Microsoft Security

Introduction to Microsoft Security Exposure Management

Presented by
Lexi Lederman, Customer Experience Engineering PdM

Agenda

- Learning objectives
- Why do we need exposure management?
- What is Microsoft Security Exposure Management?
- In-product demos
- Q&A

Learning objectives

After this training you will be able to...

- Understand the concept of exposure management and its significance in the current cyber landscape, enabling you to identify and prioritize vulnerabilities within your organization's digital infrastructure.
- Effectively utilize the Microsoft security-exposure management solution, including in-product exploration and practical demonstrations, to enhance your organization's security posture and reduce risks.
- Integrate exposure-management data across various Microsoft Defender products, allowing for a unified approach to security operations and improved decision-making in response to potential threats.

Acronyms

Acronym	What it means
MSEM	Microsoft Security Exposure Management
MDI	Microsoft Defender for Identity
MDO	Microsoft Defender for Office
MDA	Microsoft Defender for Cloud Apps
MDE	Microsoft Defender for Endpoint
MDC	Microsoft Defender for Cloud
MDVM	Microsoft Defender Vulnerability Management
CSPM	Cloud Security Posture Management
EASM	External Attack Surface Management
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System

Evolution of vulnerability management

1 TI-based vulnerability management

- Asset discovery (endpoints, servers)
- CVE enumeration
- CVSS rating

2 Risk-based vulnerability management

- Asset discovery (+ Mobile, identity, apps, web)
- Weakness enumeration
- Contextual prioritization
- Security validation

3 Unified Exposure Management

- Asset discovery (+ SaaS, cloud, data, supply chain)
- Continuous assessment
- Risk reduction mobilization
- Business integration

The demands of security teams are increasing

The average security team is responsible for:

393,419 assets

(Apps, data, devices, controls, network, users...)

The average number of exposures per org:

830,639 exposures

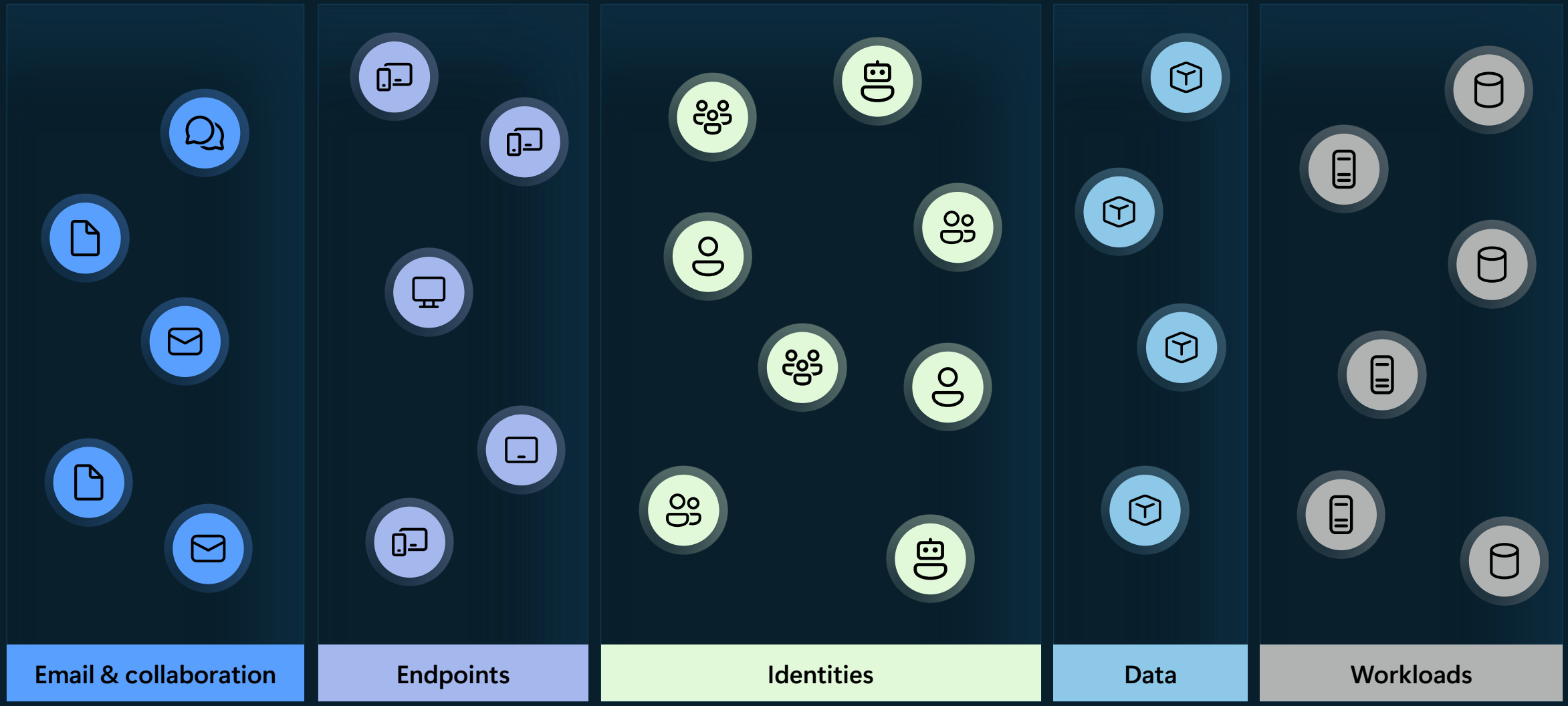
(CVEs, misconfigured controls, privileged identities, secrets...)

The average time to reduce exposures:

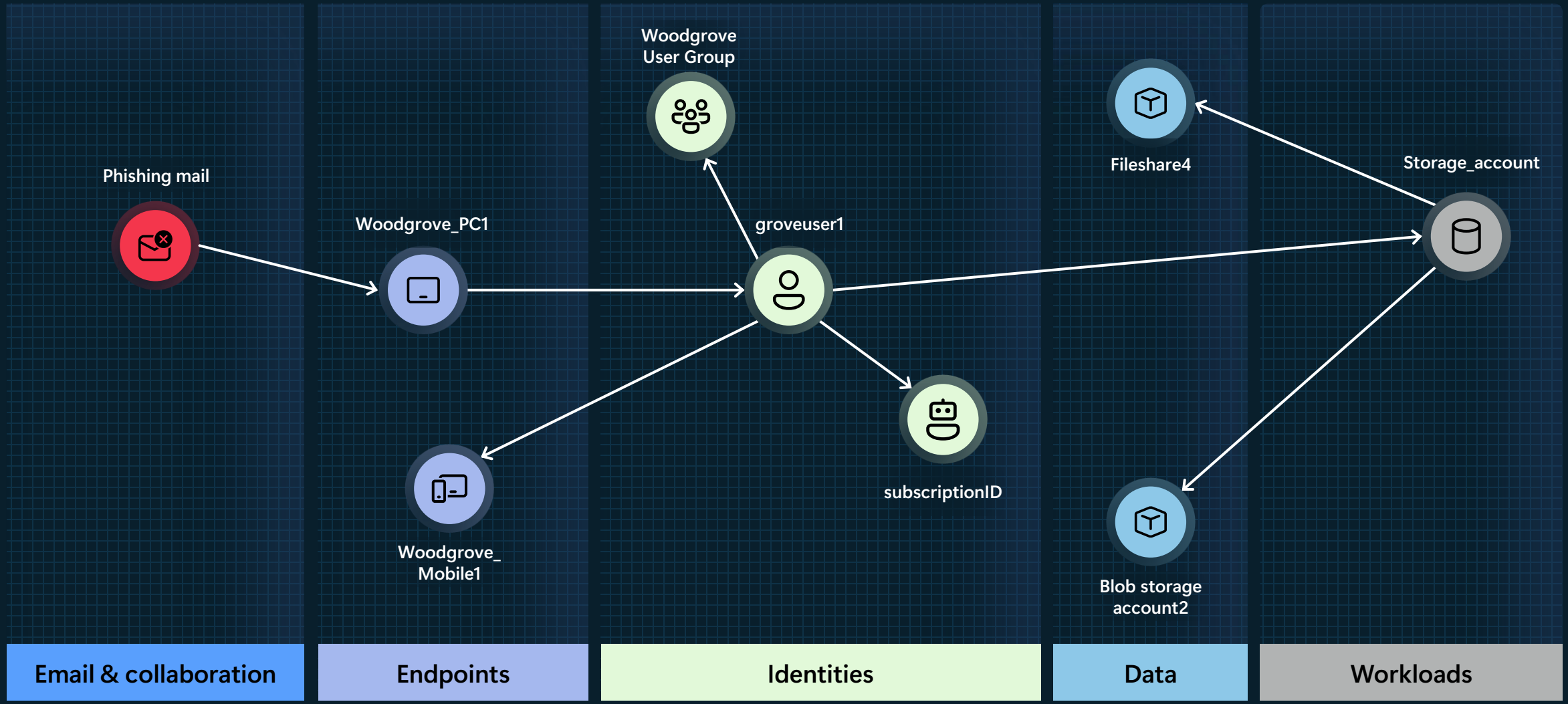
58 days

(Prioritize by risk, validate feasibility, mobilize teams)

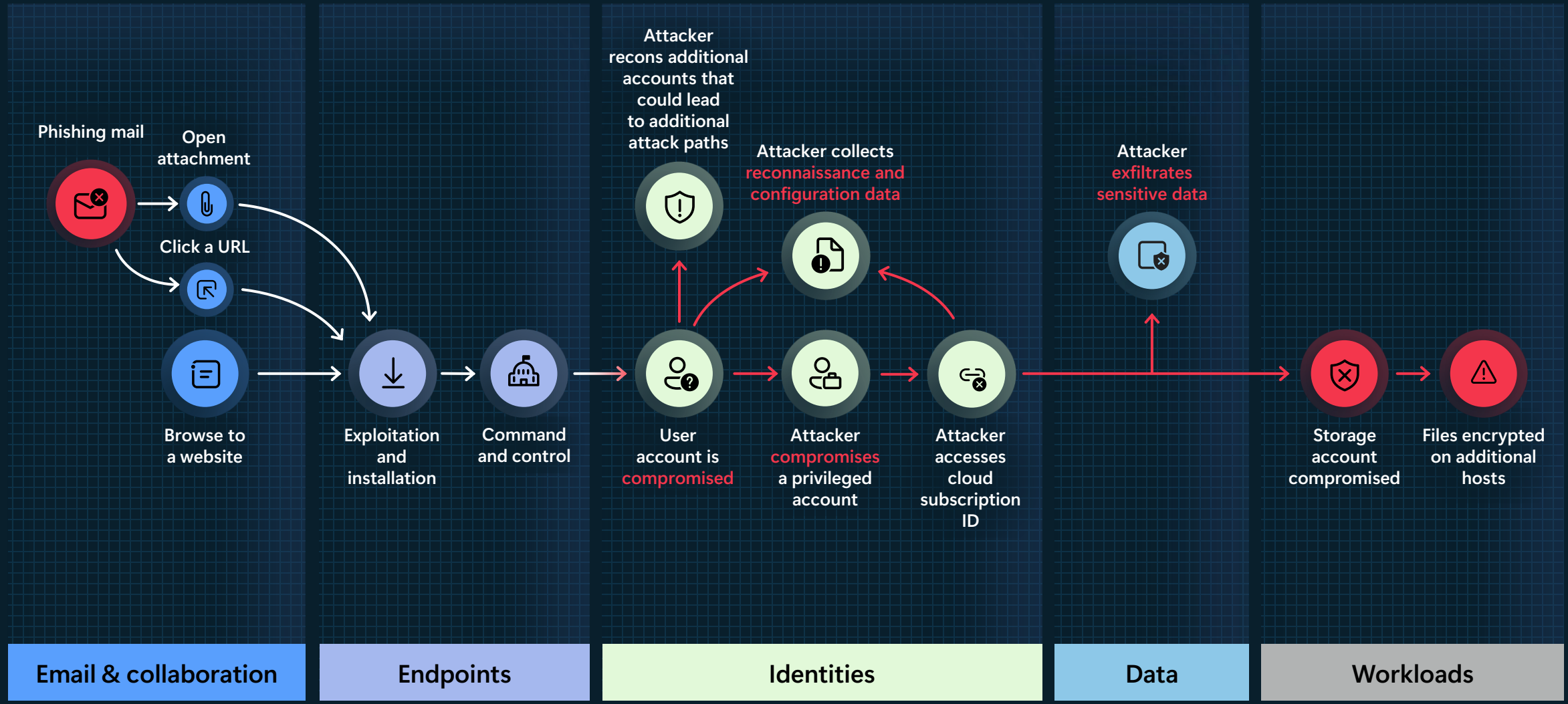
Security teams defend in silos



Attackers think in graphs, surveying potential attack paths



...that become successful breaches if left unaddressed



Unified asset inventory with connector ecosystem

Native integration with Microsoft security products, connectors to integrate with non-Microsoft security

Endpoint security	Email security	Identity security	Vulnerability management	SaaS security	Application security	Cloud security	External attack surface	Configuration management database
Microsoft Defender for Endpoint	Microsoft Defender for Office 365	Microsoft Entra ID	Microsoft Defender Vulnerability Management	Microsoft Defender for Cloud Apps	Microsoft Defender for Cloud	Microsoft Defender for Cloud- CSPM	Microsoft Defender EASM	ServiceNow
Microsoft Defender for IoT	Proofpoint	Microsoft Defender for Identity	Qualys*	Obsidian	Synk	Wiz	Censys	
CrowdStrike	Avanan	Okta	Tenable*	Adaptive Shield	Checkmarx	Prisma Cloud		
SentinelOne		Duo	Rapid7*					

*Available today

Asset metadata | Operational usage | Configuration data | Policy state | Security findings | Health state

See beyond silos with the exposure graph

Collect, dedupe and normalize asset data

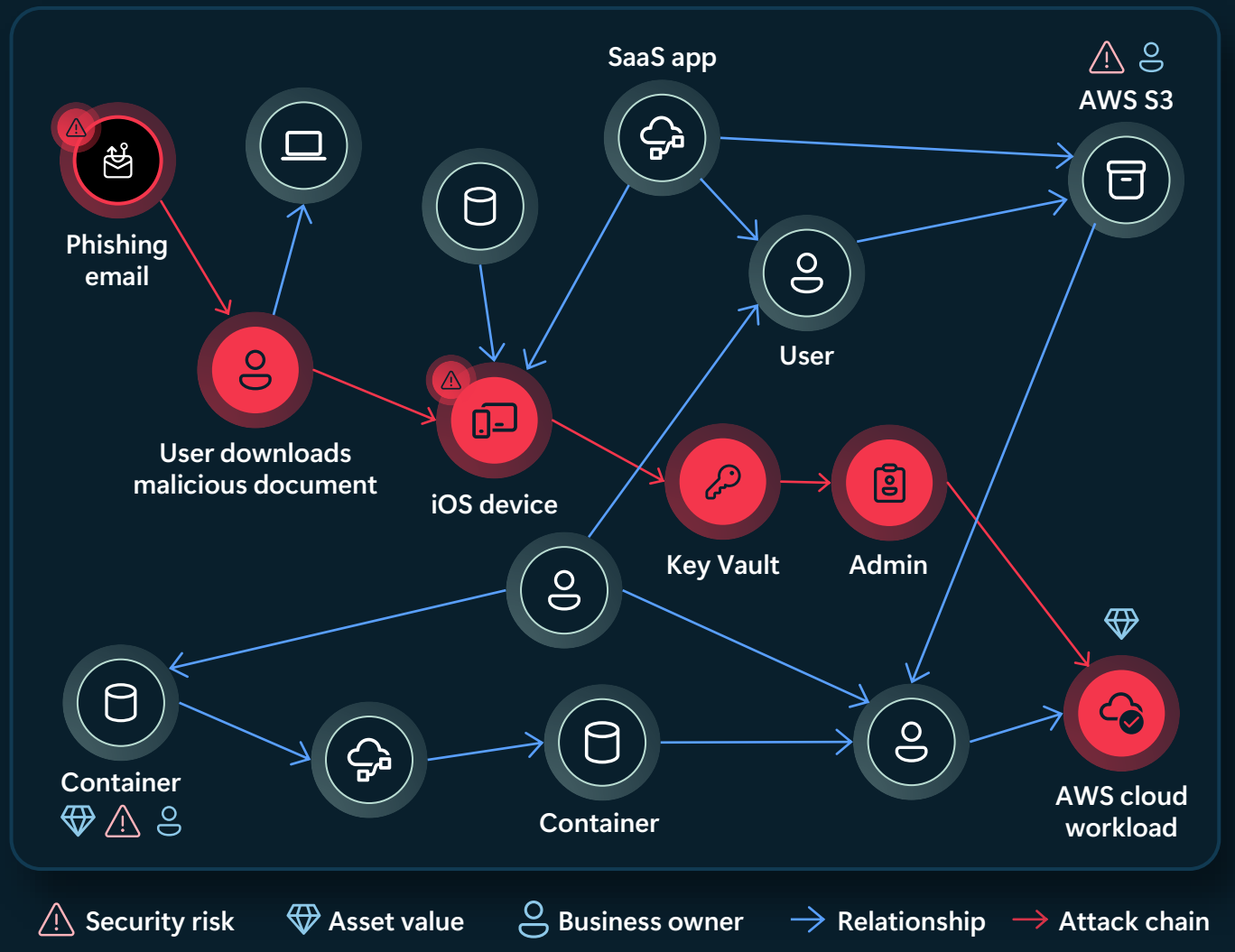
From on-premises to cloud, bring visibility into your assets to contextualize.

Map out assets and relationships

Automatically reveal unmonitored assets and map relationships to uncover gaps and risks.

Inform prioritization

Understand entire attack surface to swiftly identify, prioritize, and remediate critical issues and vulnerabilities.



Demo

Microsoft security
exposure management

Measure and prioritize exposure

Turn complex security risks into
data-driven insights

Program initiatives

Track and report your risks and obtain prioritized recommendations based on your objectives

Help answer critical questions

How secure are we against a specific threat?
Where do we stand in our mitigation efforts?

Risk quantification

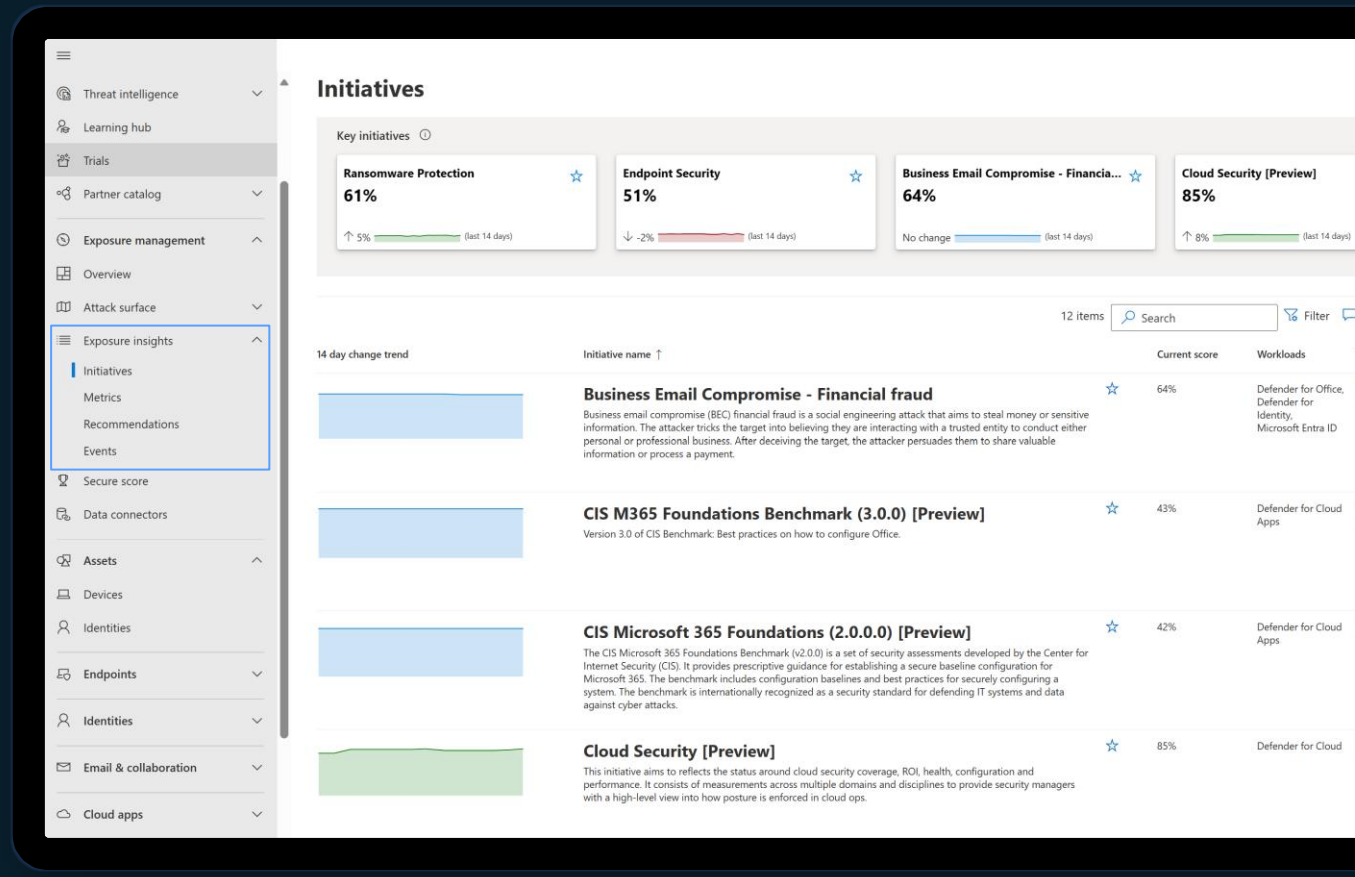
Quantify your exposure with out-of-the-box risk dashboards for your top security programs and threats.

Security metrics and recommendations

Posture and exposure recommendations across the entire attack surface in one catalog or scoped to initiatives.

Effective mobilization

Assign validated exposure findings to risk owners and validate fixes have been applied successfully.



New Unified Recommendations Catalog

One place, full coverage

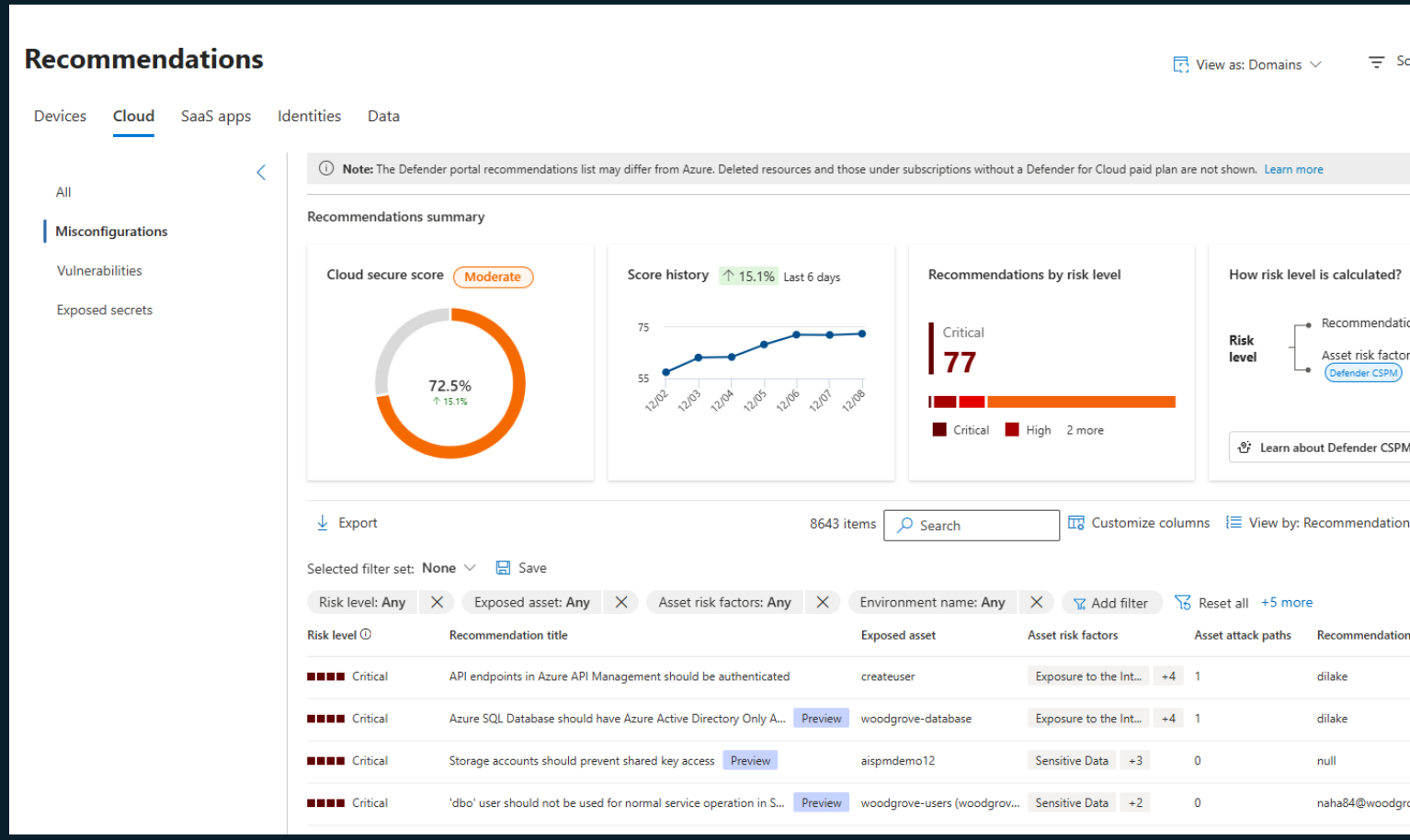
All Microsoft security recommendations in a single, streamlined experience that consolidates recommendations from Secure Score, MSEM, CSPM, MDVM, more to come

Organized by attack surfaces

The catalog is divided into tabs based on attack surfaces (Devices, Cloud, Identity, SaaS Apps, and Data)

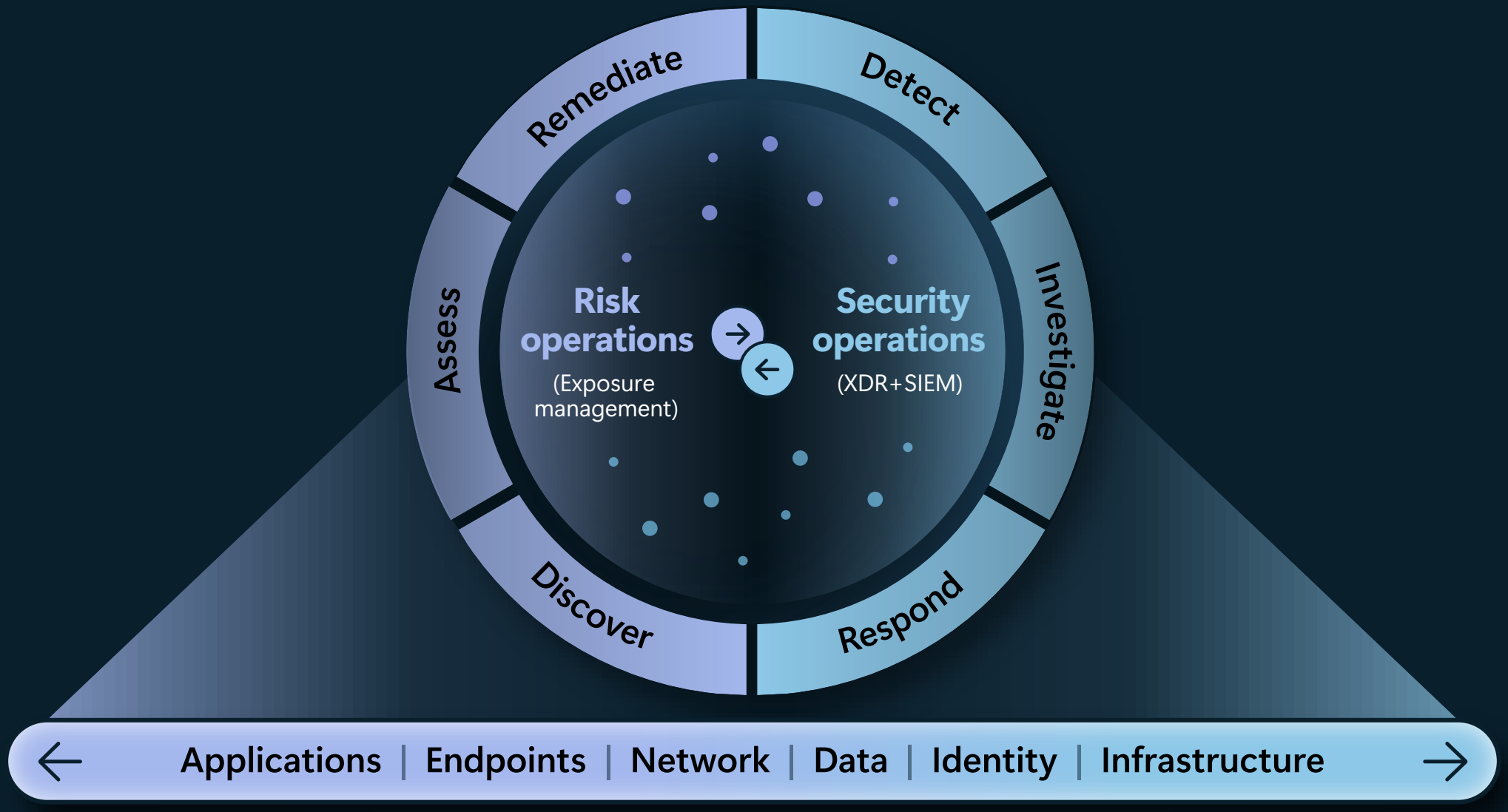
Separated workflows

Misconfiguration recommendations are separated from vulnerabilities, recognizing they represent distinct workflows handled by different personas



Demo

Strengthening the pre- and post-breach continuum



Questions?

Feedback

Help us help you!
We use your feedback to improve our trainings and deliver content that meets your needs.

Use this link (also in the chat) to rate this training.

https://aka.ms/MSEMComCallAsia

Microsoft Security

Thank you