Management (EASM)

Garima Agrawal
Cloud Solutions Architect

Shruti Ailani
Sr. Technical Specialist, Security

Experts Live Netherlands

Agenda

- **Introduction & Pulse check**
- **What** is Threat Intelligence & External Attack Surface Management (EASM)
- **Why** EASM? Modern-day challenges
- **What** is Microsoft Defender EASM
  - *How are we different*
  - *Advantages*
  - *Do more with less*
- **Who** can use Microsoft Defender EASM
  - *Integrations*
  - *Top use cases and Teams*
- **How** to use Microsoft Defender EASM
  - *A glimpse of the solution*
- **Summary & Questions**

Pulse check

Scan with your phone!

Wi-Fi, if required:
Network: 1931BBH-guest, no password needed

The industry’s highest-fidelity picture of the current state of cyber security

Defend **the world’s largest public clouds** + Protect over **1.5B endpoints** embedded across the planet + Graph the **entire internet**

65T+
security signals

15B+
internet observations

8,500+
dedicated security researchers and engineers

72B
threats blocked

Your Attack Surface is Dynamic and Growing

Cloud and digital transformation have disrupted security programs, giving adversaries the upper hand against enterprises using only an inside-looking-out perspective

The Attack Surface is Broad

EASM Tackles Modern-Day Challenges

Rapid Digital Growth

Organizations manage an unprecedented volume of workloads, applications, and infrastructure in complex multi-cloud environments.

Vulnerability Risk

Tracking and prioritizing vulnerabilities introduced by digital growth is an internet-scale challenge.

Attack Surface Visibility

The modern attack surface includes unknown and unmanaged assets such as Shadow IT, which can be hidden footholds for attackers.

Human Error

Rapid digital growth leads to configuration issues and other errors in internet-exposed apps and systems that attackers can leverage.

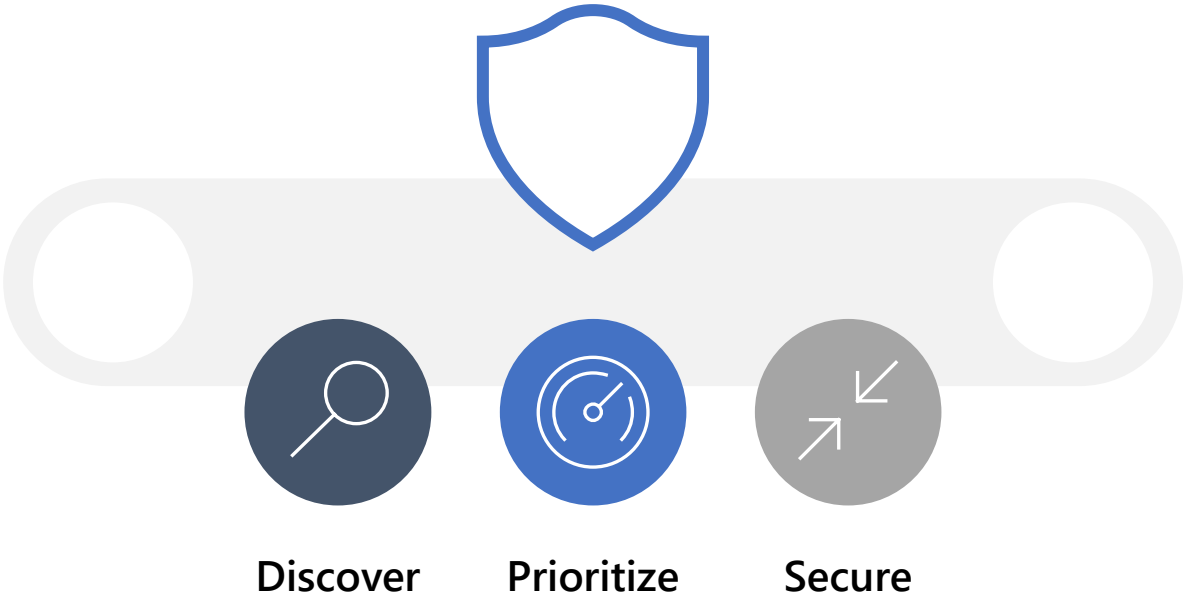
Microsoft Defender External Attack Surface Management (MDEASM)

Protect your organisation from adversaries with a 360-degree view of your threat exposure

Discover internet-facing and exposed assets and resources you didn’t know you had.

Continuously monitor discovered devices and search for new vulnerabilities without the need for agents or credentials.

Prioritise exposure and bring exposed resources under protection, ensuring stronger cloud security and improved security posture.



What is Microsoft Defender External Attack Surface Management (MDEASM)?

Key Value Propositions

Discovers and maps your externally-facing attack surface – including 1st and 3rd party infrastructure.

Identify **unknowns** and **risks**, eliminate **threats**,
and extend **vulnerability** and **exposure** control beyond the firewall.

Proactively discover **surface changes** to your external risk posture.

Show insights on the key areas of concern for your organisation.

Simplicity in Security

Built-in with Azure

- No deployment, just enable
- Built into the resource provisioning process
- Broadest protection coverage
- Remediate with a click

Multi-cloud and hybrid support

- Agentless onboarding for AWS and GCP posture management
- Auto provisioning for new resources
- Onboard on-prem resources with Azure Arc

Secure Score

- Birds-eye view of the security posture of all your clouds
- Prioritised security recommendations
- Track and manage your security posture state over time

Advanced Threat Protection

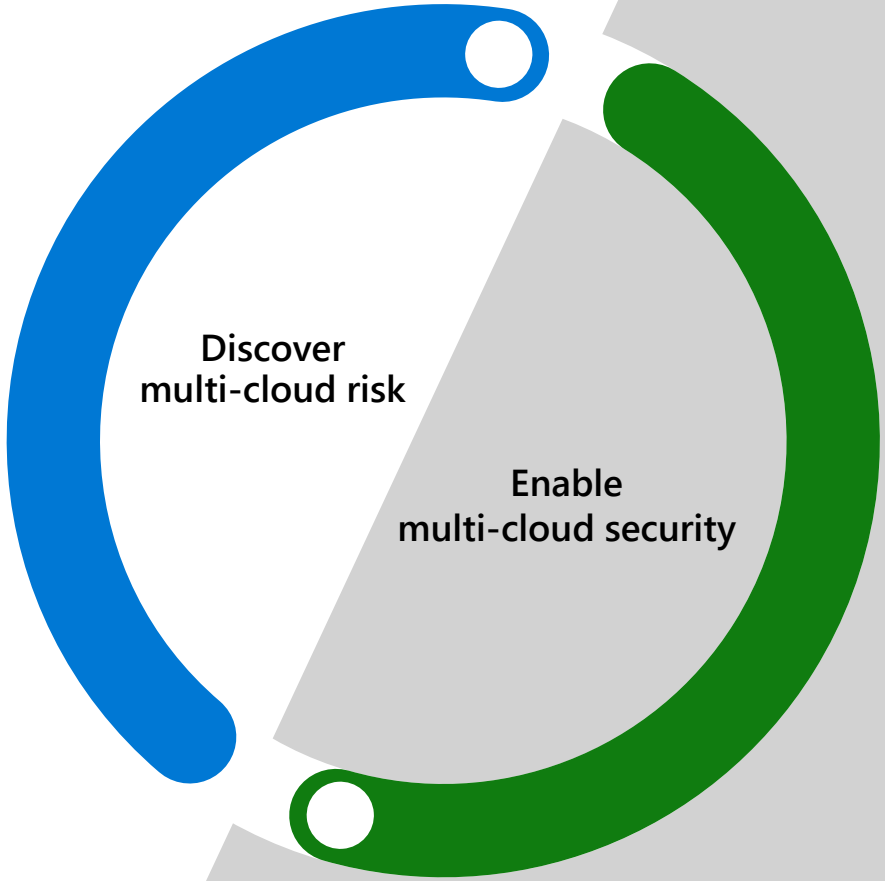
- Workload-specific signals and threat alerts
- Deterministic, AI, and anomaly-based detection mechanisms
- Leverages the power of Microsoft Threat Intelligence with 65 trillion signals daily

Discover and Protect multi-cloud resources

MDEASM

Discover. Analyse. Prioritise.

- Discover digital assets outside-in
- Continuous monitoring for internet facing assets
- Vulnerability analysis and prioritization
- Attack surface insights and remediation strategies



SIEM+XDR

Protect. Monitor. Respond.

- Security Posture and Compliance
- Adaptive Protection and Control
- Cloud mapping and attack simulation
- Automated detection & response for emerging threats

Possible Integrations (Preview till date)

Log Analytics Workspace

Enrich security incidents
Build investigation playbook
Train ML algos
Trigger remediation

Azure Data Explorer

Visualization
Query
Ingestion
Management

REST API

Automate Workflows
Integrate into existing processes
Create new apps or clients
Data and Control Plane Endpoints

Top use cases for External Attack Surface Management

Discover
Shadow IT

Find and report on
Deprecated Technology

Find and banner grab
Open Ports

Find, show, report
Expiring & Expired SSL Certificates

Passively identify
Vulnerability Exposure

Find, identify, profile
Newly Added Assets

Find occurrences of
Internal Assets Exposure

Map and identify
Contractors and 3rd Party Risks

Common MDEASM Users

- Threat and Vulnerability Management Teams
- 3rd Party Risk/M&A Teams
- GRC/IT Asset Management Groups
- Red/Purple Teams
- Application Security

Microsoft Security

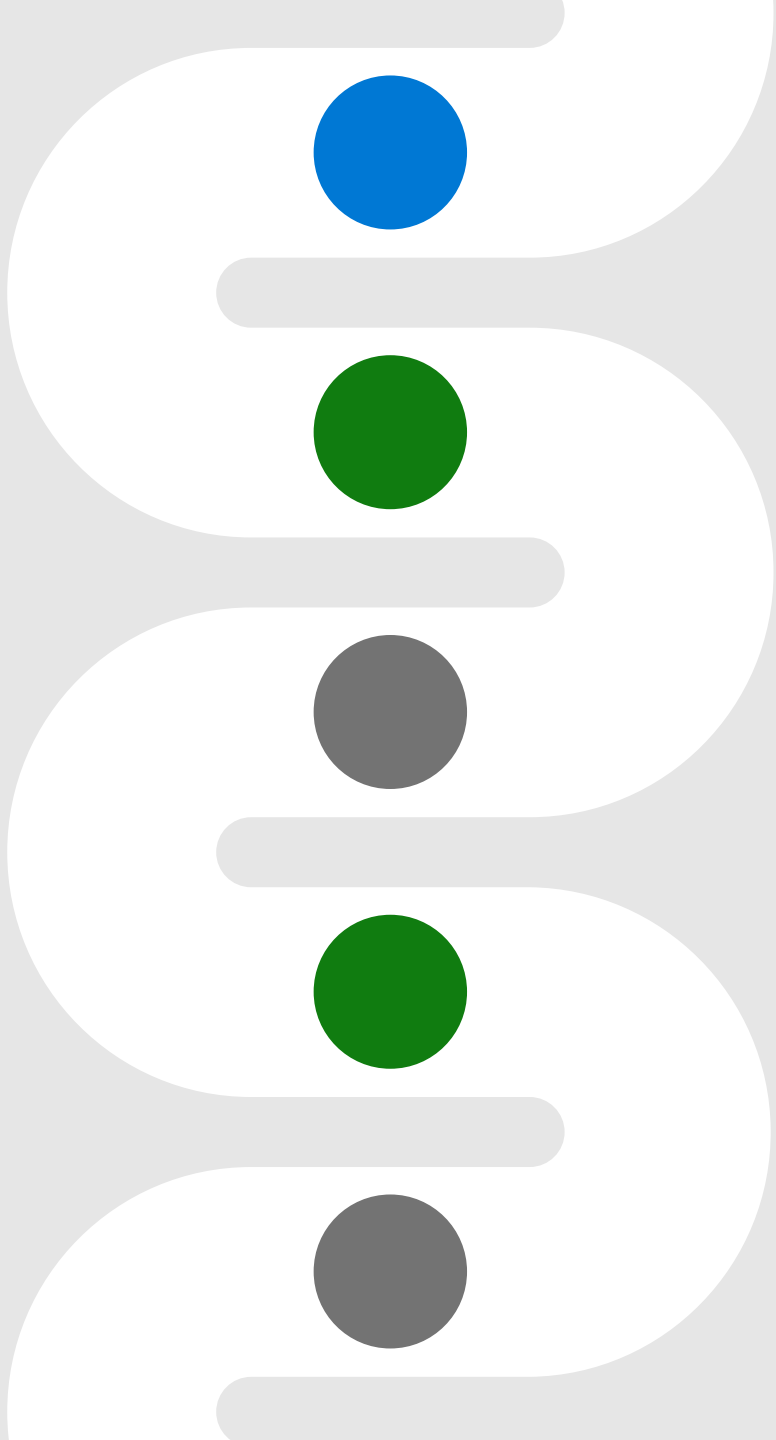
How to use Microsoft Defender EASM

A glimpse of the solution

Microsoft Security

Summary

- MDEASM continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure.
- More resources:
  Defender EASM Overview - Microsoft Learn;
  Creating a Defender EASM Azure resource | Microsoft Learn
- Did we get you curious? Sign up here to try the MDEASM solution for **free for 30 days**
- Watch out for Security Webinars at aka.ms/SecurityWebinars and Ninja trainings at aka.ms/BecomeAnMDEASMNinja.
- MDEASM pricing: depends on attack surface size



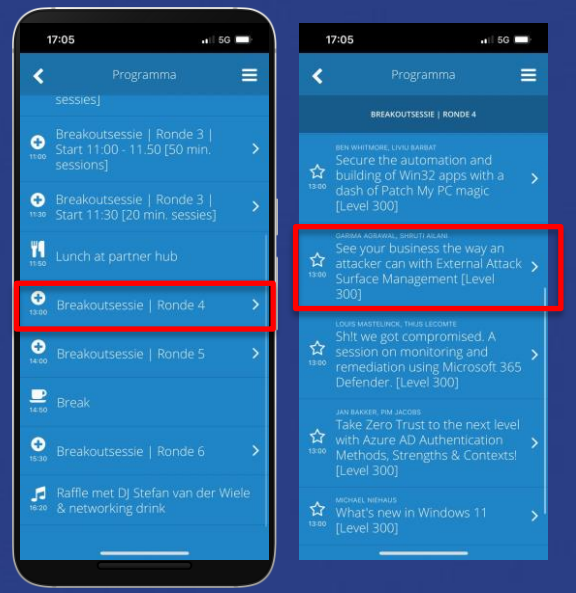
Thank you! Questions?

Don't forget to rate our session
You can do that in the Yellenge App

Scan for Slides

Garima Agrawal
Cloud Solutions Architect

Shruti Ailani
Sr. Security Technical Specialist



> Knowing others is intelligence; knowing yourself is true wisdom.

Laozi

Chinese philosopher, and writer
Founder of Taoism

Experts Live Netherlands