Microsoft Security

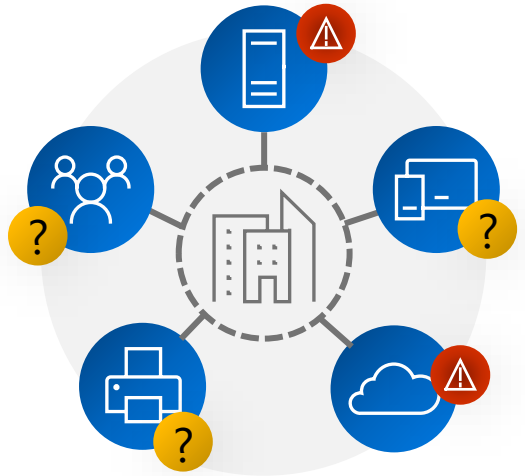
Microsoft Defender External Attack Surface Management (EASM)

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

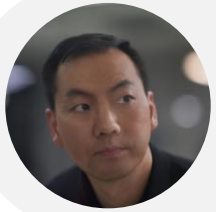
Your attack surface is dynamic and growing

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



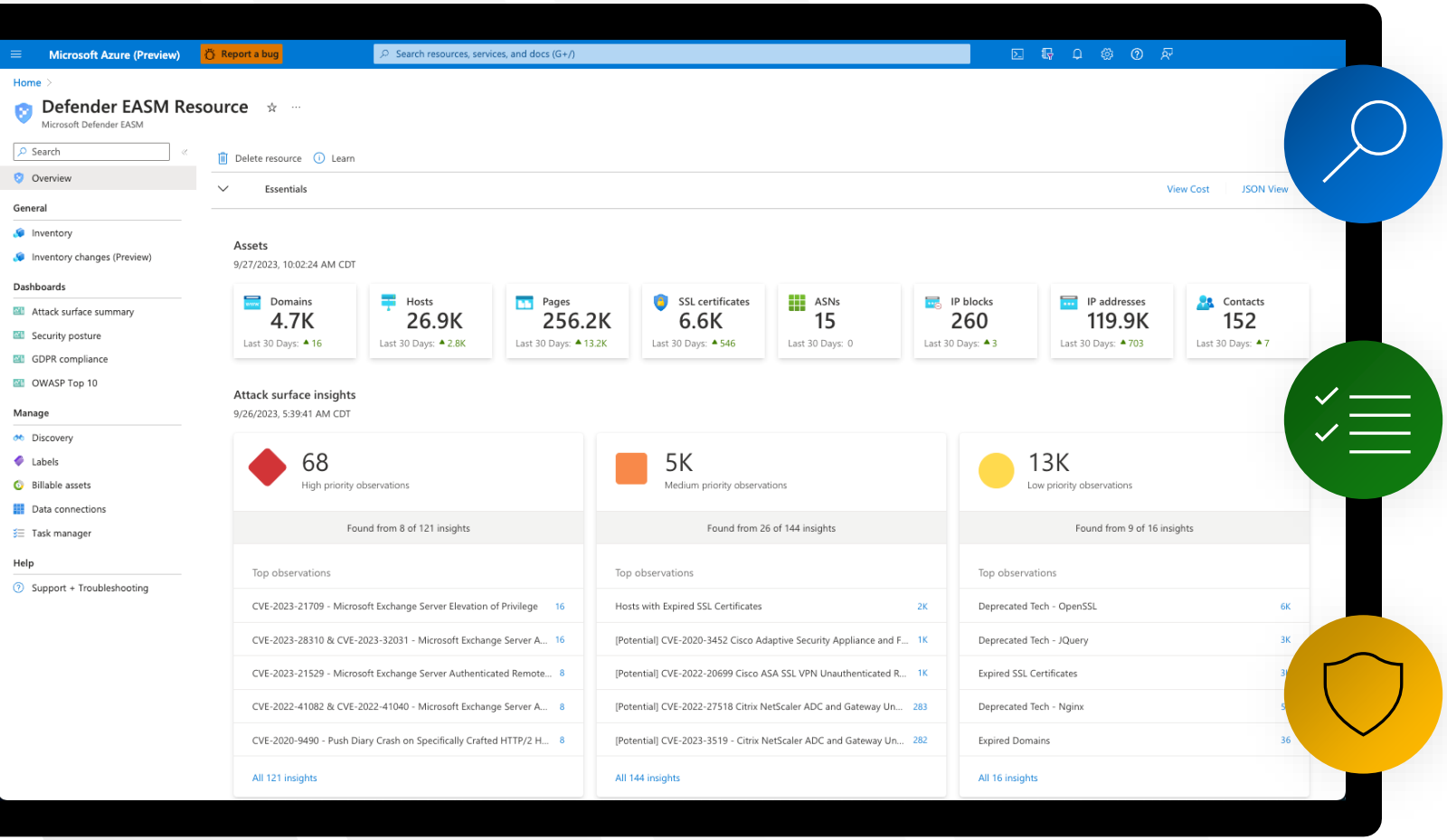
As a member of the Contoso Governance, Risk, and Compliance (GRC) team, I want to identify domain assets in our external attack surface that have been registered with an employee company email addresses instead of the official email address reserved for domain registration (domain-admin@constoso.com),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

Shadow IT attack path example

	Employee policy failure	Vulnerable over time	Open source intelligence	Exploitable exposure
	Employee buys website domain registered to work email address →	Employee creates internet-exposed website →	Unknown website excluded from Contoso patch process →	Attacker sees employee email address used for domain registration →	Unpatched website using domain found and remotely exploited
Microsoft Defender EASM in action	Defender EASM discovers domain asset in Contoso's external attack surface	Contoso's GRC team executes a filtered Whois search in Defender EASM to learn about domain registration origins	The search returns all domains that have been registered with a Contoso employee's company email address	Upon analyzing the asset information provided by Defender EASM, the Contoso team sees it's against policy, labels the asset, and remediates potential risk

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

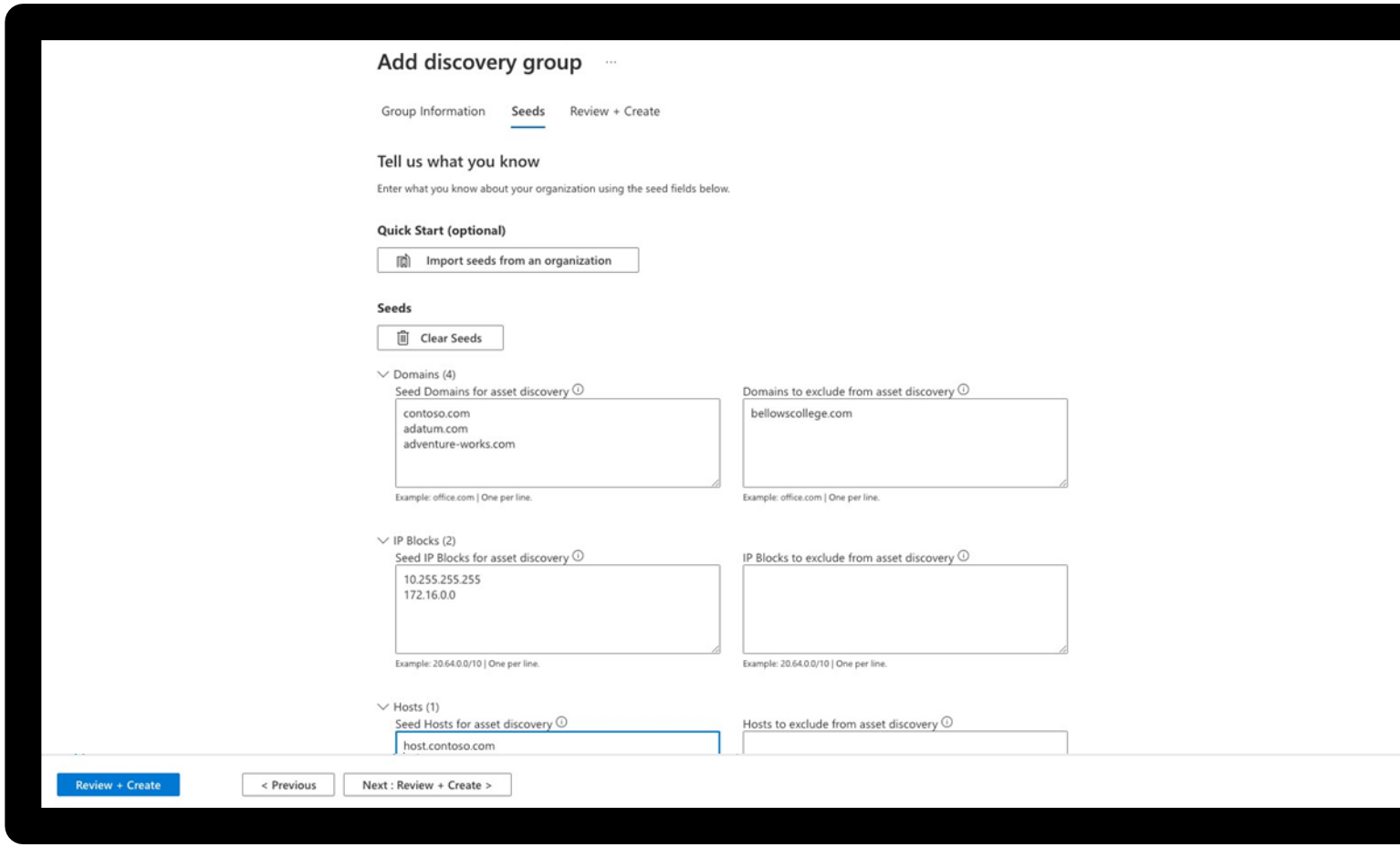
Secure your organization by continuously monitoring discovered devices and search for new vulnerabilities without the need for agents or credentials

Discover your external attack surface

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

Discover Prioritize Secure

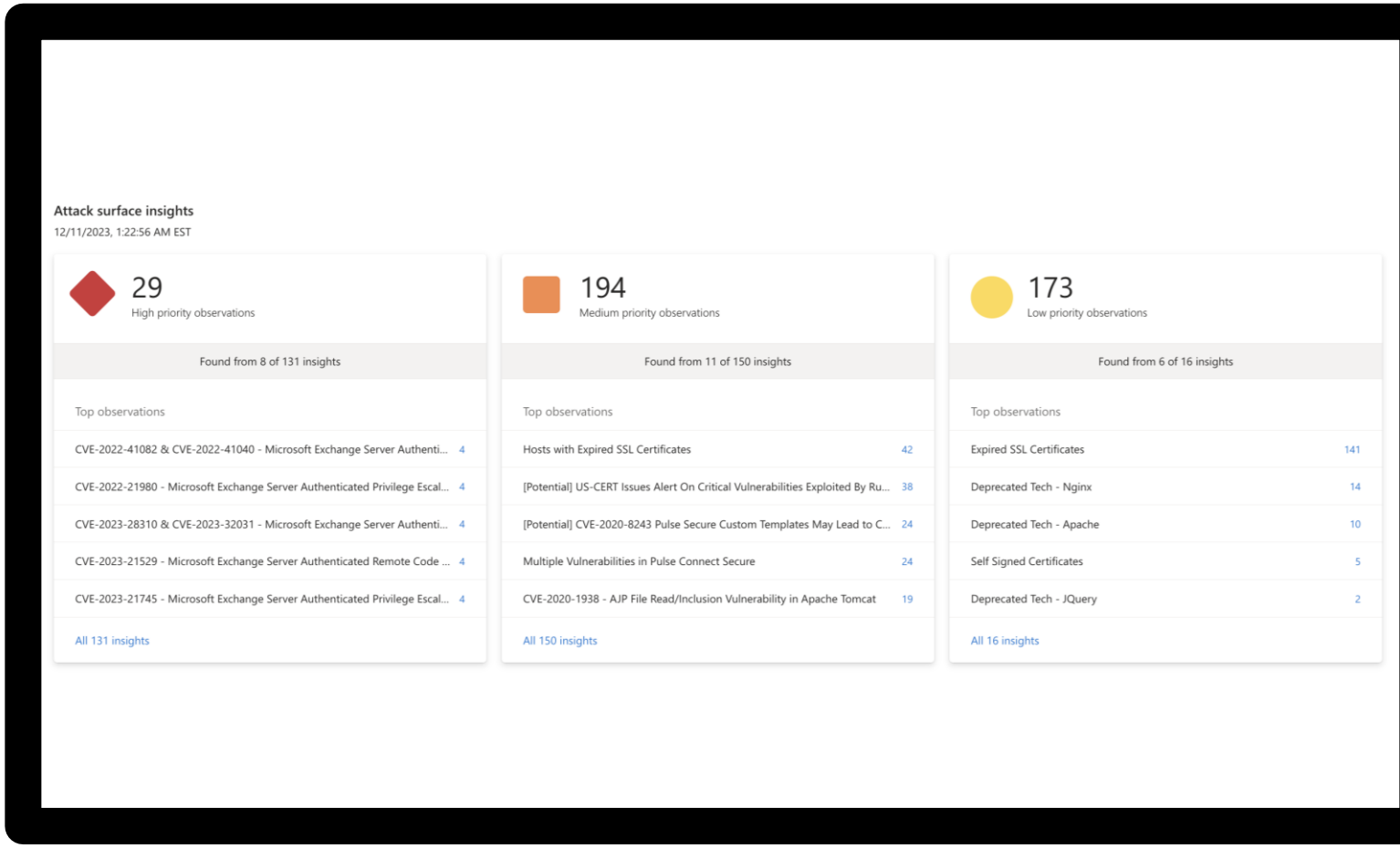
- Gain visibility into your external, internet-facing profile with continuous internet scanning
- Understand the unknown assets, shadow IT and legacy services you still have operating online
- Build an accurate, and up-to-date catalogue of your organization's resources and assets



Prioritize any vulnerabilities

Understand your exposure, and how to fix it

- 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



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

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

Microsoft Security

Thank you!

Appendix