

Experts Live Denmark

Copenhagen, 2026



Hybrid Identity Under Fire: Detection & Disruption of Hybrid Attack Paths

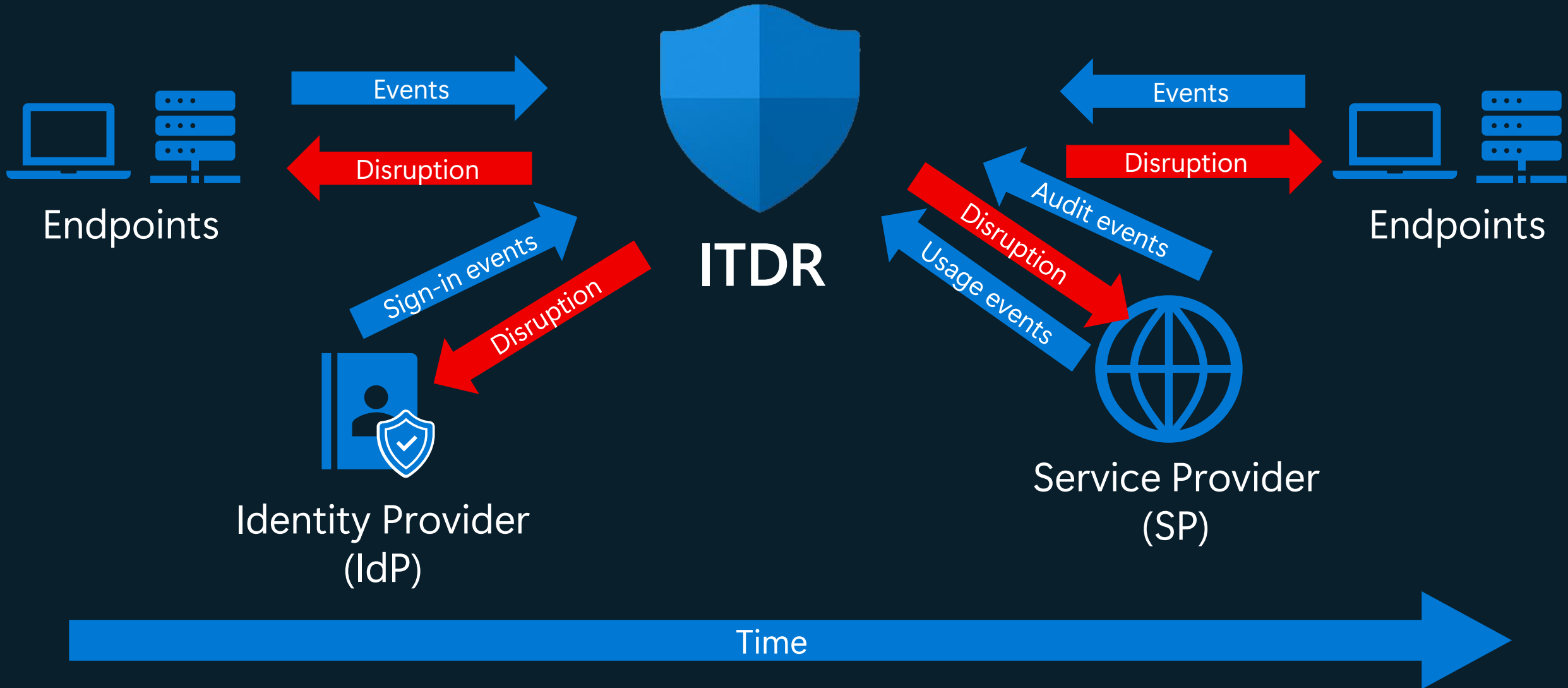
Dr Nestori Syynimaa
Principal Identity Security Researcher
Microsoft Threat Protection



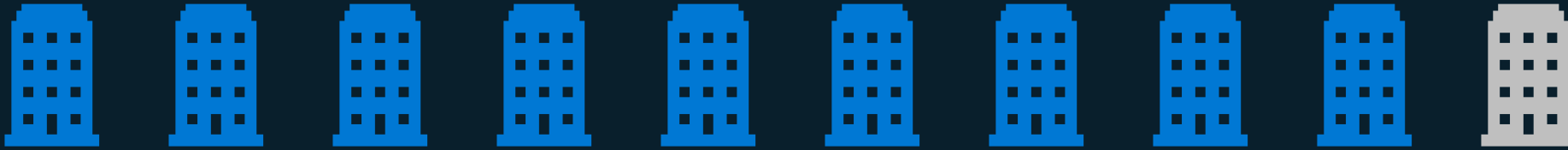
KQL ANONYMOUS



Protecting *identities*: ITDR big picture



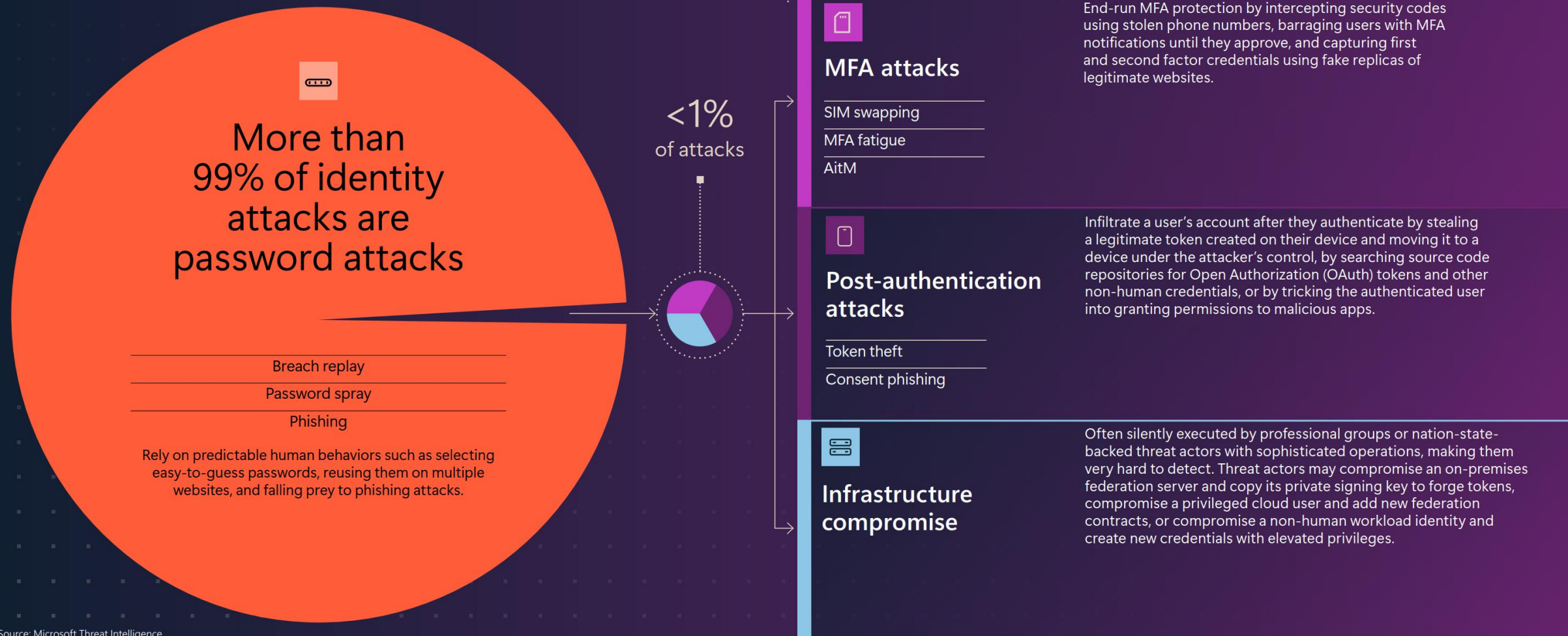
Hybrid is the norm



Over **90%** of our customers have hybrid environments

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.



Source: Microsoft Threat Intelligence

Identity attacks in perspective

More than **97%**
of identity attacks are
password spray or
brute force attacks

Less than 3%
of attacks are...

(A) Token theft by malware

2.4042%

(B) AiTM

0.2375%

(C) Infrastructure

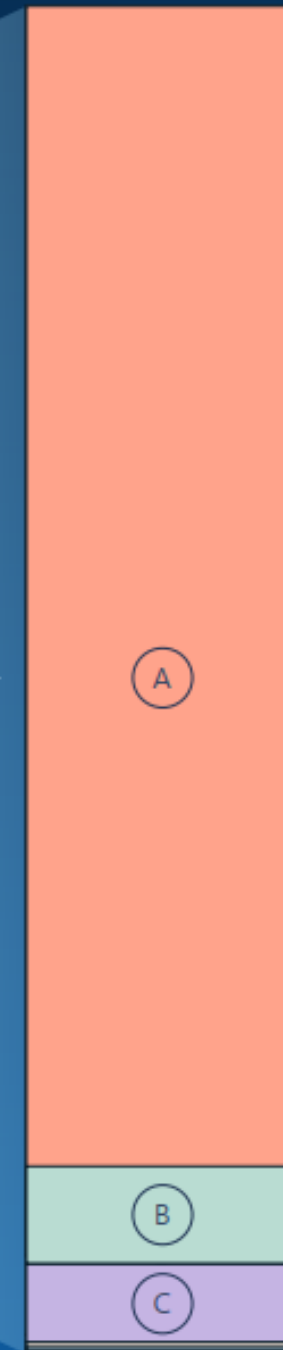
0.1692%

(D) Attacks on MFA

0.0033%

(E) Consent phishing

0.0005%



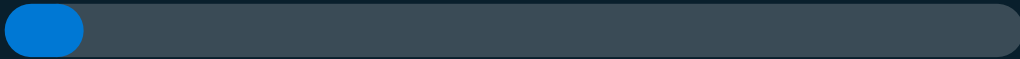
Source: Microsoft Defender XDR and Entra ID Protection alerts (April-June 2025)

<https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>



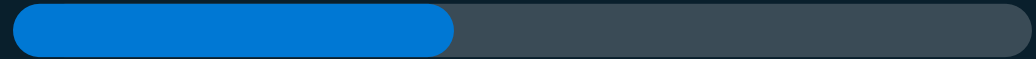
**While everyone went hybrid for flexibility,
attackers went hybrid for invisibility.**

2023



<5% of attacks involved hybrid components

2025

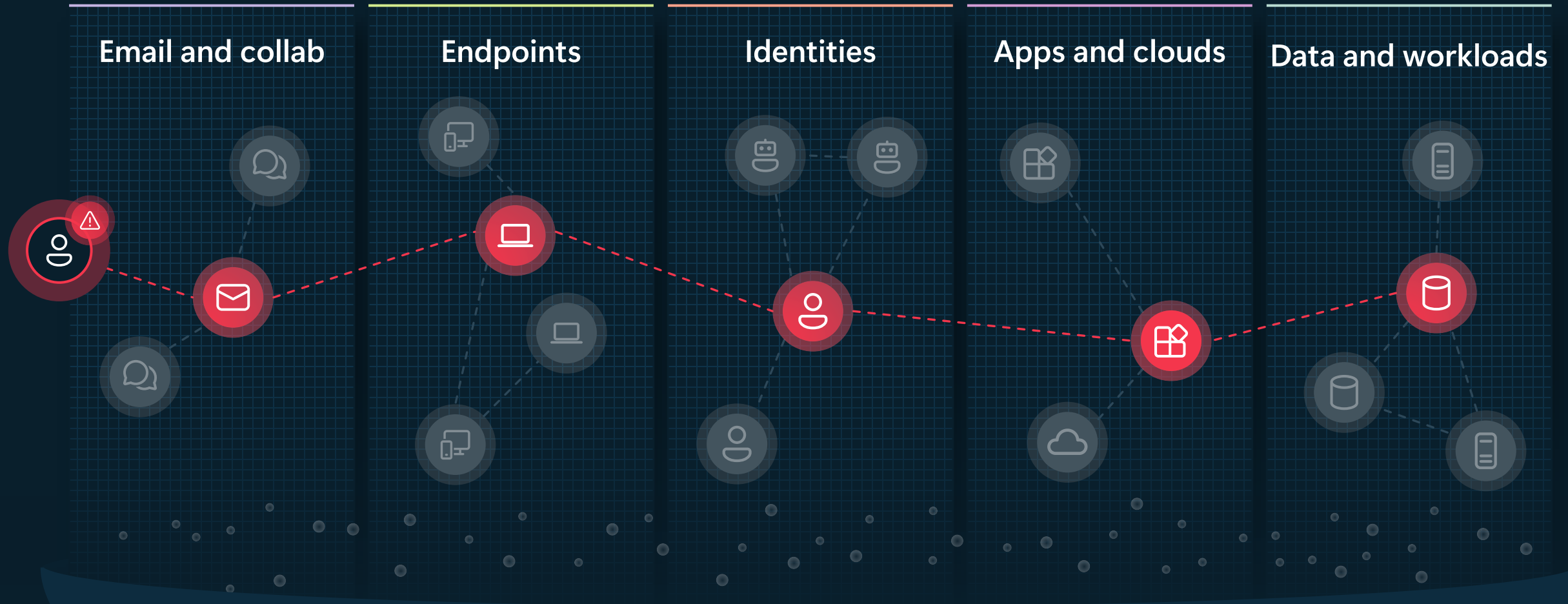


>40% of attacks now involve hybrid components



Hybrid attacks span across cloud and on-prem, blending multiple vectors to stay invisible.

Hybrid Attacks



On-Prem



Cloud



On-Prem

Cloud



On-Prem

Cloud



On-Prem

Cloud



On-Prem



Active Directory

Cloud

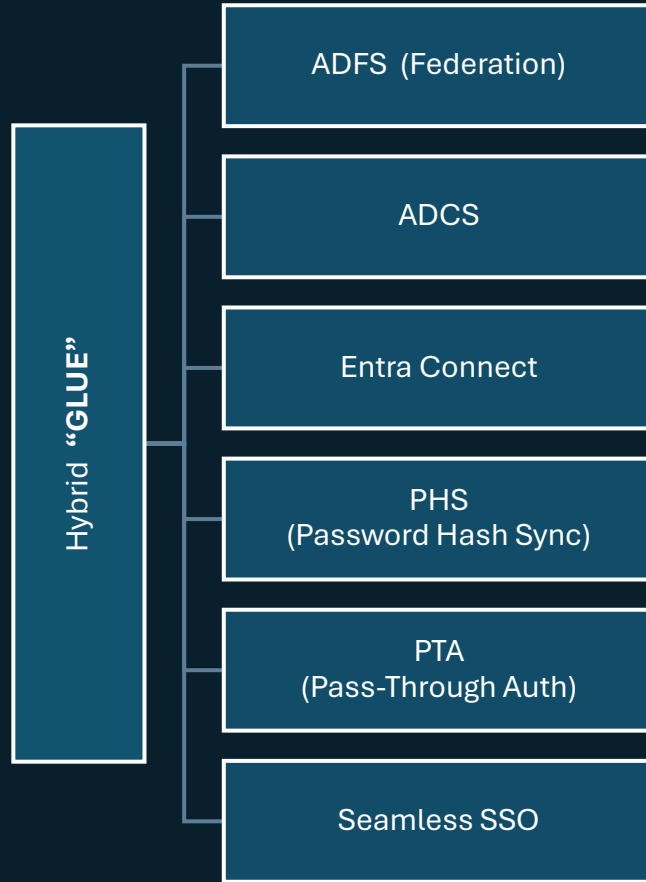
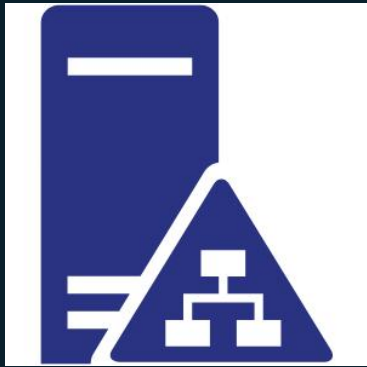


Entra ID

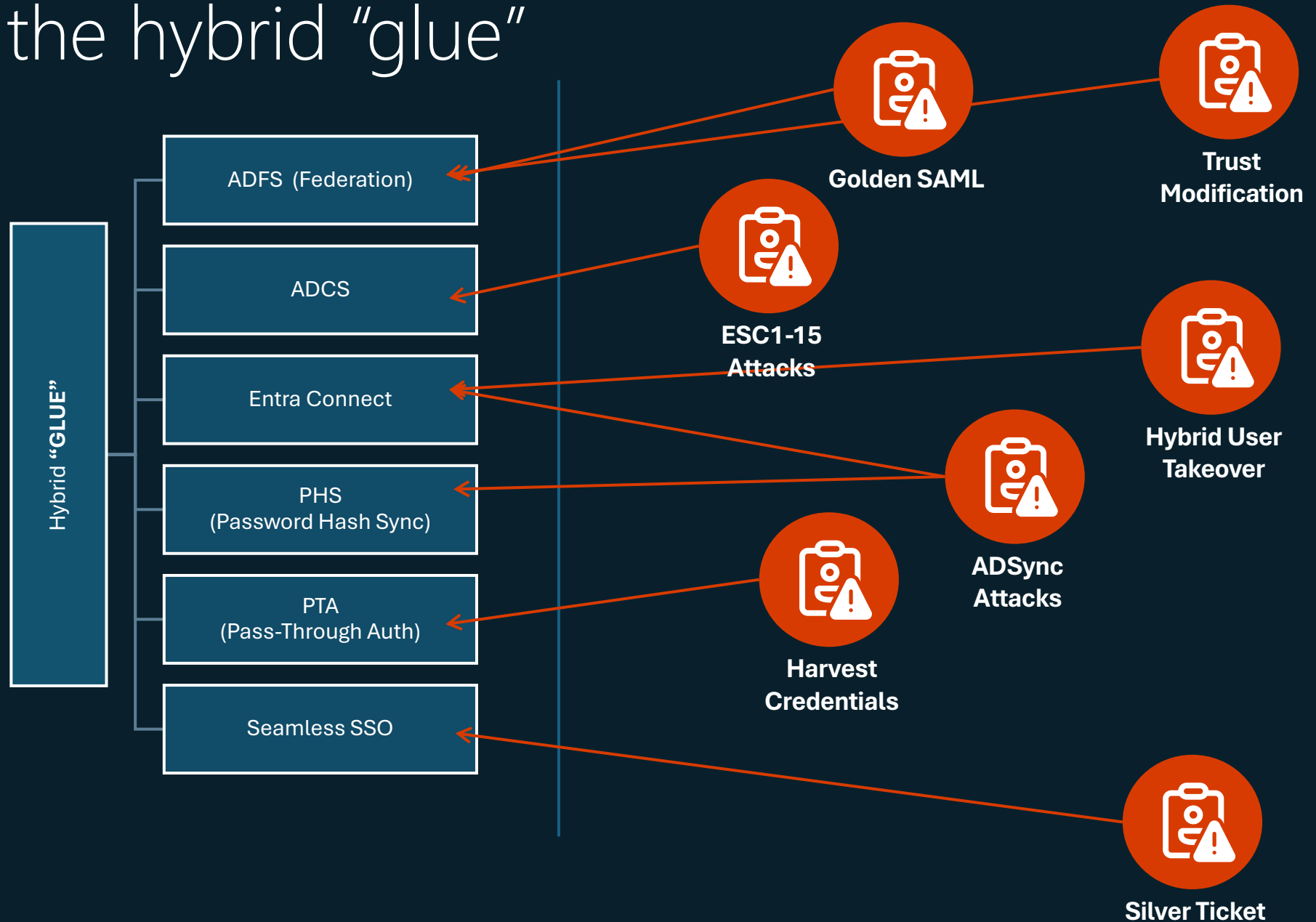


On-Prem

Cloud

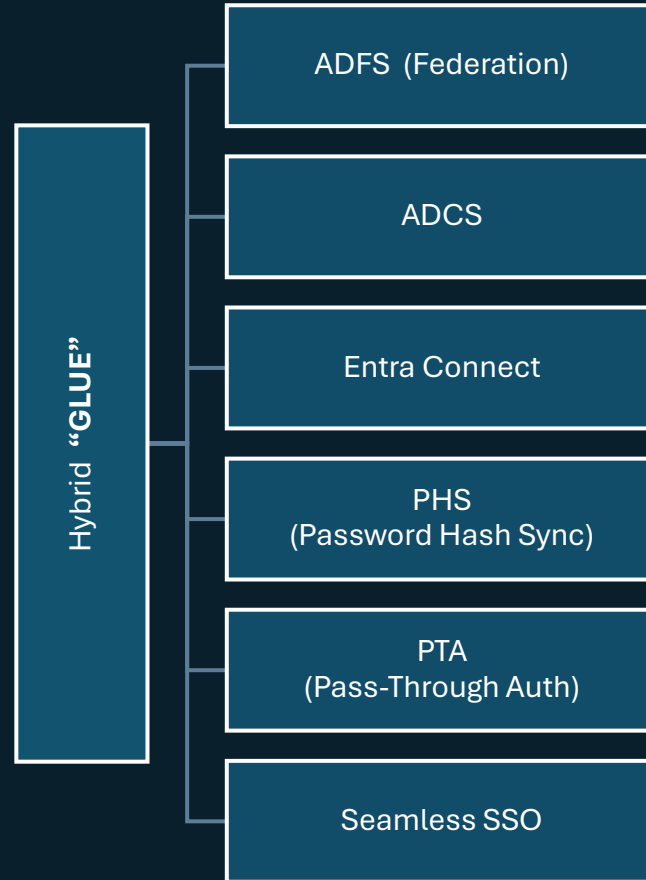
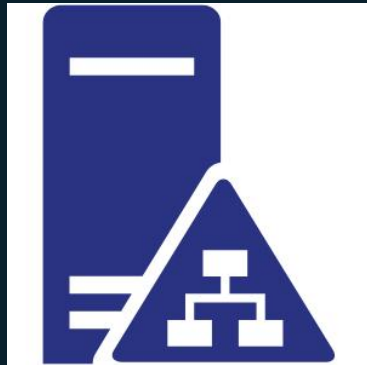


Attacking the hybrid "glue"



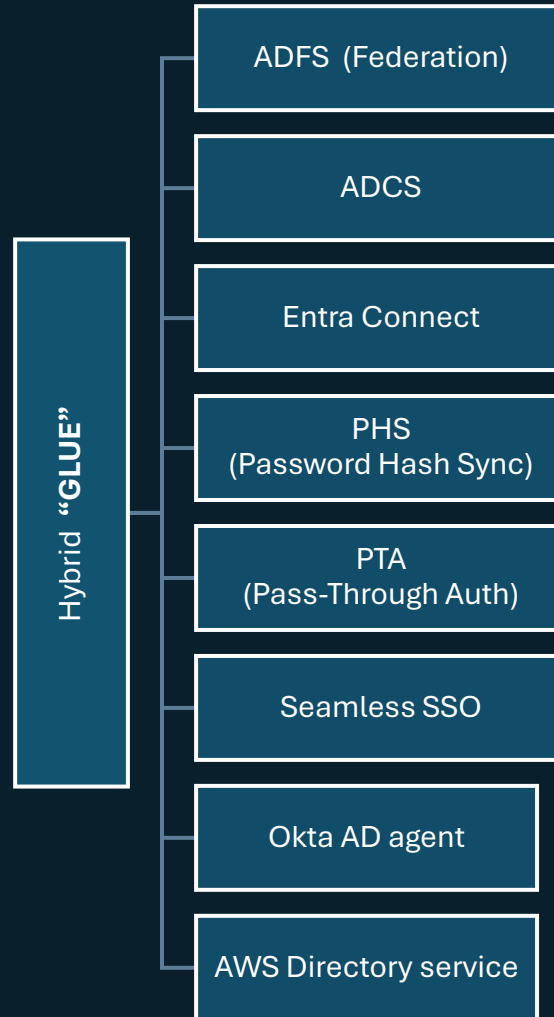
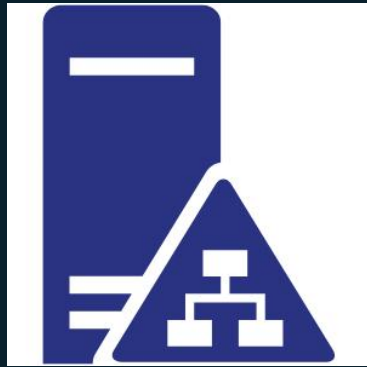
On-Prem

Cloud

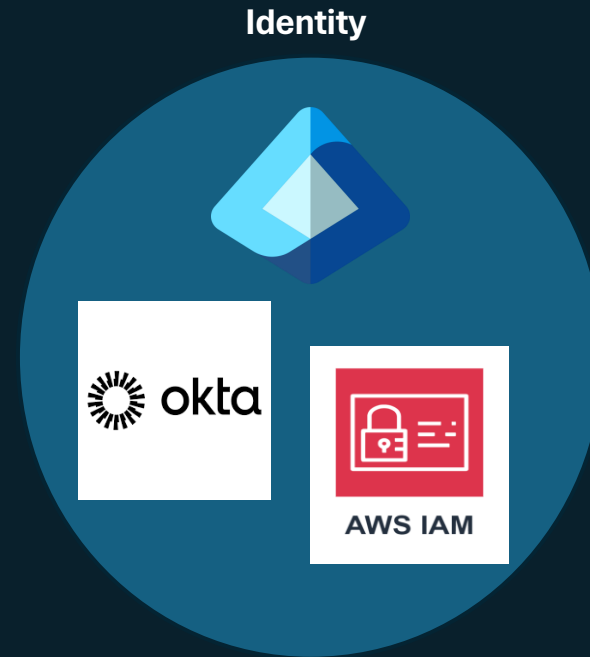


On-Prem

Cloud

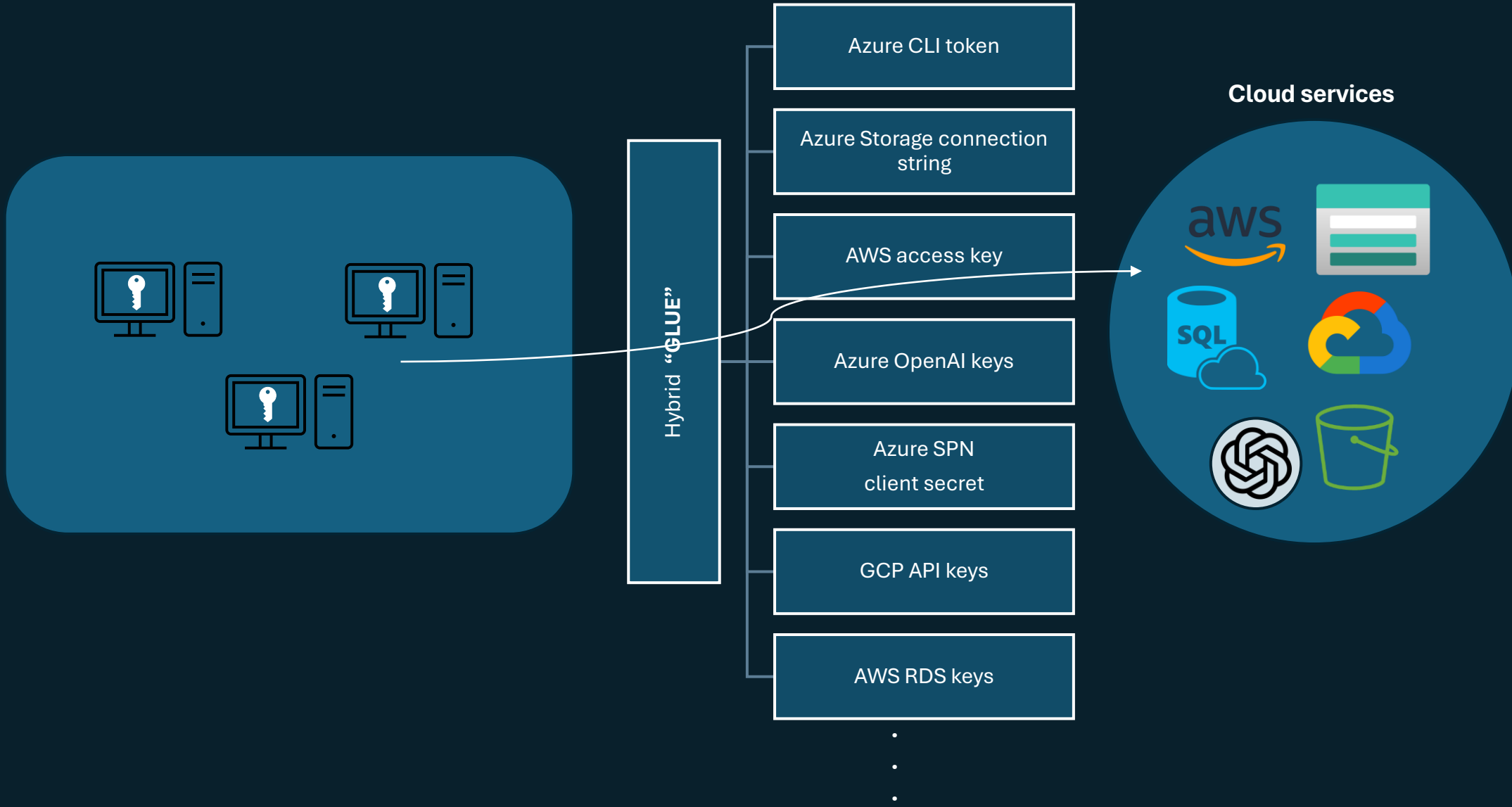


⋮



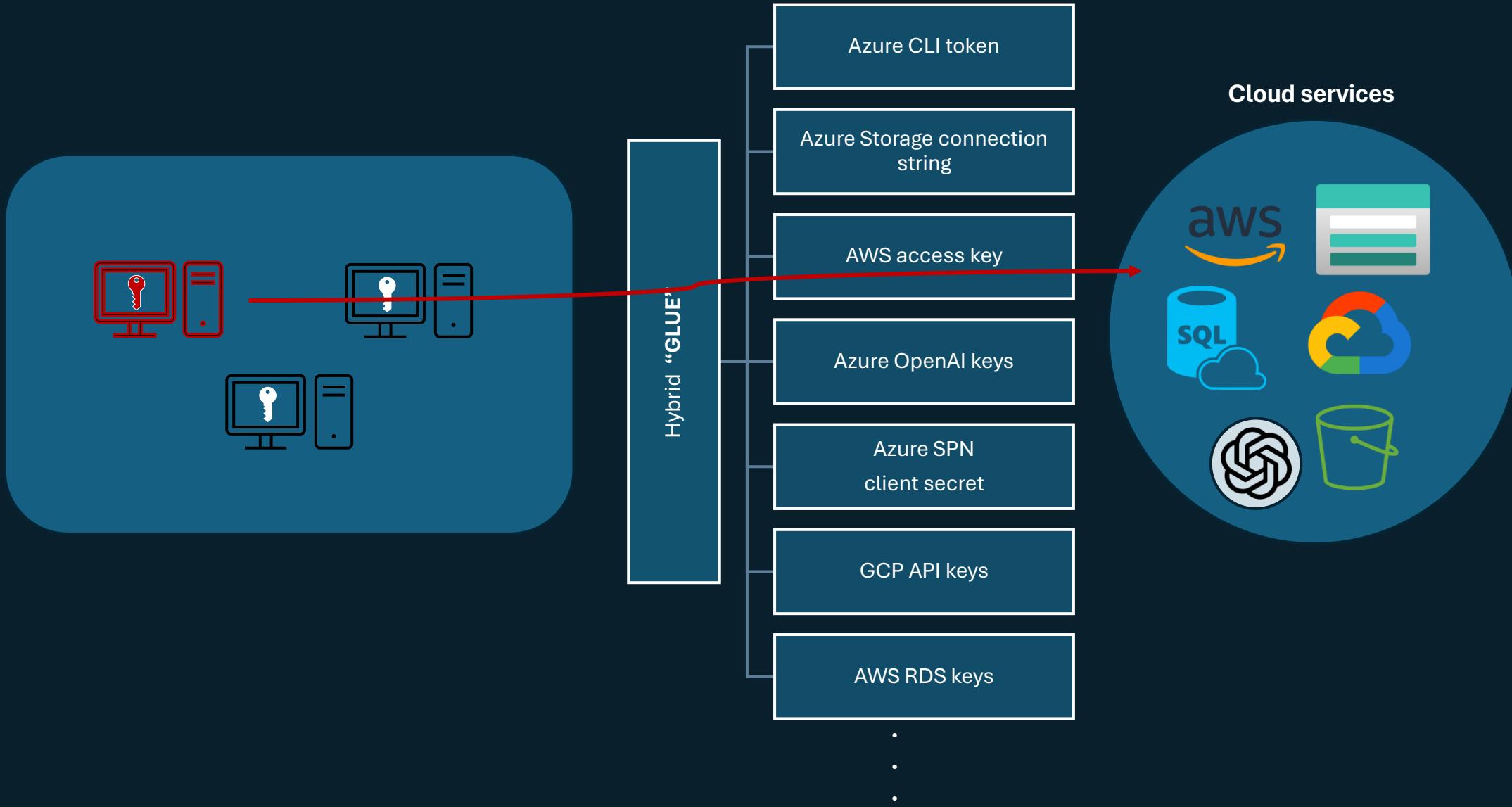
Not only identities sync

Secrets are also a “glue”



Not only identities sync

Secrets are also a “glue”



Threat Landscape Evolution



Past (On-Prem)

- Target individual systems via single domain
- Compromise Users in AD
- Modify OS config, disable security settings
- Deploy untrusted binaries
- Move laterally from machine to machine with predictable path and protocols
- Need backdoors and C2 for Persistence



Present (Hybrid)

- >>> Target **systems on-prem, services, VM, Containers**
- >>> Compromise **Users in AD and in IdP, Sync servers, Tokens, Certs**
- >>> Modify **OS, IdP, Cloud config, can disable wide range of settings**
- >>> Install **binaries, but also VM, cloud apps, extensions, flows**
- >>> Move **laterally and vertically** with **hard to see** attack paths and unexpected protocols
- >>> Can persist **in many ways and without binaries** (e.g. add new user, service principal, cloud extension, register MFA)

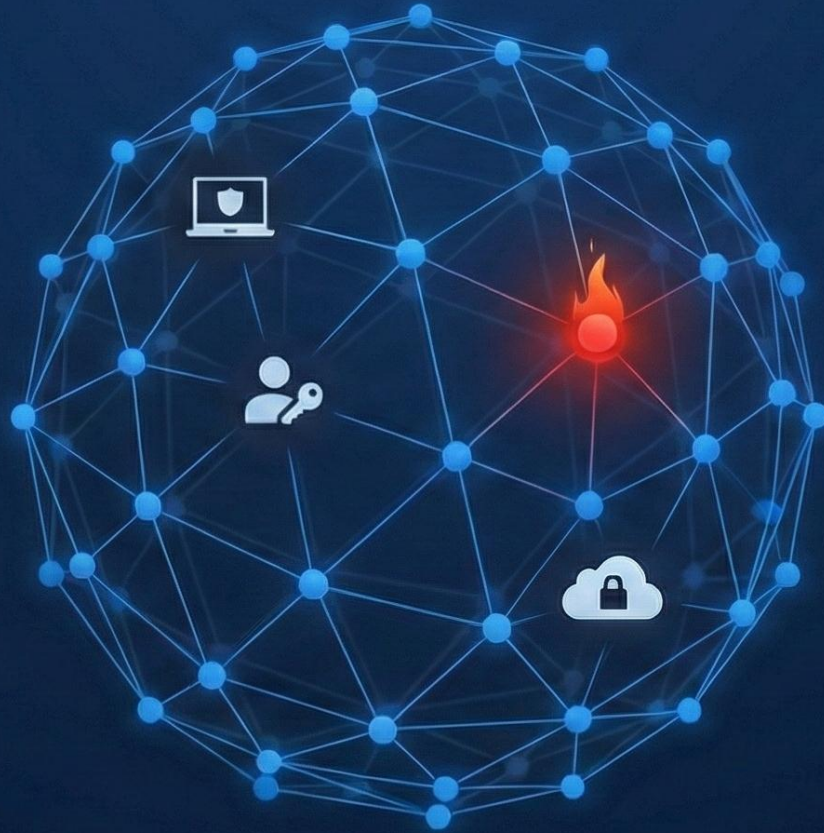


Biggest problem with network defense is that defenders think in lists. Attackers think in graphs.

As long as this is true, attackers win.

John Lambert, 2014

Corporate Vice President, Security Fellow, Microsoft



Graph: See Everything. Correlate Across Domains.

Security Graph - a map of the enterprise

Entity resolution and enrichment

Clean, normalize, aggregate, de-duplicate, contextualize

Vulnerability management

Email security

Identity security

Endpoint security

SaaS security

Application security

Cloud security

External attack surface

Asset metadata

Activity logs

Admin actions

Configuration data

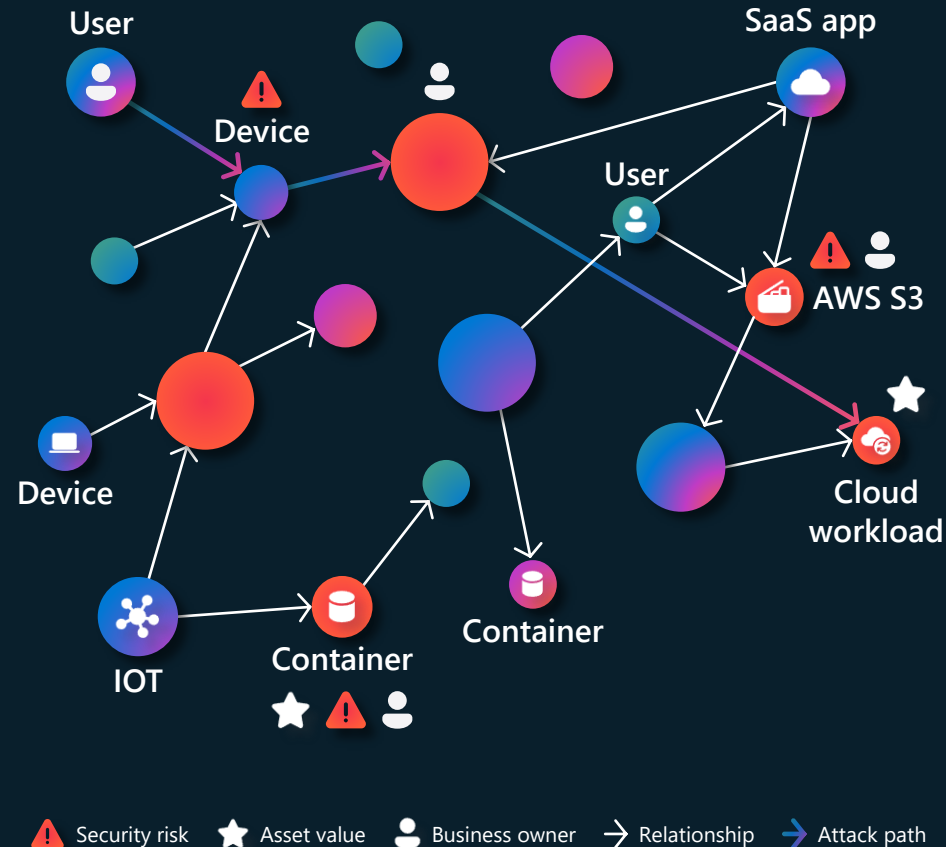
Policy state

Security findings

Health state

Input

Output



Attack surface discovery

Continuously discover, inventory and contextualize the organization's asset attack surface

Attack path analysis

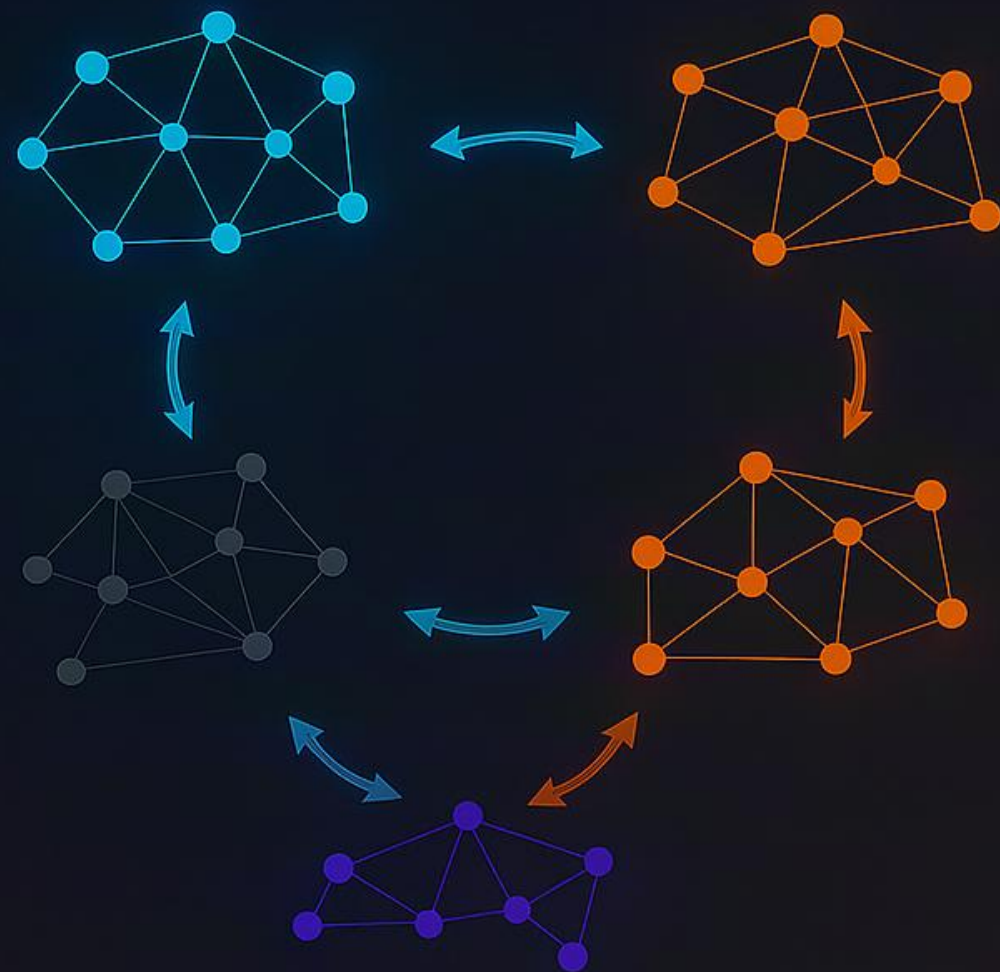
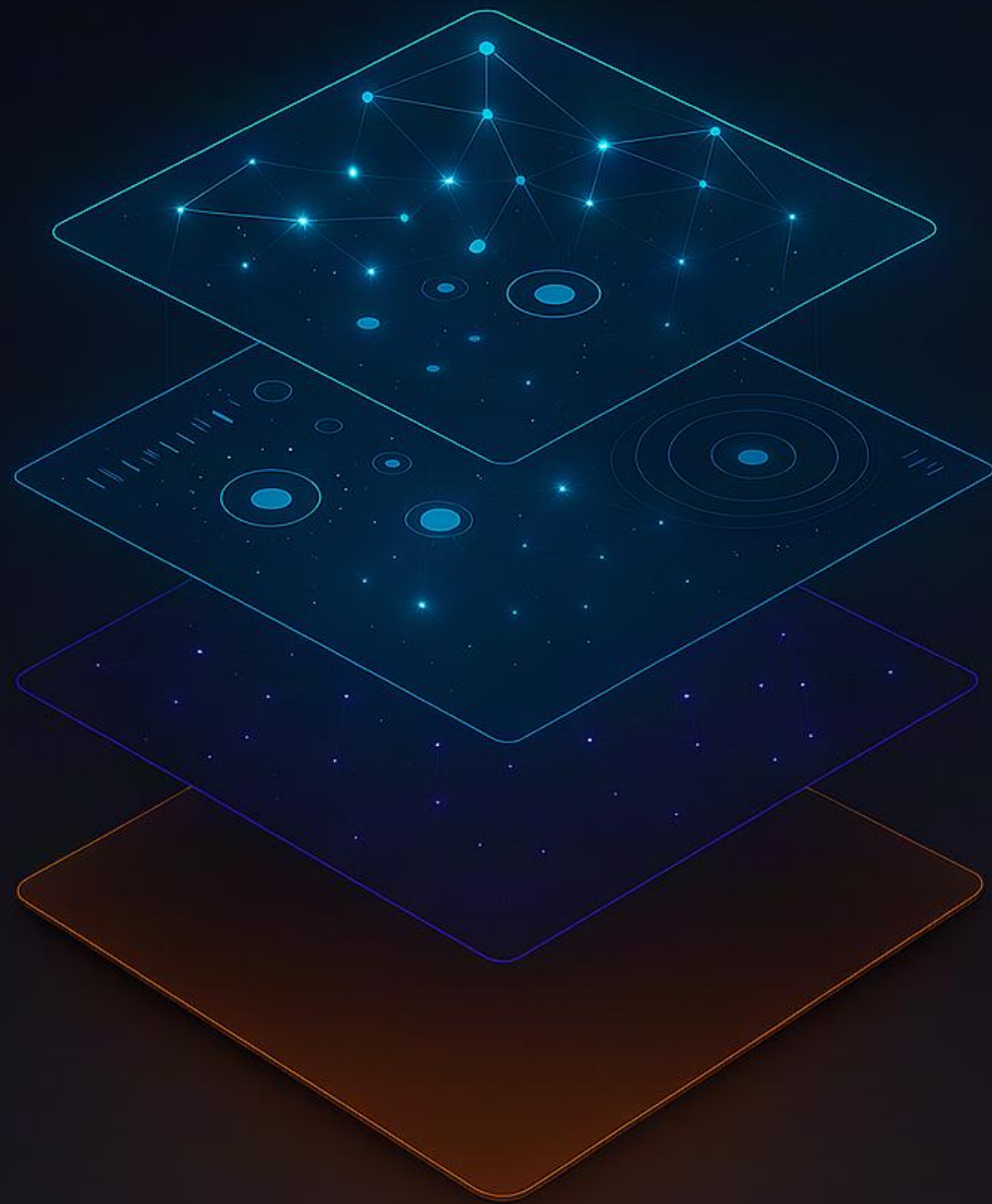
Prioritize weaknesses by considering the attacker's perspective, moving away from the traditional siloed approach

Critical assets identification

Identify the assets in your org you should care more about

Understand blast radius

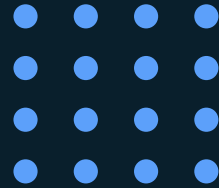
Understand potential downstream impact of attack as they happen and take appropriate measures



Attack Paths

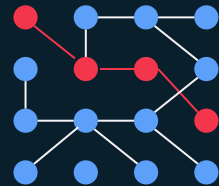
Collect, dedupe and normalize asset data

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



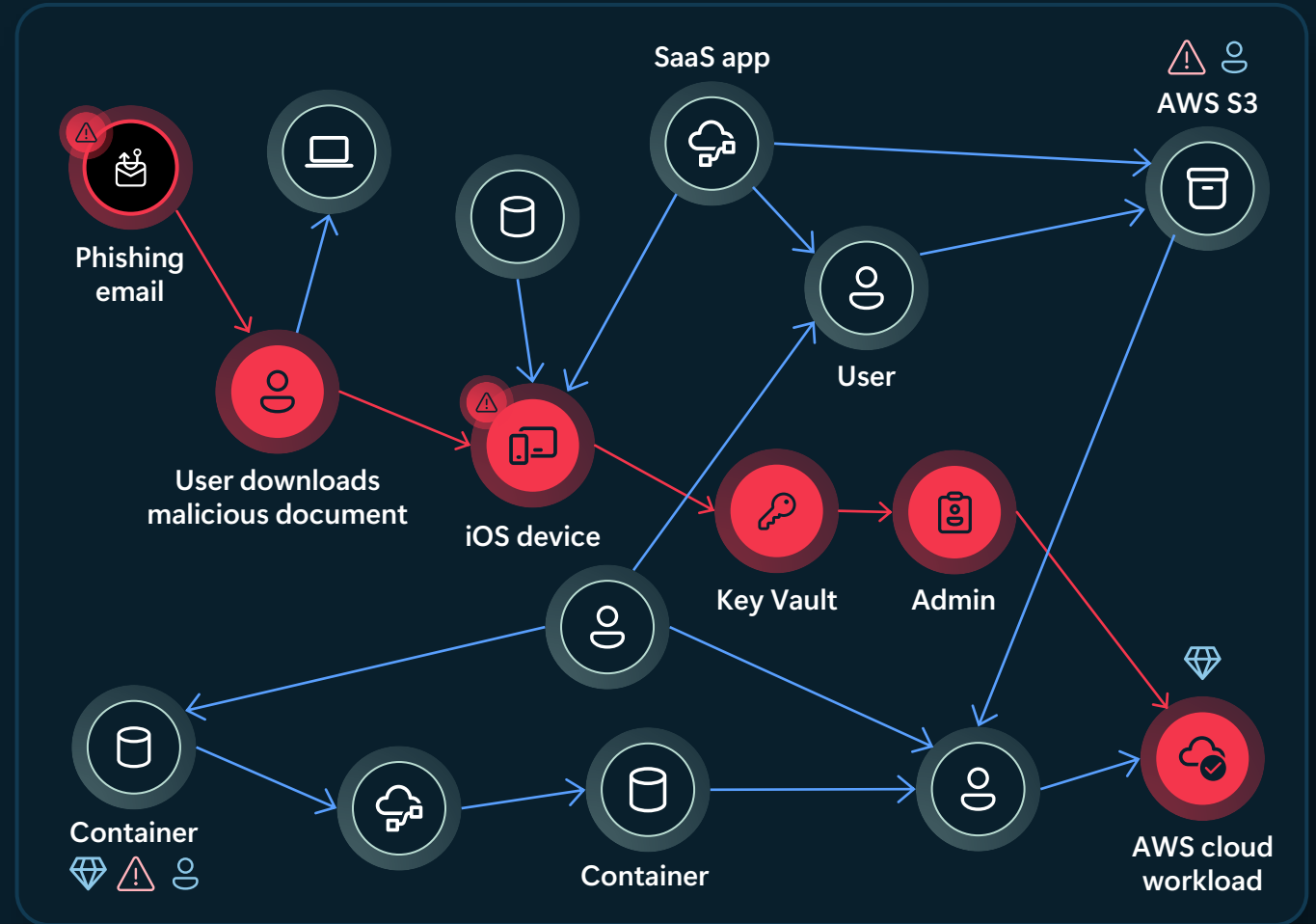
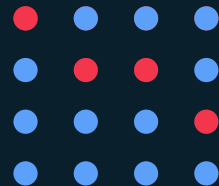
Map out assets and relationships

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



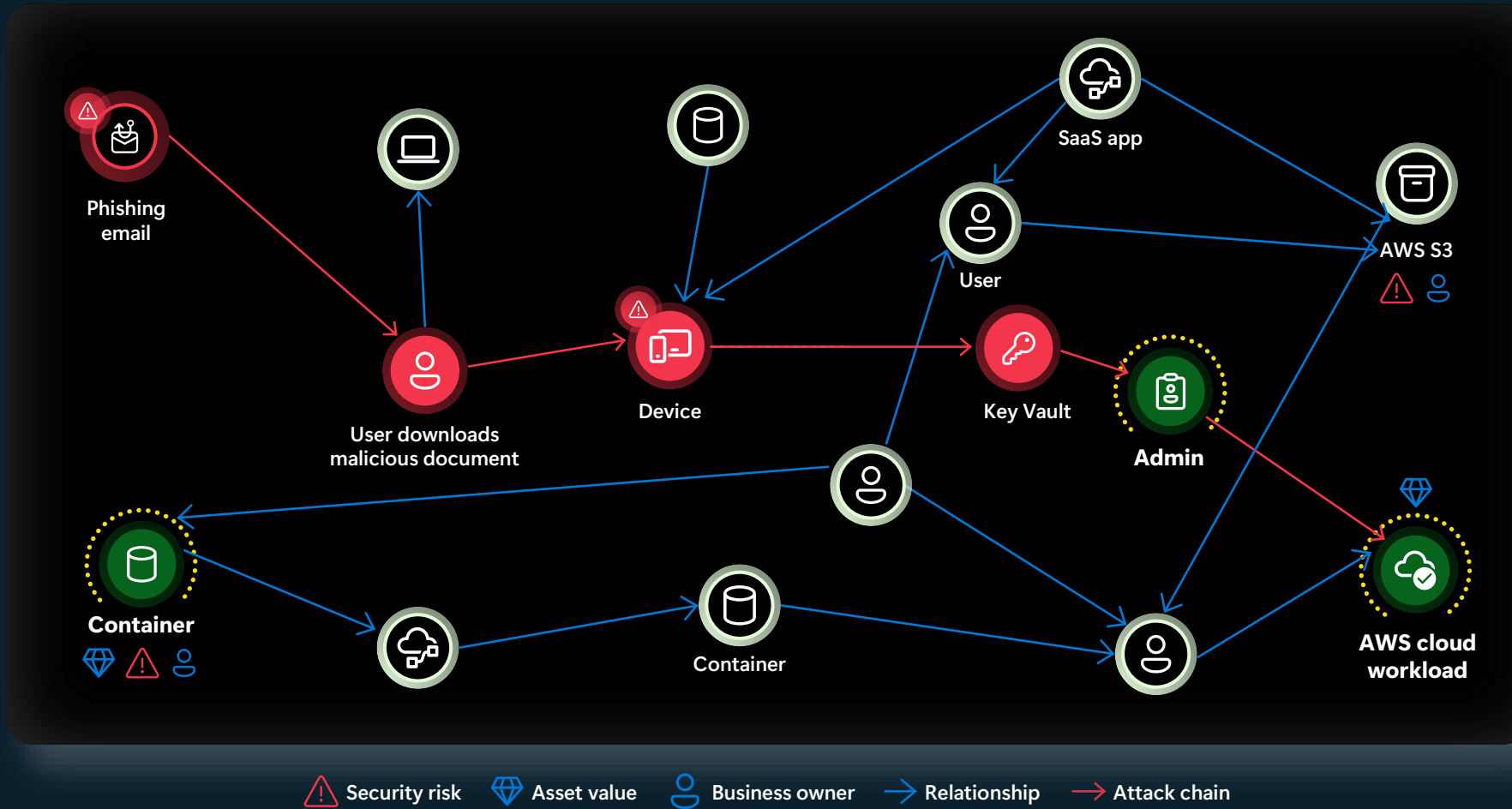
Inform prioritization

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



⚠ Security risk 💎 Asset value 👤 Business owner ➡ Relationship ➡ Attack chain

Critical Assets, the graph that matters most



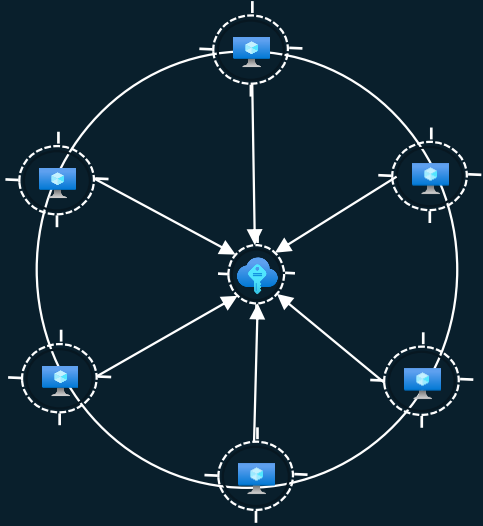
80%
of organizations have at least one open attack path to a critical asset

61%
of attack paths lead to sensitive user accounts

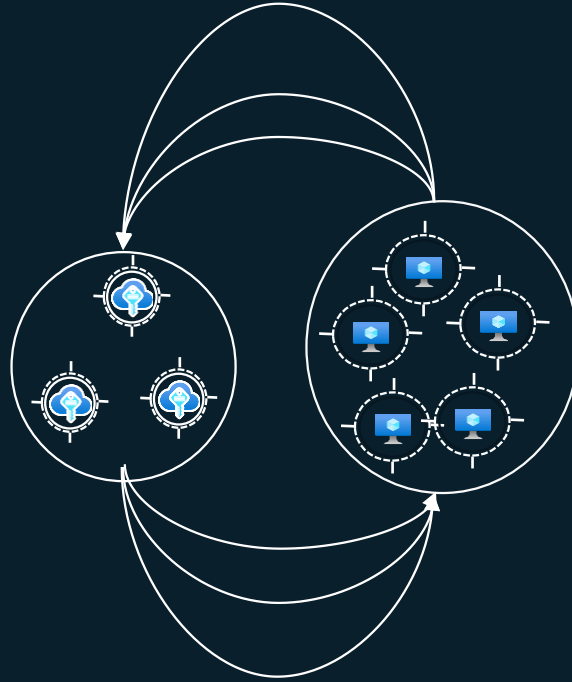
1%
of total assets in an organization are critical or sensitive

Common Graph Patterns in Attack Paths

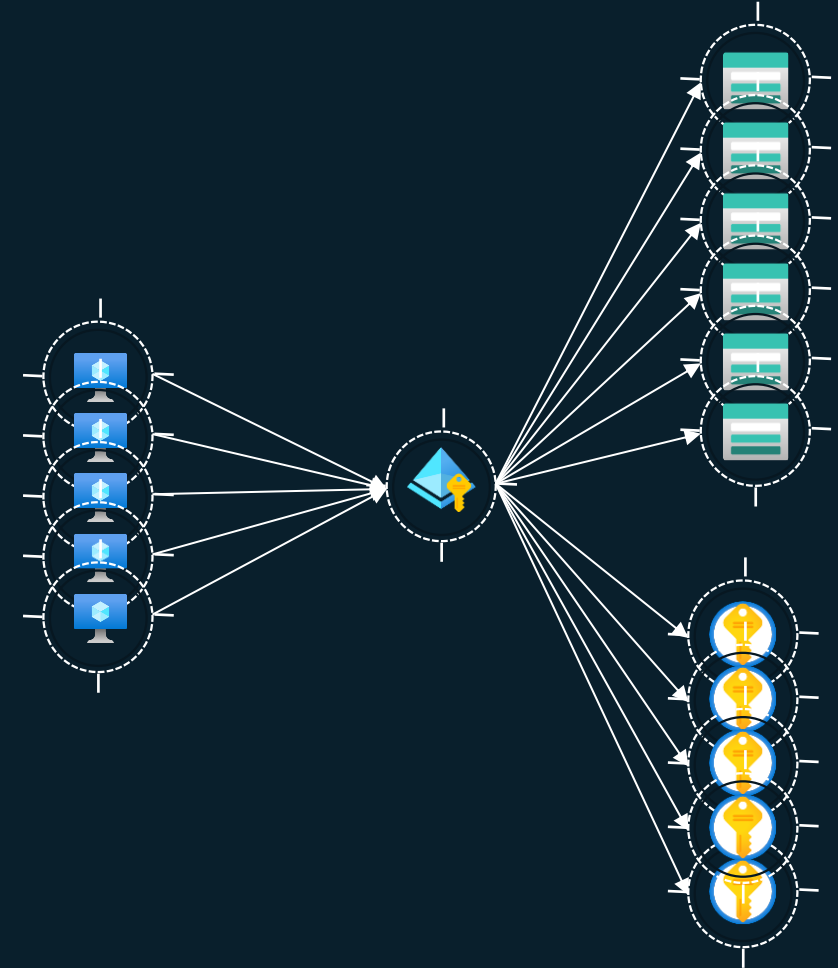
Star



Vortex



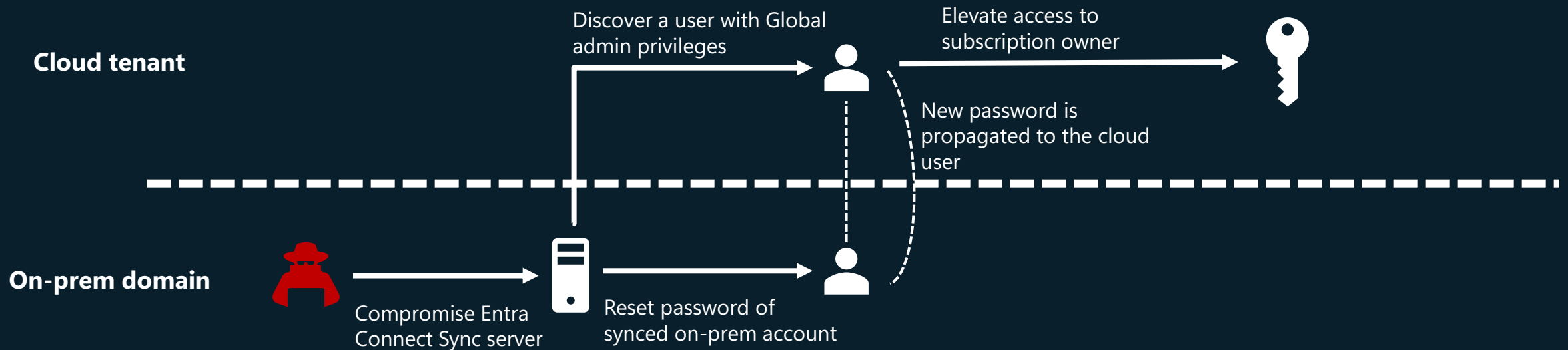
Choke point



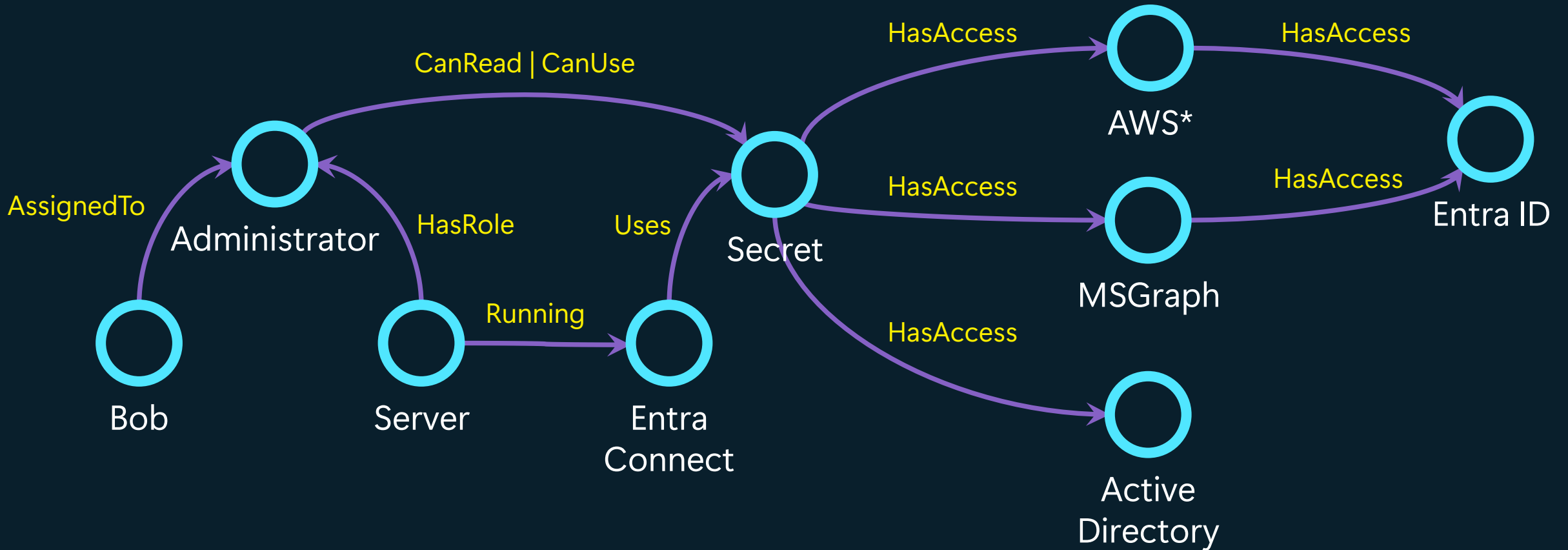
Real-life attack

On-prem to cloud pivoting

Threat actor abused Entra Connect Sync servers to move from on-prem domain to cloud tenant.

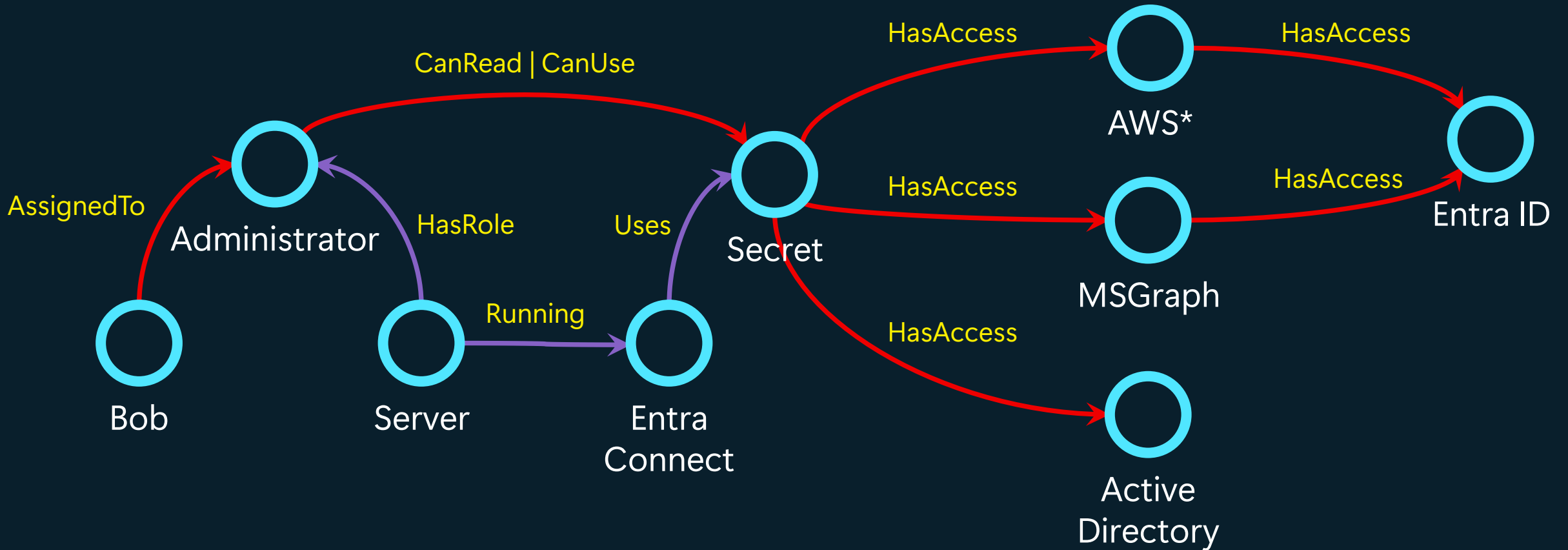


Entra Connect Sync attack graph

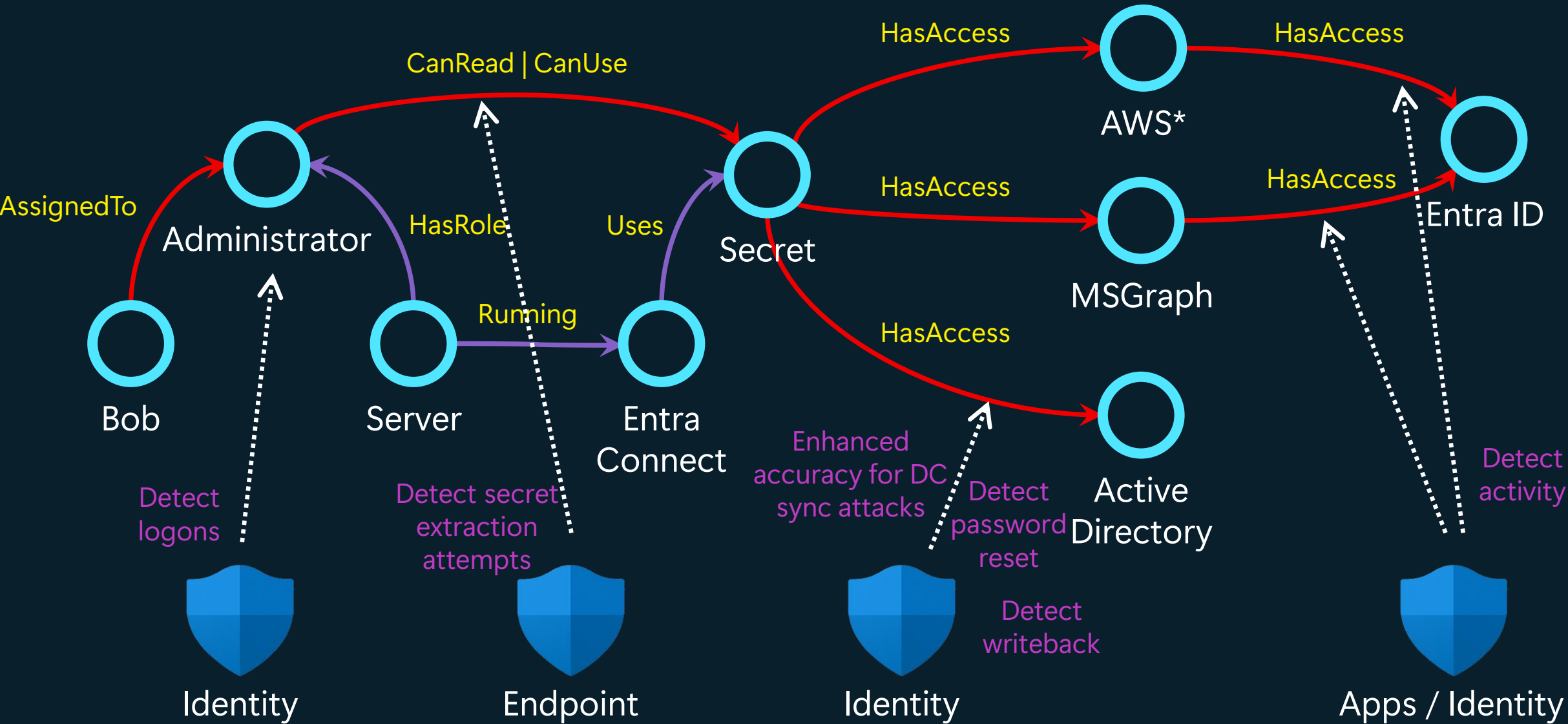


* Admin Web Service

Entra Connect Sync attack graph



Entra Connect Sync attack graph



Disrupting the most prominent attacks seen today

Scenarios



Human-operated
ransomware



Hands-on-
keyboard



Fraud and abuse
(BEC)



Initial access
(AiTM, OAuth)



Hybrid attacks



Disruption actions

- Contain device
- Contain user
- Contain IP

- Disable user on-prem & in the cloud
- Confirm user as compromised
- Revoke user session

- Disable OAuth app
- Harden GPO propagation
- Harden Safe boot



Hybrid
identities



Endpoints
and IoT



Email and
collaboration



SaaS
apps



Data

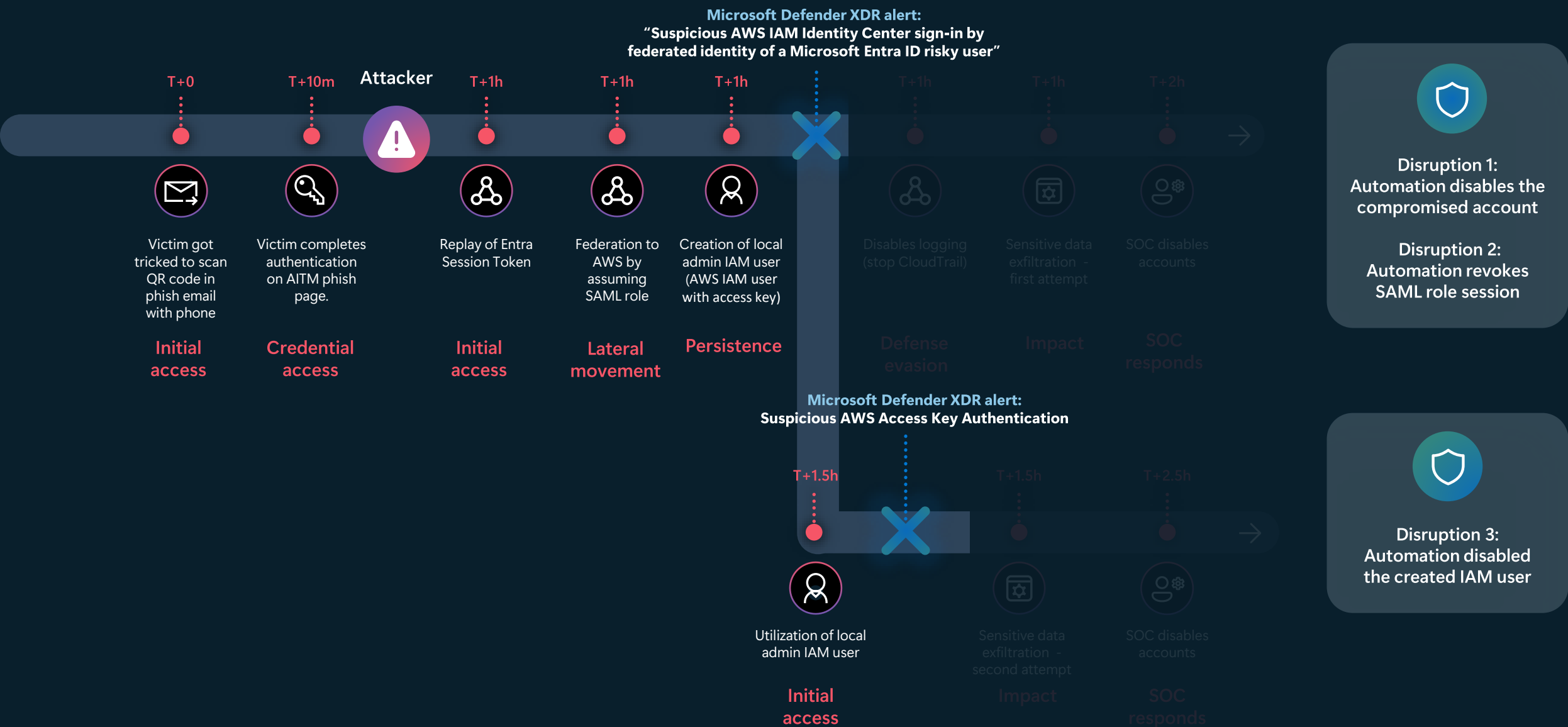


Cloud
workloads

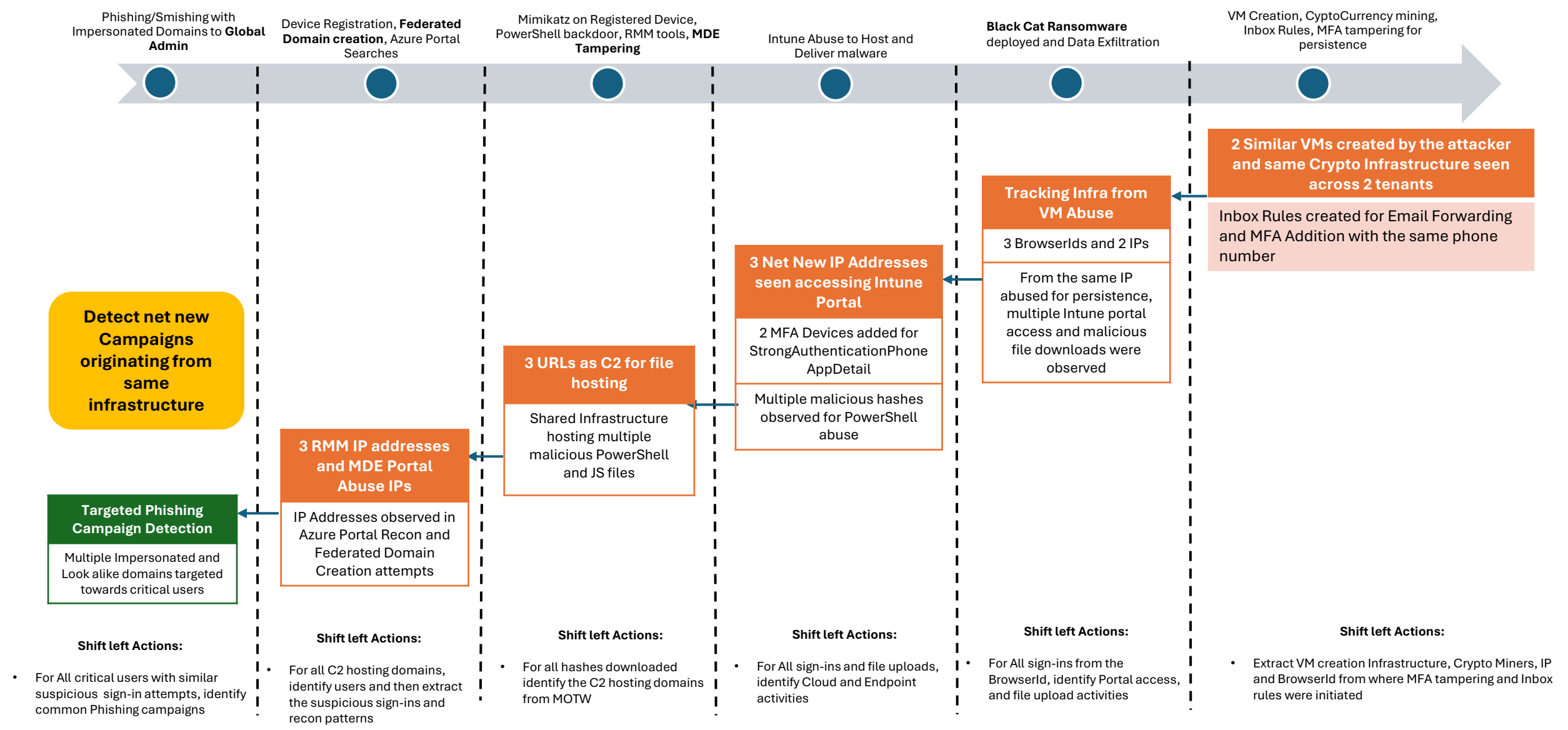


Non-Microsoft

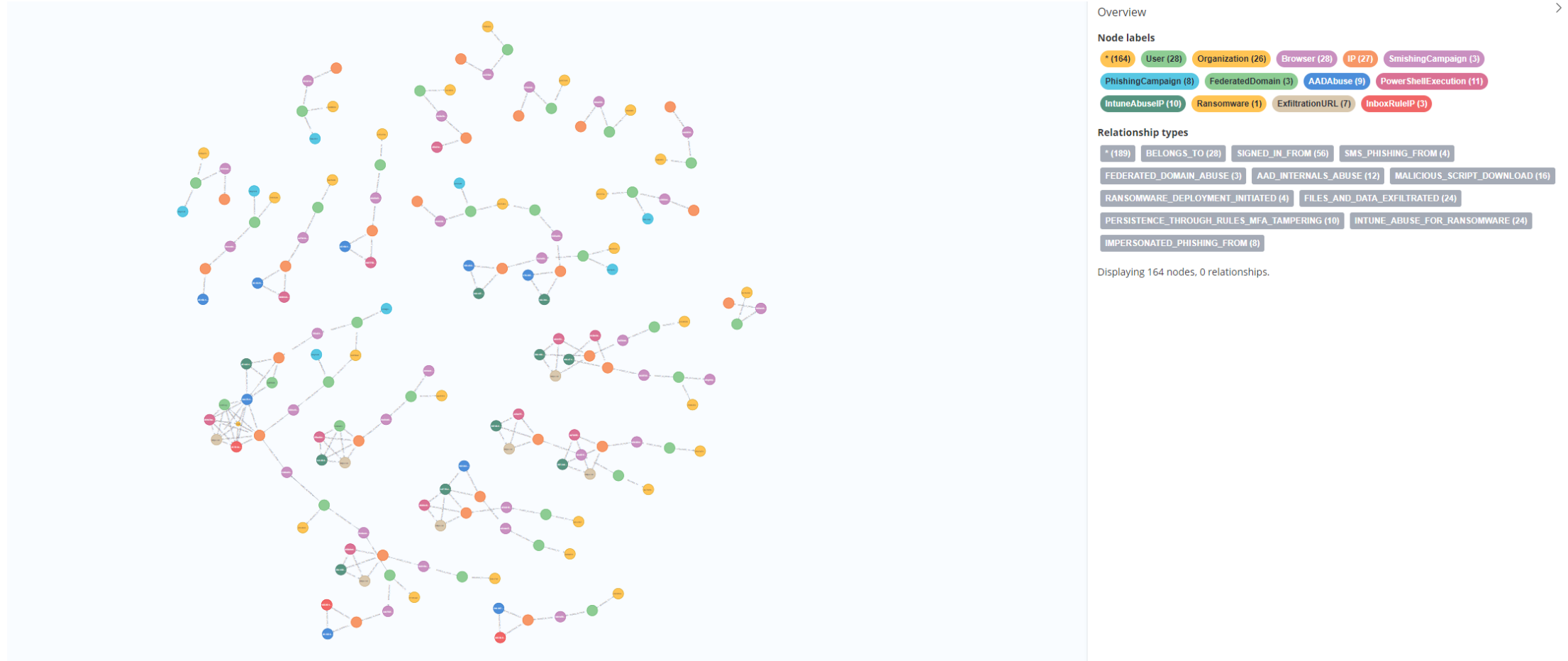
Extending Attack Disruption to AWS



Hybrid Ransomware Attacks – Shift Left

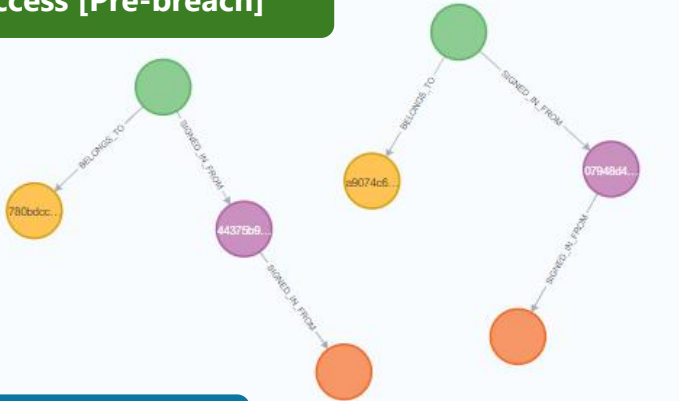


Shift Left - Hybrid Ransomware Attack

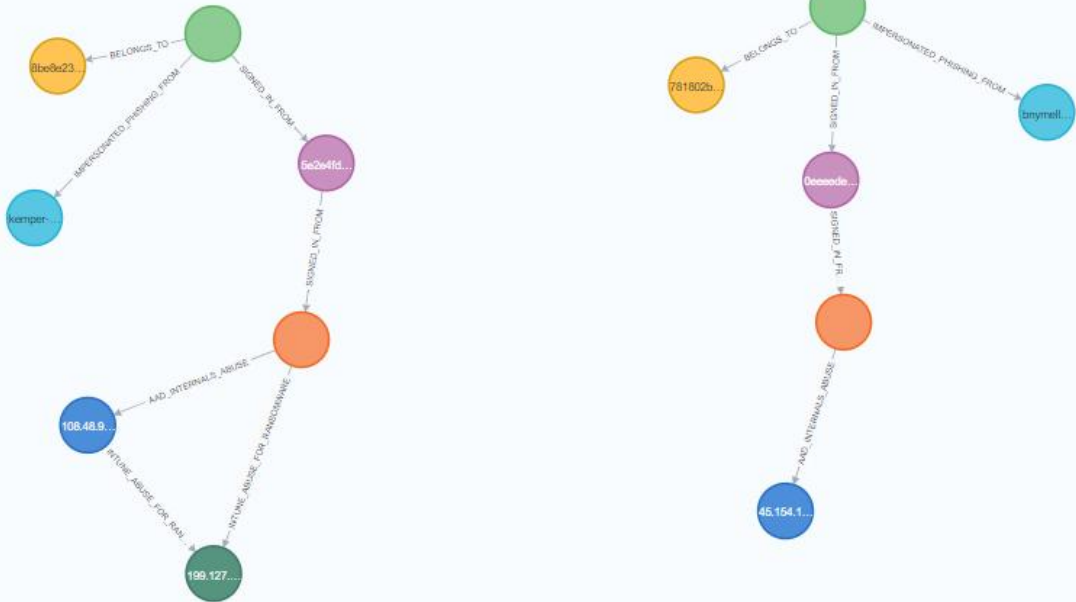


The graph reveals stages of progression & provides opportunities for shifting left

Attack at Initial Access [Pre-breach]



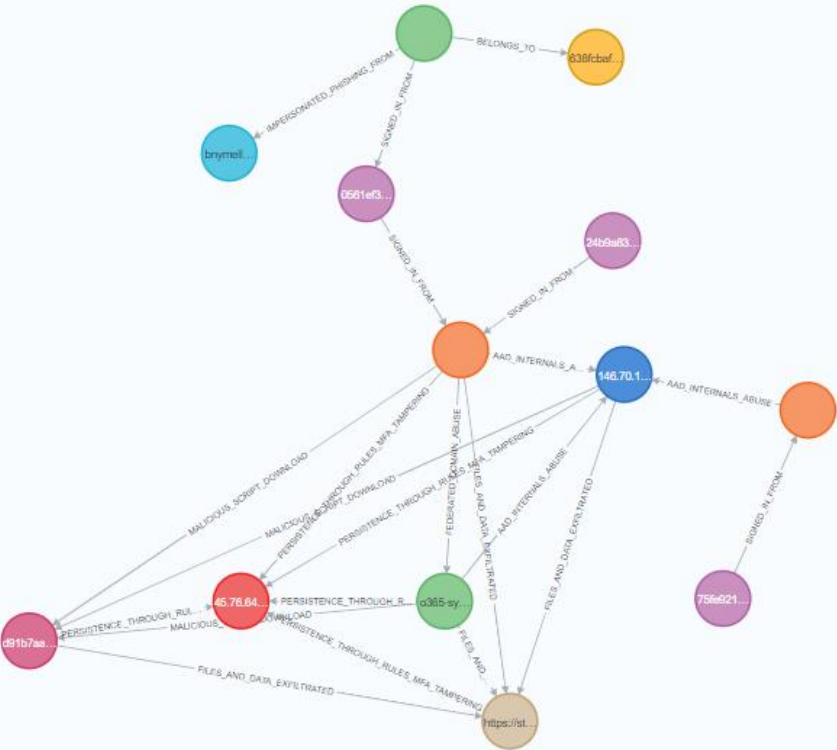
Attack at Execution / Preparation



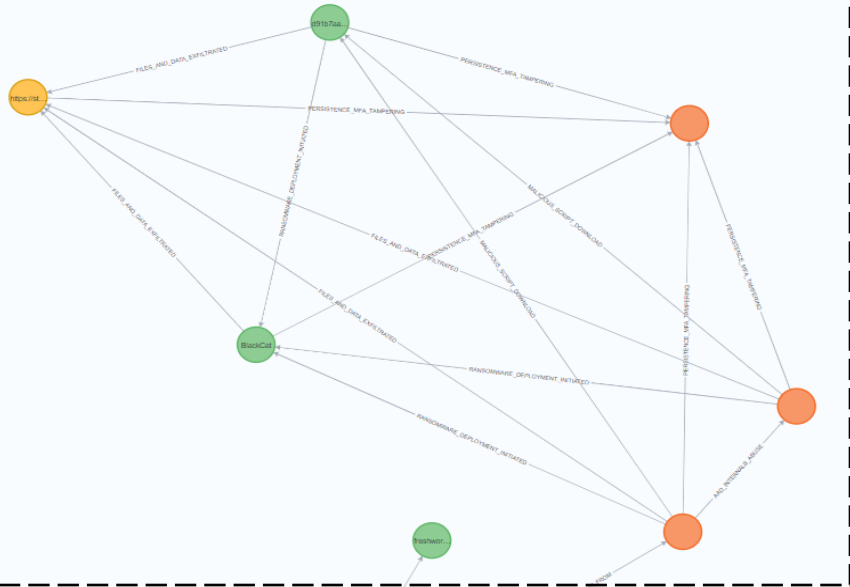
Node labels

- * (124)
- User (20)
- Browser (22)
- SmishingCampaign (3)
- PhishingCampaign (6)
- AADAbuse (7)
- PowerShellExecution (9)
- IntuneAbuseIP (7)
- ExfiltrationURL (6)
- InboxRuleIP (3)
- Organization (21)
- IP (19)
- FederatedDomain (1)

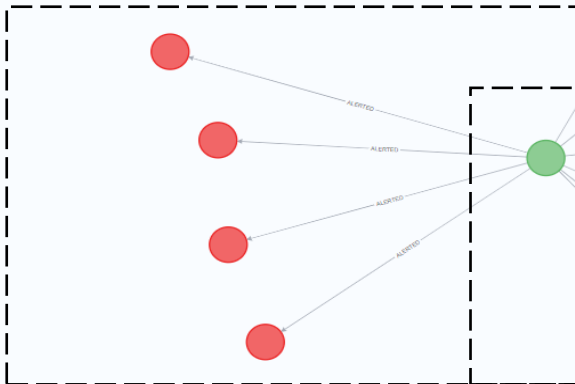
Attack at Encryption / Impact Phase



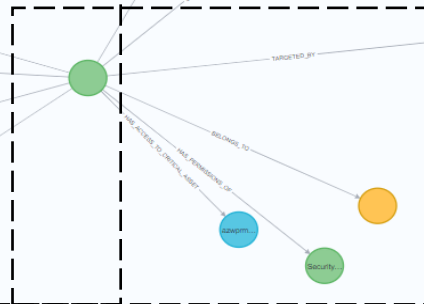
Hybrid Ransomware Attack



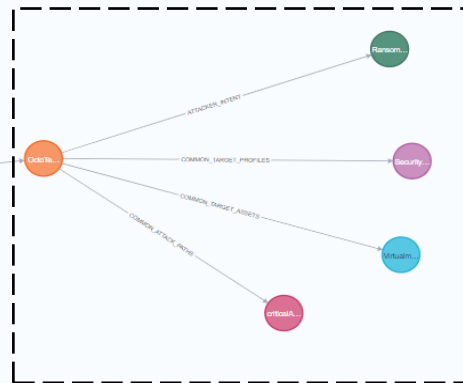
INCIDENT GRAPH



EXPOSURE GRAPH



KNOWLEDGE GRAPH



INDICATOR GRAPH

Relationship, Context and Confidence for Attacker Infra

Nodes: Sign In IP Address, Persistence IP, Sign-in BrowserId, Intune Abuse IP, Smishing Campaigns

Edges: Relationship between the indicators defining the attacker Infrastructure

INCIDENT GRAPH

Compromised users, Relationship with indicators, context and attribution

Nodes: Impacted Entities, Alerts, Incidents, Evidences of the Attack

Edges: Historical alerts on the entities, targets in the environment, customers resolution and scope of the attack

EXPOSURE GRAPH

Posture Profile, Context, Asset Risk score for Compromised User graph nodes

Nodes: All assets in the Organizations (Devices, Users and Apps)

Edges: Walkable Paths for attacker in the Organization

KNOWLEDGE GRAPH

Graph of Targeted users with their attack paths, profiles and attribution

Nodes: Actor and Targeted Entity Profiles

Edges: Profiles of the users targeted, attack paths exploited by the attacker and attacker intent

The journey towards autonomous defense



Level of
autonomy

Zero Assistive Partial High Full >

I'll do it

Assistive

Autonomous

Do it with me

Do it for me

Thank you!

