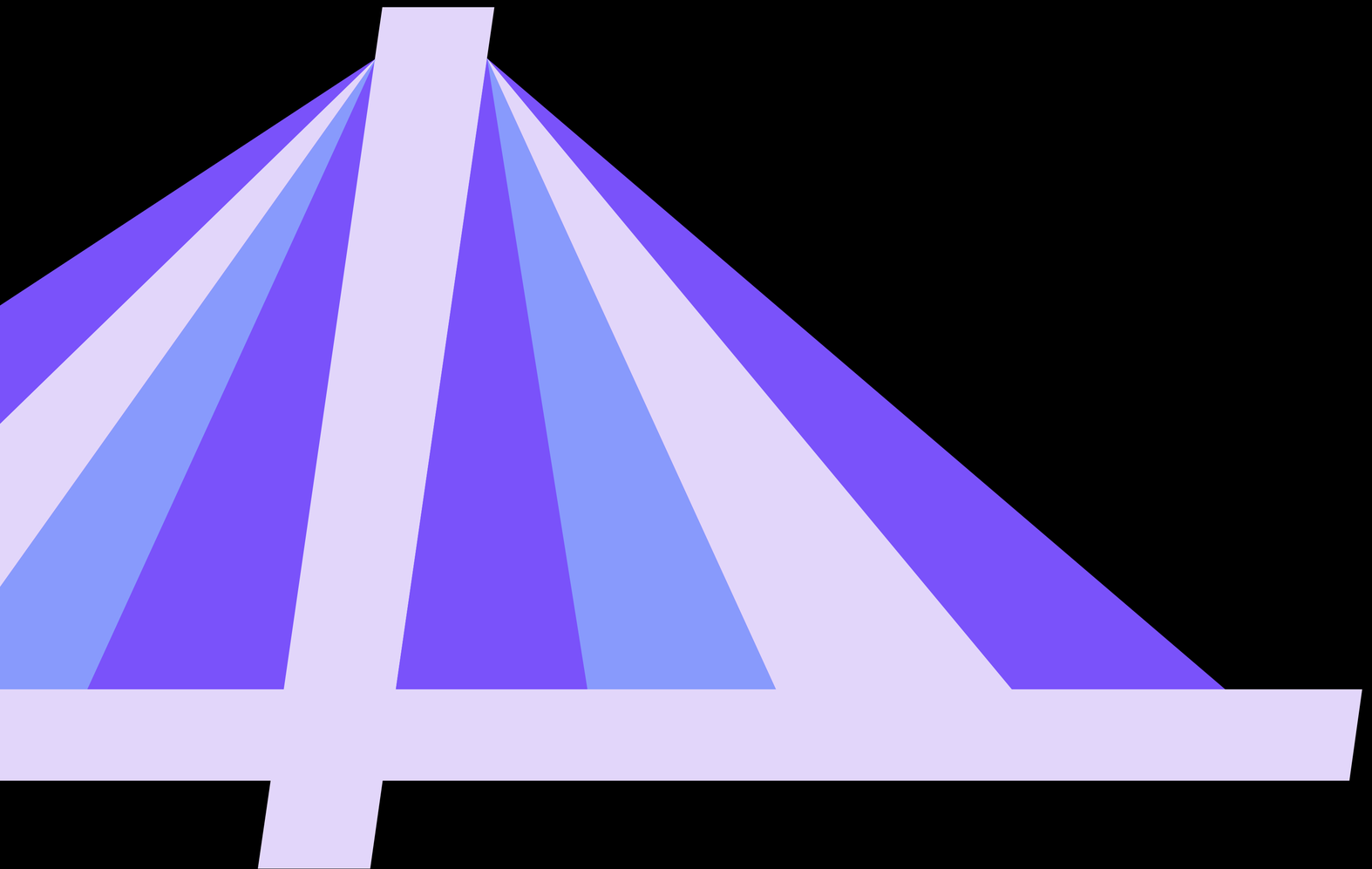
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



Exposing Hidden Attack Paths: How Threats Get Past Your Best Defenses

Justin Kohler
Chief Product Officer

A Quick Shoutout to Dirk-Jan Mollema

Pinned

Dirk-jan
@_dirkjan

Follow

I've been researching the Microsoft cloud for almost 7 years now. A few months ago that research resulted in the most impactful vulnerability I will probably ever find: a token validation flaw allowing me to get Global Admin in any Entra ID tenant. Blog:

dirkjanm.io
One Token to rule them all - obtaining Global Ad...
While preparing for my Black Hat and DEF CON talks in July of this year, I found the most ...

6:20 AM · Sep 17, 2025 · **424.3K** Views

142 988 3K 1.4K

https://dirkjanm.io/obtaining-global-admin-in-every-entra-id-tenant-with-actor-tokens/

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

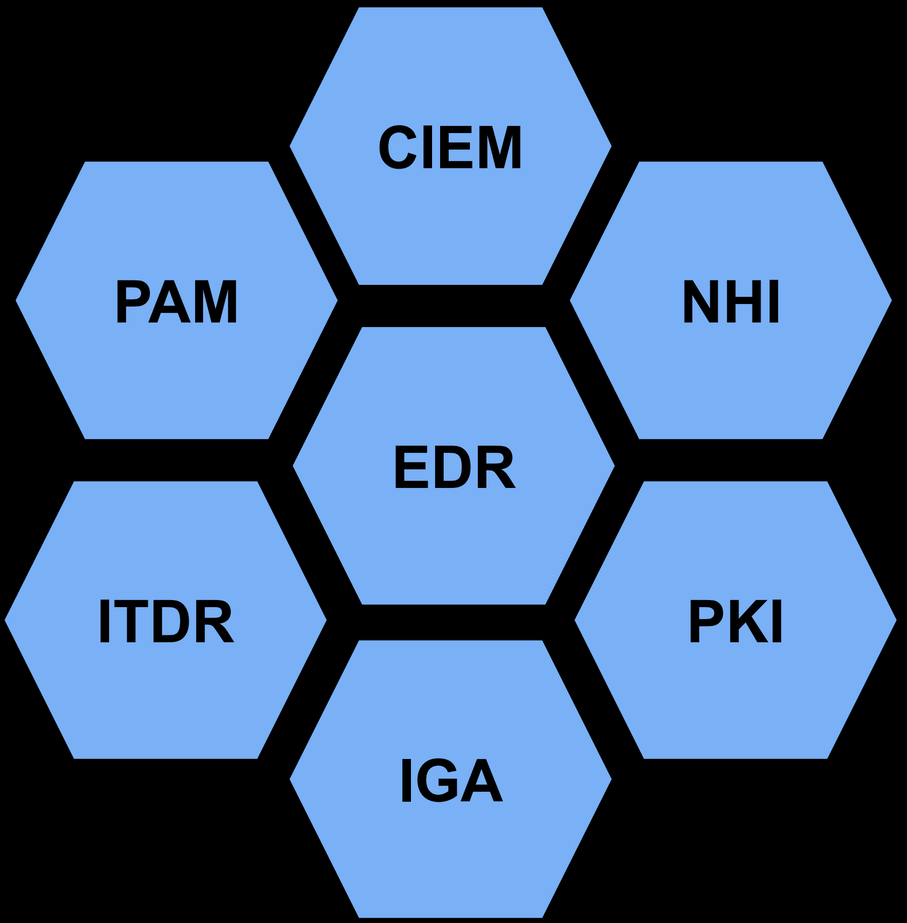
Justin Kohler

Chief Product Officer @ SPECTEROPS

- Leads development for BloodHound Community Edition and BloodHound Enterprise
- Former Network Forensics, Detection and Response
- Air Force SIGINT Veteran
- Various speaking engagements, podcasts, etc

“We Did Everything Right…”

- Built a security-aware culture
- Aligned to NIST, MITRE, Zero Trust
- Implemented best-in-class tools



“….So Why Are We Still Getting Breached?”

275%

increase in human-operated **ransomware**

71%

of detections were **malware-free**,

80%

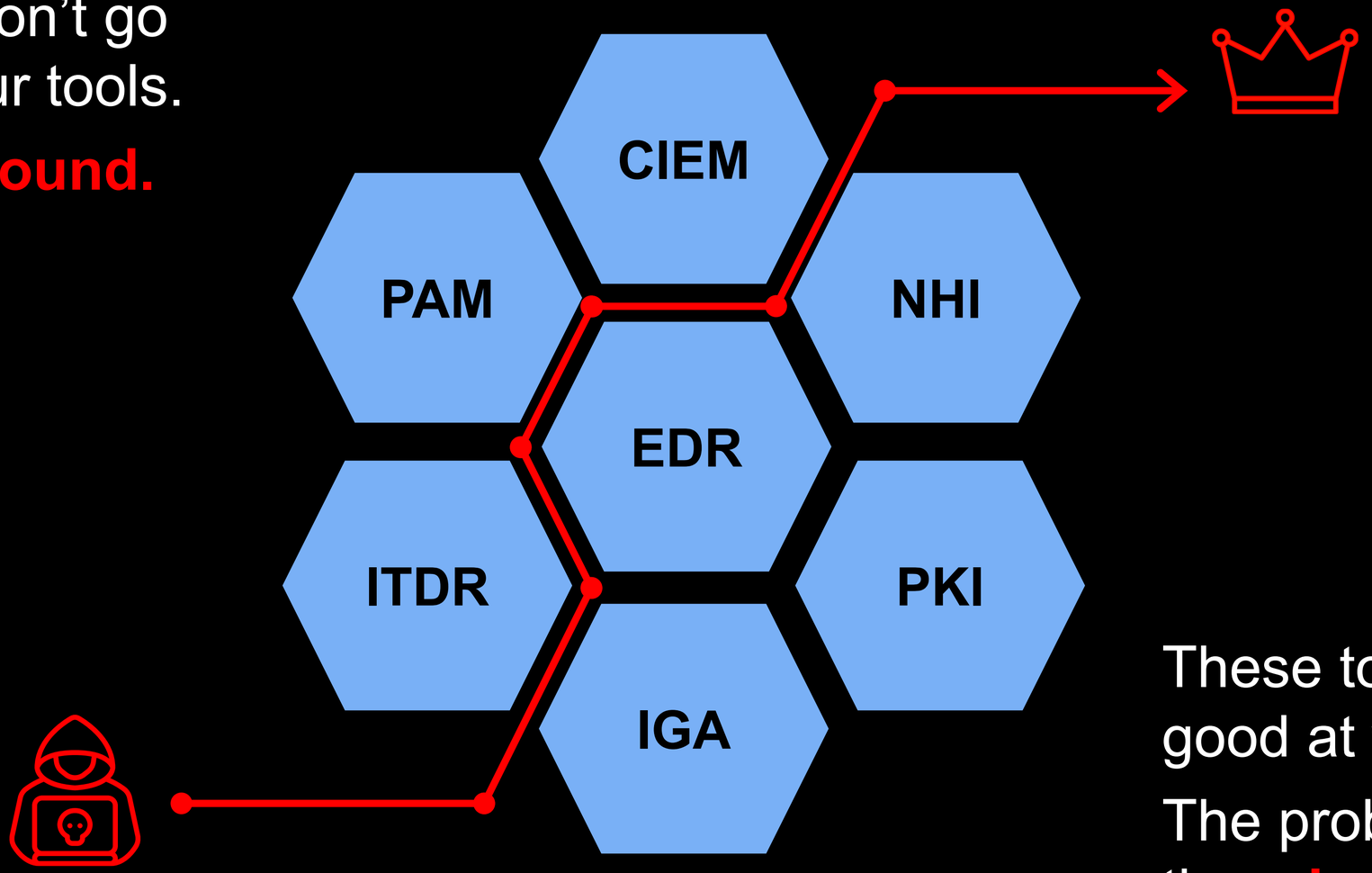
of organizations have attack paths that expose **critical assets**

Even with modern tooling, attackers are succeeding.

Sources: Microsoft Digital Defense Report 2024 and CrowdStrike 2025 Global Threat Report

Attackers don’t go through your tools.

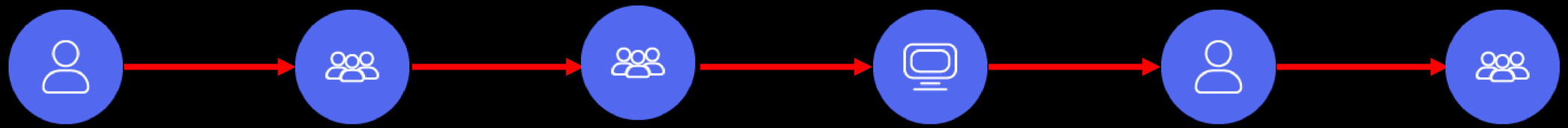
They go around.



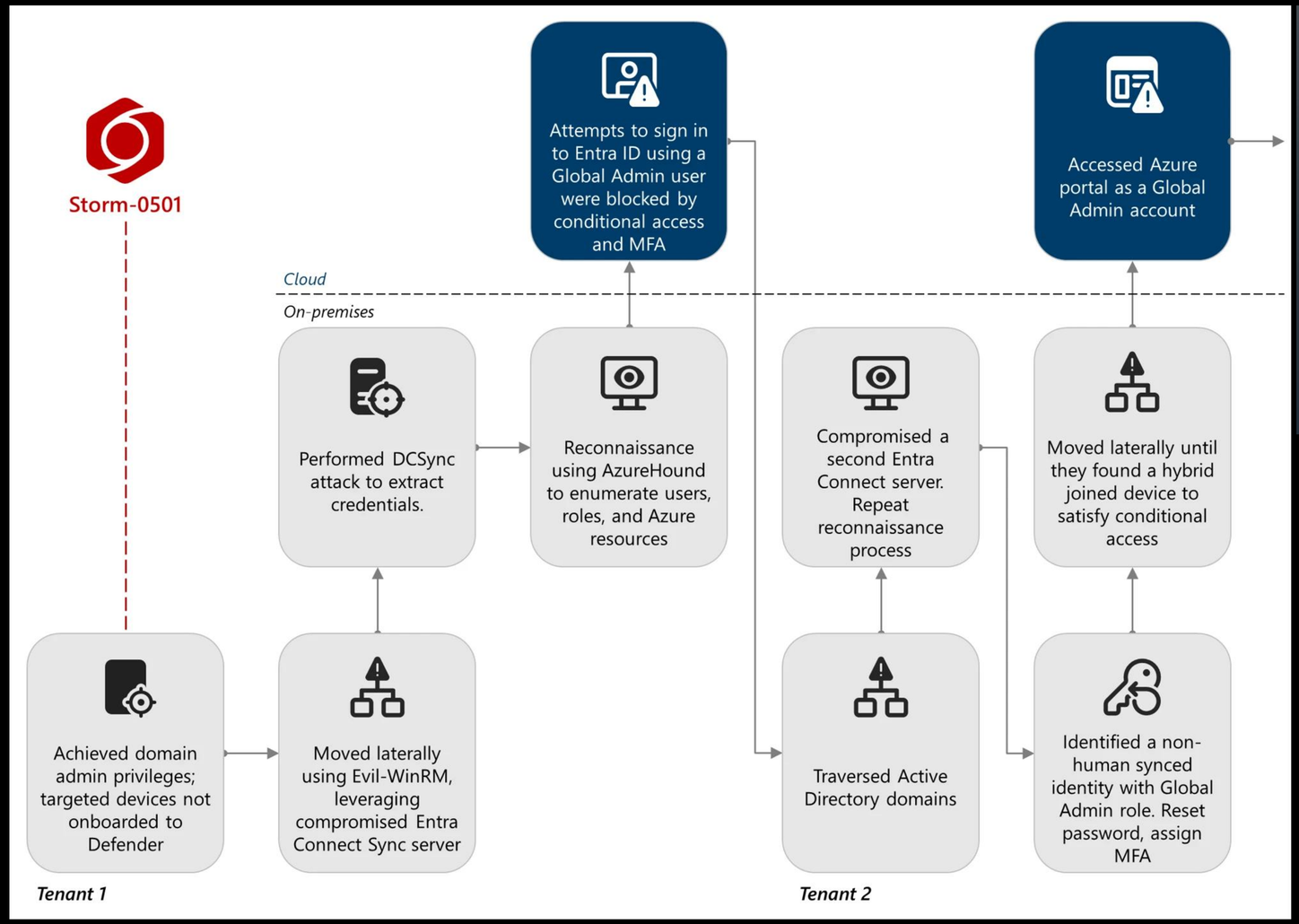
These tools are good at what they do.

The problem is what they **don’t do**.

Attack Paths are chains of abusable privileges and user behaviors that create connections between identities and resources.



Attack Paths pivot through hybrid environments

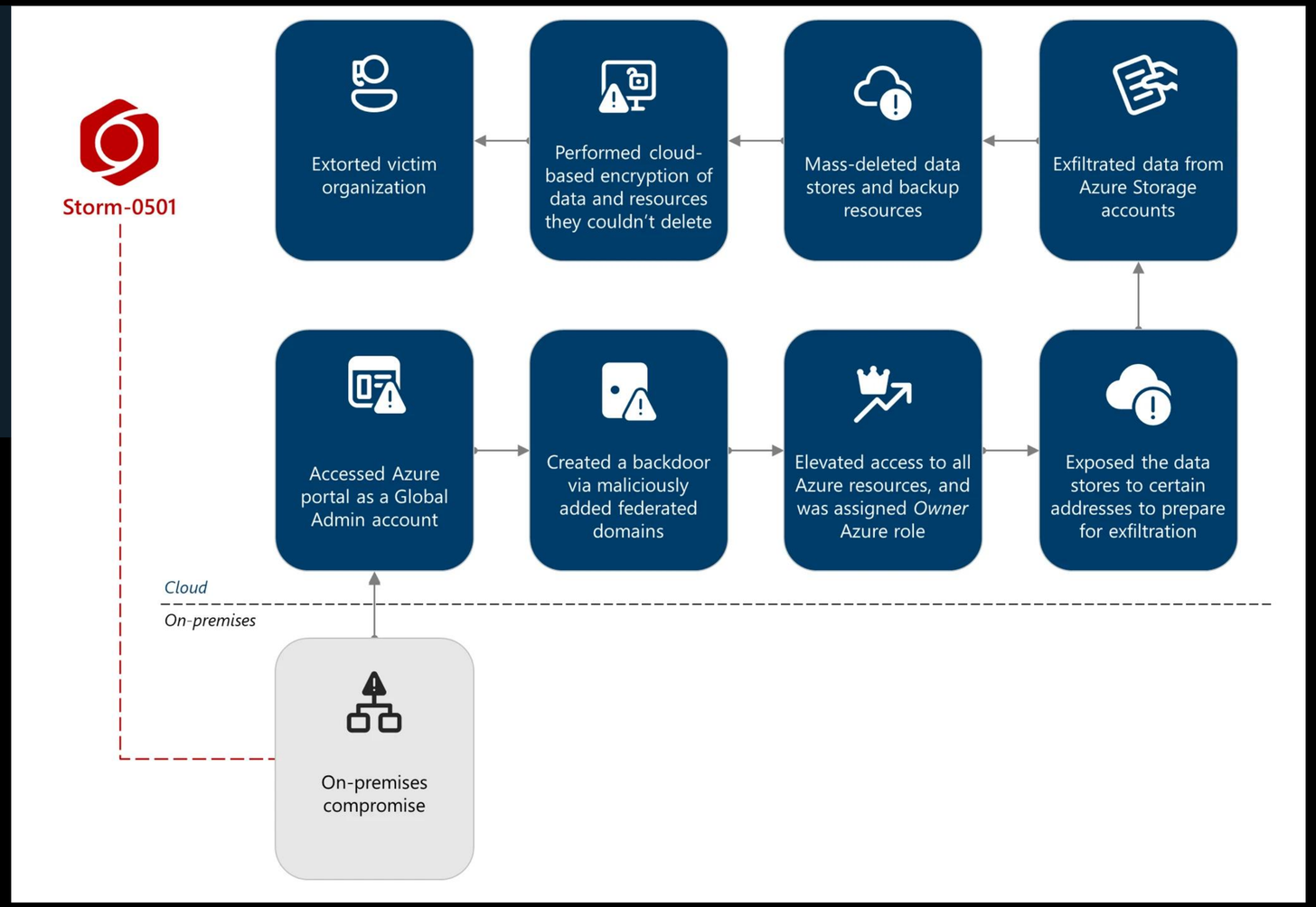


Source: Storm-0501's evolving techniques lead to cloud-based ransomware

Attack Paths pivot through hybrid environments

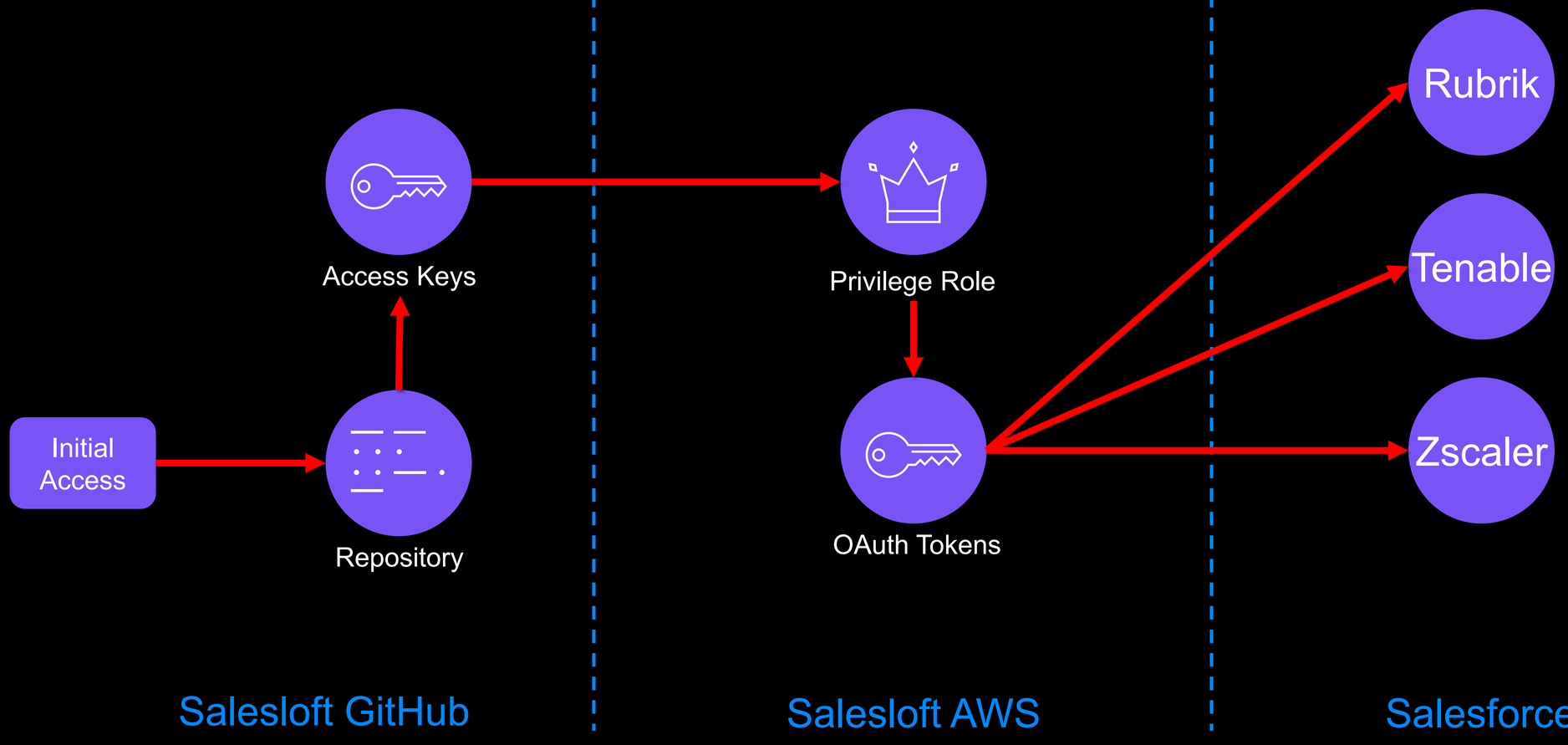
Storm-0501's evolving techniques lead to cloud-based ransomware

By Microsoft Threat Intelligence



Source: Storm-0501's evolving techniques lead to cloud-based ransomware

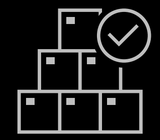
Salesloft Breach Attack Path



Source: Widespread Data Theft Targets Salesforce Instances via Salesloft Drift

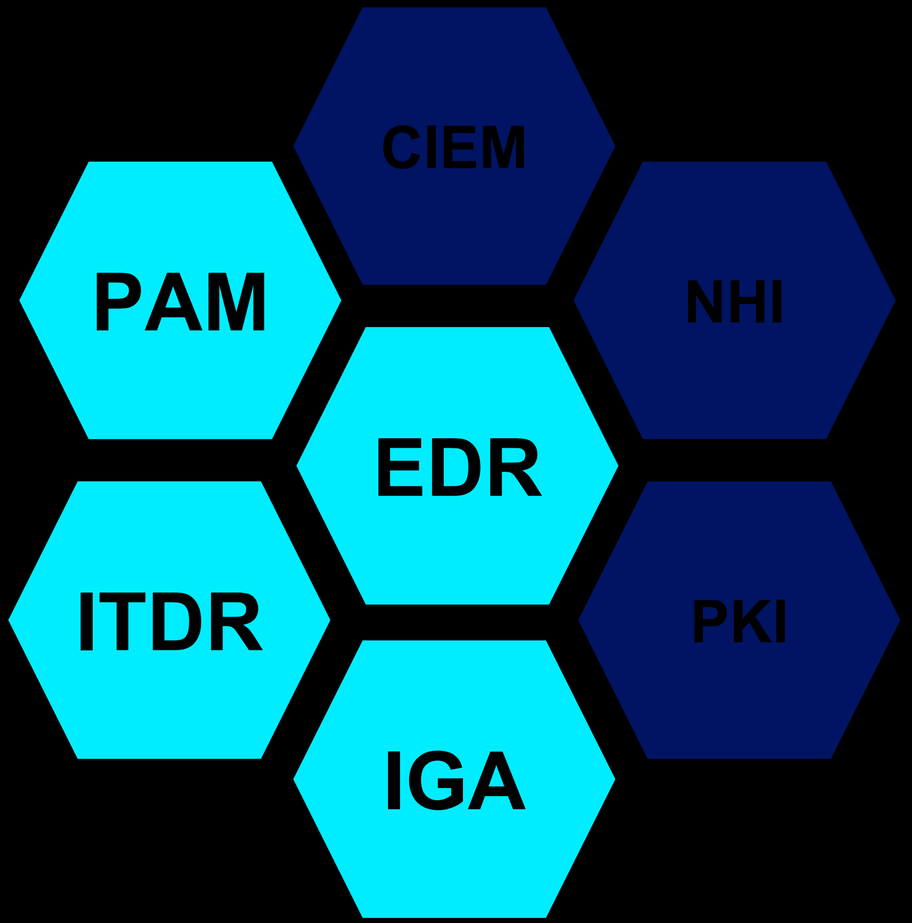
How
Attack Paths
Bypass Controls

The Scale of
Attack Paths



Attack Path
Management

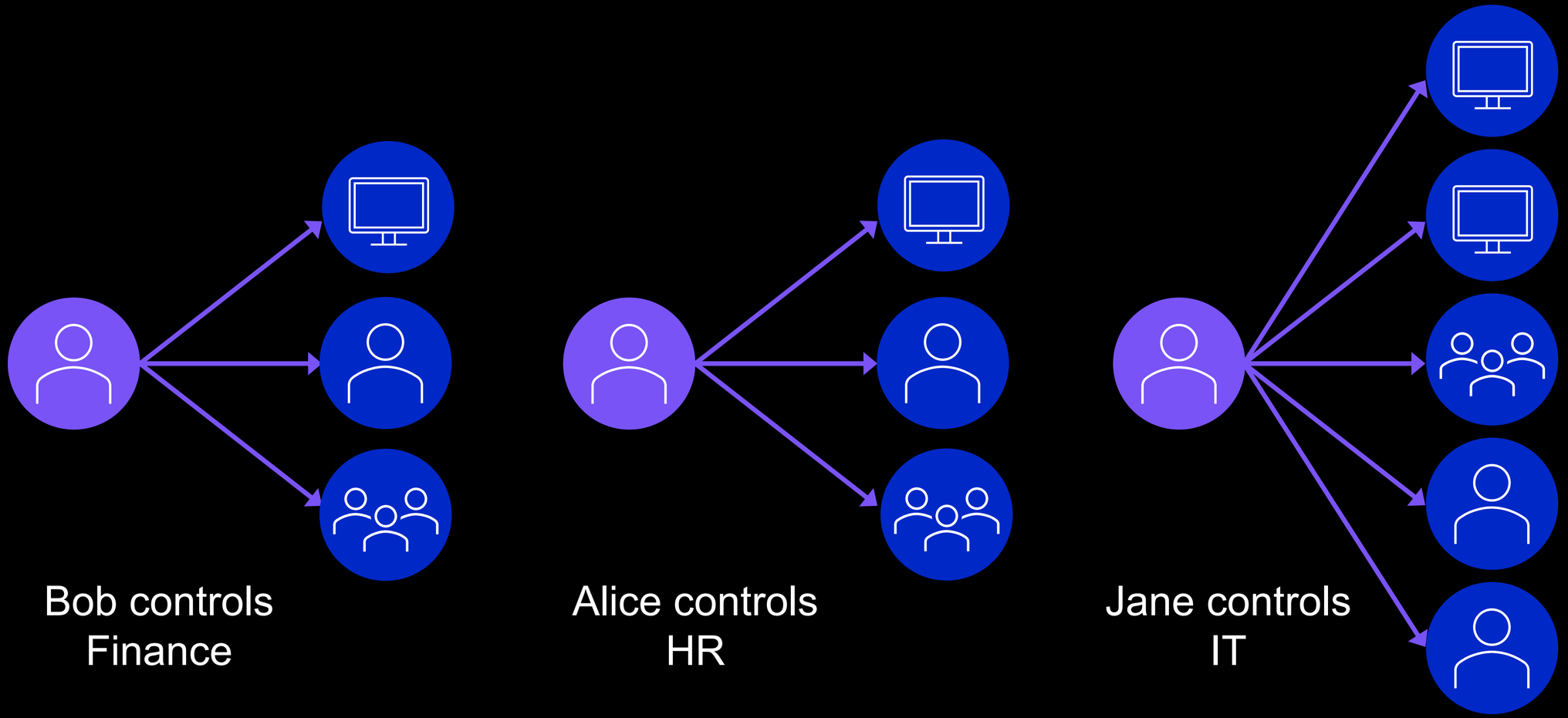
How
Attack Paths
Bypass Controls



Identity Governance and Administration

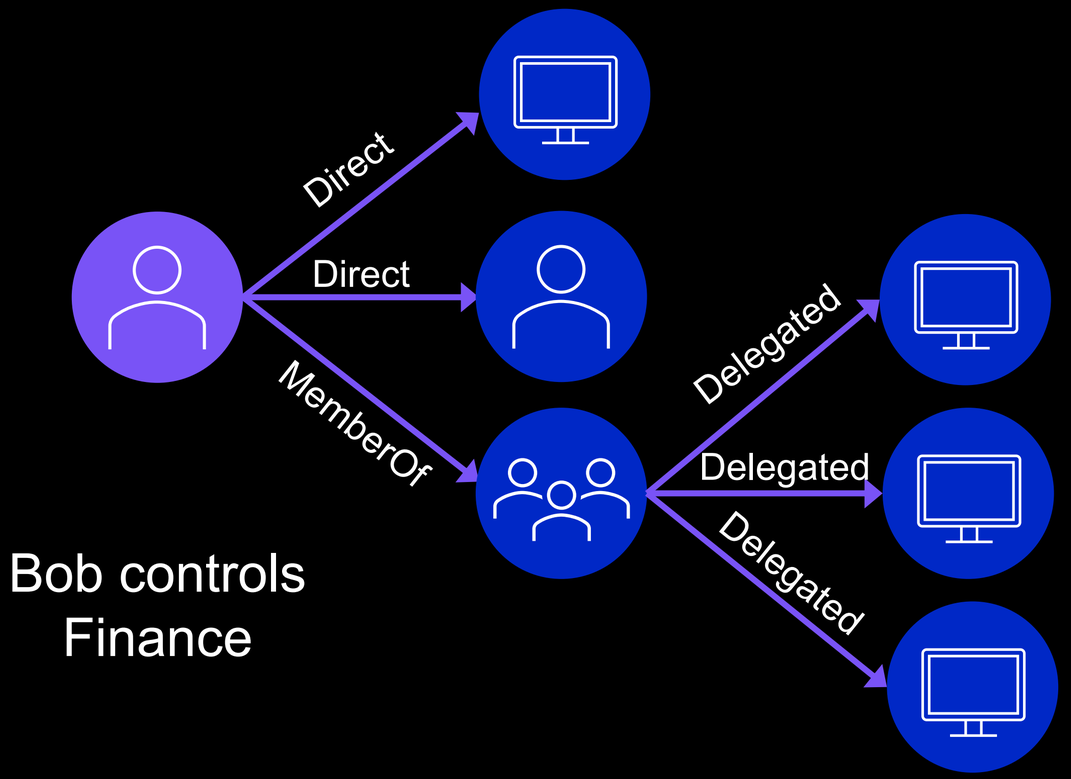
Identity Governance and Administration

Identities are analyzed in silos

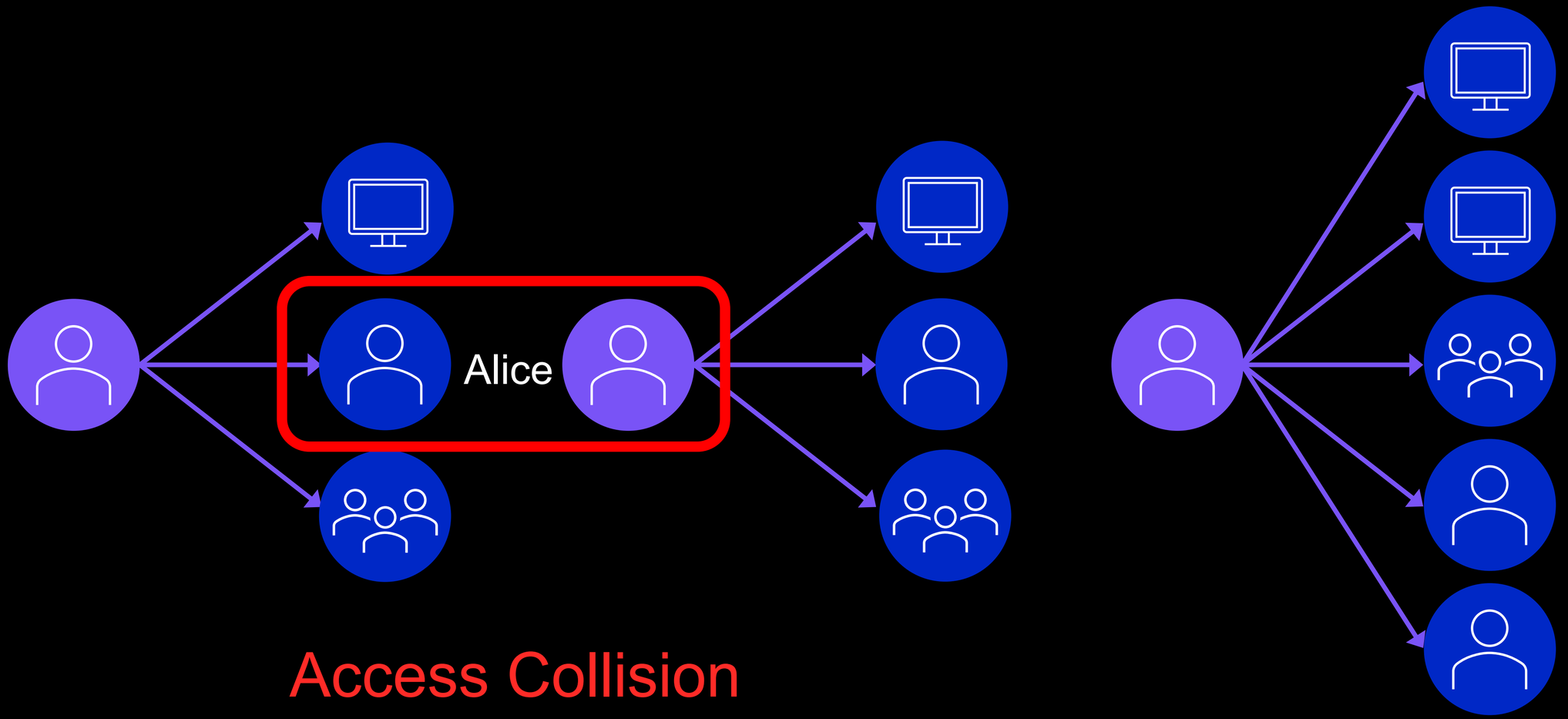


Identity Governance and Administration

Access Graphs

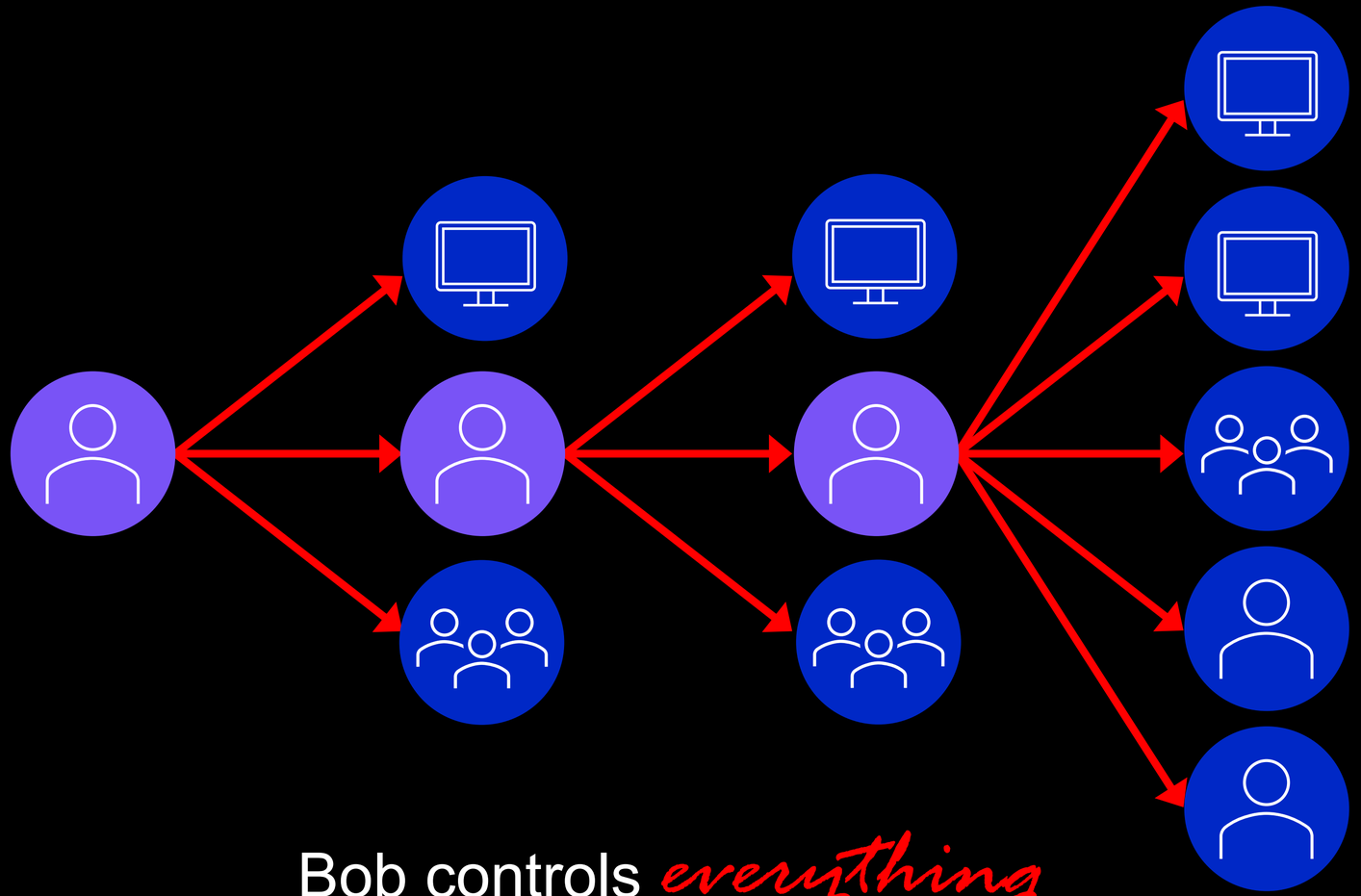


Identity Governance and Administration



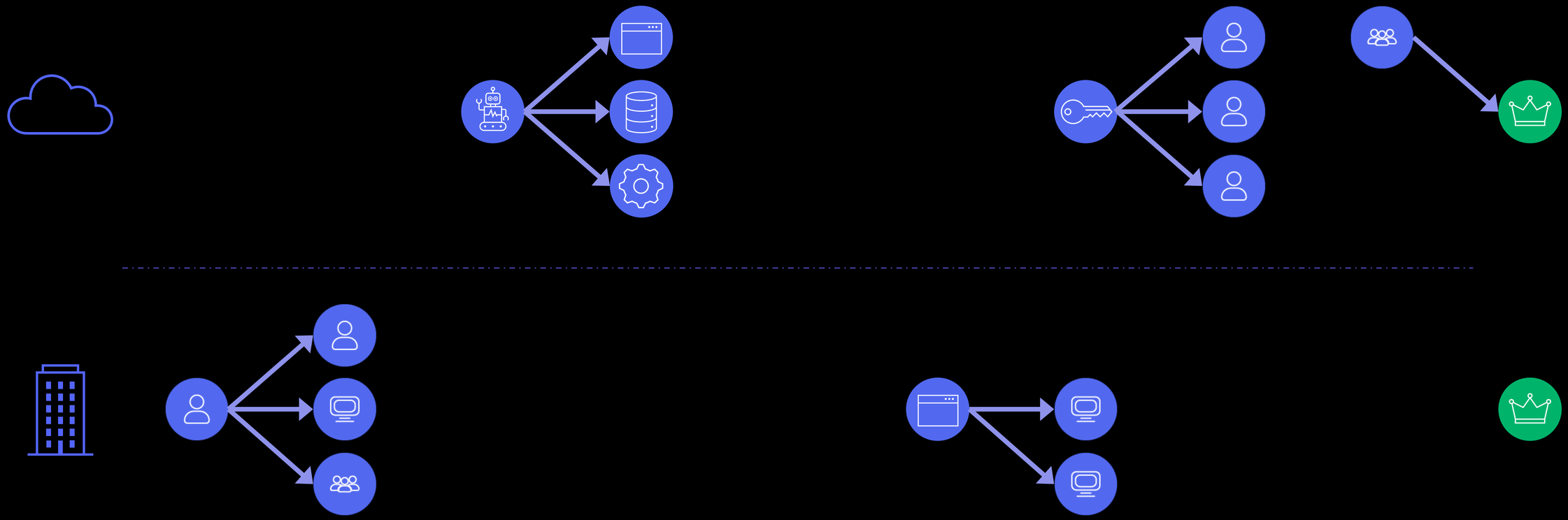
Identity Governance and Administration

Attack Graph

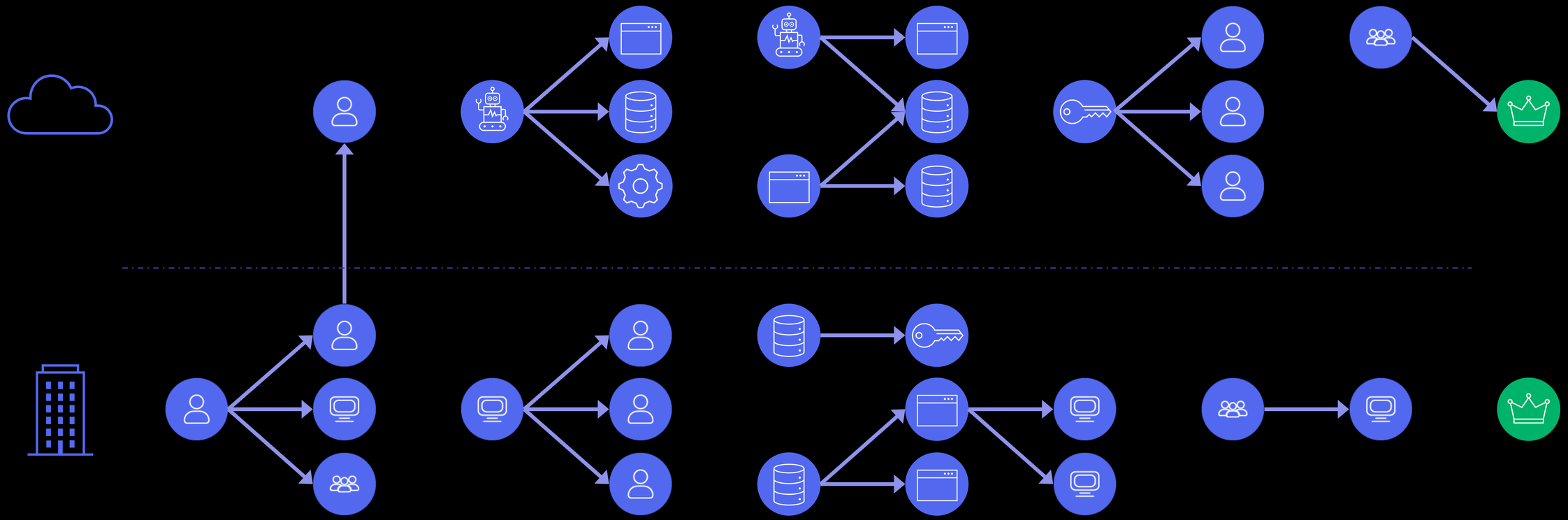


Bob controls *everything*

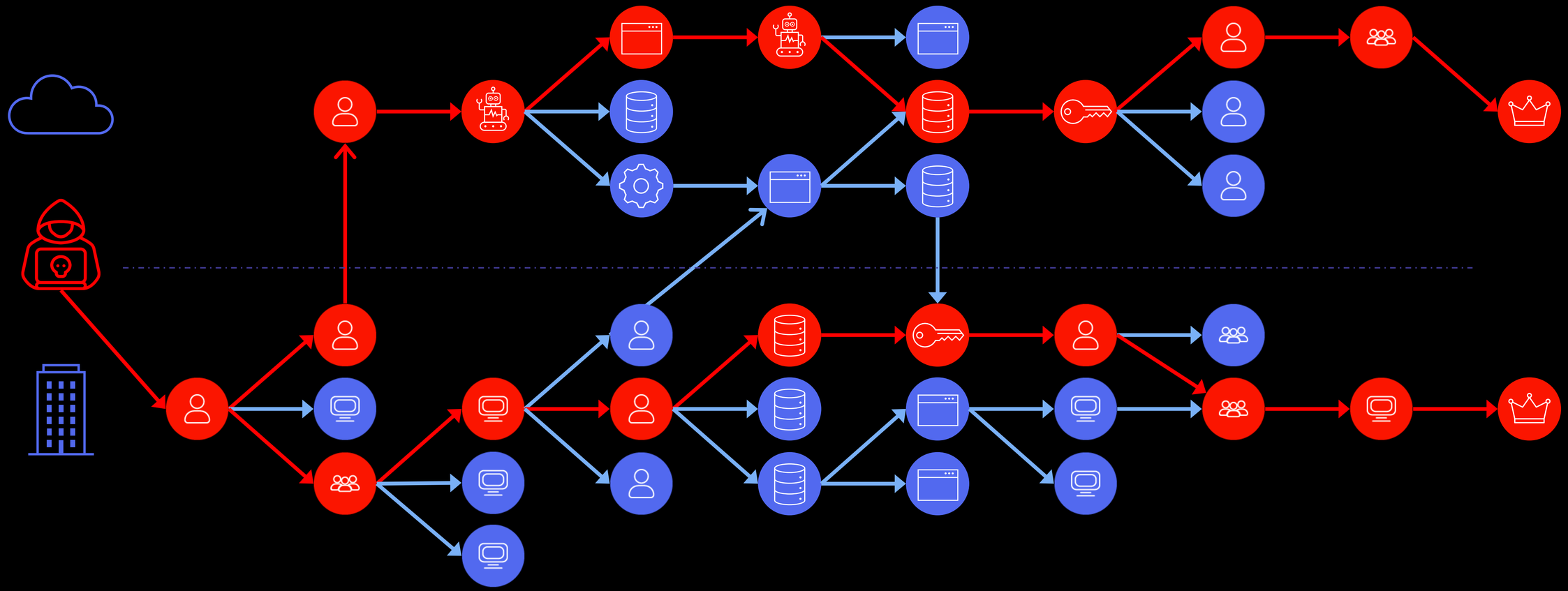
Individual access decisions appear benign



…but form access collisions invisible to IGA



Which form Attack Paths



Identity Governance and Administration

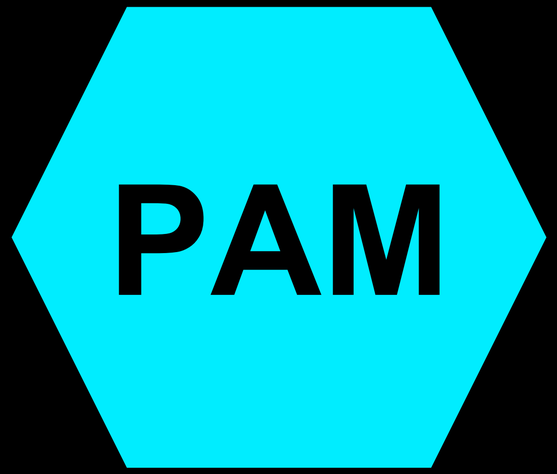
- IGA is great for provisioning access at scale

Identity Governance and Administration

- IGA is great for provisioning access at scale
- Assigned Access ≠ Effective Access

Identity Governance and Administration

- IGA is great for provisioning access at scale
- Assigned Access ≠ Effective Access
- Access Collisions create Attack Paths for adversaries



Privileged Access Management

Privileged Access Management

Identity At Rest	Identity In Transit

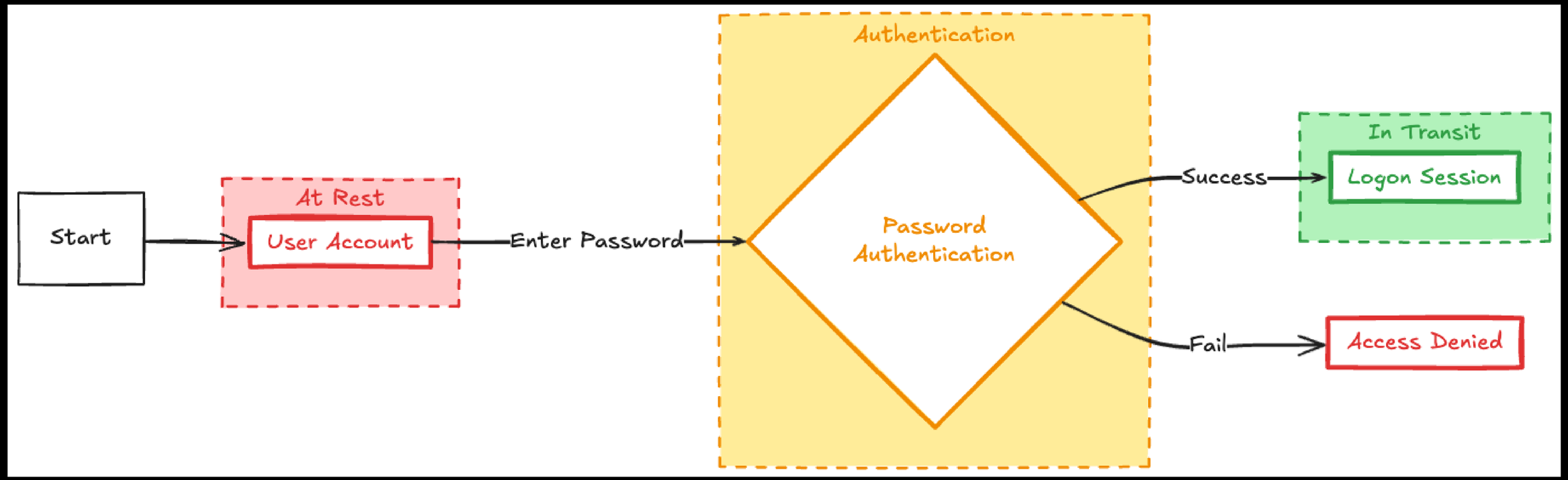
Privileged Access Management

	Identity At Rest	Identity In Transit
Definition	A pre-authentication account with a credential	Sessions, Tokens, Processes. Created post authentication.

Privileged Access Management

	Identity At Rest	Identity In Transit
Definition	A pre-authentication account with a credential	Sessions, Tokens, Processes. Created post authentication.
Attacks	Password Dumping, Brute Forcing	Token Impersonation, Session hijacking, process injection, Cookie Theft, Pass-the-Ticket

Identity States during Authentication Flow



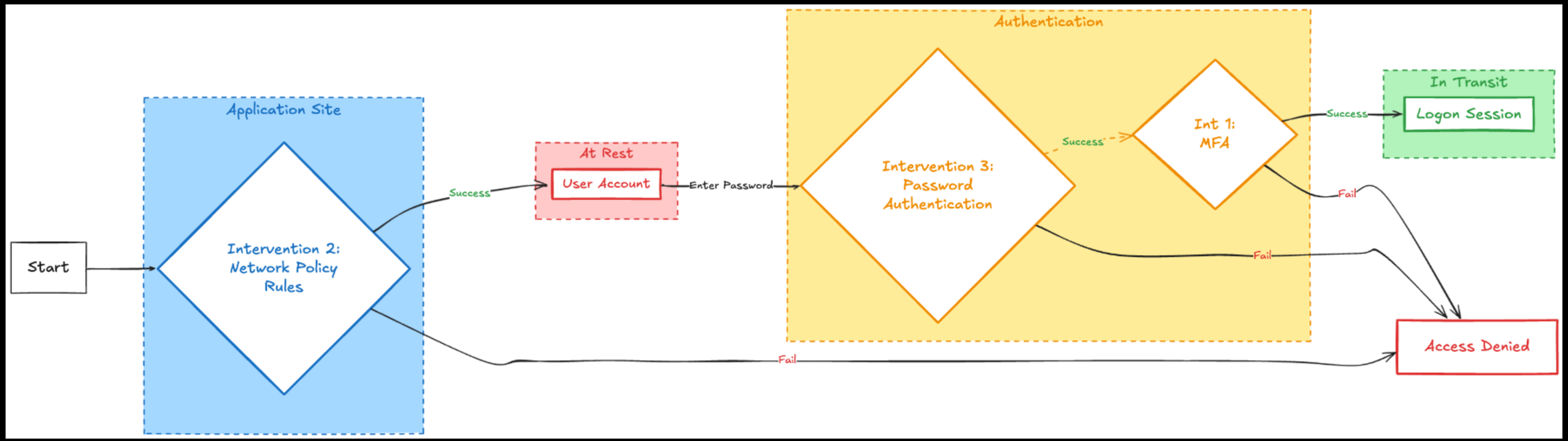
Case Study: 2024 Snowflake Attack

According to Mandiant, these victims' Snowflake identities were compromised via a contractor's laptop also used for personal activities.

Snowflake and Mandiant recommendations:

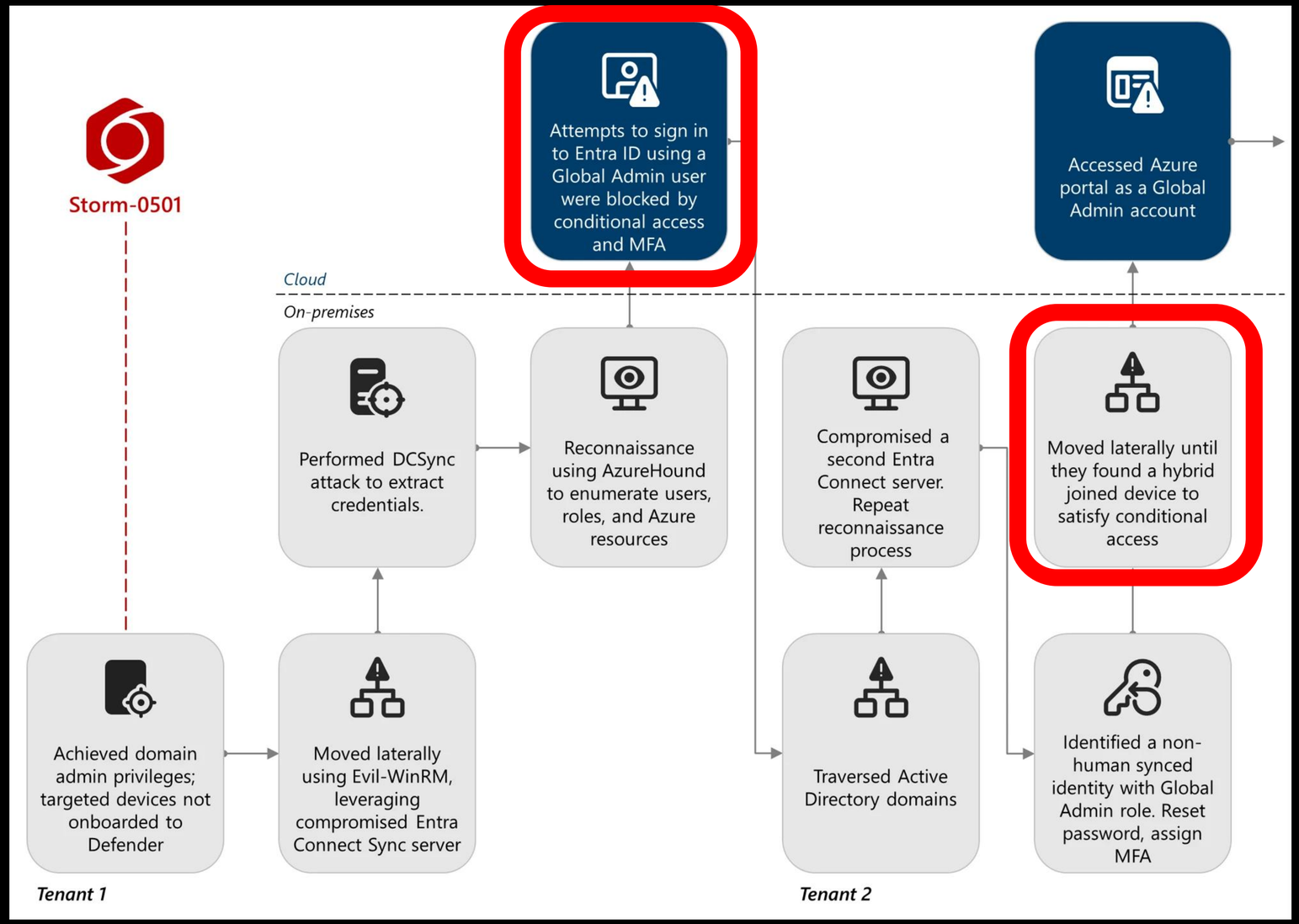
1. Enforce Multi-Factor Authentication on all accounts
2. Set up Network Policy Rules to allow authorized users & locations
3. Reset and rotate Snowflake credentials

Recommendations in the Authentication Flow



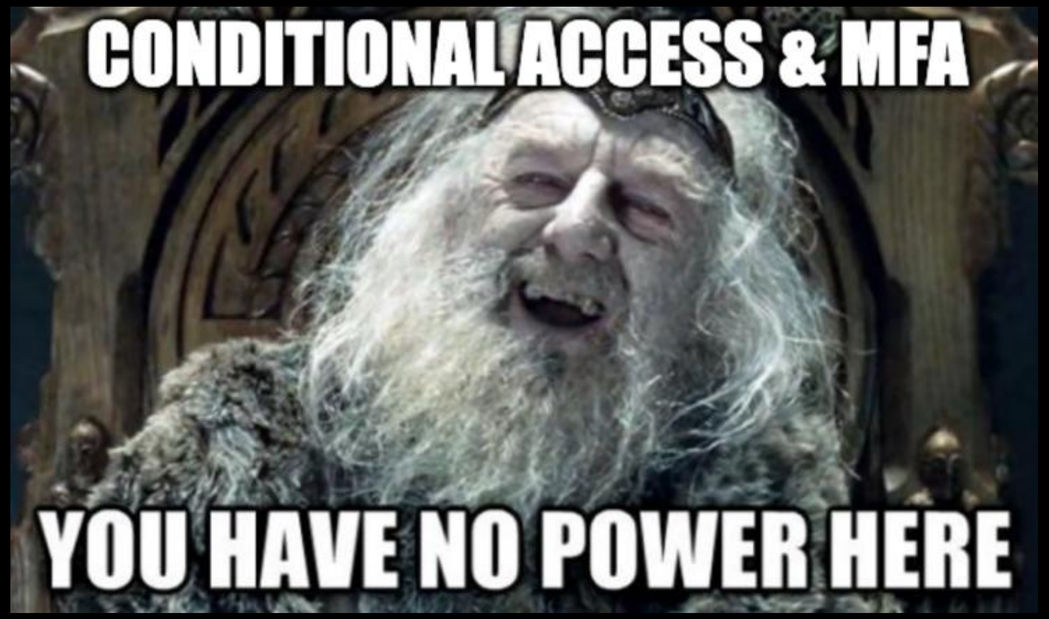
Nothing for the In Transit identity = **I can still pivot**

But we use Conditional Access!

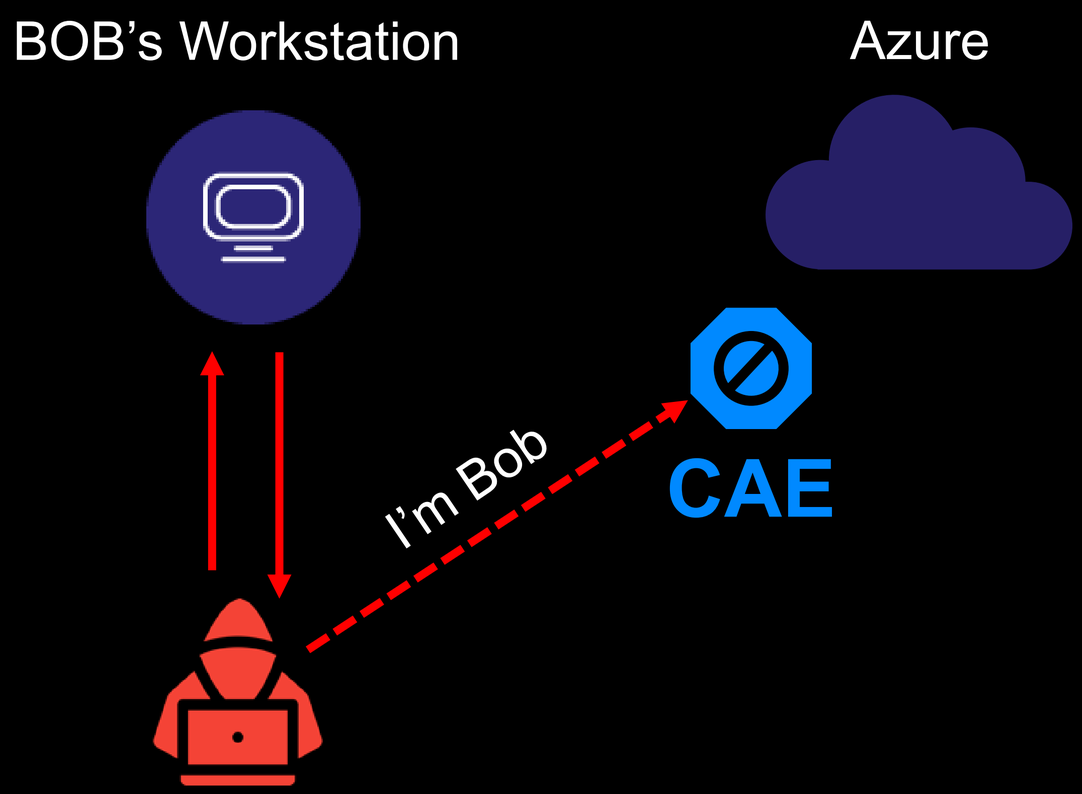


Identity In Transit attacks & Conditional Access

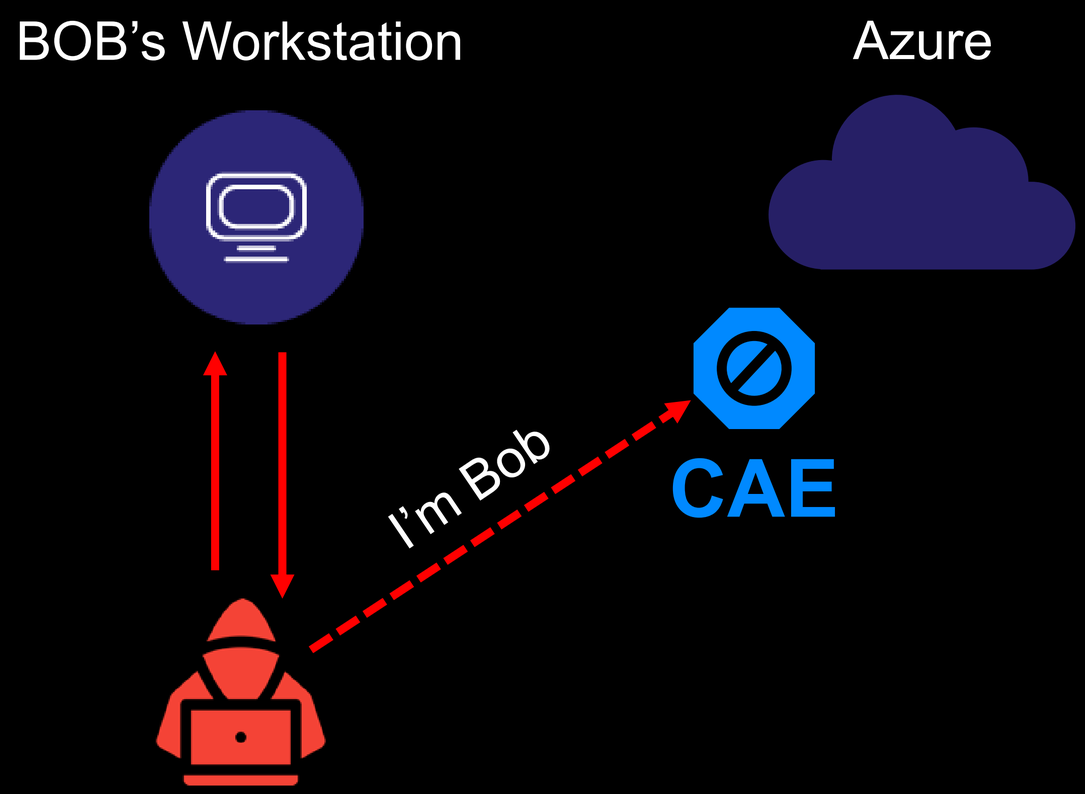
- Bob logs in
- Satisfies Conditional Access + MFA
- Bearer token / JWT created on host
- Attacker harvests token
- Attacker uses token from their host
- *Attacker is Bob*



But we use Conditional Access *with* Continuous Access Evaluation

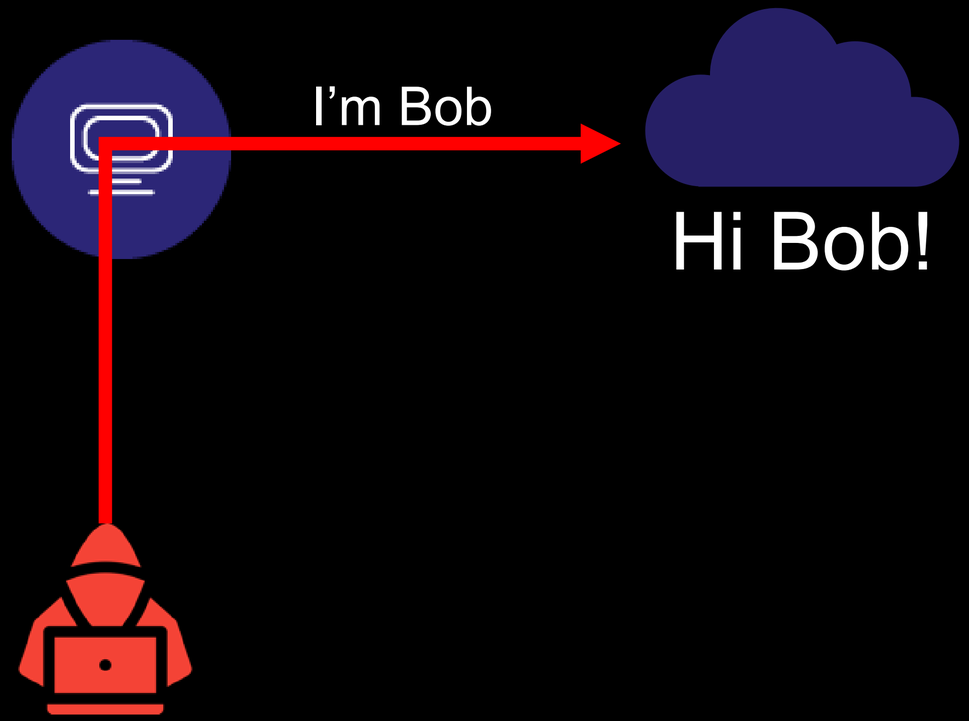


But we use Conditional Access *with* Continuous Access Evaluation



I’ll just use *your* host

But we use Conditional Access *with* Continuous Access Evaluation



I’ll just use *your* host

Privileged Access Management

- PAM / JIT / CAP are all powerful tools that should be used

Privileged Access Management

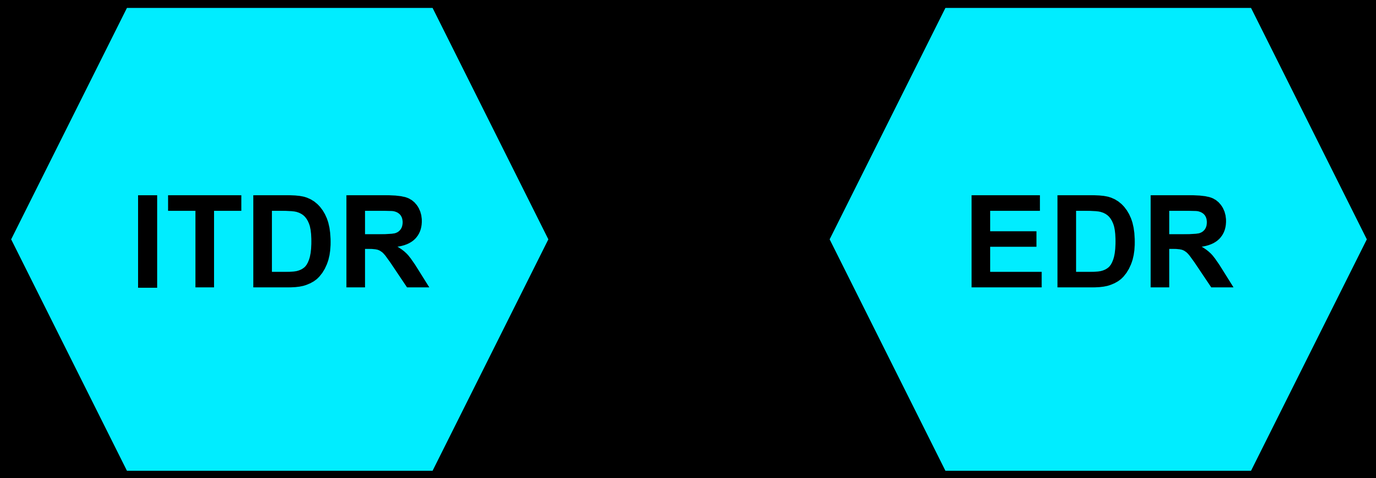
- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused

Privileged Access Management

- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused
- Attackers don’t need the password, they steal sessions

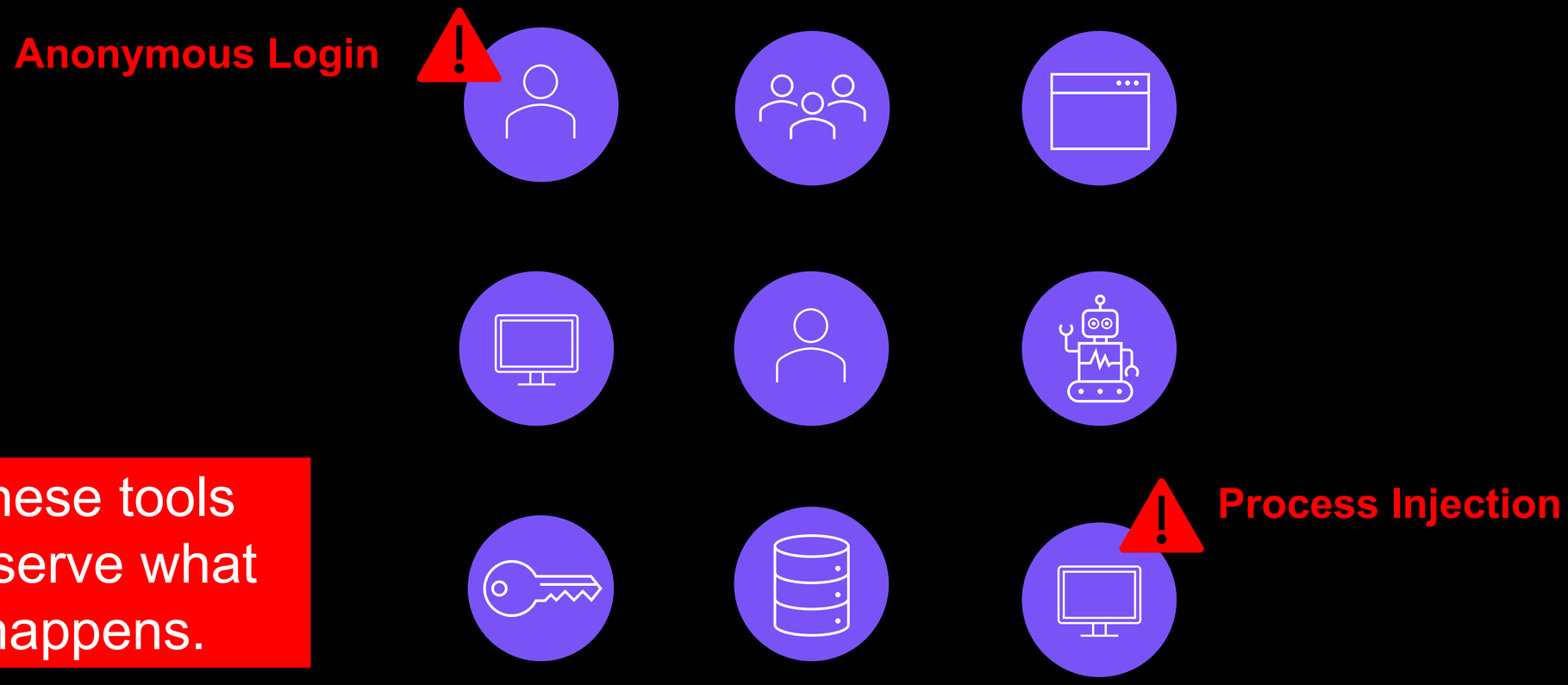
Privileged Access Management

- PAM / JIT / CAP are all powerful tools that should be used
- User login sessions create artifacts that can be abused
- Attackers don’t need the password, they steal sessions
- PAM secures Identities At Rest, not what happens next



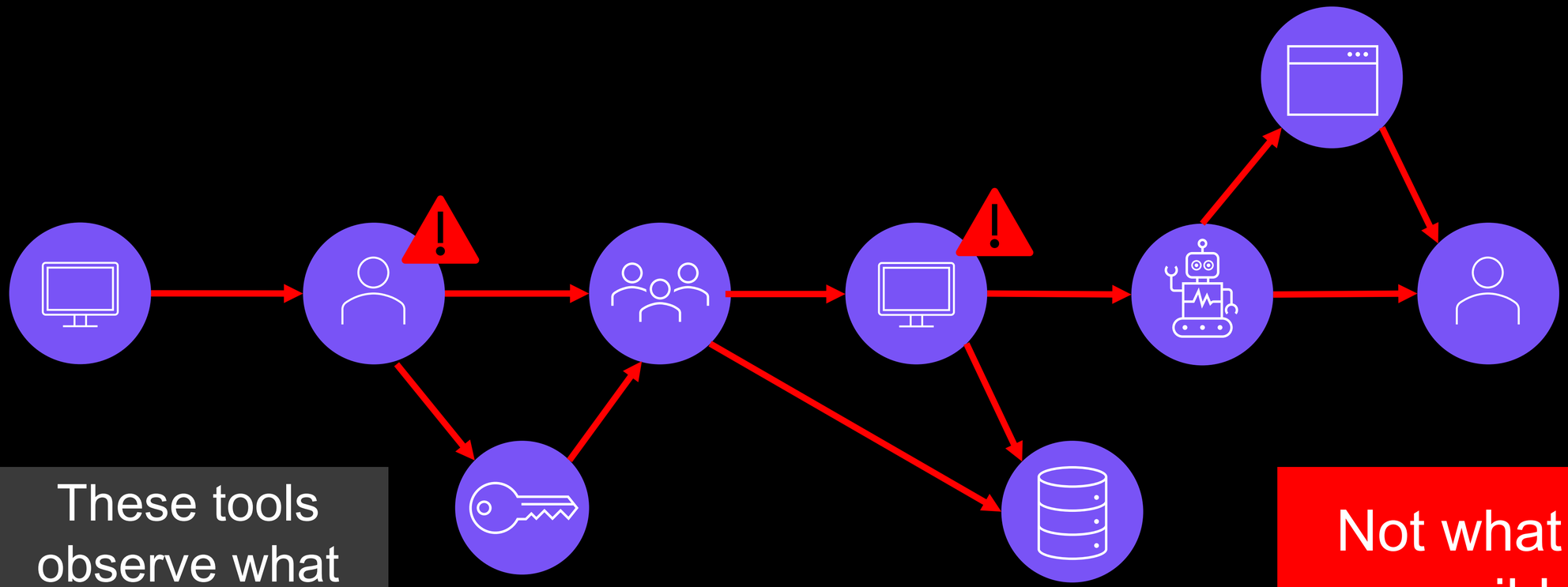
Endpoint & Identity Detection Response

Endpoint & Identity Detection and Response



These tools observe what happens.

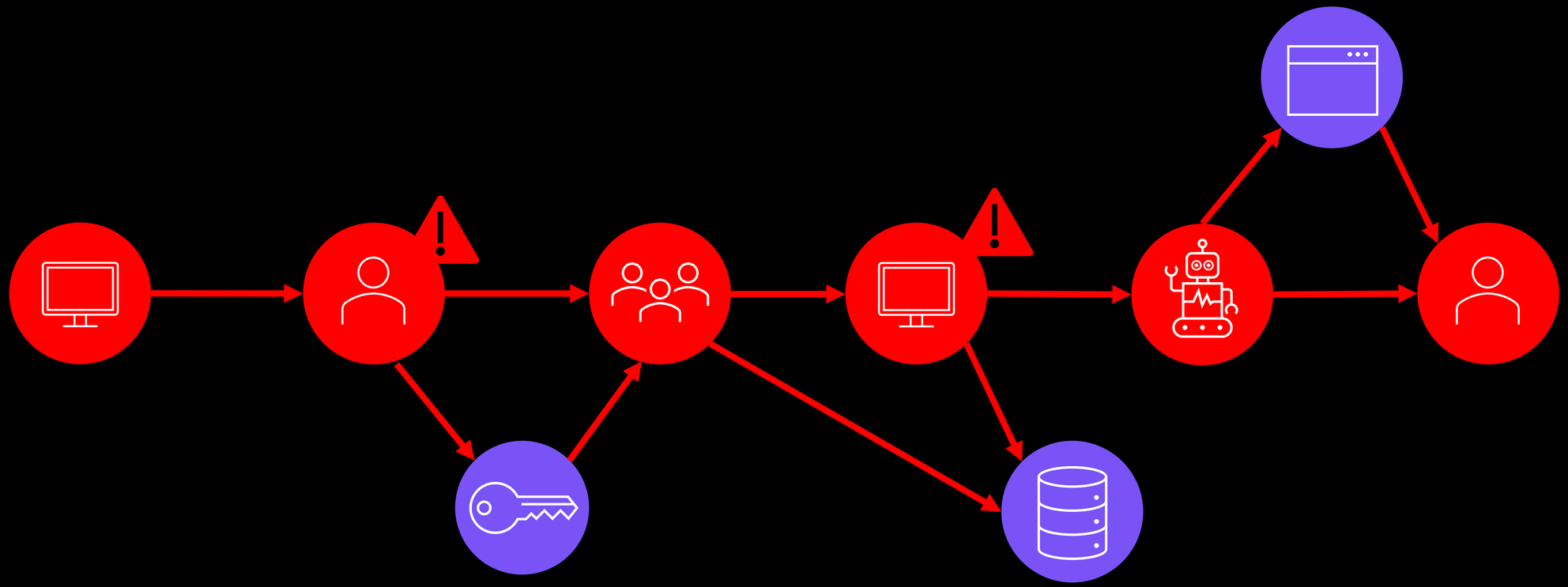
Endpoint & Identity Detection and Response



These tools observe what happens.

Not what is possible

Endpoint & Identity Detection and Response



They detect the *symptom*, not the ***condition***.

Case Study: Red Team Engagement

- Advanced organization, modern controls, strong defense

Case Study: Red Team Engagement

- Advanced organization, modern controls, strong defense
- How about Command and Control (C2) in Perl?

Case Study: Red Team Engagement

- Advanced organization, modern controls, strong defense
- How about Command and Control (C2) in Perl?
- Attackers are now only limited by their creativity

Nation state attacker tradecraft, for everyone!

Yesterday's Attacker:

Manual

Expensive

Repeatable TTPs

Today's Attacker:

Agentic

Cheap

Customized

Endpoint & Identity Detection and Response

I don’t need to beat the E/ITDR, I just need to beat ***you***

Endpoint & Identity Detection and Response

- E/ITDR monitor systems & behaviors – often miss structure

Endpoint & Identity Detection and Response

- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected

Endpoint & Identity Detection and Response

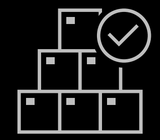
- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected
- AI/LLMs are lowering the bar for advanced attacks

Endpoint & Identity Detection and Response

- E/ITDR monitor systems & behaviors – often miss structure
- Lateral movement can look legitimate and go undetected
- AI/LLMs are lowering the bar for advanced attacks
- Even once detected, attacker may have moved on

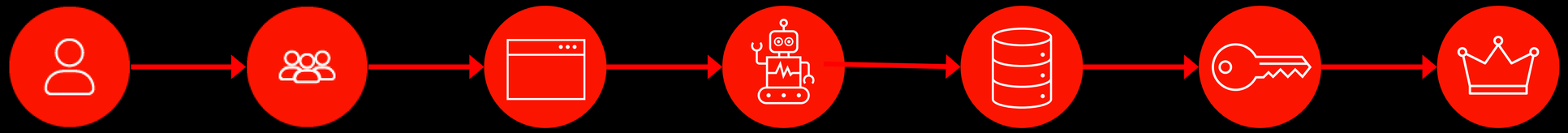
How
Attack Paths
Bypass Controls

The Scale of
Attack Paths



Attack Path
Management

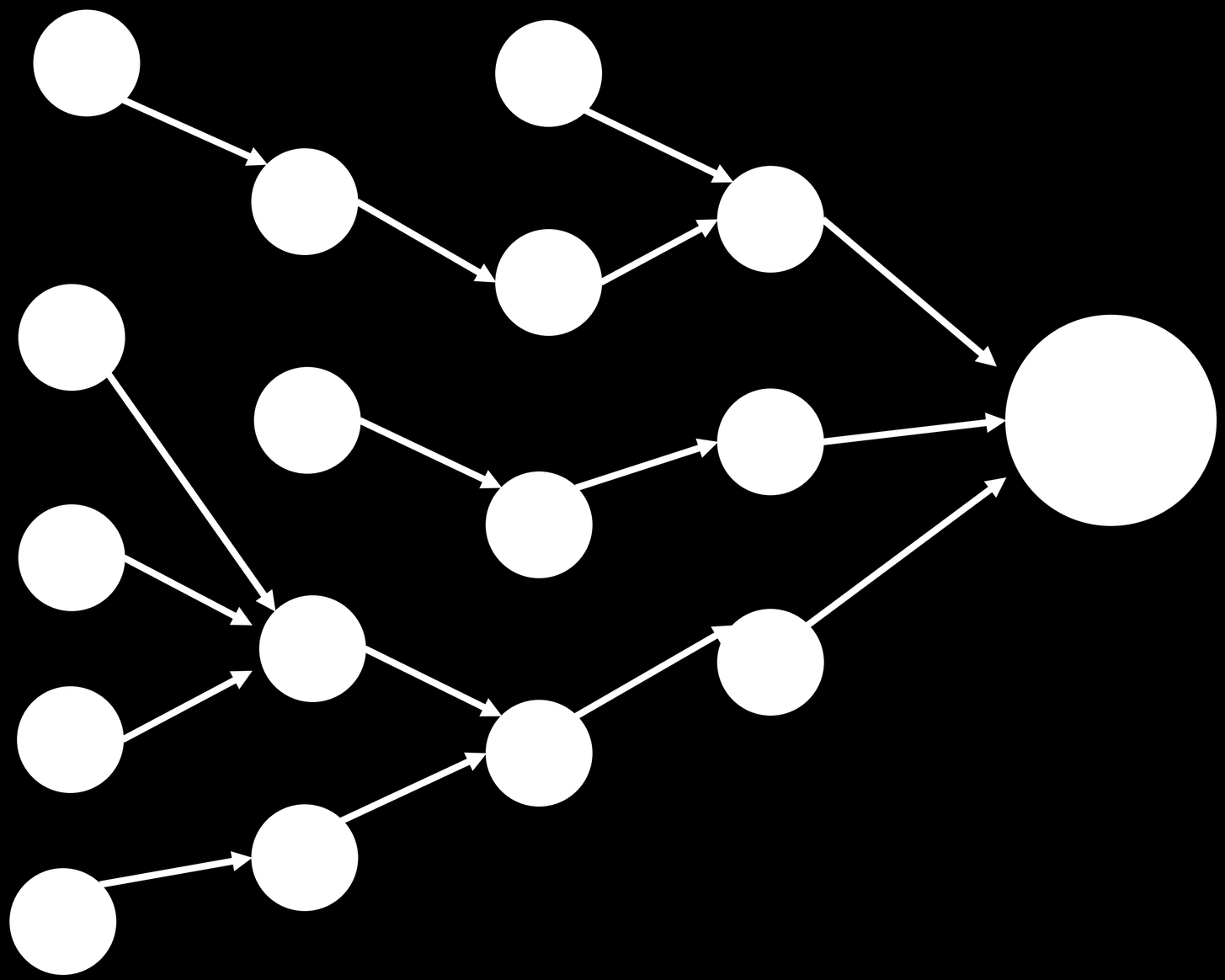
How can we quantify this problem?



The count of unique attack paths…

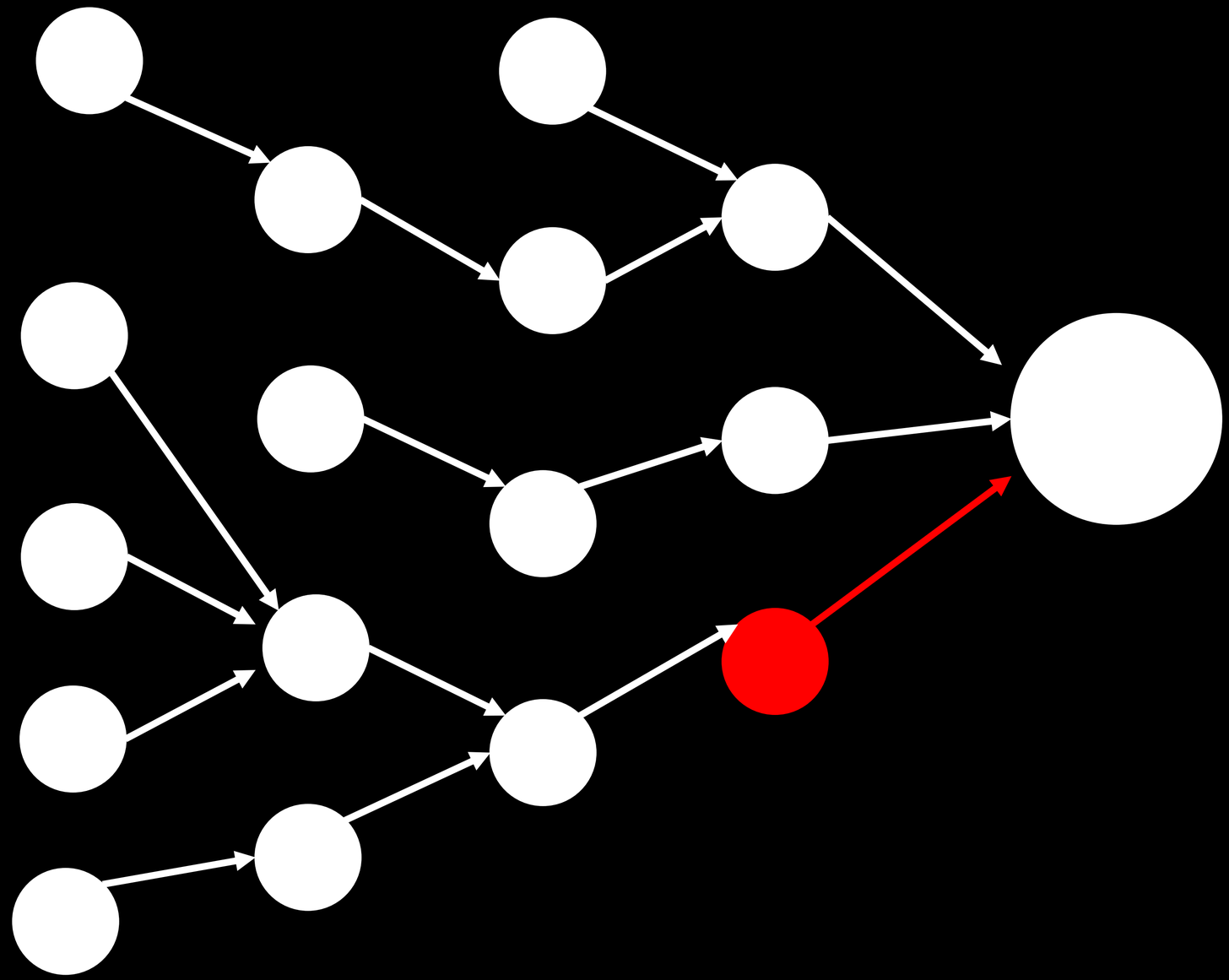
using any available abuseable relationship…

between any identity to a destination



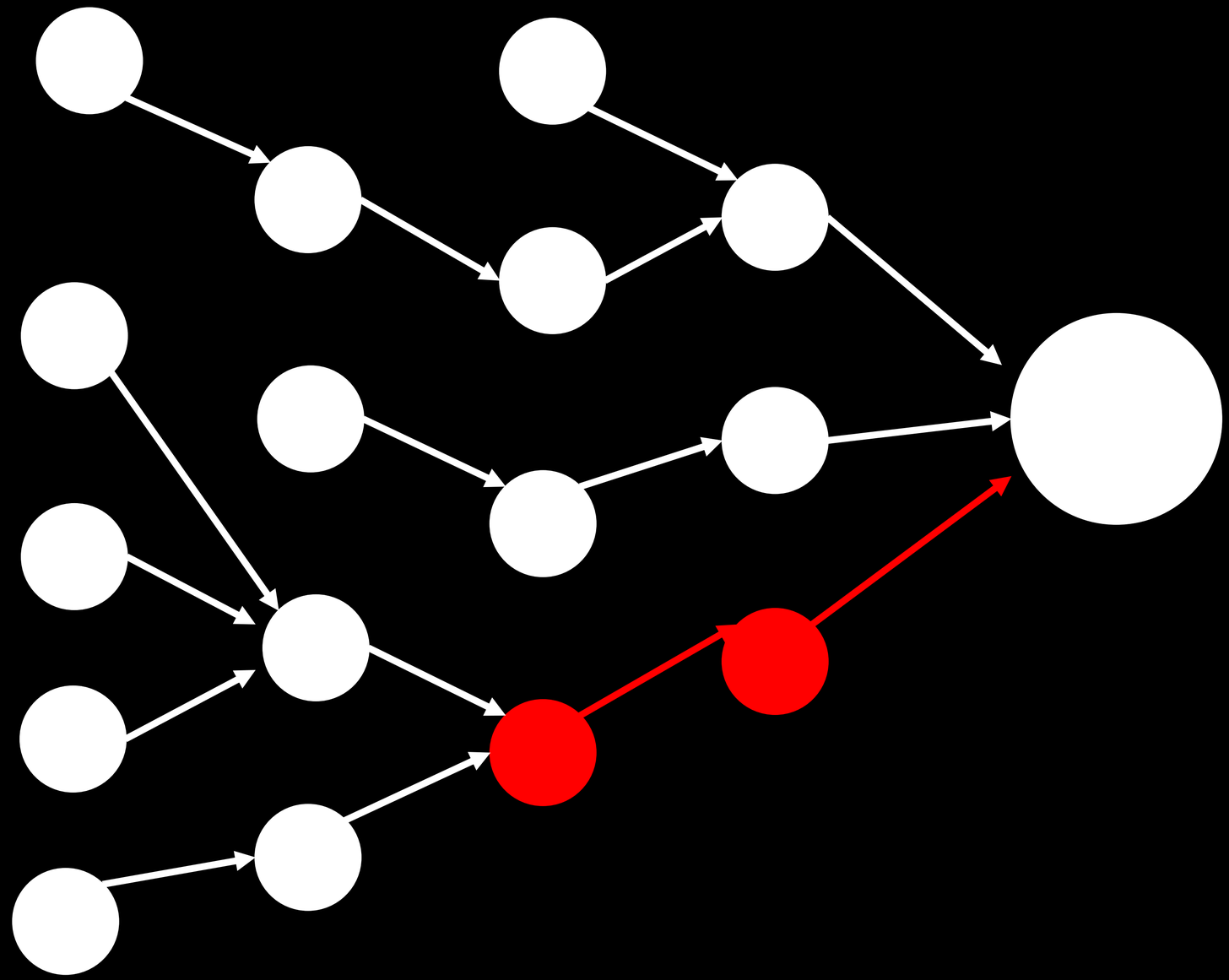
Attack Path Count:

1



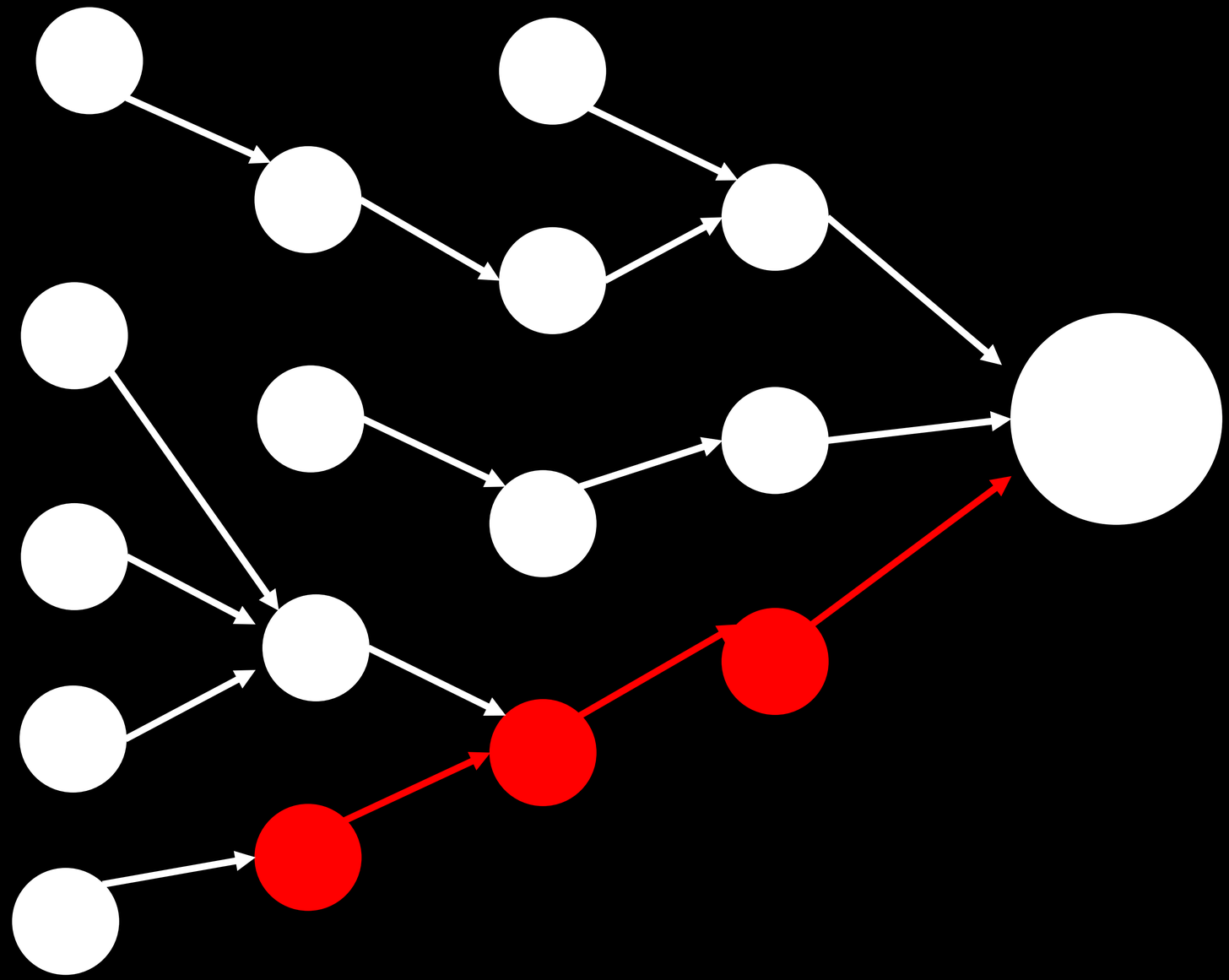
Attack Path Count:

2



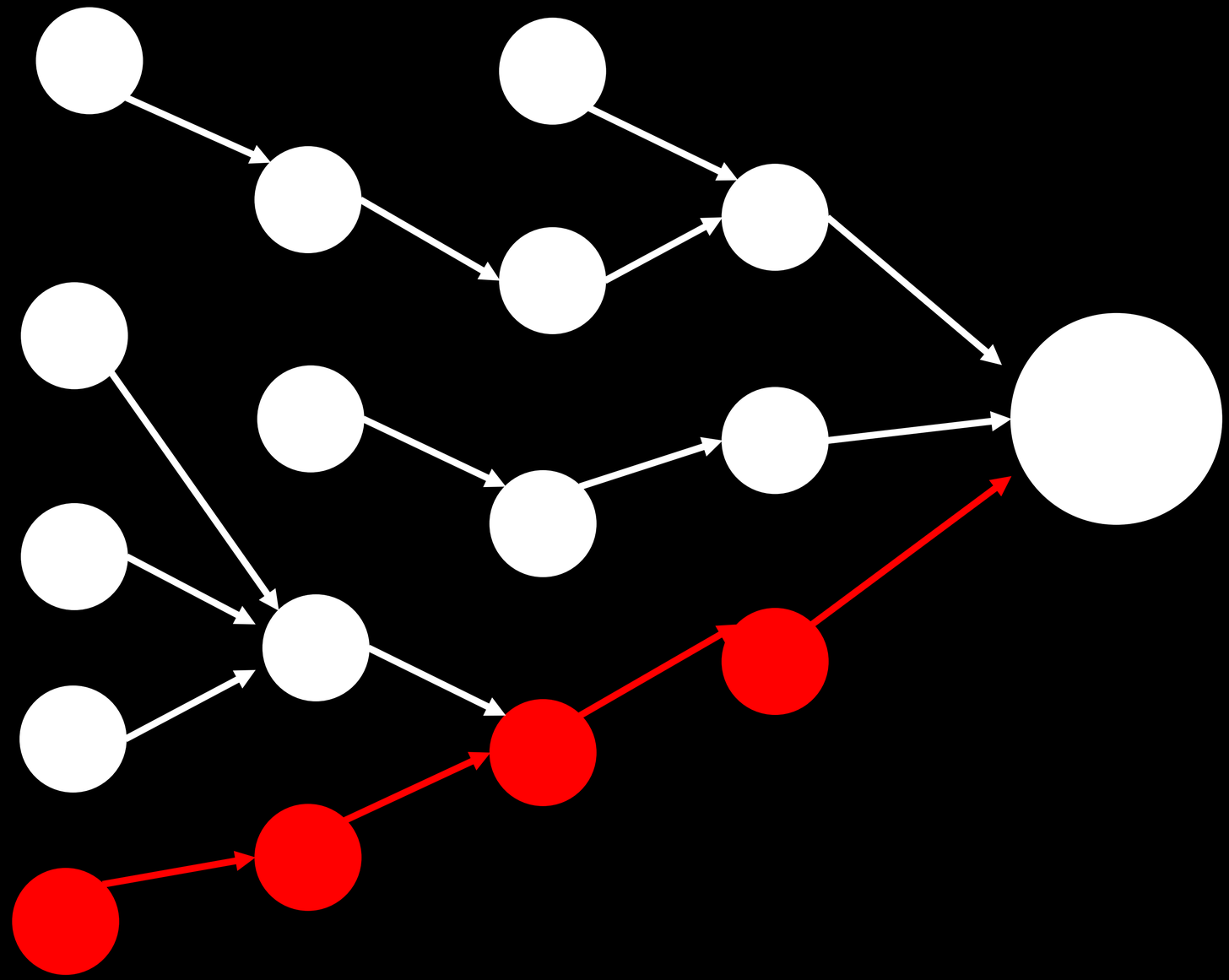
Attack Path Count:

3



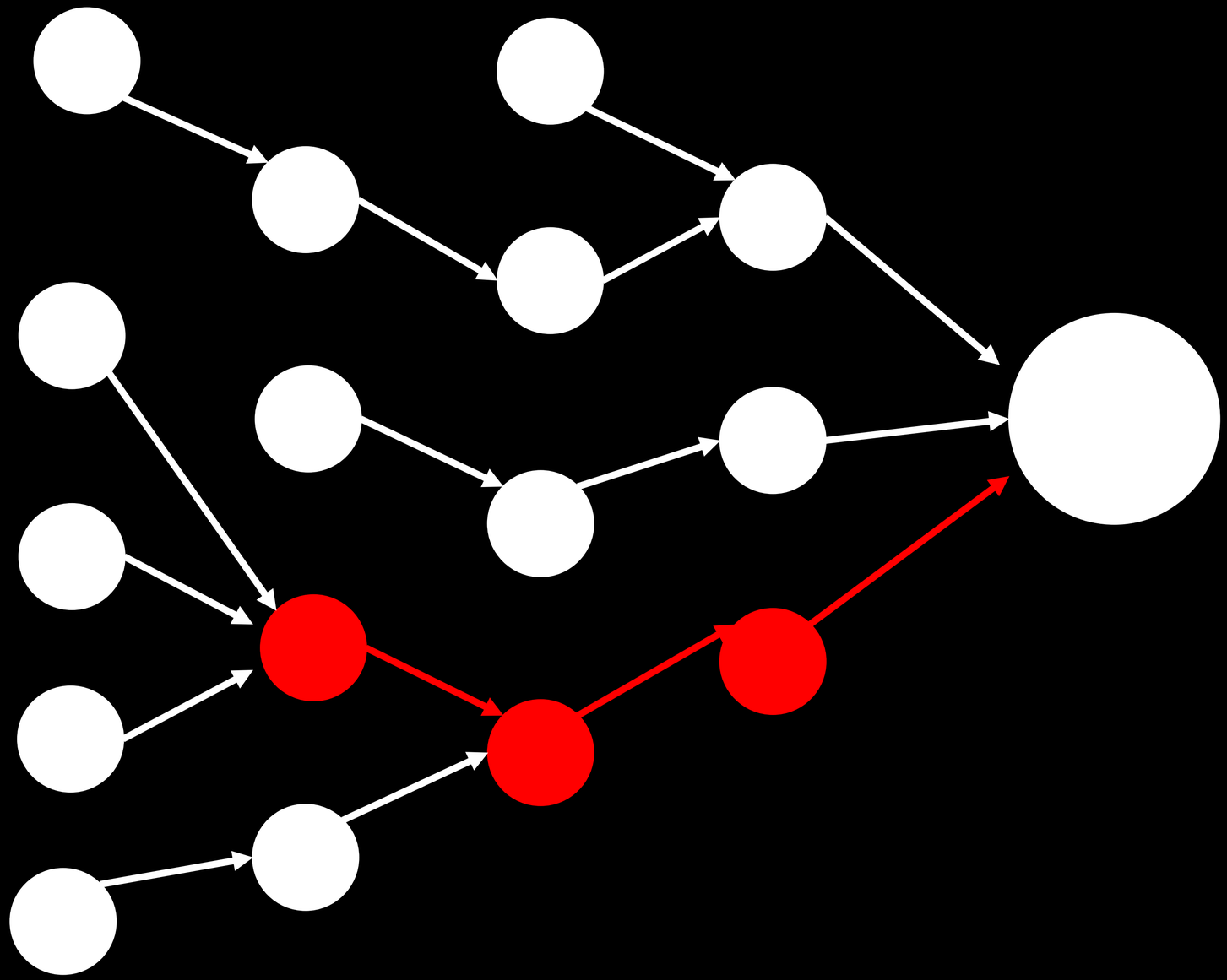
Attack Path Count:

4



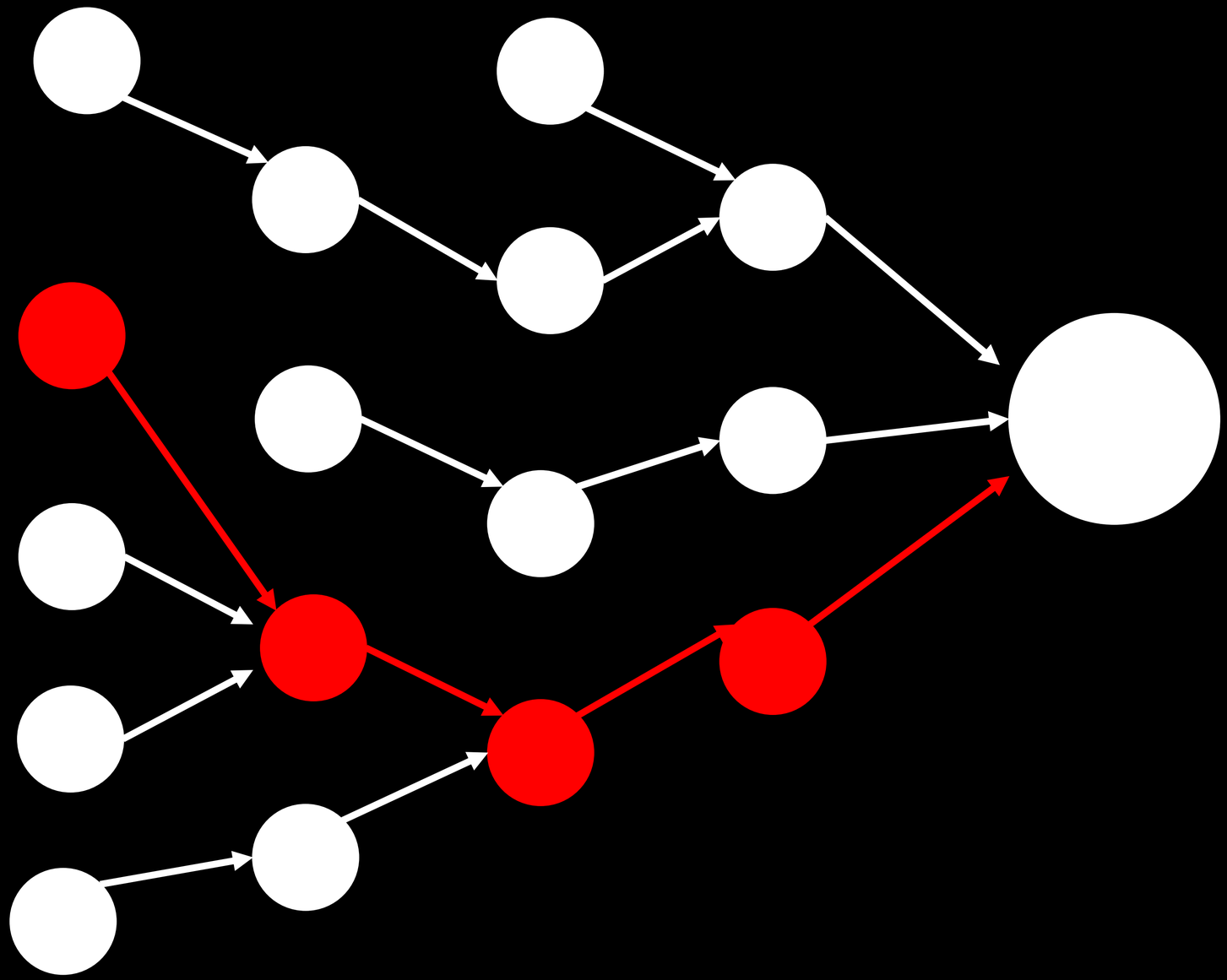
Attack Path Count:

5



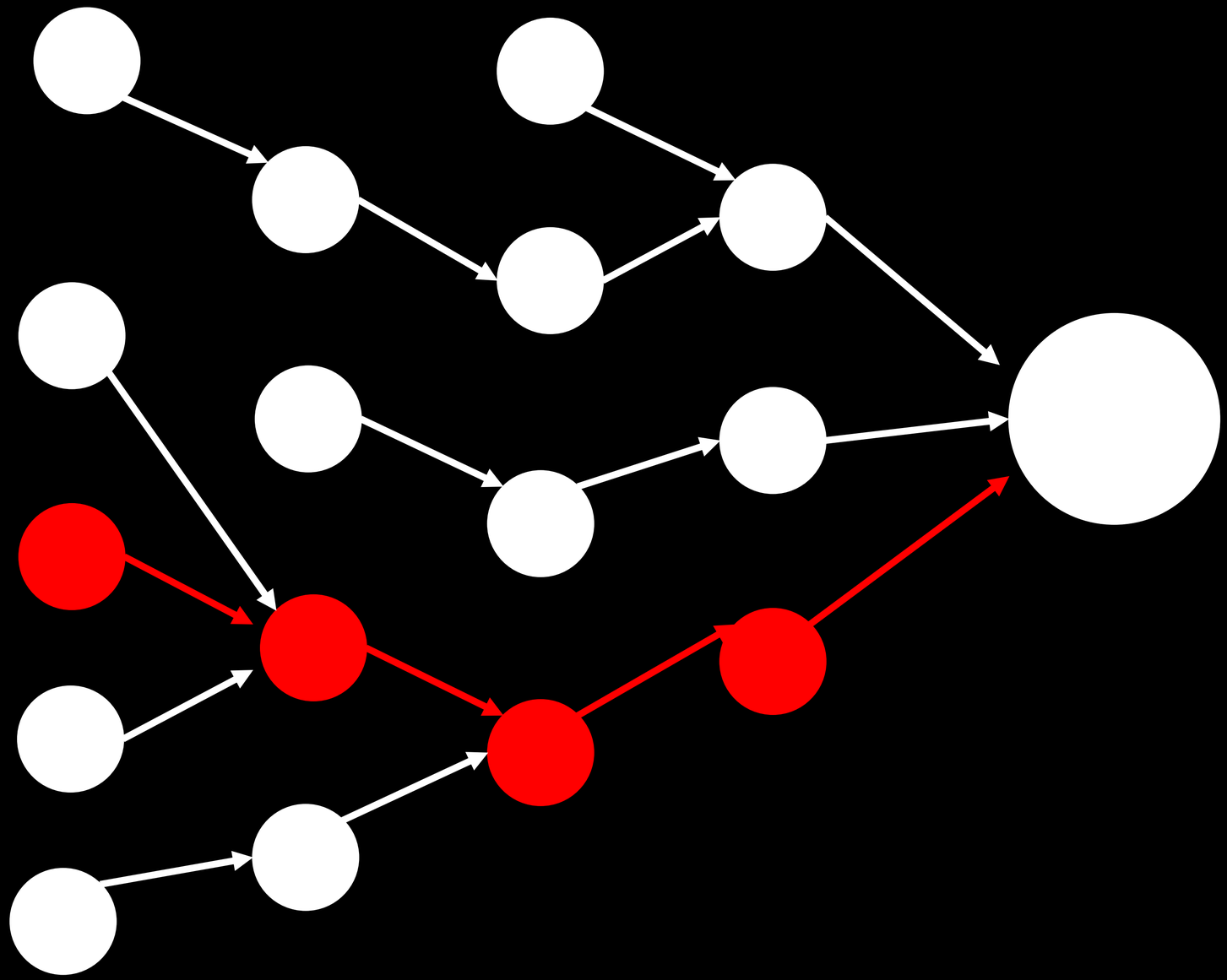
Attack Path Count:

6



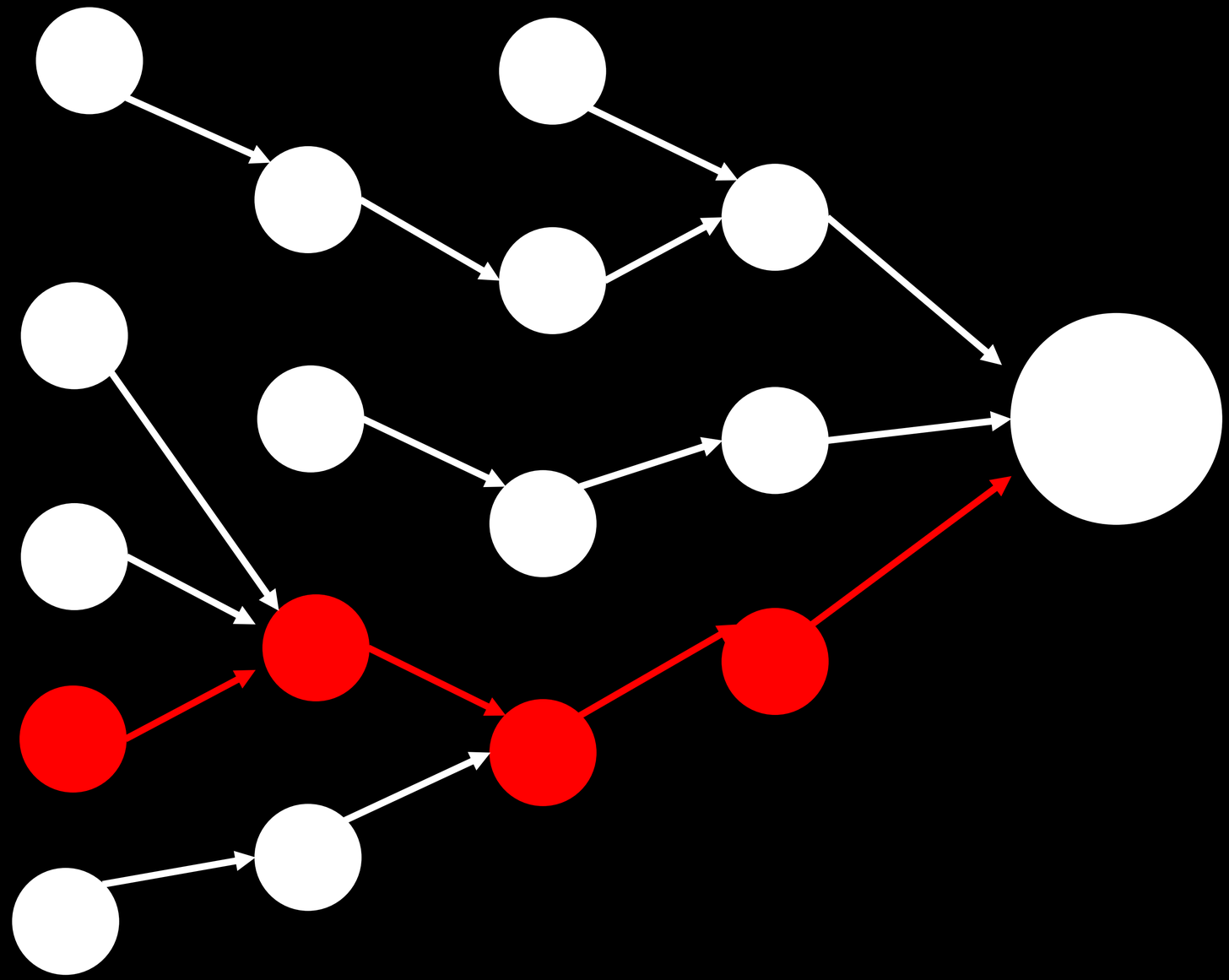
Attack Path Count:

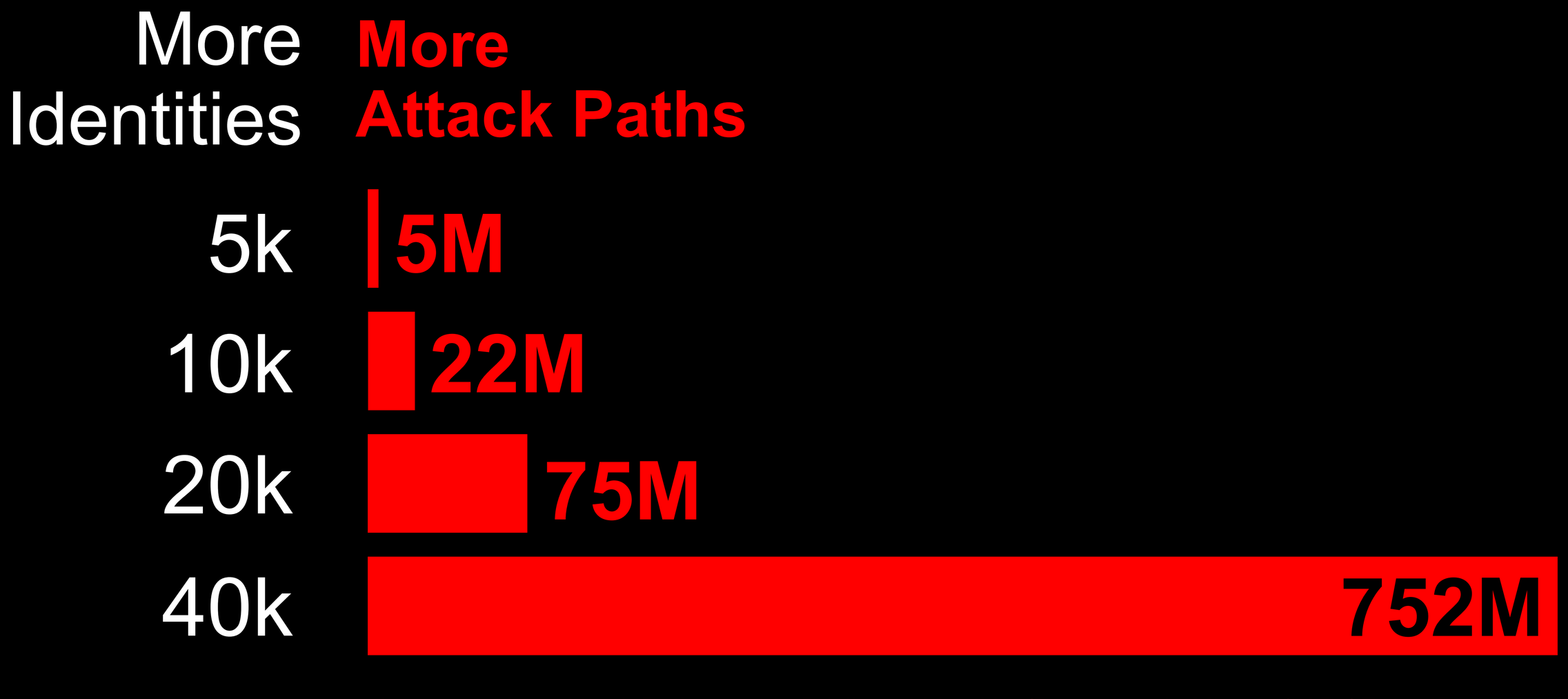
7



Attack Path Count:

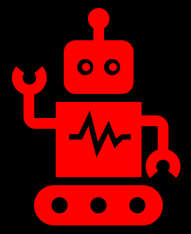
8





Average unique Attack Path count to Privileged Identities/Resources in Microsoft AD / Entra ID

And like all problems, worse with AI



Every AI agent needs an identity

20:1

NHIs outnumber Humans 20-to-1

150%

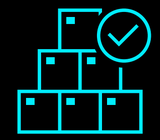
Growth in NHIs this year

Sources: CyberArk State of Machine Identity Report and 2024 ESG NHI Report

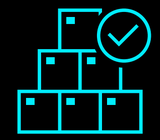
How Attack Paths Bypass Controls

The Scale of Attack Paths

Attack Path Management



The continuous discovery, mapping, and risk assessment of Attack Path Choke Points.



Attack Path Management

Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword

Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound **(FREE)** to visualize attack paths

Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound **(FREE)** to visualize attack paths
3. Identify and prioritize attack path choke points

Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound **(FREE)** to visualize attack paths
3. Identify and prioritize attack path choke points
4. Once established, address hybrid attack path risk

Getting started with Attack Path Management

1. Understand that “Attack path” is not a red team buzzword
2. Use BloodHound **(FREE)** to visualize attack paths
3. Identify and prioritize attack path choke points
4. Once established, address hybrid attack path risk
5. Track and report Key Performance Indicators (KPIs)

*"**Implement least-privilege** access principles."*

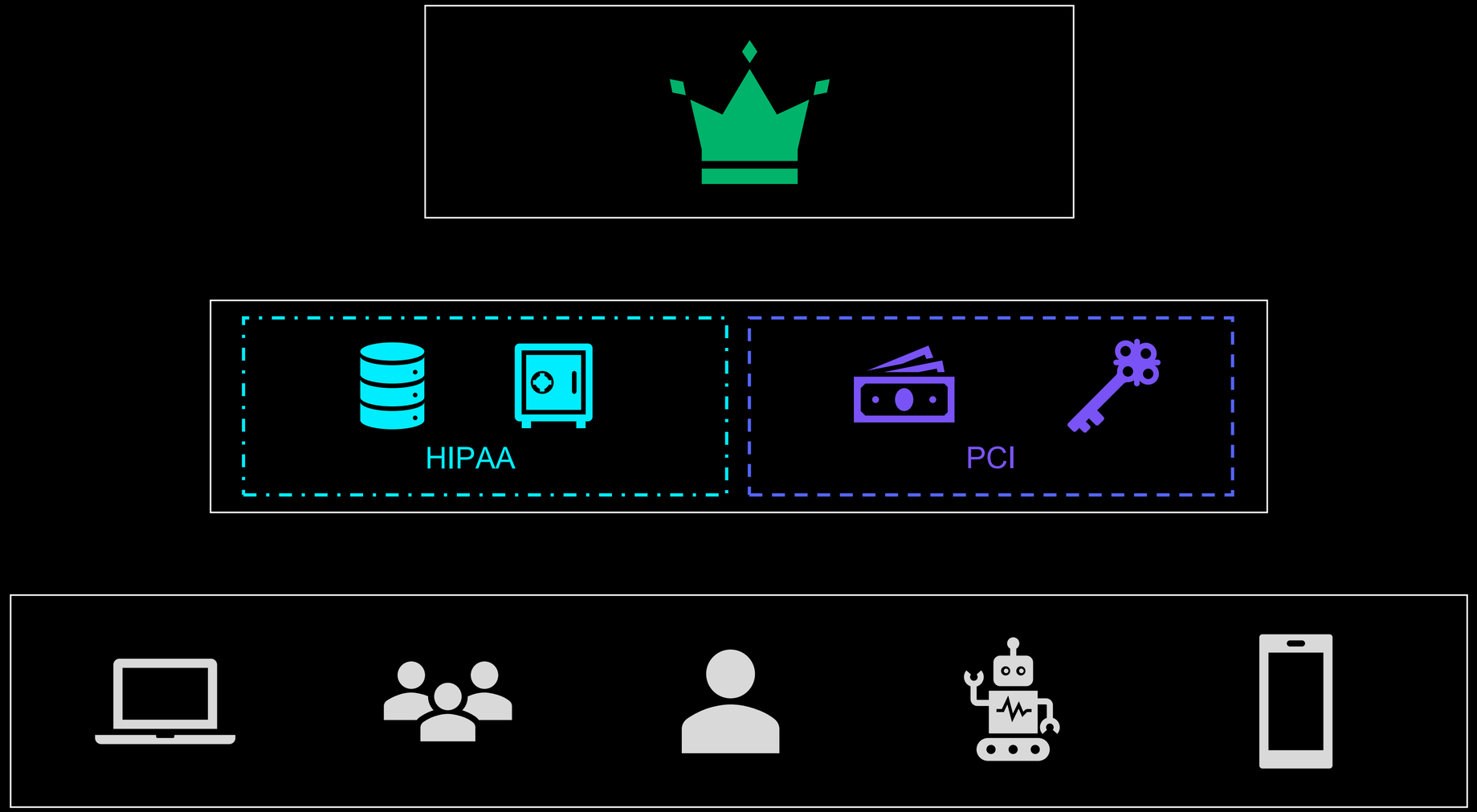
CrowdStrike 2025 Global Threat Report

*"**Restrict Administrator Privileges** to Dedicated Administrator Accounts"*

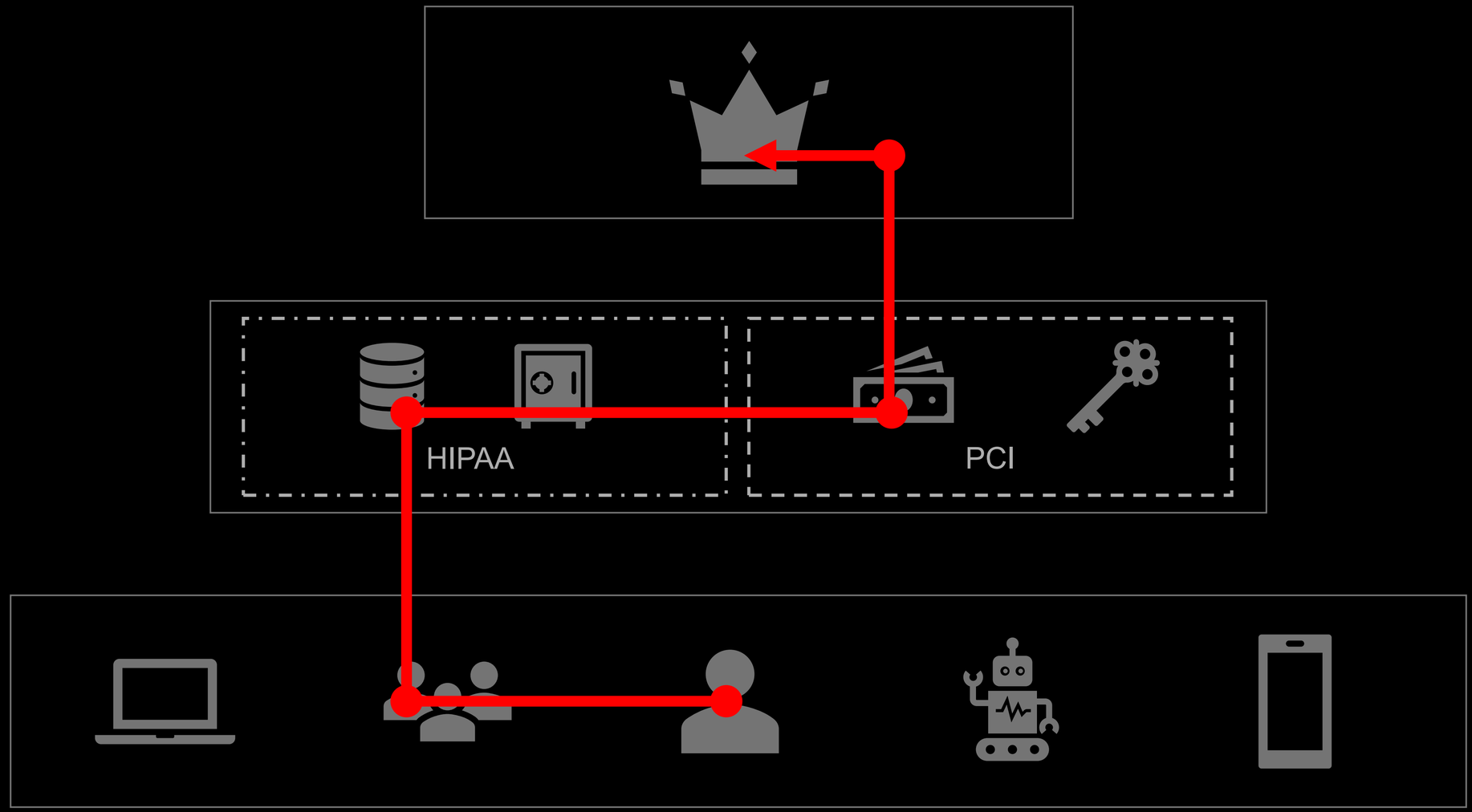
Verizon 2025 DBIR

*"Govern permissions to ensure identities have **only the privileges they need.**"*

Microsoft 2024 Digital Defense Report

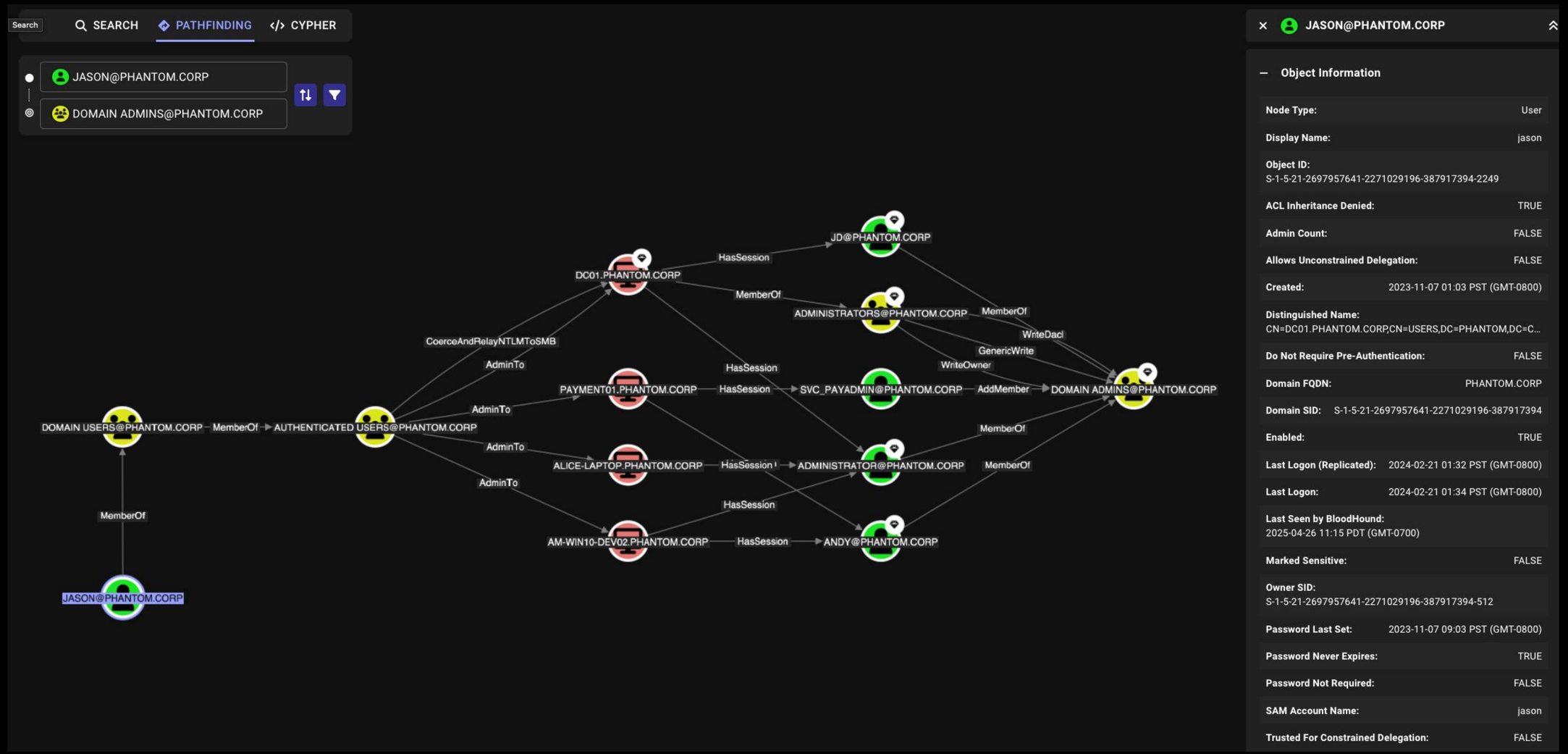

HIPAA
PCI

1. “Attack Path” is not a red team buzzword

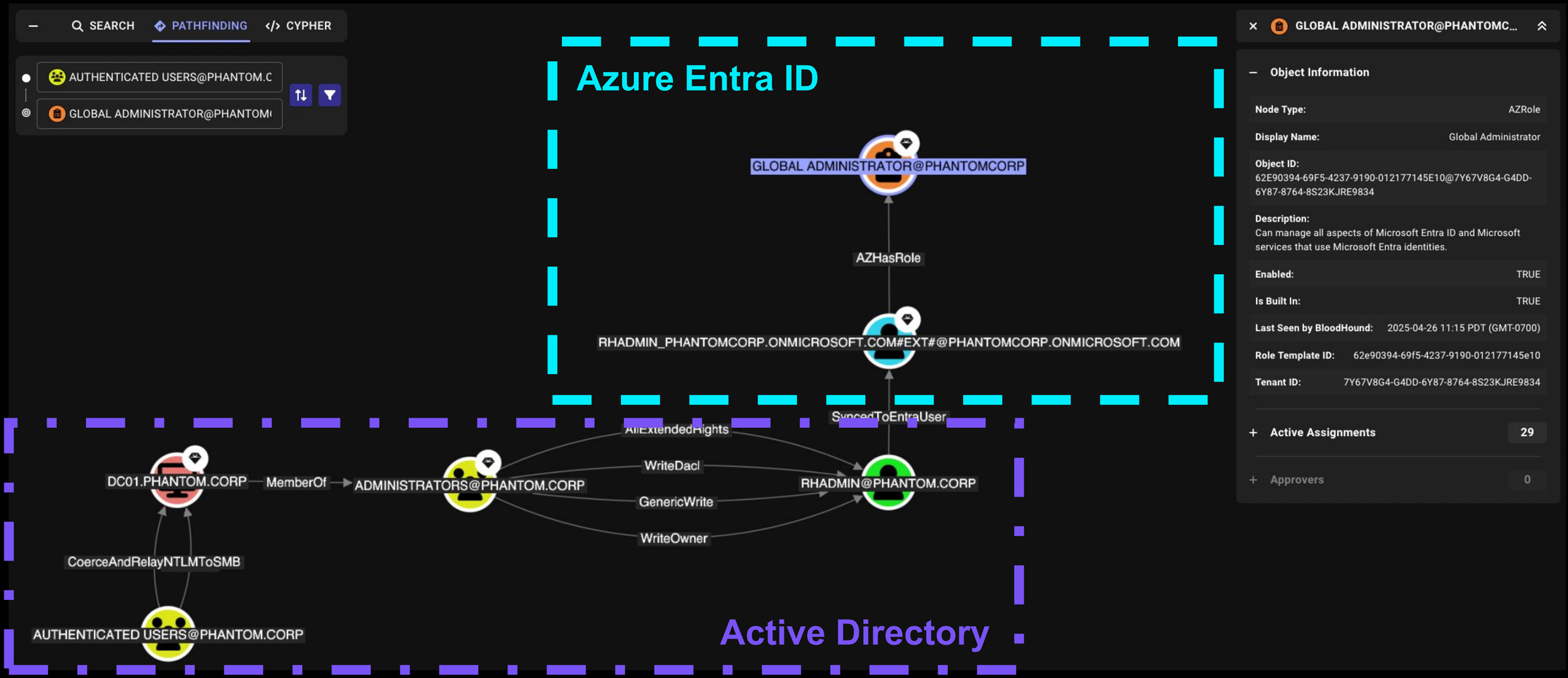


Attack Paths are violations/vulnerabilities of privilege boundaries

2. Use BloodHound to visualize Attack Paths

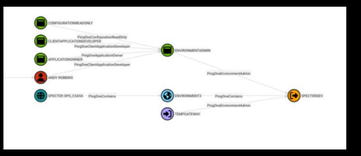


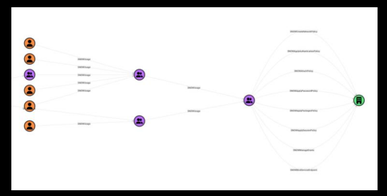
2. Use BloodHound to visualize Attack Paths



1Password

Microsoft

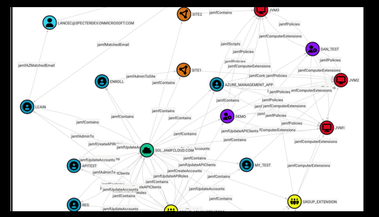


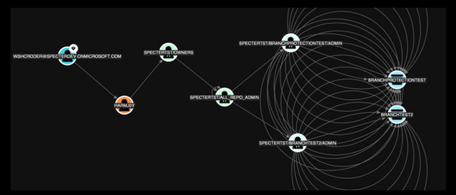


snowflake

BLOODHOUND
OpenGraph

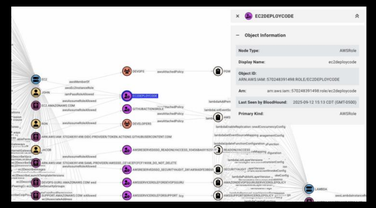
jamf



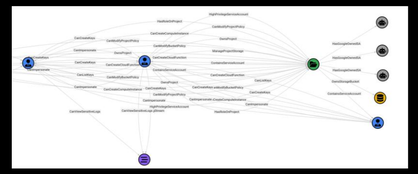


GitHub

aws

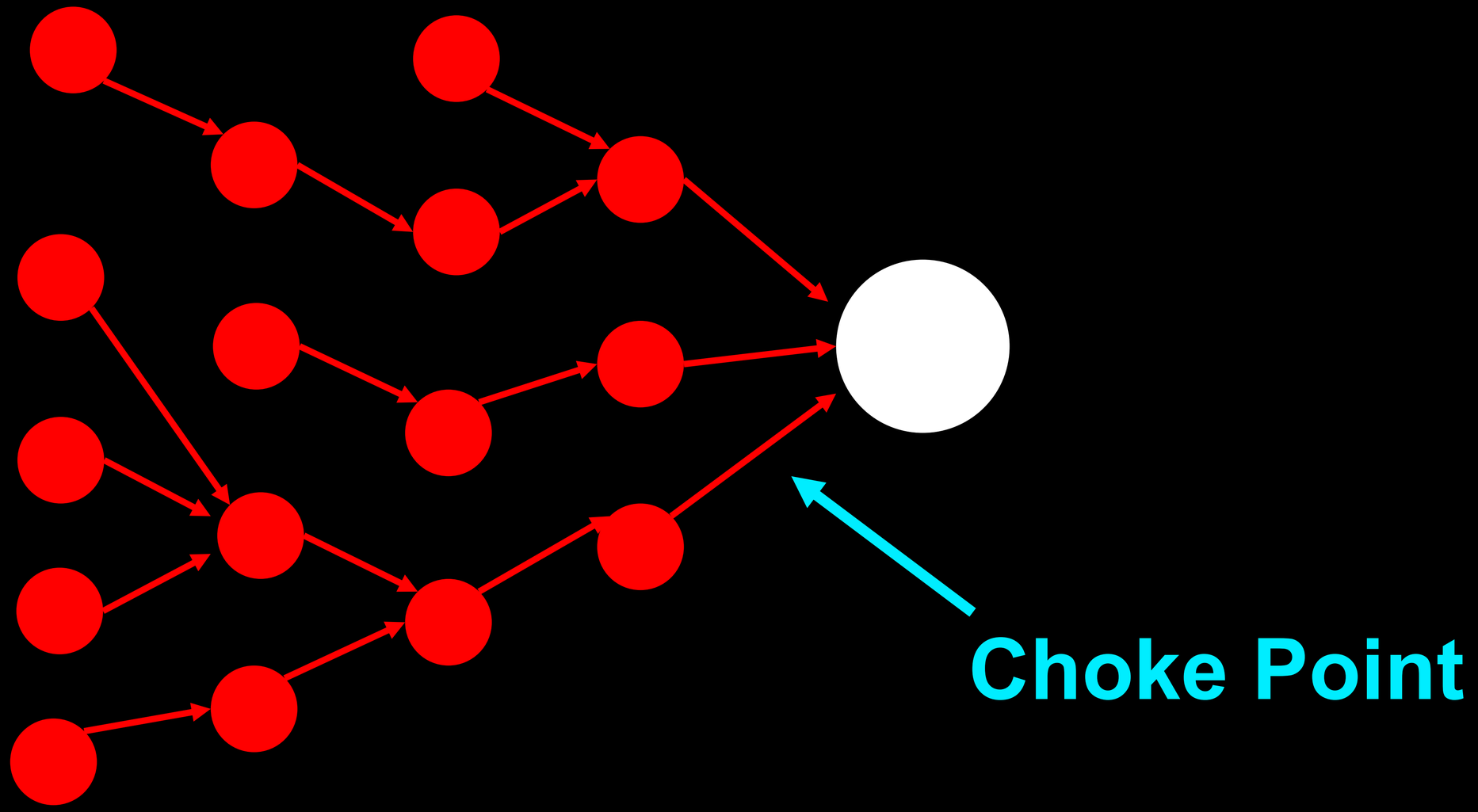


Google Cloud

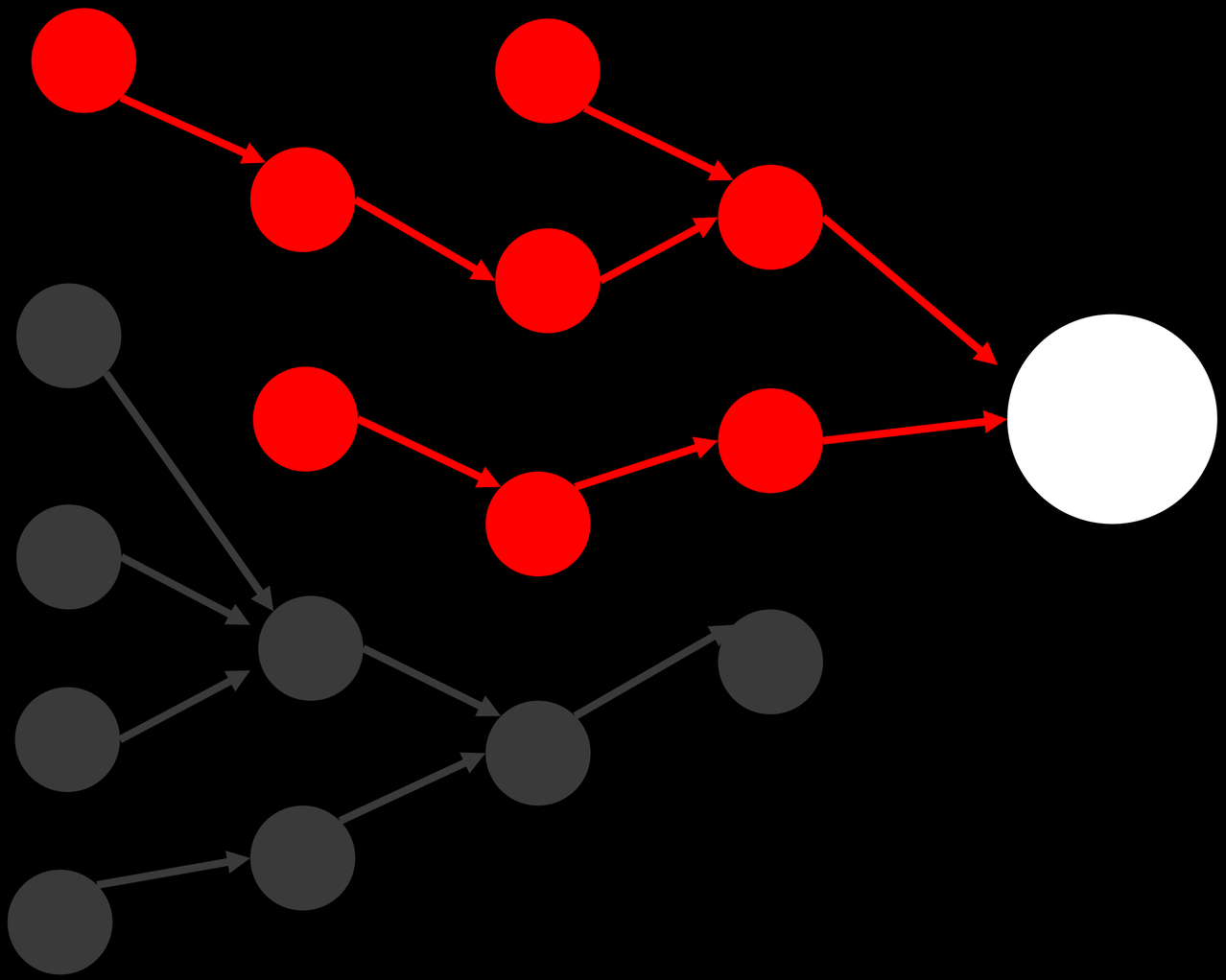


vmware
by Broadcom

3. Identify and Prioritize Attack Path Choke Points



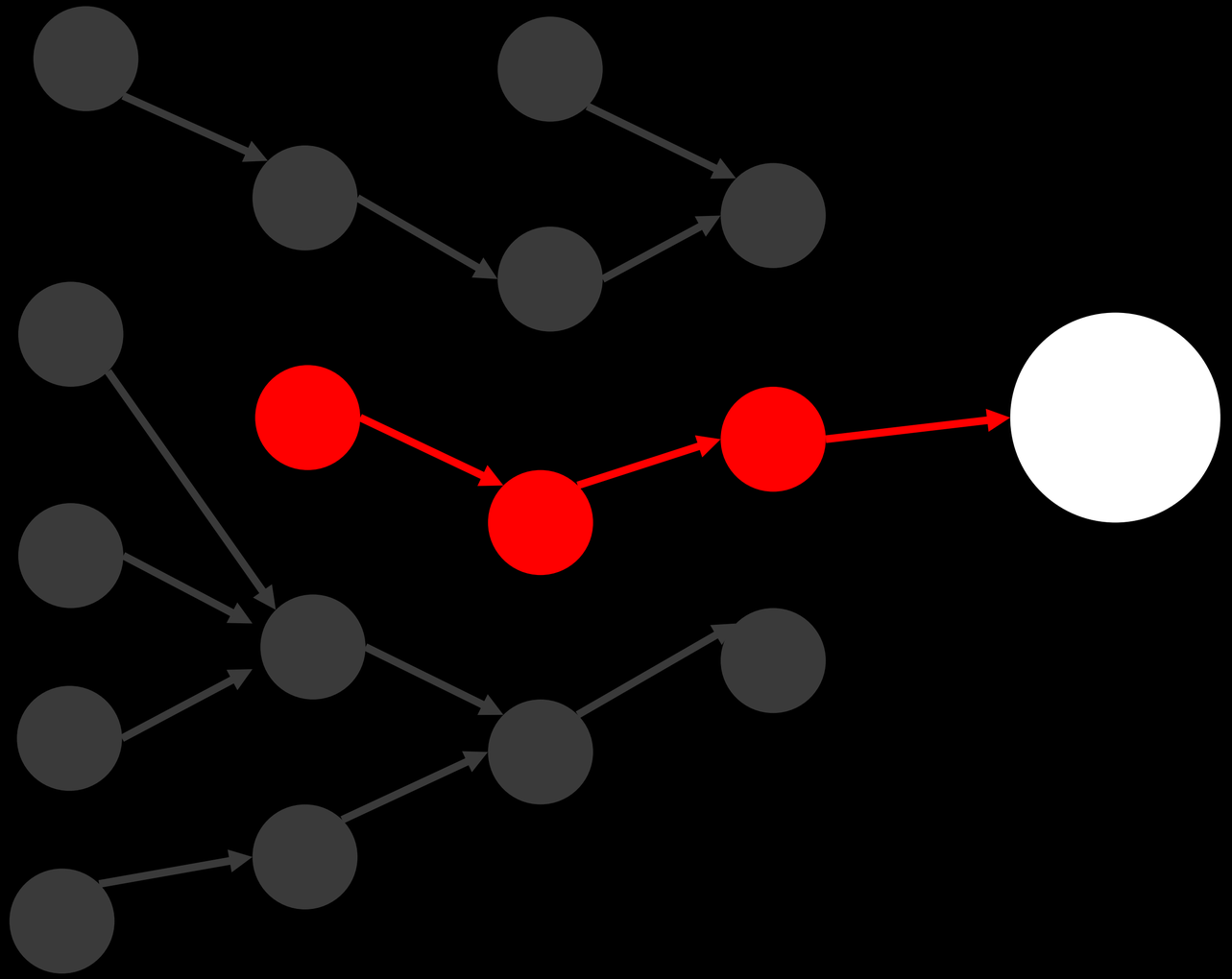
3. Identify and Prioritize Attack Path Choke Points



Attack Paths Removed:

8

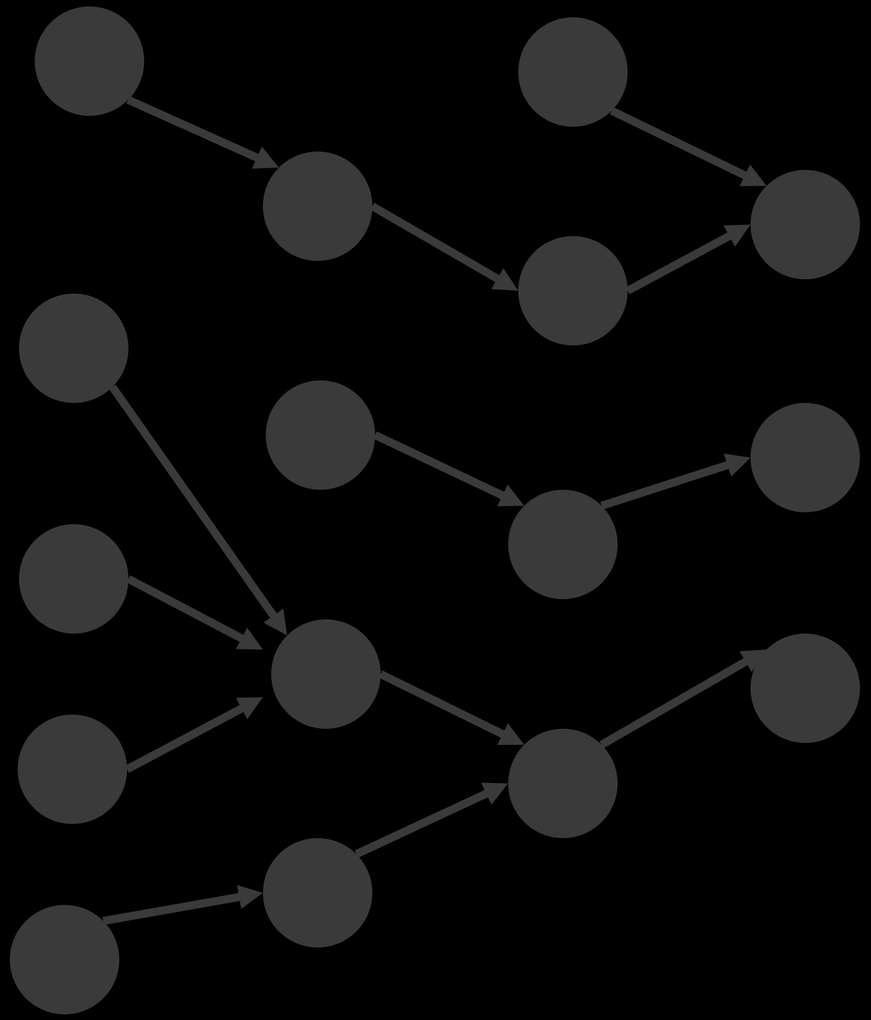
3. Identify and Prioritize Attack Path Choke Points

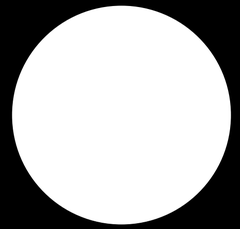


Attack Paths Removed:

13

3. Identify and Prioritize Attack Path Choke Points

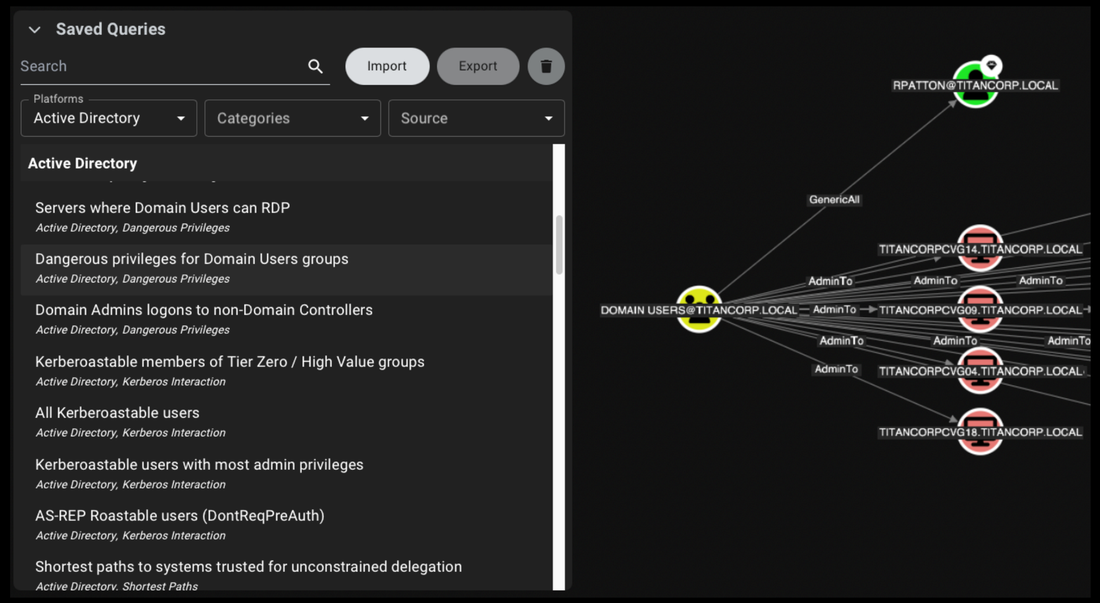


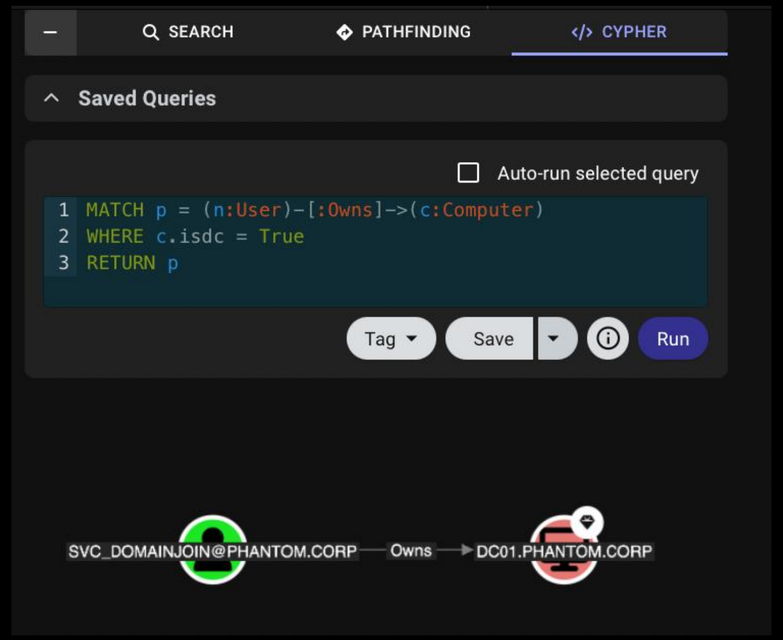


Attack Paths Removed:

16

3. Identify and Prioritize Attack Path Choke Points

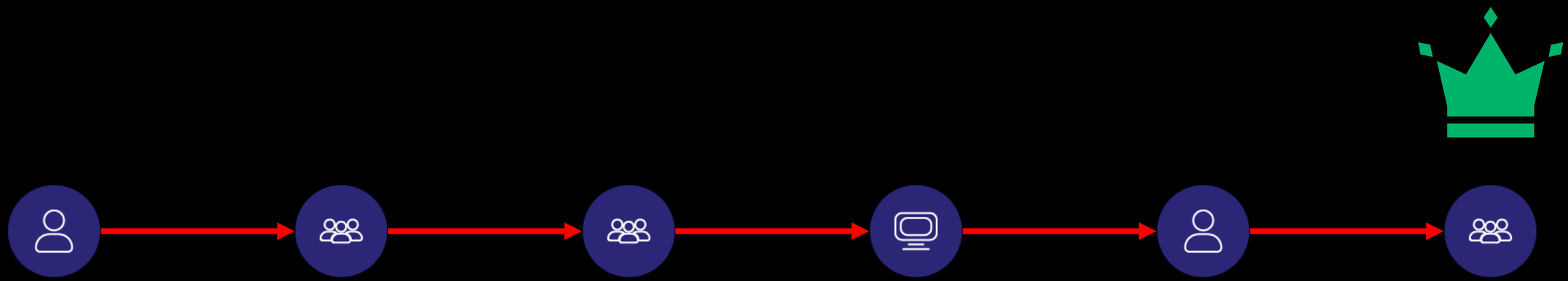




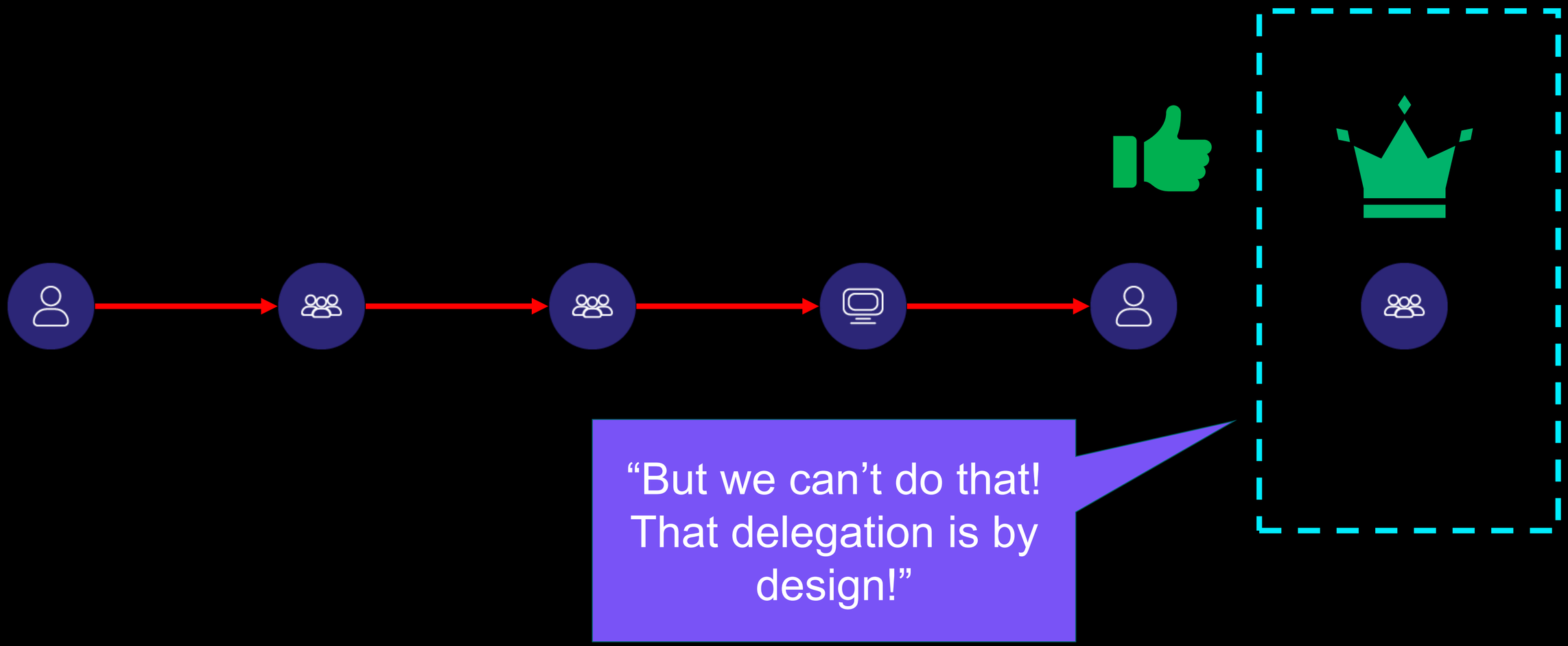
Initial Access Choke Points:
Privileges held by large groups

Destination Choke Points:
Privileges over critical identities and resources

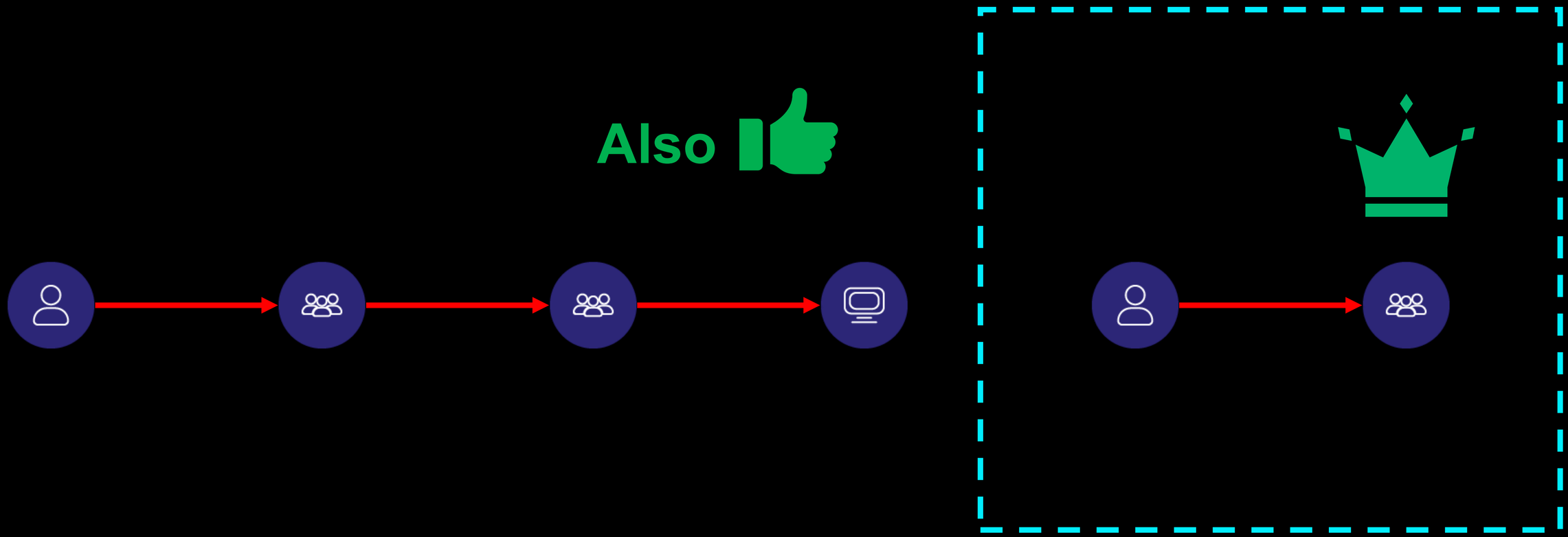
3. Identify and Prioritize Attack Path Choke Points



3. Identify and Prioritize Attack Path Choke Points



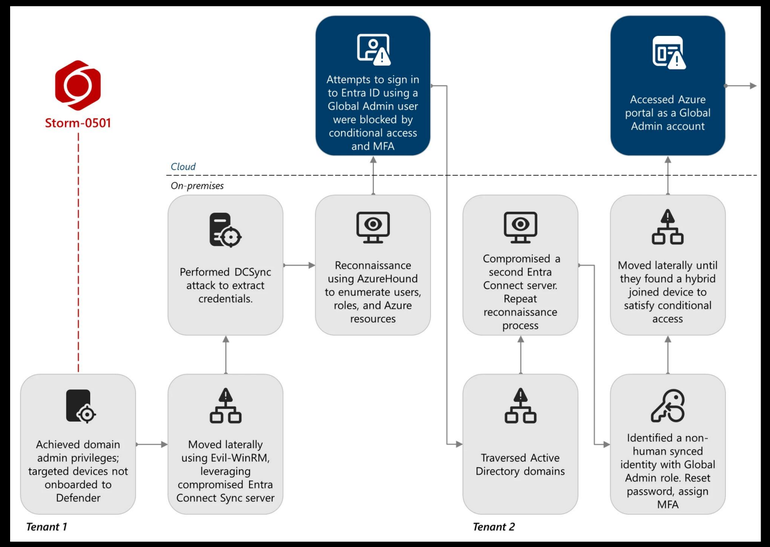
3. Identify and Prioritize Attack Path Choke Points



4. Once Established, Address Hybrid Attack Path Risk

Storm-0501's evolving techniques lead to cloud-based ransomware

By Microsoft Threat Intelligence

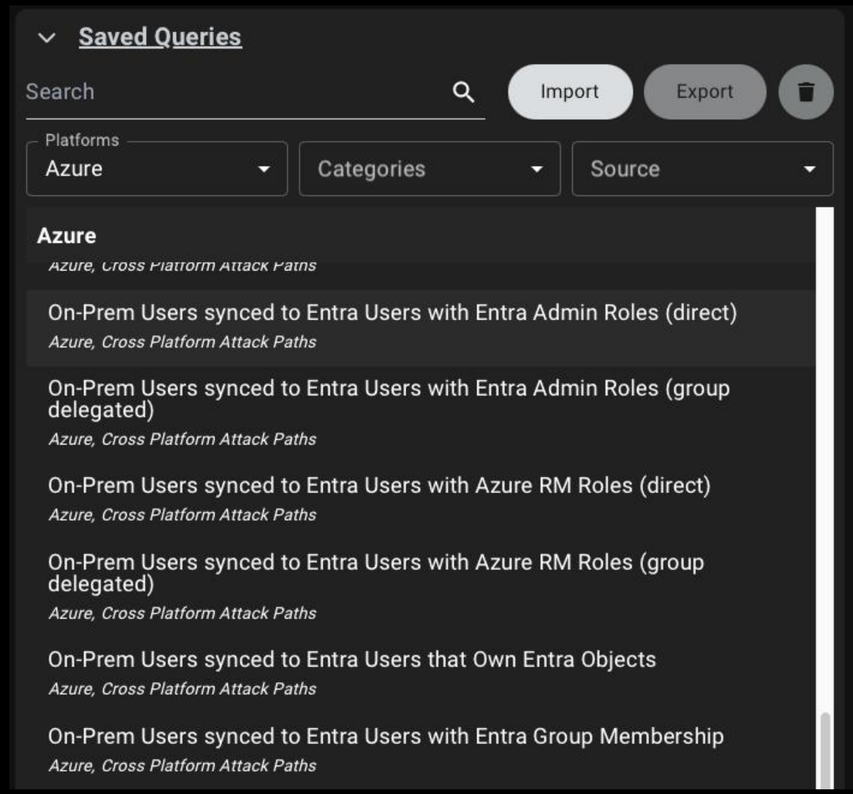


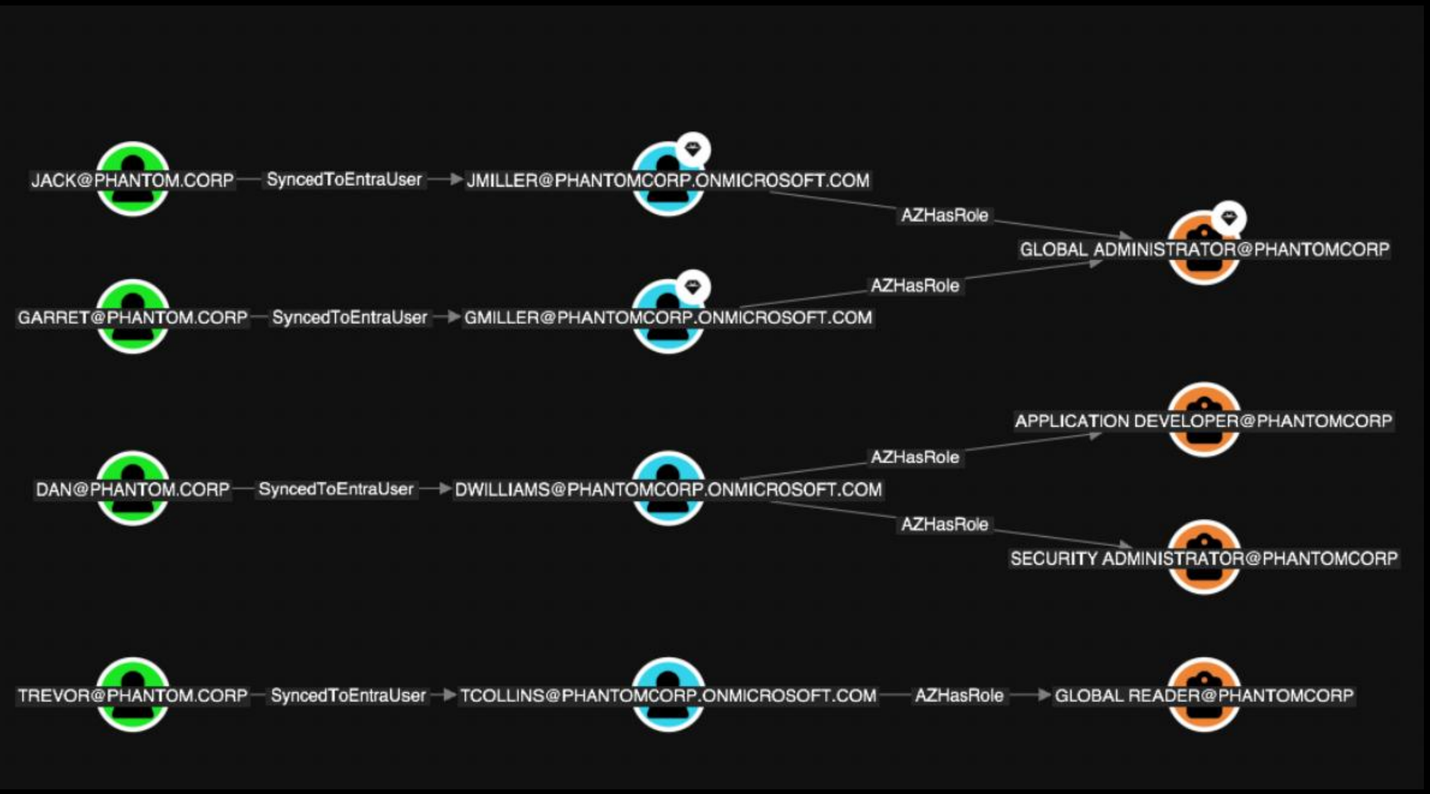
Ensure separate user accounts and mail forwarding for Global Administrator accounts

Personal email accounts are regularly phished by cyber attackers, a risk that makes personal email addresses unacceptable for Global Administrator accounts. To help separate internet risks from administrative privileges, create dedicated accounts for each user with administrative privileges.

- Be sure to create separate accounts for users to do Global Administrator tasks.
- Make sure that your Global Administrators don't accidentally open emails or run programs with their administrator accounts.
- Be sure those accounts have their email forwarded to a working mailbox.
- Global Administrator (and other privileged groups) accounts should be cloud-only accounts with no ties to on-premises Active Directory.

4. Once Established, Address Hybrid Attack Path Risk





6. Track Key Performance Indicators (KPIs)

Baseline

- # of attack paths to privileged identities
- # of Choke Points (findings)

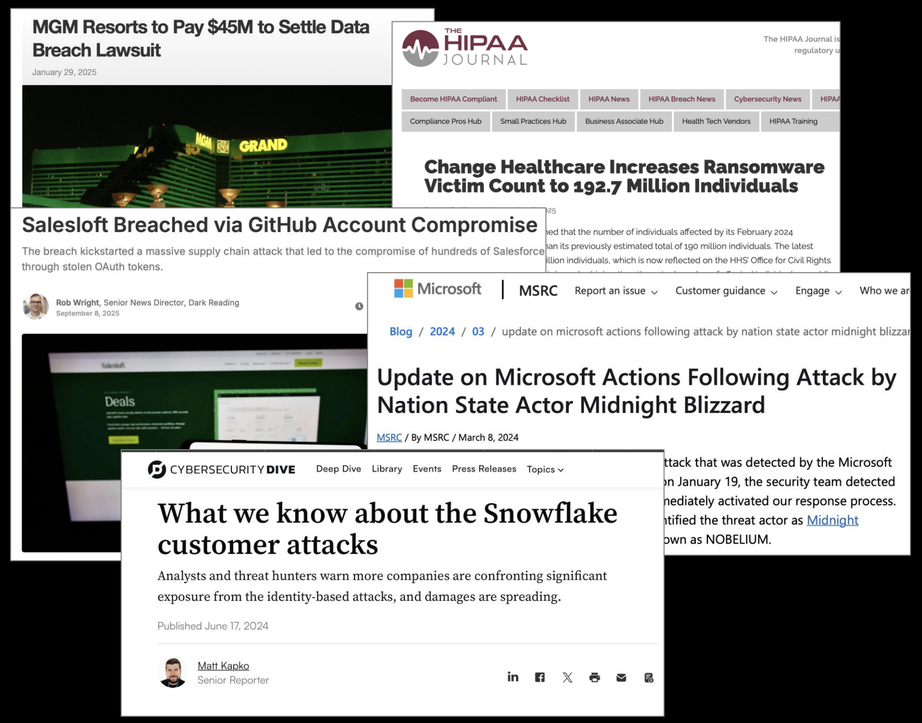
Remediations

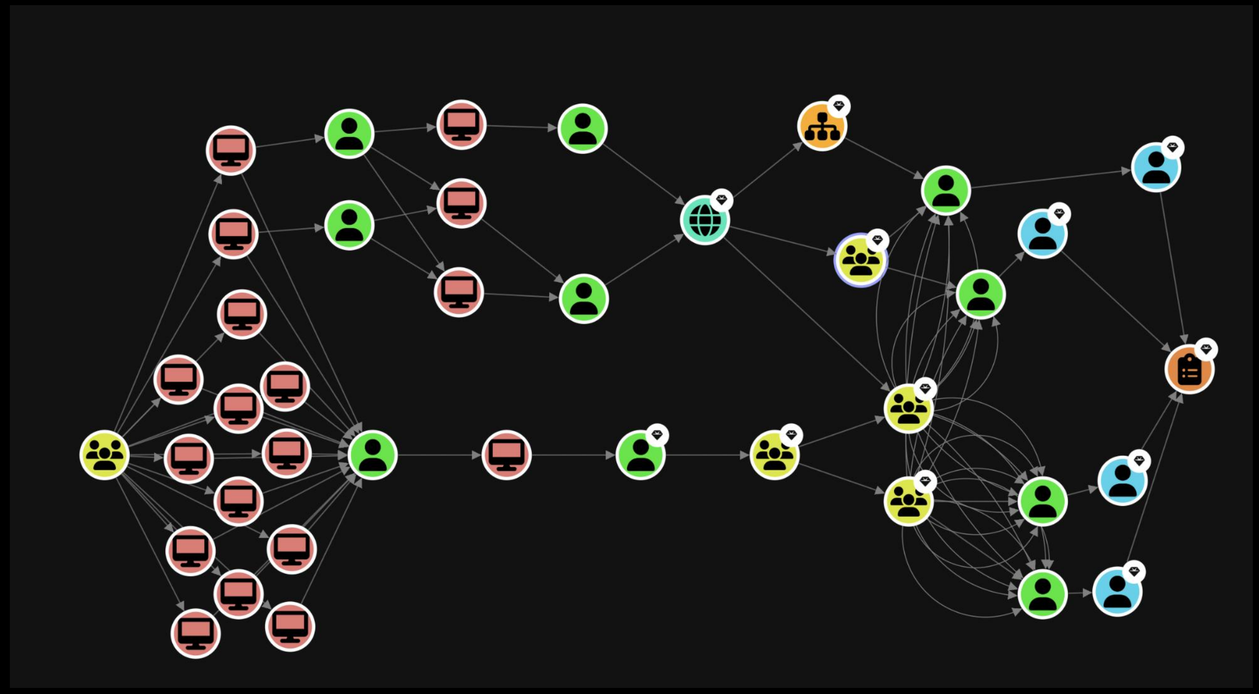
- # of resolved choke points
- # of resolved attack paths
- Remediation cycle time

Scope

- # of identities
- # of privileged identities
- # of relationships

Attackers see a map, do you?





"How did this happen?"

"How did this **[take so long to]** happen?"

1. Attackers bypass tools, not break them.

Even the strongest security stack (MFA, Conditional Access, EDR, PAM) can be sidestepped through *identity attack paths* across hybrid environments.

2. Identity Attack paths are the real risk surface.

Individual access or privilege decisions may look safe in isolation but combined they create *invisible collisions* that attackers exploit like the SalesLoft Breach

3. Attack Path Management is essential.

Treat attack paths as measurable, trackable risks. Use BloodHound Community Edition to get started **visualizing** attack paths, BloodHound Enterprise to **automatically identify choke points and remediate continuously**. What you can see, you can control.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Exposing Hidden Attack Paths:
How Threats Get Past Your Best Defenses

Questions?