



Microsoft Defender External Attack Surface Management (EASM)

Get continuous global attack surface insights

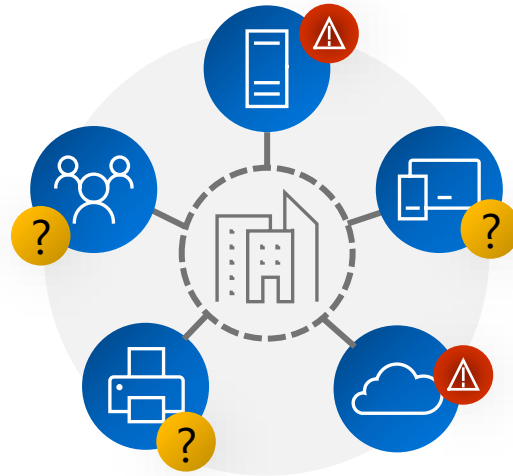
Speaker name
Speaker title



The external attack surface management challenge



In this era of hybrid work, shadow IT creates an increasingly serious security risk



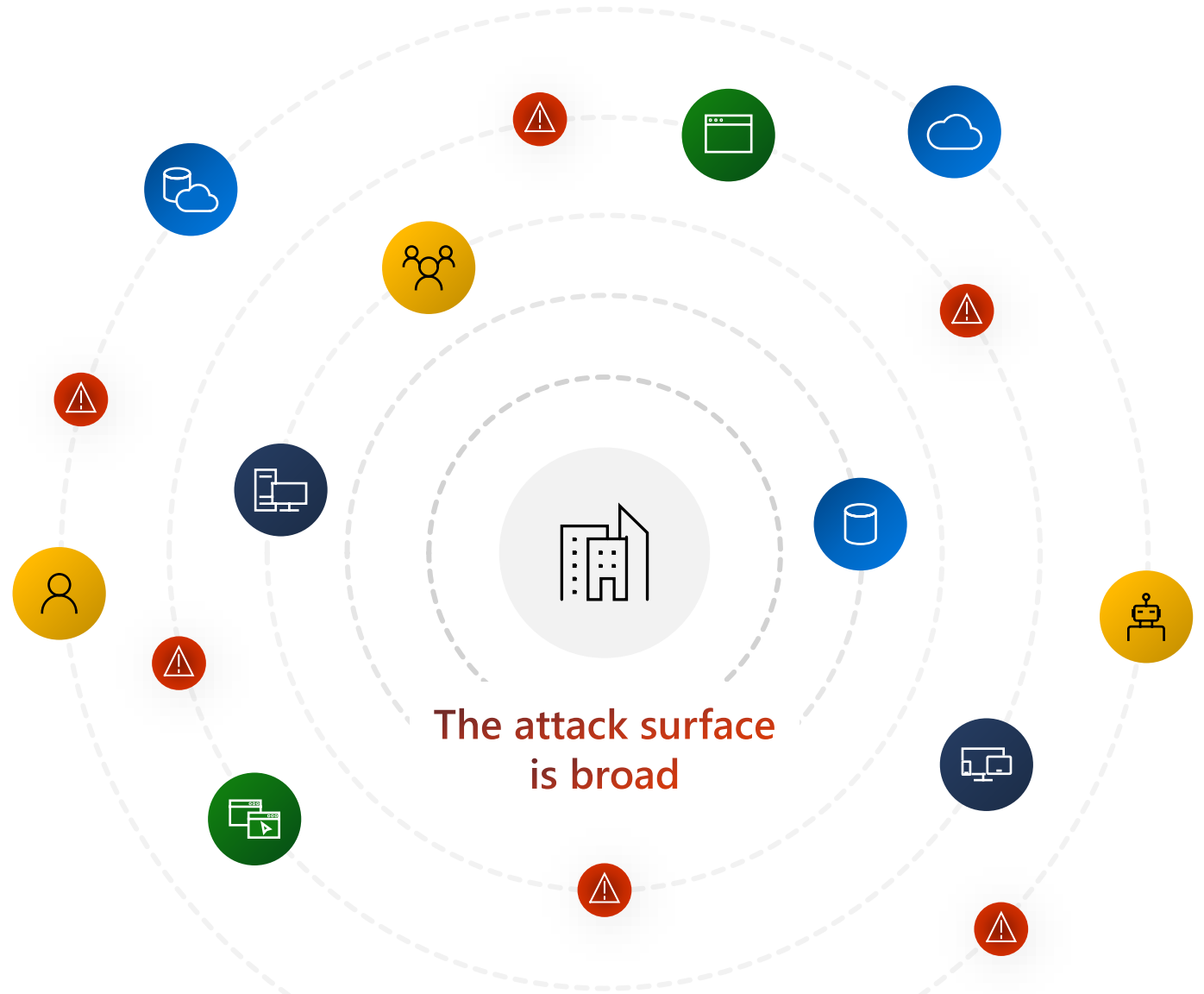
Internet-exposed assets are often unknown and unmanaged resources, creating security risk to the organization



Organizations are moving to the cloud at rapid pace, expanding and increasing complexity in how the external attack surface is comprised

Your attack surface is dynamic and growing

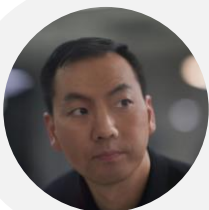
Cloud and digital transformation have disrupted security programs, giving adversaries the upper hand against enterprises using only an inside-looking-out perspective



Defender EASM helps security teams see unknown and unmanaged resources outside the firewall

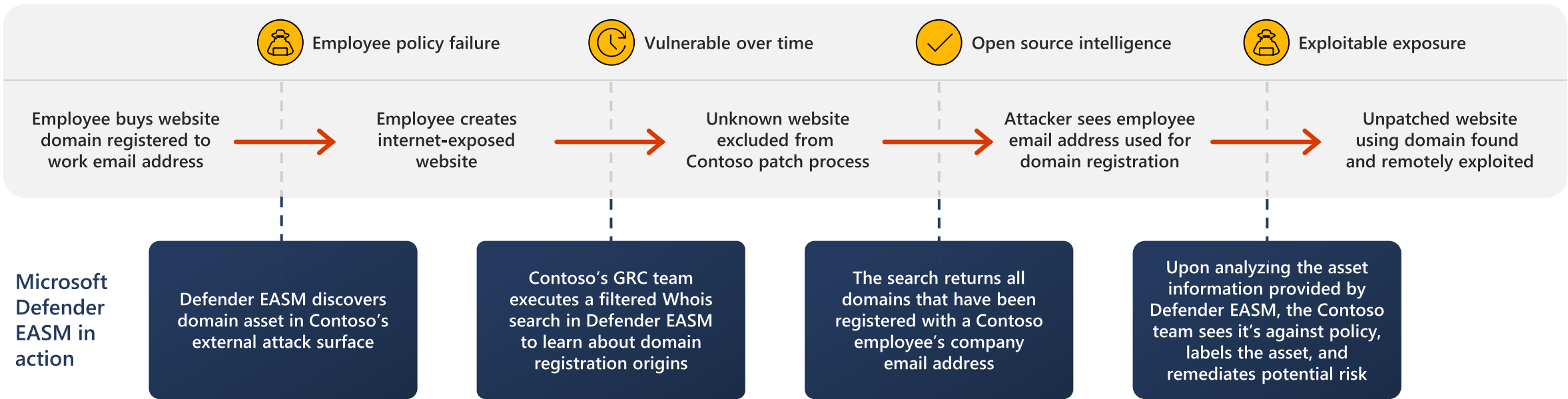
How Microsoft Defender EASM finds Shadow IT:

A real-life story at Contoso



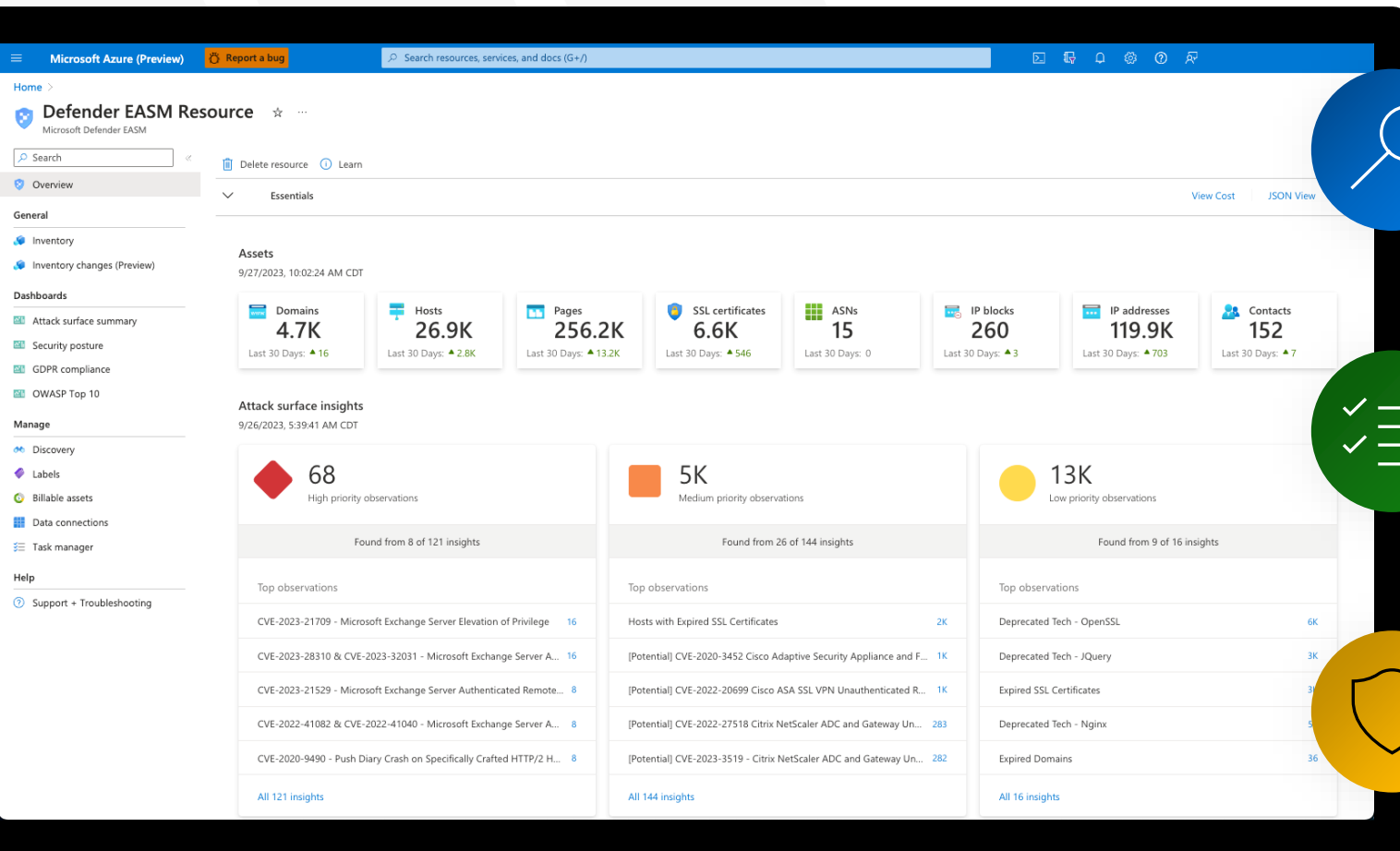
As a member of the Contoso Governance, Risk, and Compliance (GRC) team, I want to identify domain assets in our external attack surface that have been registered with an employee company email addresses instead of the official email address reserved for domain registration (domain-admin@constoso.com), which is against Contoso policy and creates risk.

Shadow IT attack path example



Microsoft Defender EASM

Bring your organization's external digital estate under management through a single pane of glass



Discover

Continuously discover known internet-facing assets and unknown, unmonitored properties to define your internet-exposed attack surface over time

Prioritize

Prioritize risk by using observations to bring exposed resources under protection, ensuring stronger security posture

Secure

Secure your organization by continuously monitoring discovered devices and search for new vulnerabilities without the need for agents or credentials

Discover your external attack surface

Look at your organization from the outside-in, the same way an attacker would



Discover



Prioritize



Secure

- Gain visibility into your external, internet-facing profile with continuous internet scanning
- Understand the unknown assets, shadow IT and legacy services you still have operating online
- Build an accurate, and up-to-date catalogue of your organization's resources and assets

The screenshot displays the 'Add discovery group' interface with the 'Seeds' tab selected. The interface includes a 'Quick Start (optional)' section with a button to 'Import seeds from an organization'. Below this, there are sections for 'Domains (4)', 'IP Blocks (2)', and 'Hosts (1)'. Each section has a text area for 'Seed' and a text area for 'Exclude'. The 'Domains' section shows 'contoso.com', 'adatum.com', and 'adventure-works.com' in the seed area, and 'bellowscollege.com' in the exclude area. The 'IP Blocks' section shows '10.255.255.255' and '172.16.0.0' in the seed area. The 'Hosts' section shows 'host.contoso.com' in the seed area. At the bottom, there are navigation buttons: 'Review + Create', '< Previous', and 'Next : Review + Create >'.

Add discovery group ...

Group Information **Seeds** Review + Create

Tell us what you know

Enter what you know about your organization using the seed fields below.

Quick Start (optional)

Import seeds from an organization

Seeds

Clear Seeds

Domains (4)

Seed Domains for asset discovery ⓘ

contoso.com
adatum.com
adventure-works.com

Example: office.com | One per line.

Domains to exclude from asset discovery ⓘ

bellowscollege.com

Example: office.com | One per line.

IP Blocks (2)

Seed IP Blocks for asset discovery ⓘ

10.255.255.255
172.16.0.0

Example: 20.64.0.0/10 | One per line.

IP Blocks to exclude from asset discovery ⓘ

Example: 20.64.0.0/10 | One per line.

Hosts (1)

Seed Hosts for asset discovery ⓘ

host.contoso.com

Hosts to exclude from asset discovery ⓘ

Review + Create < Previous Next : Review + Create >

Prioritize any vulnerabilities

Understand your exposure, and how to fix it



Discover



Prioritize



Secure

- View the complete collection of assets and resources operated inside, and outside, the firewall
- Identify the most severe risks and exposures, so they can be mitigated or removed
- Extend your understanding of risk with deep insights from Microsoft researchers

Attack surface insights

12/11/2023, 1:22:56 AM EST



29

High priority observations

Found from 8 of 131 insights

Top observations

CVE-2022-41082 & CVE-2022-41040 - Microsoft Exchange Server Authenti...	4
CVE-2022-21980 - Microsoft Exchange Server Authenticated Privilege Escal...	4
CVE-2023-28310 & CVE-2023-32031 - Microsoft Exchange Server Authenti...	4
CVE-2023-21529 - Microsoft Exchange Server Authenticated Remote Code ...	4
CVE-2023-21745 - Microsoft Exchange Server Authenticated Privilege Escal...	4

[All 131 insights](#)



194

Medium priority observations

Found from 11 of 150 insights

Top observations

Hosts with Expired SSL Certificates	42
[Potential] US-CERT Issues Alert On Critical Vulnerabilities Exploited By Ru...	38
[Potential] CVE-2020-8243 Pulse Secure Custom Templates May Lead to C...	24
Multiple Vulnerabilities in Pulse Connect Secure	24
CVE-2020-1938 - AJP File Read/Inclusion Vulnerability in Apache Tomcat	19

[All 150 insights](#)



173

Low priority observations

Found from 6 of 16 insights

Top observations

Expired SSL Certificates	141
Deprecated Tech - Nginx	14
Deprecated Tech - Apache	10
Self Signed Certificates	5
Deprecated Tech - JQuery	2

[All 16 insights](#)

Secure your infrastructure

Close the gaps before they can be exploited



Discover



Prioritize



Secure

- Bring the external facing, unmanaged catalogue of resources under management
- Follow recommended actions to mitigate specific risks
- Close the gaps in the perimeter and improve your security posture

Attack surface composition

12/7/2023, 12:01:36 PM EST

Visibility is key to operating a business on the internet today. Knowing about all your assets allows you to better inform your internal security practices and mitigate your overall risk.

Total

17.0K

Domains
264

ASNs
1

Hosts
5.2K

IP blocks
13

Pages
6.7K

IP addresses
4.5K

SSL certificates
351

Contacts
15

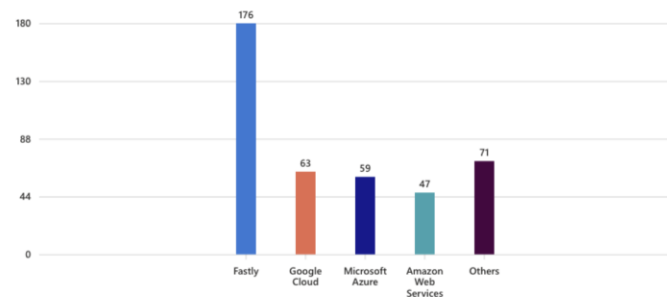
Securing the cloud

12/7/2023, 12:01:36 PM EST

Many organizations adopt the cloud gradually, creating a hybrid environment that can be difficult to manage. Defender EASM is able to understand the usage of specific hosting providers and CDNs (content delivery networks) that can inform your cloud adoption program and ensure it's compliant with your organization's process.

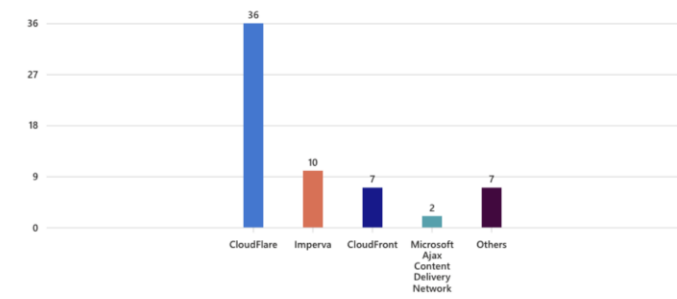
Hosting providers

12/7/2023, 12:01:36 PM EST



CDNs

12/7/2023, 12:01:36 PM EST



The Defender EASM advantage

Dynamic external attack surface discovery

- Utilize proprietary discovery mechanisms to identify the external attack surface, including Shadow IT
- Identify new assets at the internet changes with automatic continuous monitoring
- Ensure transparency with discovery chain capabilities
- Gain deeper infrastructure insights with custom discovery capabilities



Extended security posture visibility

- Get a birds-eye-view of your external risk posture
- Integrate and unify security posture across Microsoft Security solutions
- Find known and unknown assets across any cloud, then profile them to discover vulnerabilities across the global attack surface
- Regional availability through the Azure platform



Contextual vulnerability prioritization

- See observation insights to reveal high, medium, and low priorities for potentially impacted assets
- Contextualize data to help prioritize vulnerabilities, risk, and compliance issues with multiple dashboard views
- Dig deeper into asset information with seamless integration into Microsoft Defender Threat Intelligence
- Gain new insights by exporting EASM vulnerability data into other security tools



Custom inventory organization

- Apply business context with customer-defined labeling
- Update assets in bulk and utilize task tracking to ensure awareness of completion
- Easily see newly discovered assets on dashboards to organize them accordingly
- Flexible inventory search capabilities based on asset characteristics



MDEASM use cases

Demo



MDEASM resources



»» Learn more: aka.ms/mdeasm

»» Try it today: azure.microsoft.com/free



Thank you!

Appendix