SentinelOne®

XDR meets Identity Threat Detection and Response

Speaker

Thomas Drews – Solution Engineer, Central Europe

Attackers Target Enterprise Identity Data

65%

of users use the **same password** on multiple accounts

(Google 2019 security survey)

80%

of web application breaches were attributed to **credential theft**

(Verizon 2022 Data Breach Investigation Report)

63%

of social engineering attacks compromised credential data

(Verizon 2022 Data Breach Investigation Report)

50%

of businesses suffered **AD attacks** in the last 2 years

(EMA Research AD is Under Siege 2021)

42%

of the attacks on AD **were successful**

(EMA Research AD is Under Siege 2021)

86%

of surveyed businesses plan to **increase AD security funding**

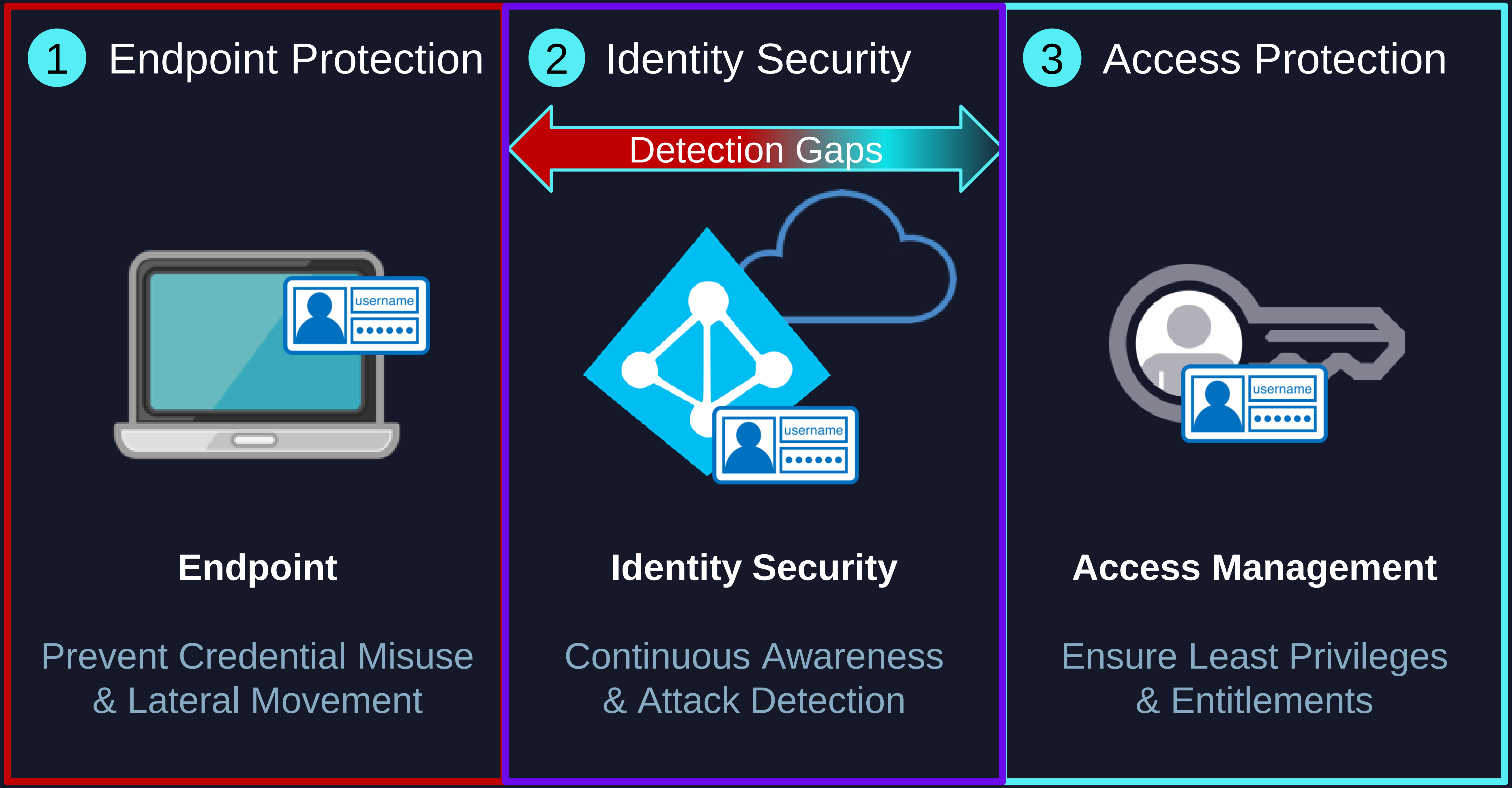
(EMA Research AD is Under Siege 2021)

Gartner considers Identity-first Security a top trend and points out that misused credentials are now the top technique used in breaches.

(Gartner Top Security and Risk Trends for 2021)

Traditional Defenses Don’t Protect Identities

Credentials, privileges, and the systems that manage them (AD)



1 Endpoint Protection

2 Identity Security

3 Access Protection

Detection Gaps

Endpoint

Prevent Credential Misuse & Lateral Movement

Identity Security

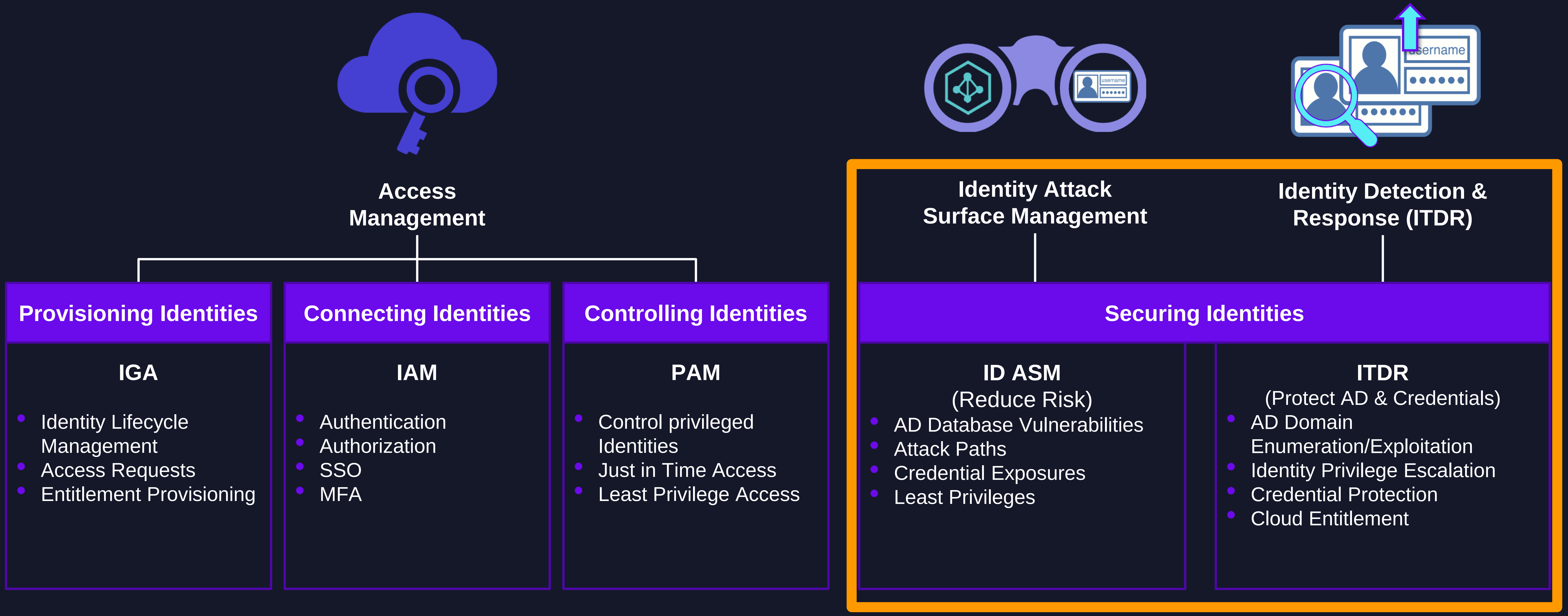
Continuous Awareness & Attack Detection

Access Management

Ensure Least Privileges & Entitlements

Identity Protection

IAM, PAM, IGA + ID Attack Surface Management & Identity Threat Detection & Response (ITDR)



Access Management

Provisioning Identities

IGA

- Identity Lifecycle Management
- Access Requests
- Entitlement Provisioning

Connecting Identities

IAM

- Authentication
- Authorization
- SSO
- MFA

Controlling Identities

PAM

- Control privileged Identities
- Just in Time Access
- Least Privilege Access

Identity Attack Surface Management

Identity Detection & Response (ITDR)

Securing Identities

ID ASM
(Reduce Risk)

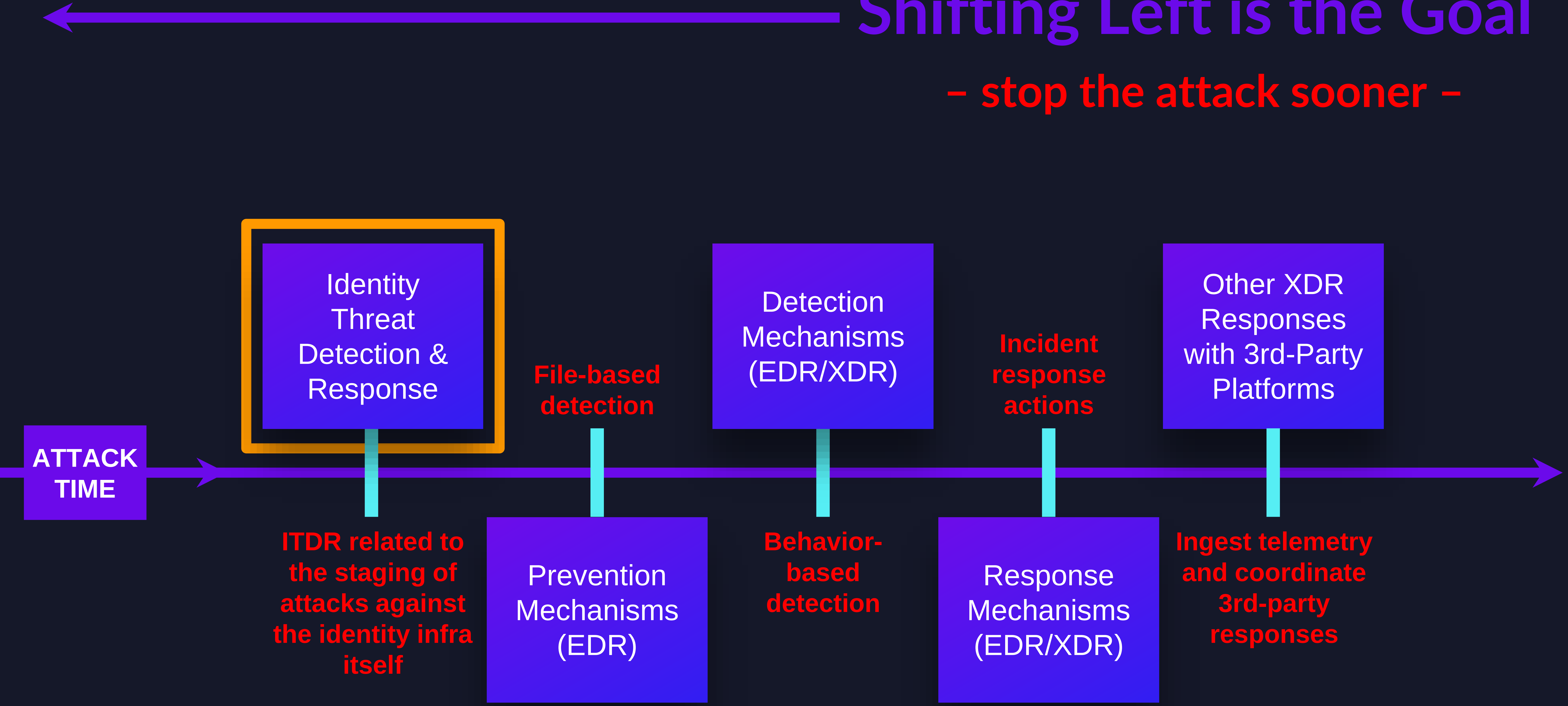
- AD Database Vulnerabilities
- Attack Paths
- Credential Exposures
- Least Privileges

ITDR
(Protect AD & Credentials)

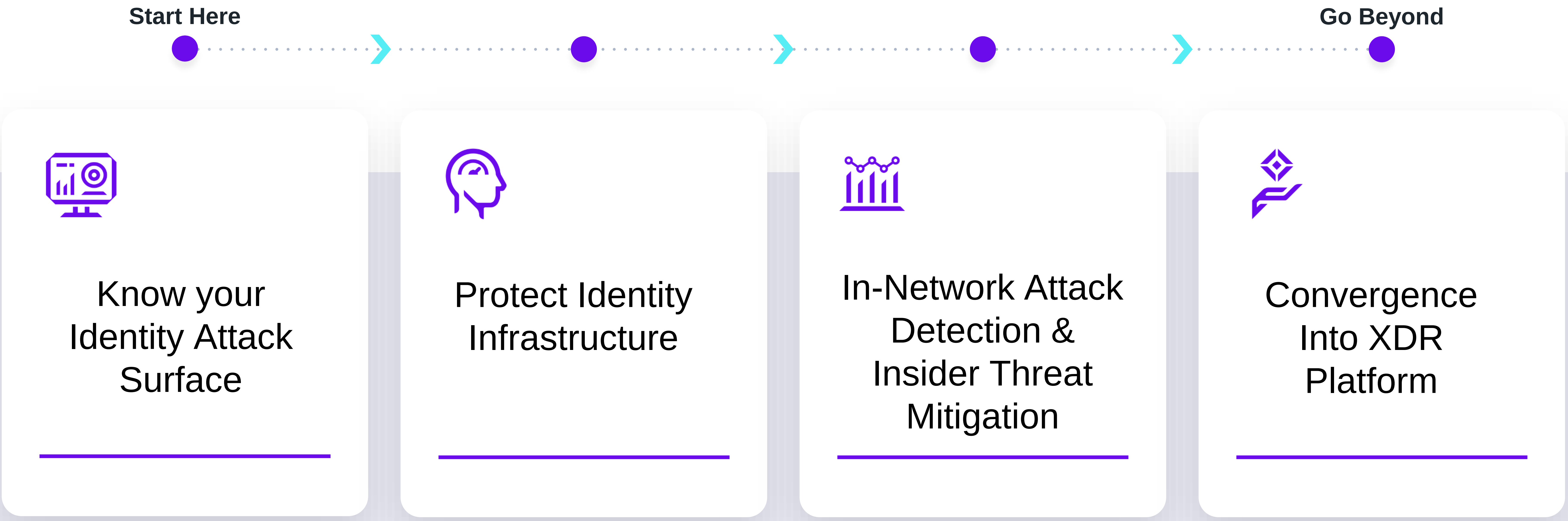
- AD Domain Enumeration/Exploitation
- Identity Privilege Escalation
- Credential Protection
- Cloud Entitlement

Shifting Left is the Goal

– stop the attack sooner –


ATTACK TIME
Identity Threat Detection & Response
ITDR related to the staging of attacks against the identity infra itself
File-based detection
Prevention Mechanisms (EDR)
Detection Mechanisms (EDR/XDR)
Behavior-based detection
Incident response actions
Response Mechanisms (EDR/XDR)
Other XDR Responses with 3rd-Party Platforms
Ingest telemetry and coordinate 3rd-party responses

Identity Security Recommendations



Start Here

Go Beyond

Know your Identity Attack Surface

Protect Identity Infrastructure

In-Network Attack Detection & Insider Threat Mitigation

Convergence Into XDR Platform

Visibility into AD Exposures

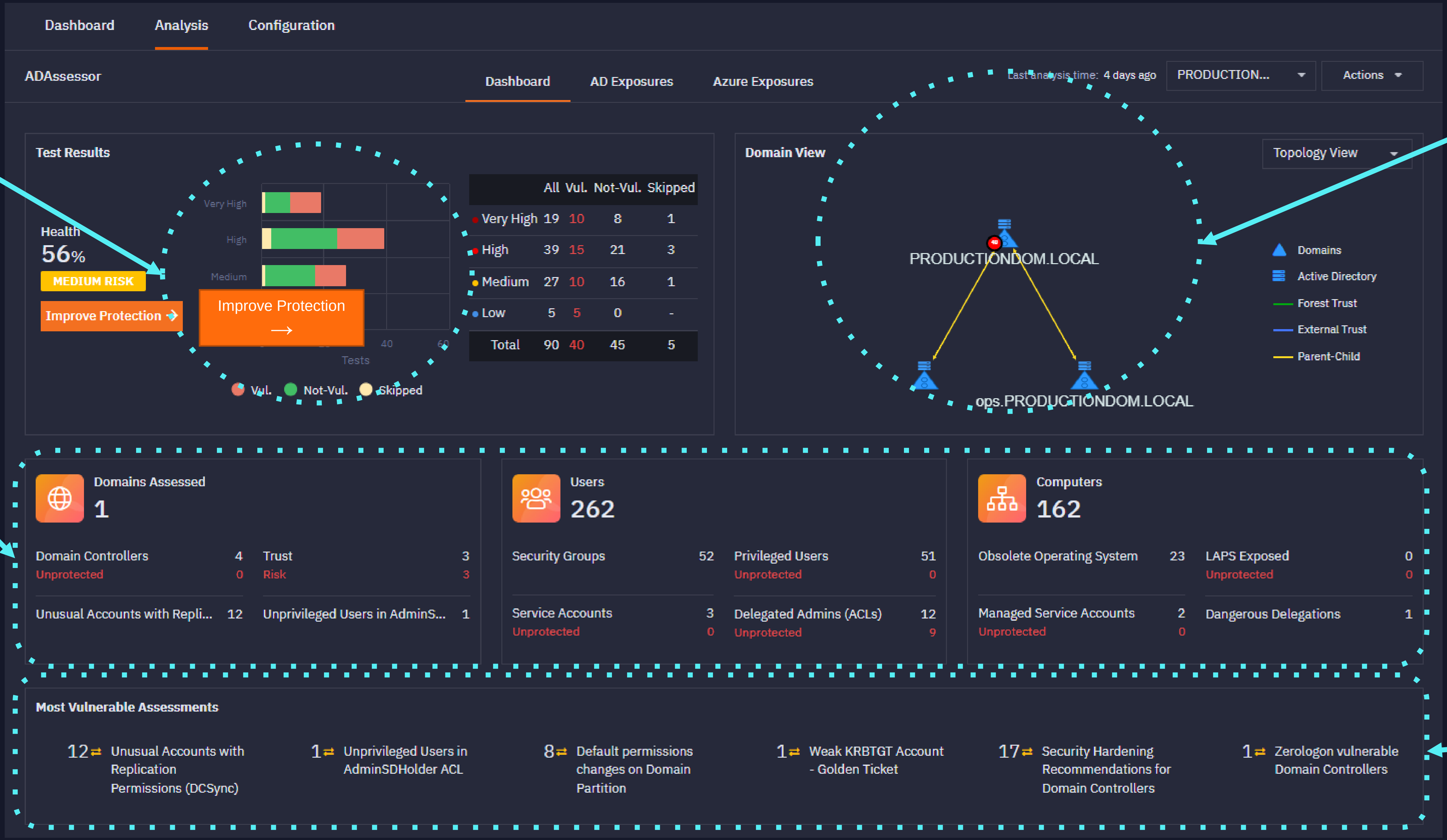
Continuous Assessment and Enforcement of Privileged Access

Health Score

Test Results
Domain, User, Computer

Trust View

Most Vulnerable Assessments



Health
56%
MEDIUM RISK
Improve Protection

	All	Vul.	Not-Vul.	Skipped
● Very High	19	10	8	1
● High	39	15	21	3
● Medium	27	10	16	1
● Low	5	5	0	-
Total	90	40	45	5

Domains Assessed
1

Domain Controllers Unprotected	4 0	Trust Risk	3 3
Unusual Accounts with Repli...	12	Unprivileged Users in AdminS...	1

Users
262

Security Groups	52	Privileged Users Unprotected	51 0
Service Accounts Unprotected	3 0	Delegated Admins (ACLs) Unprotected	12 9

Computers
162

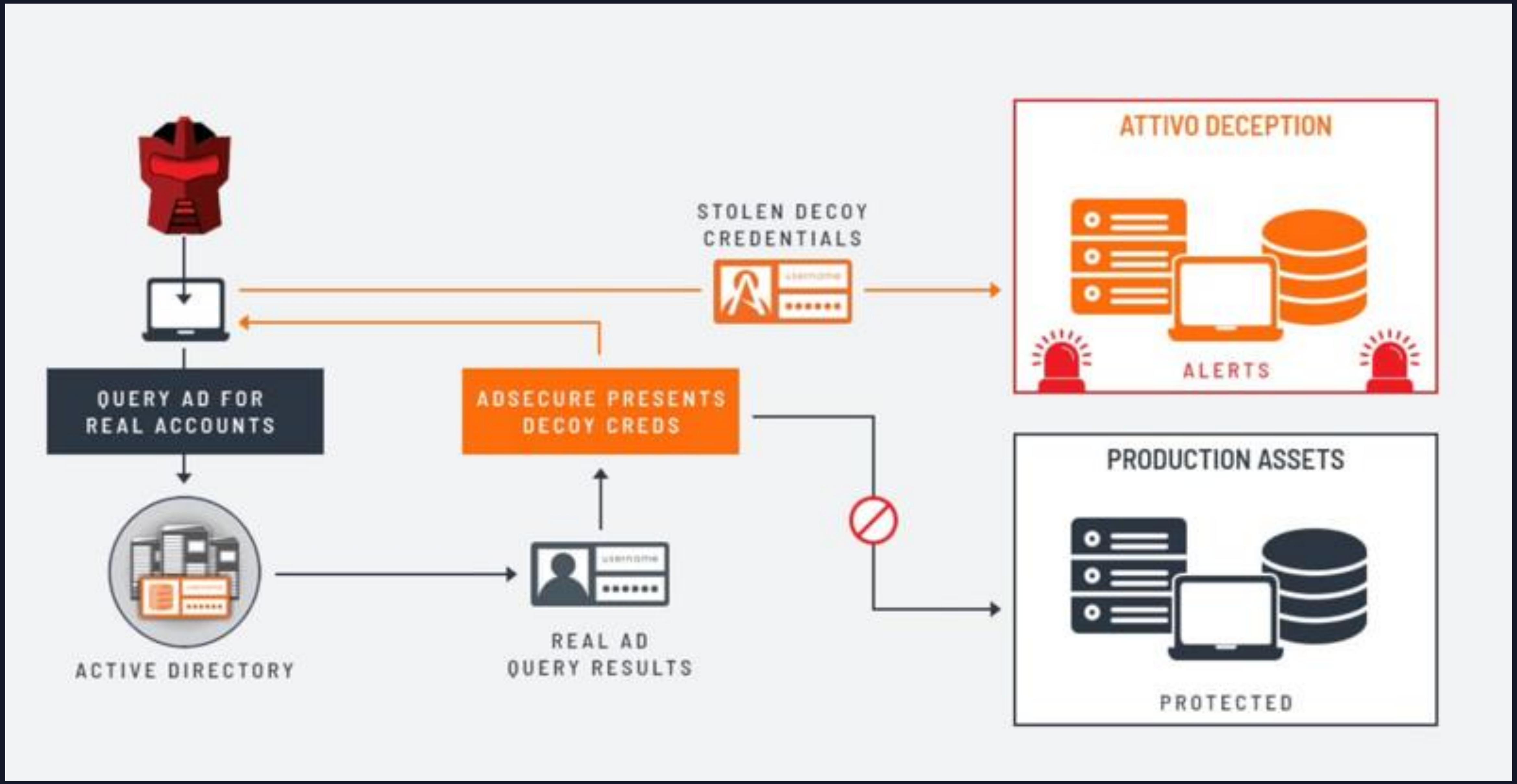
Obsolete Operating System	23	LAPS Exposed Unprotected	0 0
Managed Service Accounts Unprotected	2 0	Dangerous Delegations	1

Most Vulnerable Assessments

12 ⇄	Unusual Accounts with Replication Permissions (DCSync)
1 ⇄	Unprivileged Users in AdminSDHolder ACL
8 ⇄	Default permissions changes on Domain Partition
1 ⇄	Weak KRBTGT Account - Golden Ticket
17 ⇄	Security Hardening Recommendations for Domain Controllers
1 ⇄	Zerologon vulnerable Domain Controllers

Endpoint AD Attack Detection / Misdirection

Detect Attacker Activity, Misdirect from Production Assets



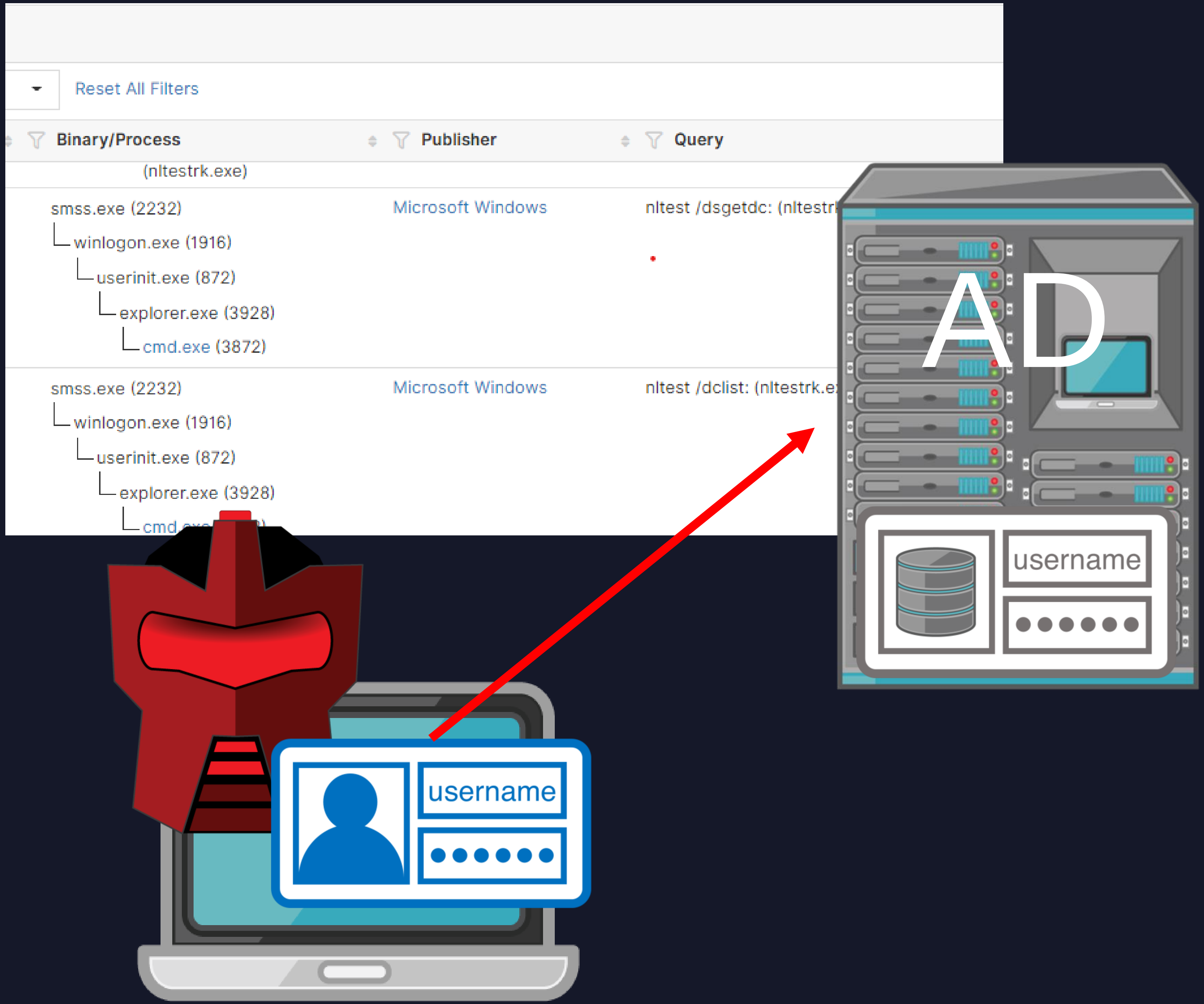
- Hides info, protect critical objects
- Returns deceptive objects
- Fake data steers attackers to decoys
- Telemetry for visibility & hunting

* Supports all AD objects (admin, service, critical computers, net sessions)

Live AD Attack Detection/Prevention

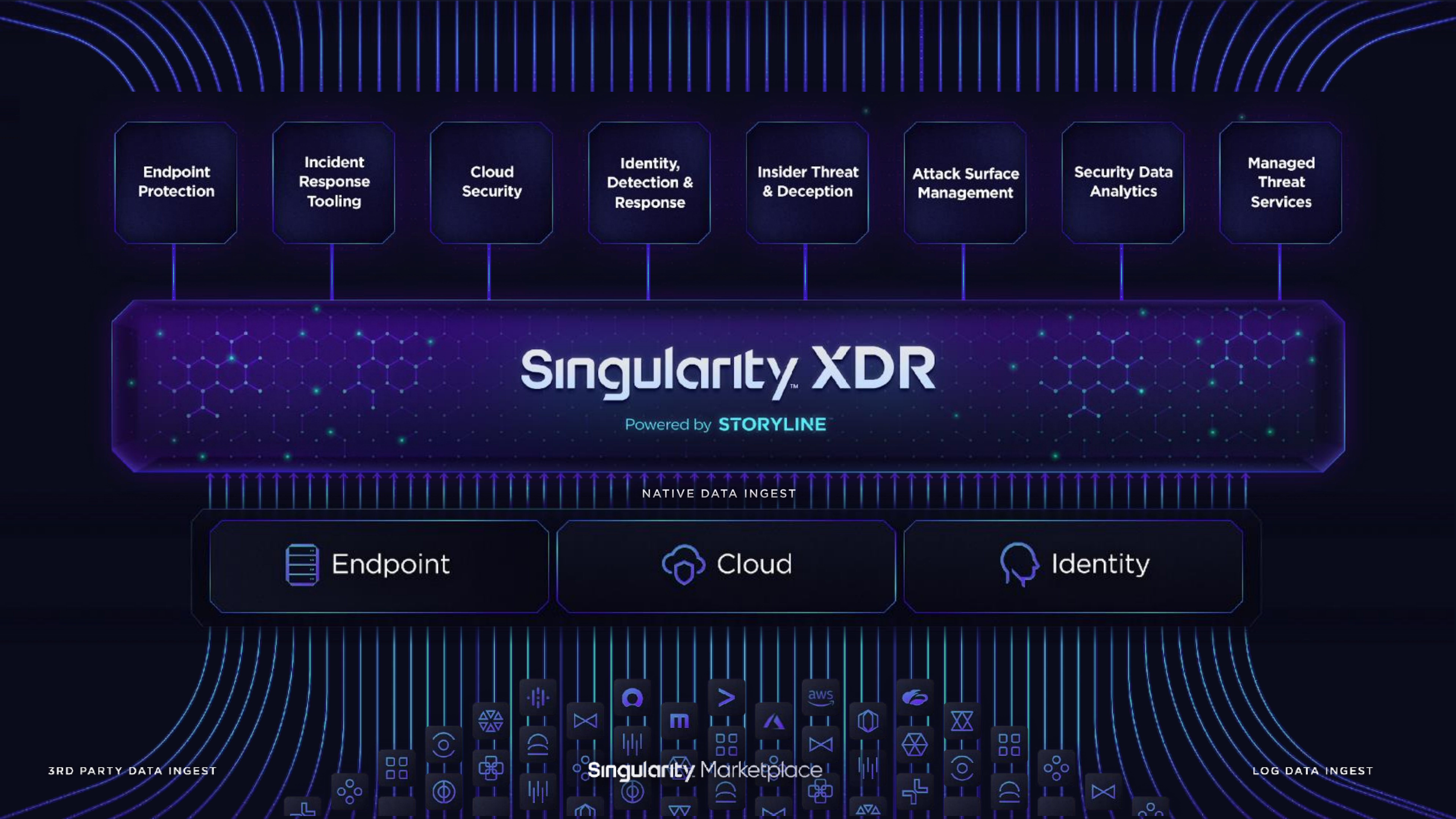
See and Respond to Domain Controller Attacks

- Golden Ticket or Silver Ticket attacks
- DCSync or DCShadow attacks
- Pass-the-Ticket and Pass-the-Hash Attacks
- Recon of Privileged and Service Accounts
- Skeleton Key Attacks
- Forged PAC Attacks
- AS REP Roasting Attacks



Reset All Filters

Binary/Process	Publisher	Query
(nltestrk.exe)		
smss.exe (2232) └winlogon.exe (1916) └userinit.exe (872) └explorer.exe (3928) └cmd.exe (3872)	Microsoft Windows	nltest /dsgetdc: (nltestr
smss.exe (2232) └winlogon.exe (1916) └userinit.exe (872) └explorer.exe (3928) └cmd	Microsoft Windows	nltest /dclist: (nltestrk.e



Endpoint Protection

Incident Response Tooling

Cloud Security

Identity, Detection & Response

Insider Threat & Deception

Attack Surface Management

Security Data Analytics

Managed Threat Services

Singularity™ XDR

Powered by STORYLINE

NATIVE DATA INGEST

Endpoint

Cloud

Identity

3RD PARTY DATA INGEST

Singularity Marketplace

LOG DATA INGEST

Thank You!

Sie finden uns in Halle 7, Stand 306

SentinelOne®

sentinelone.com