



# The power of the map

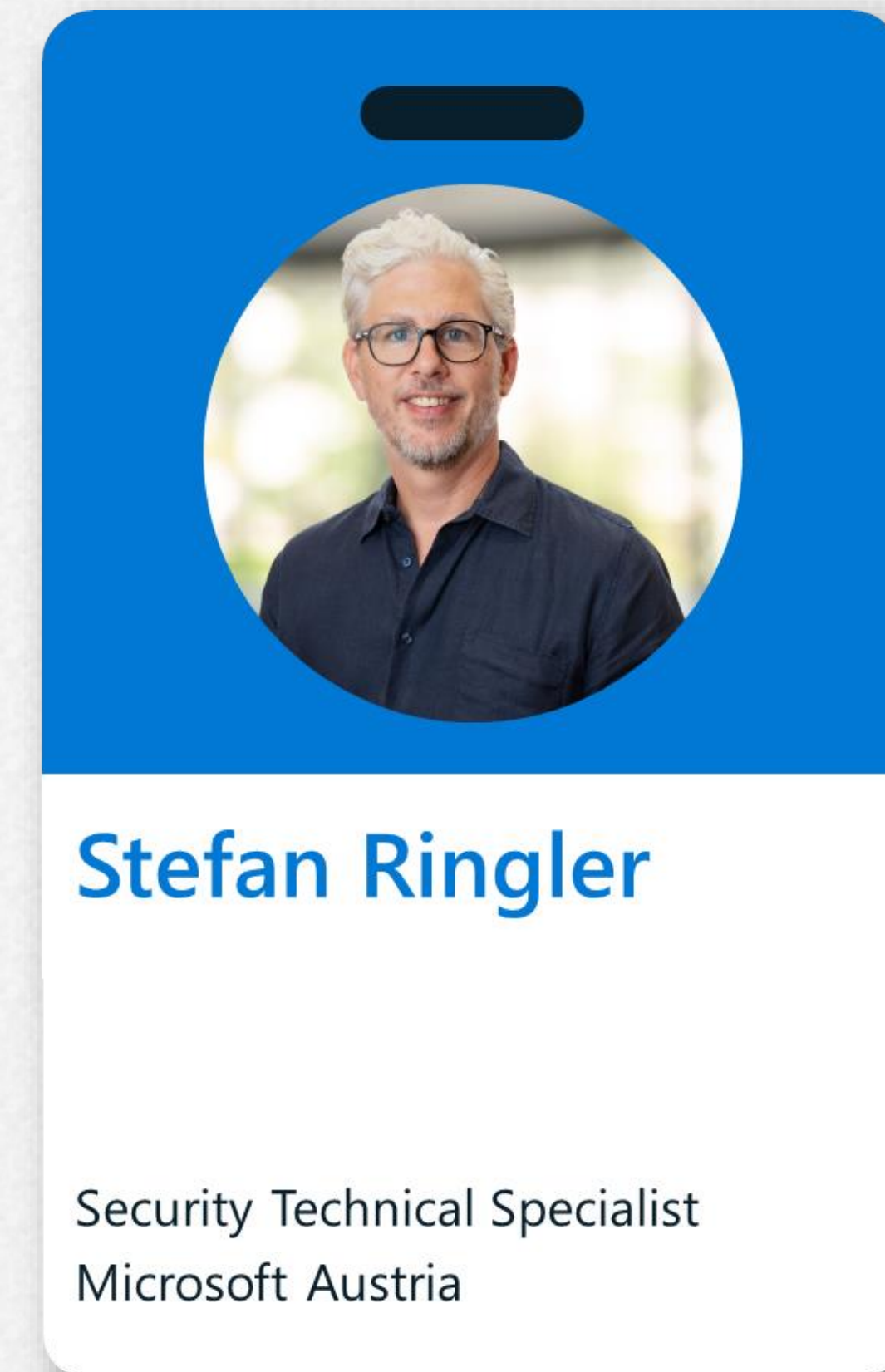






# About me

- Security Technical Specialist @Microsoft
- Former Senior Consultant @Microsoft
- Passionate Tennis player

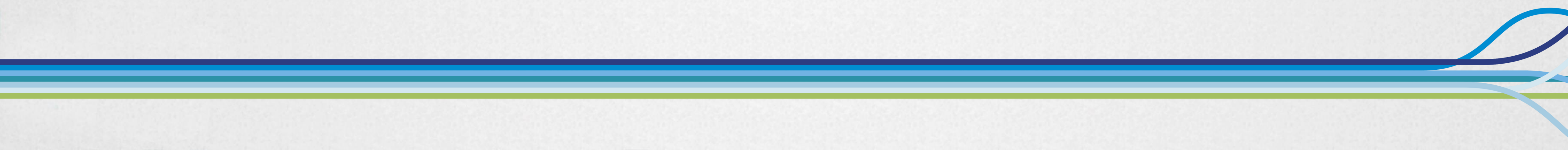






# Let's talk about...

- Your Opponents
- Match Plan
- Training priorities
- Winning formula
- Post-game review





# Adjusting to an ever-moving target

- Modern attacks operate across multiple domains
- Attack surface is expanding...
- Attacks even fueled with GenAI
- Threats quickly pivot and adopt when blocked in one area





# ***Anticipate. Position. Strike Back.***

Reading the Cybersecurity Court  
Like a Pro



→ ***"You don't just react to threats — you read your opponent and move proactively."***





# Building Blocks

The flywheels of defense

Posture

Protection

SOC team  
(detect, investigate, respond)

Pre-breach

Post breach

...the power of  
the Map (Graph)

'Toolbox'

...we will fail if we  
won't Optimize





# Building Blocks

The flywheels of defense

Posture

Protection

SOC team  
(detect, investigate, respond)

Pre-breach

Post breach

...the power of  
the Map (Graph)

'Toolbox'

...we will fail if we  
won't Optimize





# Layers of the graph

## Incident Graph

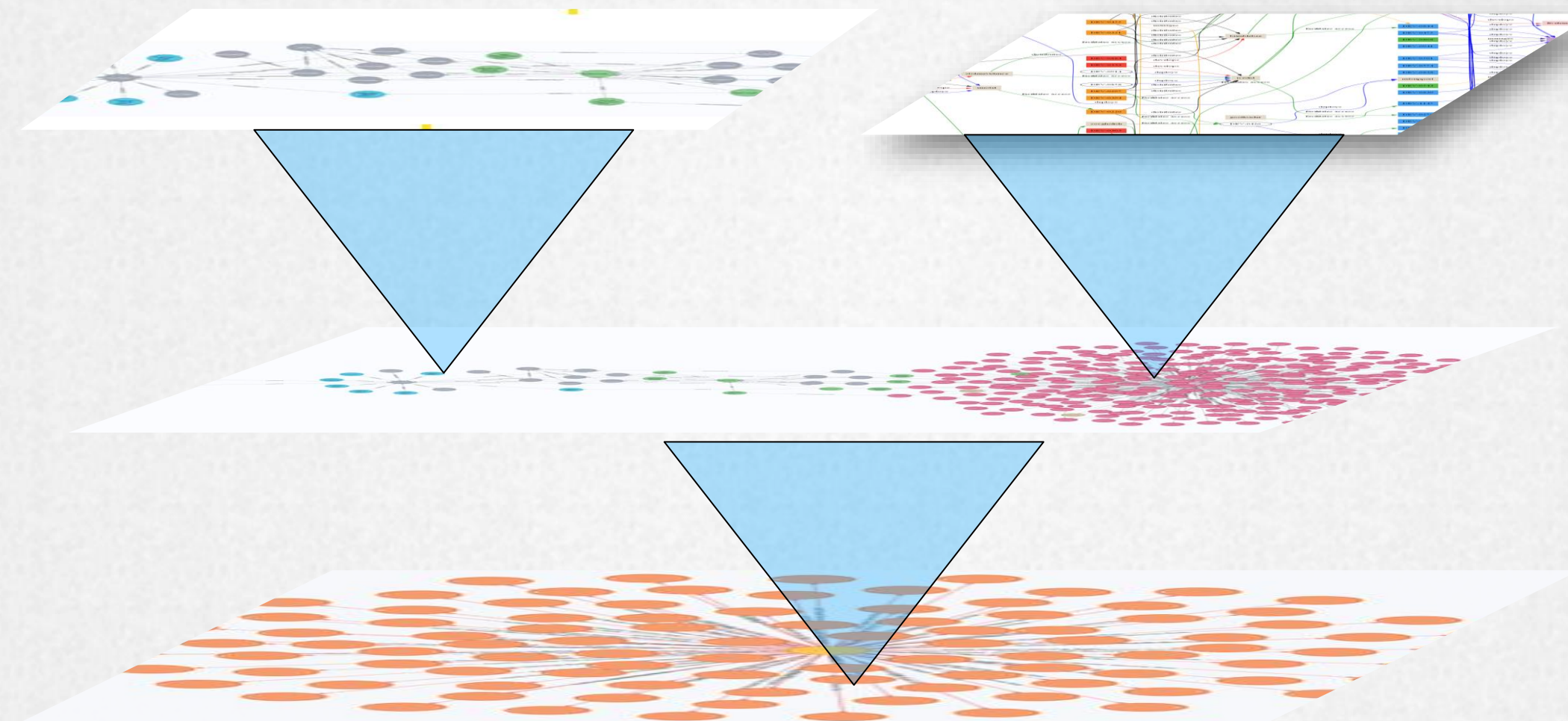
Actual Paths Observed

## Attack Graph

Theoretical Paths Possible

## Security Graph

Asset Configuration & Topology



## Threat Intel Graph

Known Attacker TTP Paths



Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to Critical Azure Key Vault

Attack path

Remediation

alpine-srv1  
Entry point

alpine-mdc-vault-demo  
Target

The diagram illustrates an attack path starting from the Internet. It branches into two paths: one through IP address 52.186.176.237 and another through IP address 135.237.6.23 (labeled as loadBalancer). Both paths converge at alpine-srv1-NIC Network interface, which then leads to alpine-srv1 Virtual machine. From there, the path continues through Managed identity (bfad49a4-8ea2-4514...) to alpine-mdc-vault-demo Key vault. The diagram includes a 'Give us feedback' button.

Insights - High risk vulnerabilities

Vulnerability

CVE-2025-5959

Description

Summary: A type confusion vulnerability in the V8 JavaScript engine of Google Chrome prior to version 137.0.7151.103 allows remote attackers to execute arbitrary code within a sandbox environment by leveraging a crafted HTML page. Impact: Successful exploitation could enable remote attackers to execute arbitrary code on the affected system, potentially compromising its security. AdditionalInformation: This vulnerability is tracked under CVE-2025-5959 and is also relevant to Microsoft Edge, which incorporates Chromium. Refer to Google Chrome Releases for further details. Remediation: Apply the latest patches and updates provided by the respective vendors. [Generated by AI]

CVE ID

CVE-2025-5959

Severity

High

CVSS vector

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:...

CVSS score

8.8

Open the vulnerability page >

Insights - Exposed to the internet

Description

The resource allows incoming network traffic from the internet

Exposure rules

Exposure rule 1



# Map the org

Extensible

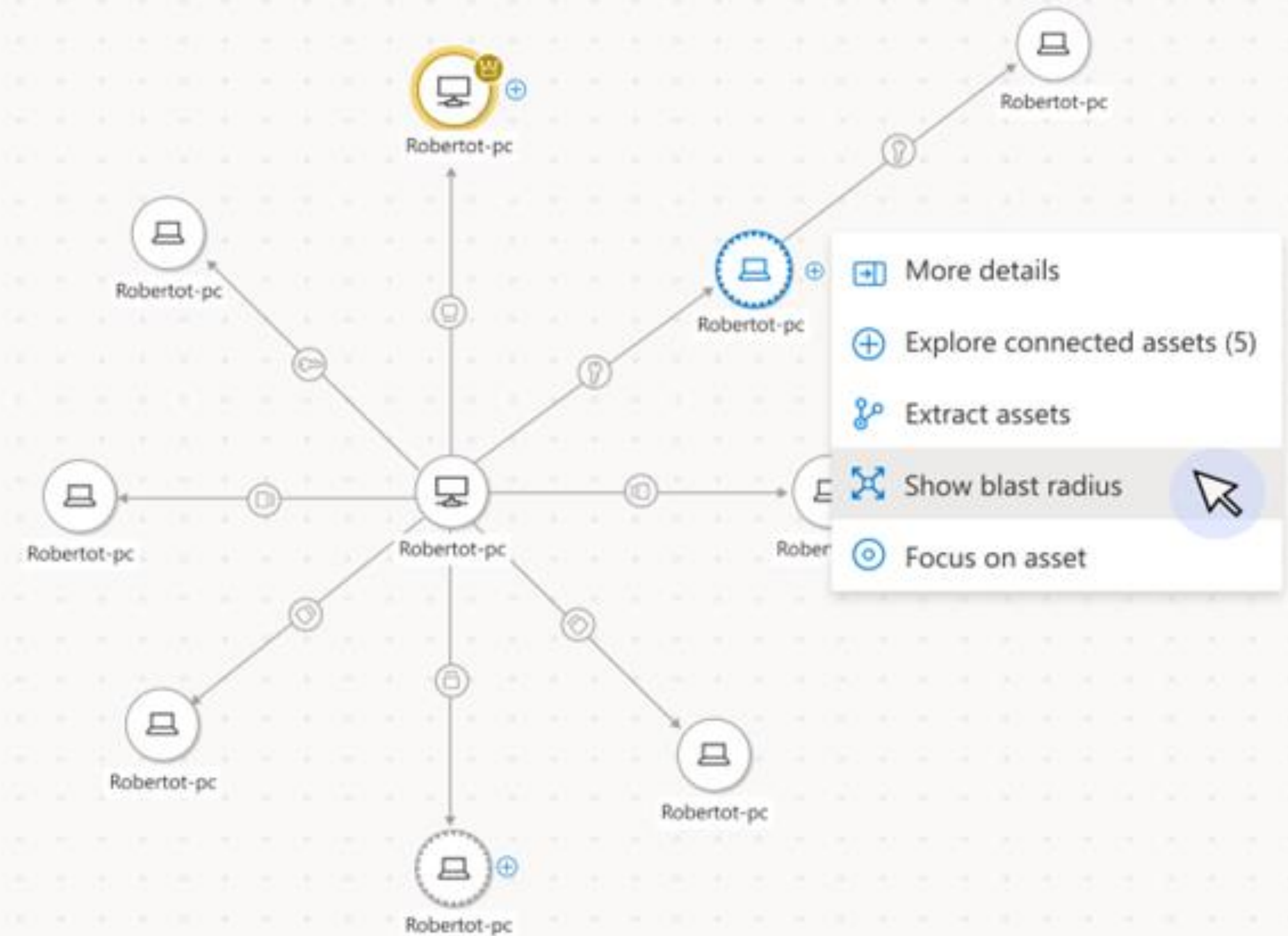
Cover your entire estate

Unified Asset Inventories

Cover all assets types

Critical Asset Management

Identify & classify enterprise critical assets





# Map the org


## Integration with Microsoft Security products out of the box

Vulnerability Assessment	Email Security Posture	Identity Security Posture	Endpoint Security Posture	SaaS Security Posture (SSPM)
Defender Vulnerability Management	Defender for Office	Defender for Identity Entra ID	Defender for Endpoint Defender for IoT	Defender for Apps
Cloud Security Posture (CSPM)	Threat Intelligence	External Attack Surface (EASM)	Application Security Posture (ASPM) *	Data Security Posture (DSPM) *
Defender for Cloud	Defender Threat Intelligence	Defender External Attack Surface Management	Defender for Cloud	Purview Data Security

## Connectors integrate with non Microsoft security tools

### External connectors

External connectors consolidate and enrich security data across your environment, providing valuable insights for effective exposure management.




**ServiceNow CMDB**

✖ Connection Error

Connect your ServiceNow CMDB service to Exposure Management to provide a single source of truth for tracking and managing IT assets. Collect and consolidate them to provide additional context to your security posture.

[View Status](#)




**Qualys**

✔ Connected

Connect your Qualys service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

[View Status](#)




**Rapid7**

✔ Connected

Connect your Rapid7 service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

[View Status](#)




**Tenable**

✔ Connected

Connect your Tenable service to Exposure Management to seamlessly access and manage all your devices and vulnerabilities in one place.

[View Status](#)



**Wiz early preview feature**

○ Not connected

Connect your Wiz account with Microsoft exposure platform to see your devices and vulnerabilities in one place.

[Connect](#)



# Attack Path Analysis drives better posture

## Discover paths to critical assets

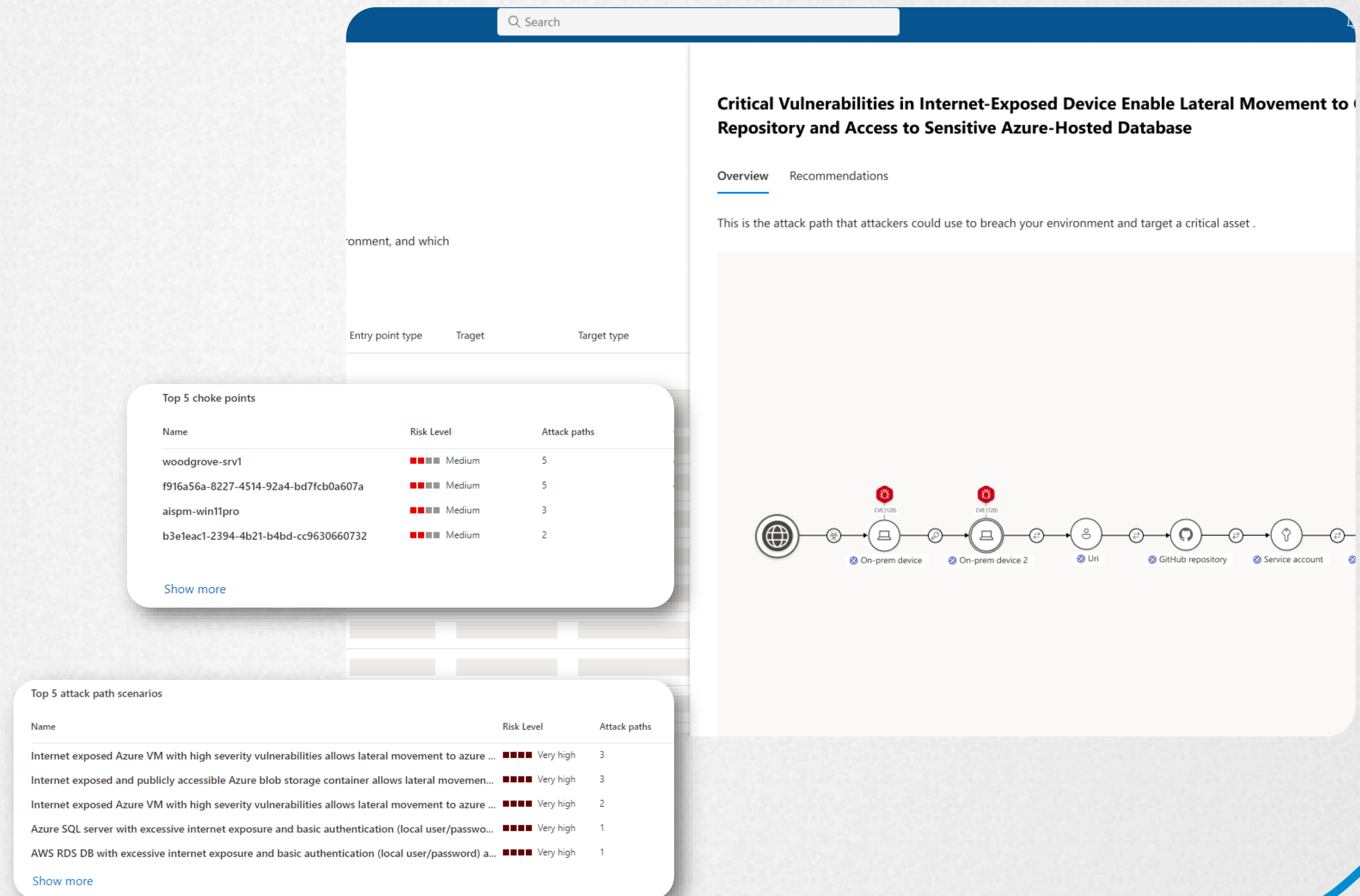
View attack paths to your critical assets across on-prem & cloud just like an attacker would.

## The attacker's perspective

Map potential routes that threat actors could take as they try to exploit weaknesses

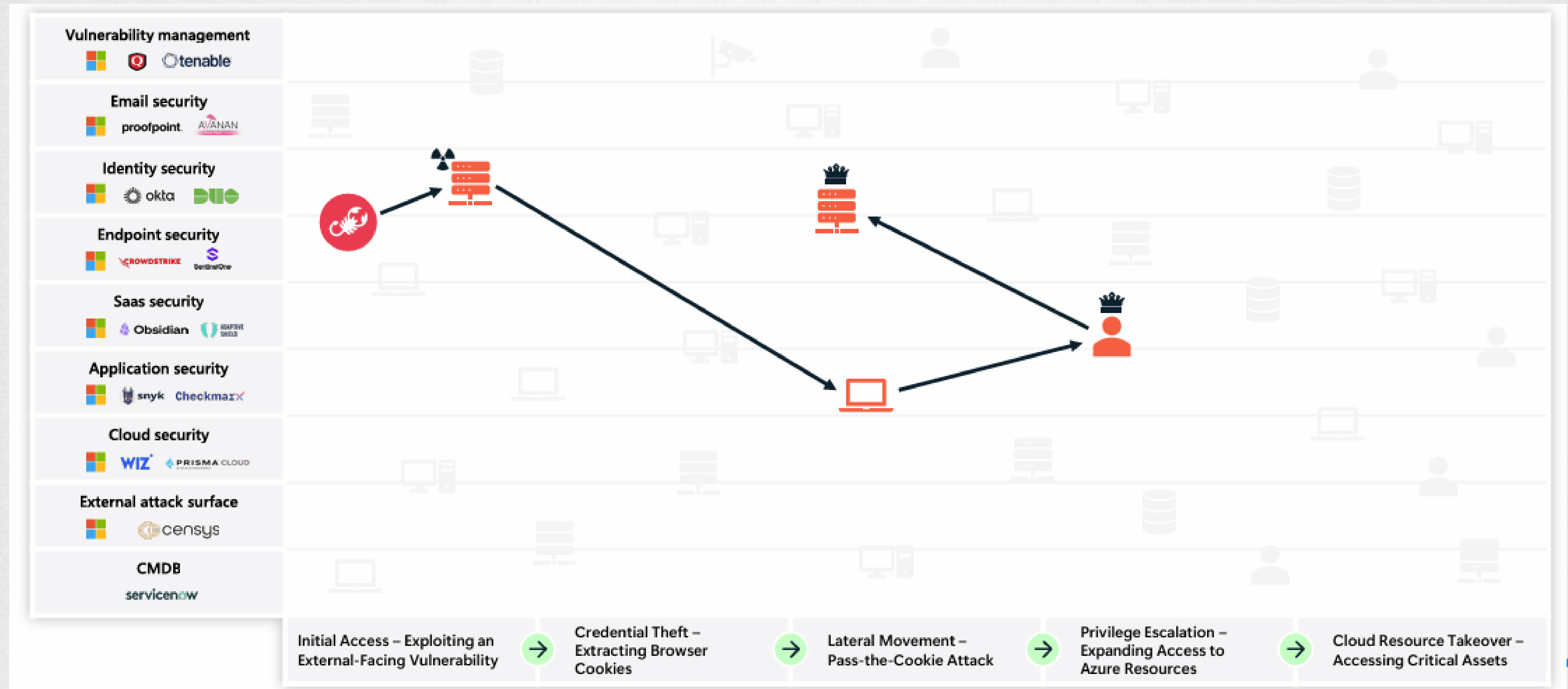
## Land and expand analysis use-cases:

- Validating security risk
- Vulnerability assessment
- Penetration testing
- Threat modeling
- Incident response





# Expand Attack Path Analysis







# Expand Attack Path Analysis

Incidents > Cloud compromise via stolen browser cookies leading to privilege escalation and data exposure

## Cloud compromise via stolen browser cookies leading to privilege escalation and data exposure

Medium | Active | Unassigned | Critical asset

Attack story | Alerts | Assets | Investigations (0) | Evidence and Response (0) | Summary | Similar incidents (5)

Alerts



Incident graph



Layout



Group similar nodes

Play attack story



Unpin all



Show all



# Expand Attack Path Analysis

Defender

Search

Overview **Attack paths** Choke points

See the potential attack paths that attackers could use to breach your environment, and which assets could be affected. [Learn more](#)

Filter set:

Entry point type: Any X Target type: Any X Target criticality: Any X Status: New, Active X Risk level: Any X Type: Any X Add filter

Attack path name	Entry point	Entry point type
Azure DevOps repository without branch protection allows lateral movement to azure ai service (232)	ADO repository	
Azure DevOps repository without branch protection allows lateral movement to azure storage accou...	ADO repository	
Azure DevOps repository without branch protection allows lateral movement to azure key vault (116)	ADO repository	
Azure DevOps repository without branch protection allows lateral movement to azure ai foundry proj...	ADO repository	
Device with high severity vulnerabilities allows lateral movement to azure key vault (90)	Device	
Azure DevOps repository without branch protection allows lateral movement to azure storage accou...	ADO repository	Storage account
Azure DevOps repository without branch protection allows lateral movement to kubernetes cluster (1...	ADO repository	Kubernetes service

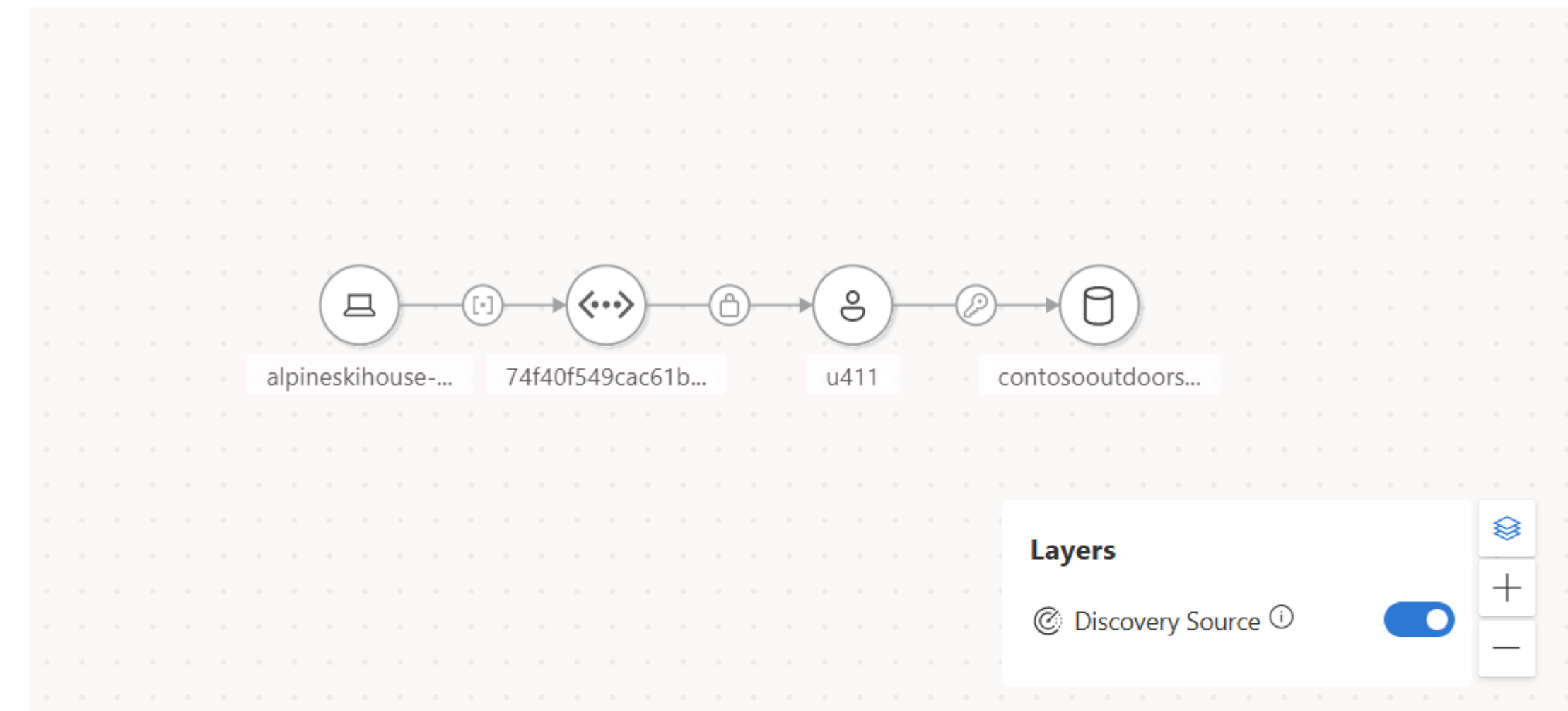
Type

- ☐ Select All
- ☐ On Prem
- ☐ Cloud
- ☒ Hybrid

Apply

## Device with high severity vulnerabilities allows lateral movement to azure storage account with sensitive data

Graph Recommendations



View in map



# Blast Radius Analysis drives better response

Track attack progress on the map

Understand potential attack destinations

"Where are they going?"

Identify alternative similar attack vectors still open

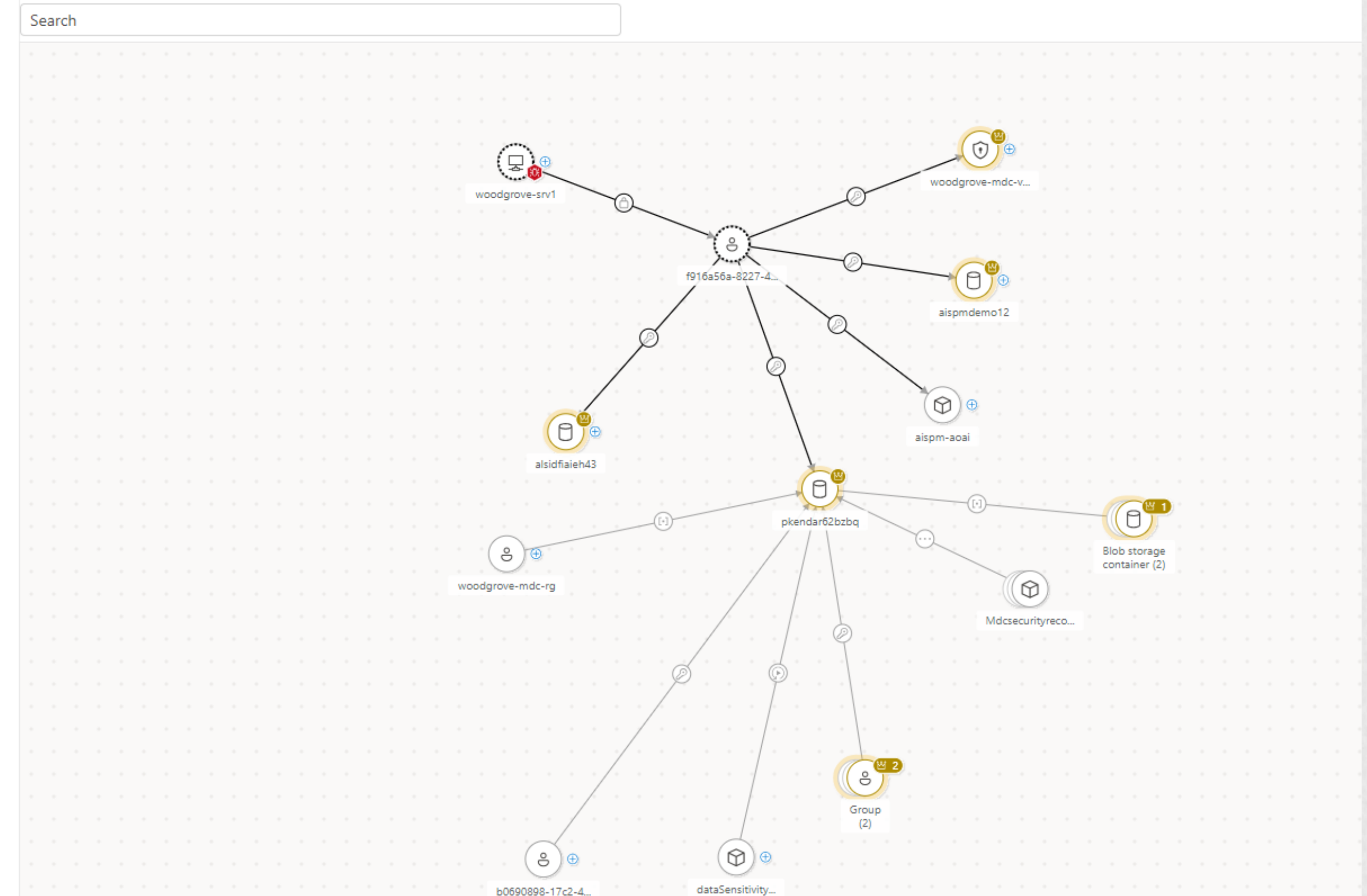
Understand the other ways attackers can exploit similar paths

Better, more informed response

"Shields up" for the potential target:

- Proactive & preemptive posture changes
- Aggressive blocking on path
- Deception in path

## Attack surface map





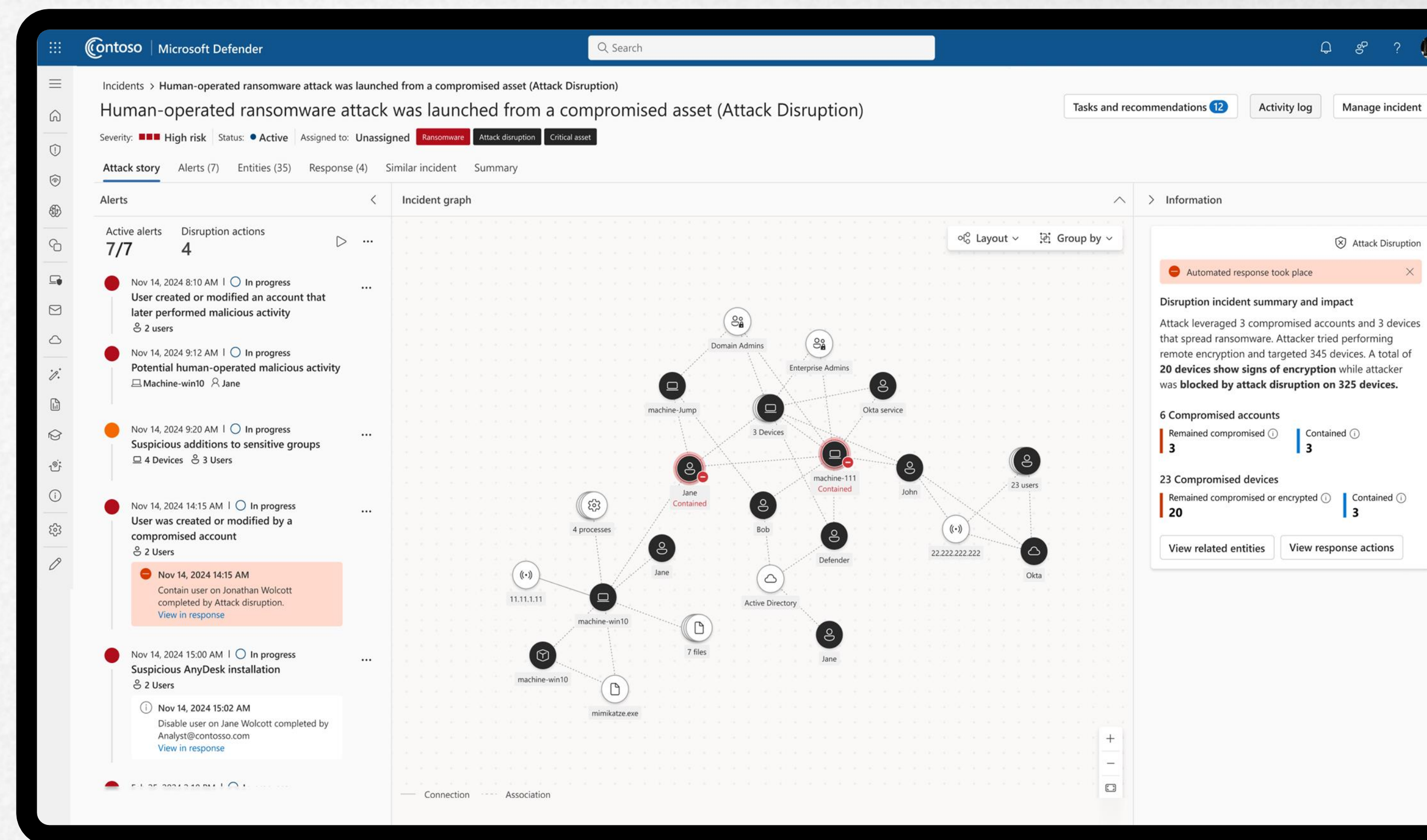


# Automatic Attack Disruption

Disrupts in-progress attacks like **ransomware**, **business email compromise**, **adversary in the middle** and **more** with above 99% confidence

Analyze the attacker's intent, **identifies the compromised assets (i.e., user, device)** and contains them in near real time

Uses the correlated signals in XDR, AI, the latest TI and ML backed models to **accurately predict the attack path** and block the attacker's next move

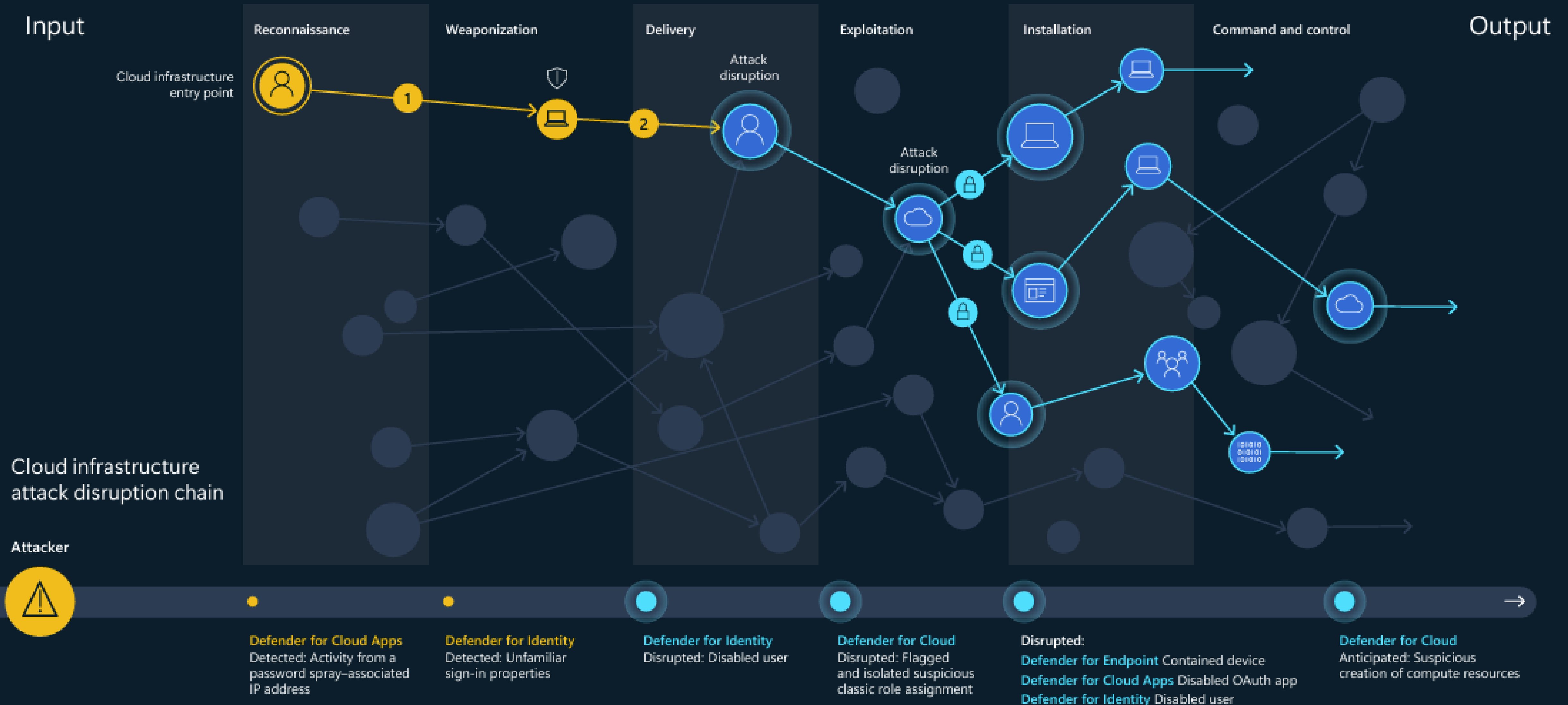




# Automatic attack disruption | Cloud infrastructure

19

Automatic attack disruption leverages cross-domain visibility to identify and stop threats earlier in the kill chain, using advanced mapping to detect malicious activity and harden protection before it progresses laterally. In this instance by using attack disruption SecOps teams have detected, intercepted, and anticipated a complex attack path, isolating real-time attempts while predicting and blocking alternative routes.





# Automatic attack disruption impact

**3 min**

average time to  
disrupt ransomware

**35k**

incidents disrupted  
per month

**6k**

AiTM attacks disrupted  
per month

**120k+**

disabled user accounts  
in the last six months

**180k+**

devices saved from an  
attack in the last six months

Uses correlated signals, the latest TI and AI to stop attacks with above **99% confidence**

## Real-life customer stories:

### A customer experienced an attack across:

- **10+** attack waves
- **10** compromised domain admin users
- **3** spreader IPs

**Attackers targeted 2,000 devices, 97% saved**

3% of devices were onboarded to a different security vendor and suffered encryption

### A customer experienced an attack across six users:

- **4** users were disabled at the initial access stage
- **2** users were disabled when the session cookie was re-used

**Early disruption** in the kill chain prevented a business email compromise attack



# Titan Integration

Microsoft Defender

Incidents > BEC financial fraud attack was launched from a compromised account (attack disruption)

## BEC financial fraud attack was launched from a compromised ...

High Resolved u101@a.alpineskihouse.co BEC Fraud Attack Disruption BEC LATEST Partial demo

Attack story Alerts (10) Assets (3) Investigations (2) Evidence and Response (9) Recommended actions (18) Summary Similar incidents (0)

**Alerts**

- Nov 22, 2024 3:58 PM Resolved  
**Anonymous IP address**  
Lee Gu
- Nov 22, 2024 4:00 PM Resolved  
**Activity from a Tor IP address**  
Lee ... Microsoft Exchange On...
- Nov 22, 2024 5:10 PM Resolved  
**Suspicious inbox manipulation rule**  
Lee Gu 2 Applications
- Nov 22, 2024 5:37 PM Resolved  
**BEC financial fraud**  
Lee Gu
- Nov 22, 2024 5:37 PM Resolved  
**Suspicious inbox manipulation rule**  
Lee Gu
- Nov 22, 2024 5:38 PM Resolved  
**Suspicious emails sent by BEC-related user**

**Incident graph** Layout Group similar nodes

**Copilot**

**Incident summary**  
May 15, 2025 08:36 AM

The high severity incident "BEC financial fraud attack was launched from a compromised account (attack disruption)" occurred between...

[See more](#)

AI-generated content may be incorrect. Check it for accuracy.

**Guided response**  
Nov 15, 2023 6:48 AM

All (7) Unfinished

**Triage**

Completed

**Classify this incident**

[View evidence](#)

AI generated content may be incorrect. Check it for accuracy.

**Contain**

New

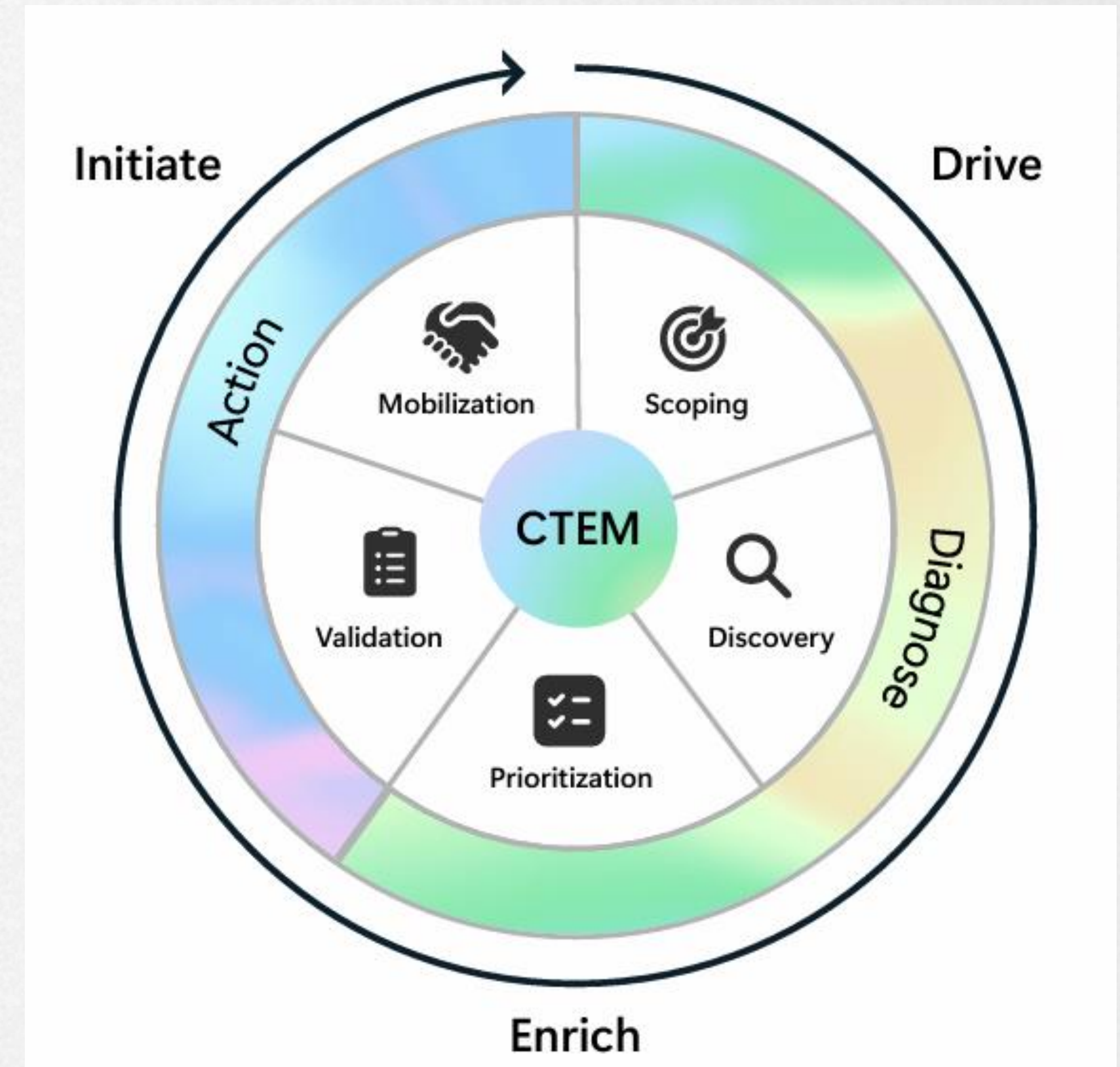
**Consider blocking the Ip Address 80.67.167.81**

The IP 80.67.167.81 was involved in suspicious activities across 14 other organizations with 8 verified True Positives in the last 48 hours, indicating a very high probability that the IP poses a threat to your organization.



# Building an Exposure Management Framework is key

- Start with Visibility
- Prioritize real risks
- Mitigate!!!





- 
- Home
- Exposure management
- Overview
- Attack surface
- Map
- Attack paths
- Exposure insights
- Secure score
- Data connectors
- Investigation & response
- Threat intelligence
- Assets
- Microsoft Sentinel
- Identities
- Endpoints

Due to a change we have made in attack path calculation, you will notice a change in the number of new attack paths discovered, as well as a difference in the number of inactive attack paths in the attack path experience.

Overview

Attack paths

Choke points

Explore the potential attack paths that attackers could use to breach your environment, and which assets could be affected. [Learn more](#)

1 of 200 selected

Search

Filter set:

Entity type: Any

Add filter

Choke point name	Risk level ⓘ	Type	Critical targets	Attack paths ↓
<input checked="" type="checkbox"/> Domain Admins	Medium	Group	22413	25950
		Device	7500	8679
		Device	7490	8669
<input type="checkbox"/> Enterprise Admins	Medium	Group	6201	6471
		User account	4994	5780
		User account	4983	5769
		Group	4545	4545
		Group	3834	4104
		Group	3636	3636
		Group	3636	3636



# MS Exposure Management e-book

## Ransomware attack mitigation

### What can Microsoft Security Exposure Management do?

#### Endpoint vulnerability analysis

Continuously scan endpoints to detect unauthorized scripts, unpatched applications, and hidden ransomware indicators. Then, integrate signals from Microsoft Defender for Endpoint and Microsoft 365 Defender to compile a prioritized remediation list.

#### Threat intelligence correlation

Take advantage of global threat intelligence feeds to identify malicious IP addresses, phishing domains, or known ransomware behaviors associated with Octo Tempest.

#### Attack path reduction

Microsoft Security Exposure Management identifies risks such as privilege escalation, external reachability, over permissions, policy misconfigurations, and visibility blind spots.

#### Mitigation guidance

Provide step-by-step recommendations to isolate infected systems, update security policies, and strengthen email hygiene configurations.

### Outcomes

#### Contained encryption spread

Visibility from the Microsoft Security Exposure Management platform enabled Global Finance Corp to reduce ransomware exposure. This allowed the organization to see the risk of certain unpatched servers, prompting swift containment and halting adversarial lateral movement.

#### Protected critical care systems

Microsoft Security Exposure Management surfaced IoT/OT segmentation vulnerabilities, enabling policy adjustments that kept ICU monitoring devices isolated from ransomware infiltration. Continuous exposure monitoring ensured no downtime for life-critical systems, maintaining operational stability.

#### Cost-effective recovery

Microsoft Security Exposure Management reports flagged nine high-priority Common Vulnerabilities and Exposures, leading to immediate patching that saved an estimated USD2.1 million in potential recovery costs. This prioritized remediation workflow cut incident response times, reducing forensics overhead.



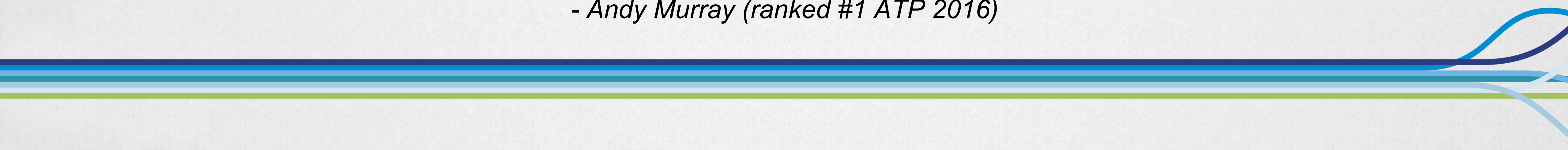


# Summary



**“Control what you can control”**

*- Andy Murray (ranked #1 ATP 2016)*





# Danke an unsere Sponsoren

PLATINUM



GOLD







# Danke!

Closing Subtext

