

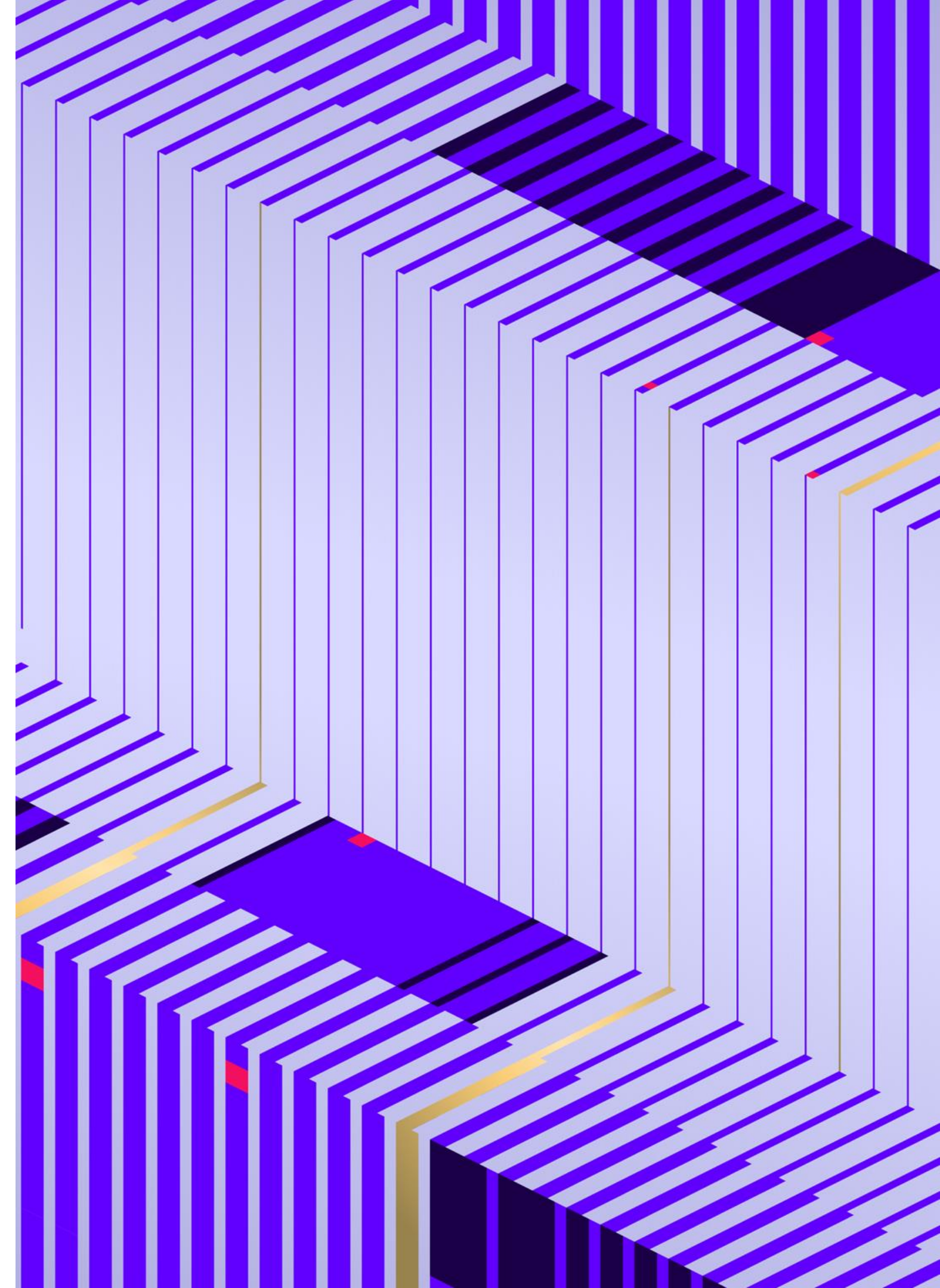
Comment déjouer plus efficacement les attaques visant les identités ?



Samuel Pages
Associate Solutions Engineer
SentinelOne



François Baraër
Staff Solutions Engineer
SentinelOne



Agenda

- Understanding Identity Risks
- Goals of Identity Protection
- Identity - Part of the Singularity Platform
- Identity Security Recommendations
- Q & A

Identity Security Challenges



Rapid
enterprise
identity
expansion



Attackers
using
advanced
techniques



Poor identity
security
hygiene
(AD/Entra ID)



Privileged
identity
management
issues

Attackers Target Identity Data

Credentials and AD are High Priority Targets

\$4.62M

the average cost of a breach due to **compromised credentials**

(IBM 2023 Cost of a Data Breach Report)

328 days

to **identify and contain** a breach due to stolen creds (longest)

(IBM 2023 Cost of a Data Breach Report)

37%

of 2023 breaches **involved credentials** (#1 entry point)

(Verizon 2024 Data Breach Investigation Report)

31%

of 2013-23 breaches, attackers **stole credentials** (#1 stolen data)

(Verizon 2024 Data Breach Investigation Report)

90%

of orgs experienced an **identity-related breach** in the past year

(IDSA 2023 Trends in Securing Digital Identities)

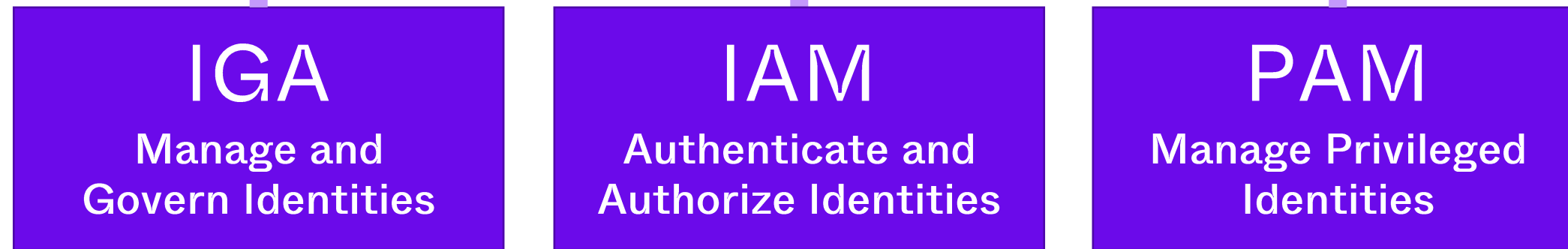
68%

orgs had a business impact from an **identity-related incident**

(IDSA 2023 Trends in Securing Digital Identities)

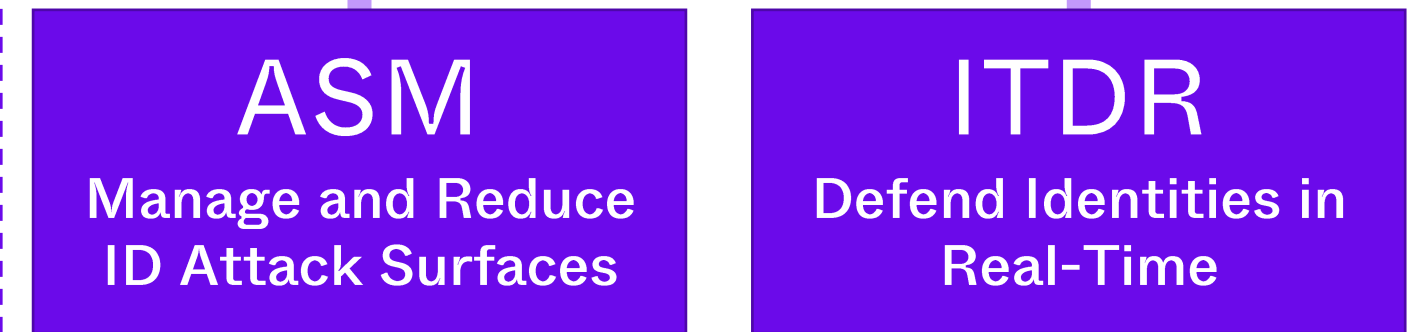
Identity Defense Solutions

Access Security



Protects Access, not Identities

Identity Security



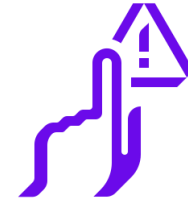
Identity Security Goals



Reduce
Attacker
Opportunities
to Succeed



Find Attackers
Early Before They
Exploit Identities

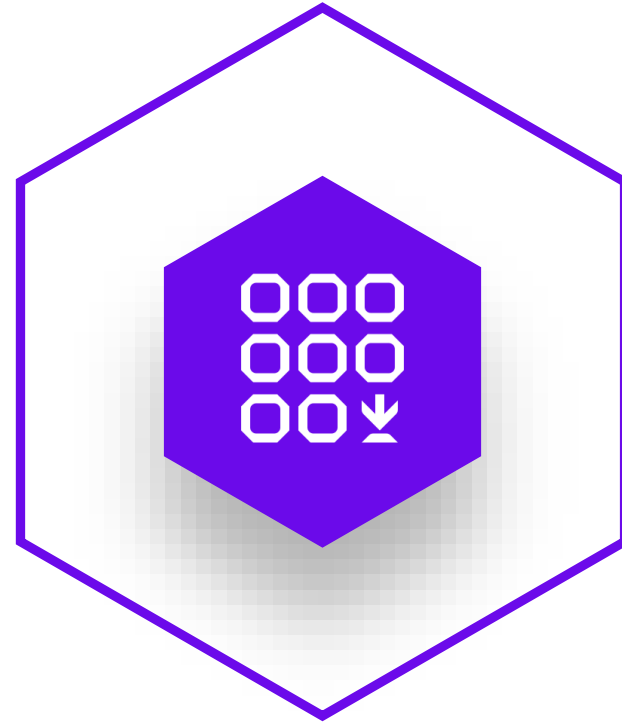


Disrupt
Attackers from
Misusing
Identities



Make Identity a
Pillar of the
Security Strategy

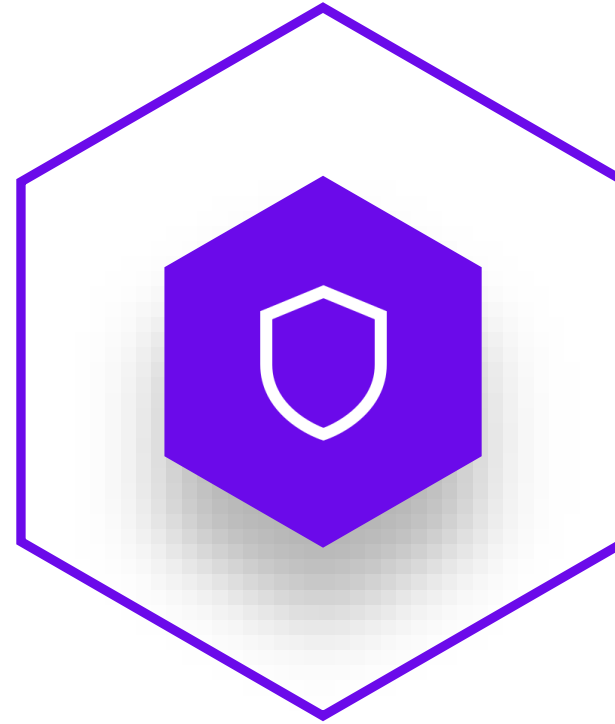
Introduction to Singularity Identity



ISPM

Identity Security Posture Management

- Installs on 1 domain-joined endpoint
- Remediation of detected vulnerabilities
- Proactive alerts on misconfiguration and exposures



IDP

Identity Provider

- Installs on Domain Controllers
- Protects against attacks to AD regardless of source
- Employs deep packet inspection and analysis of AD logs



IDR

Identity Detection & Response

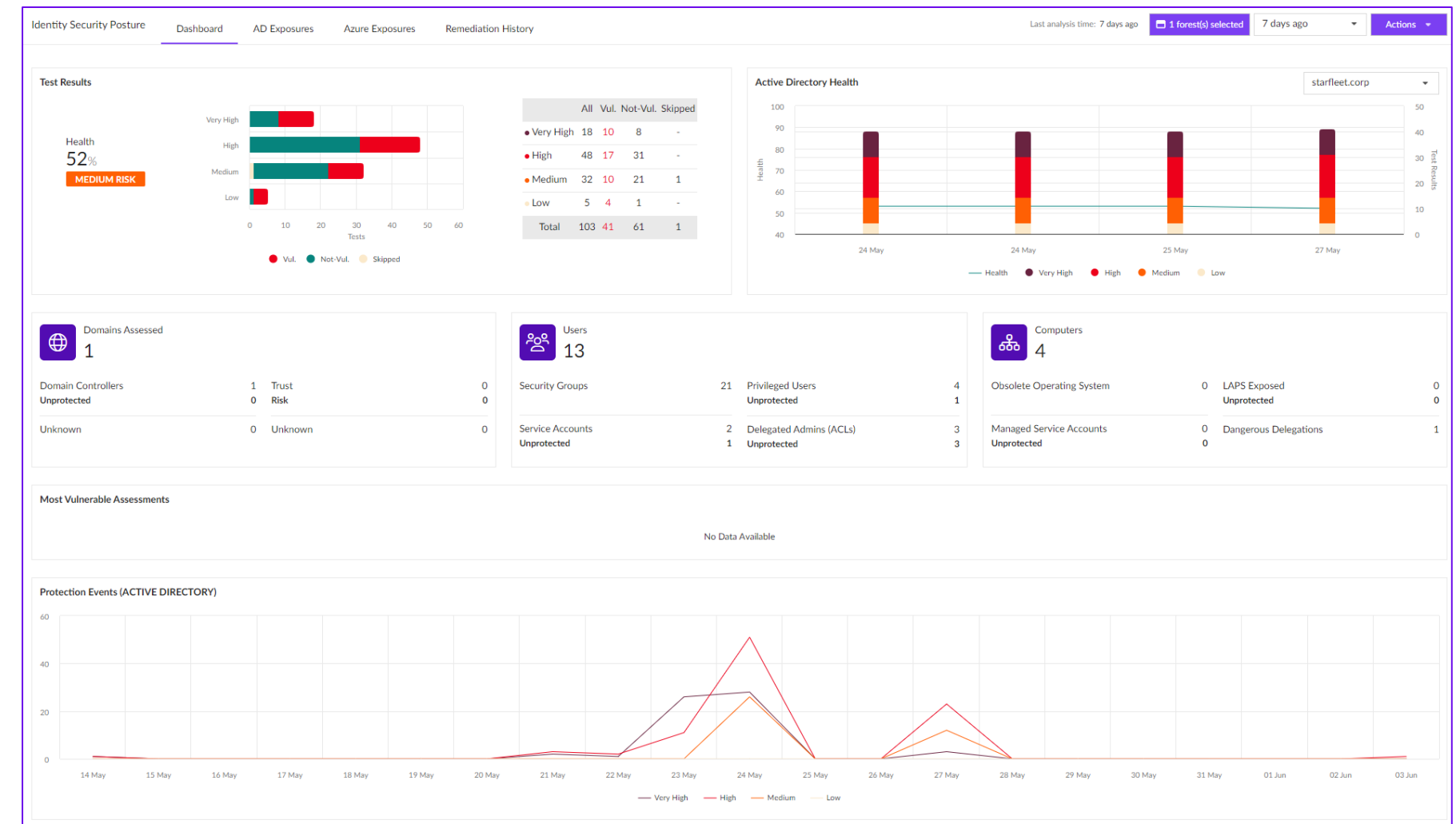
- Protects against attacks at endpoints
- Detailed insights from the endpoint
- Employs intercepting queries to AD and manipulating the results

Singularity | Identity Posture Management

AD and AAD Attack Surface Control

Singularity Identity Posture Management shrinks the identity attack surface by identifying and remediating identity infrastructure misconfigurations, exposures, and vulnerabilities in on-premises Active Directory & cloud-based Entra ID (formerly Azure AD).

- Systematically monitor Active Directory and Entra ID for misconfigurations and exploitable vectors
- Gain actionable information needed to correct exposures
- Stay informed of suspicious AD change events and over-provisioned entitlements



Implements AD Security Best Practices



Single Device Installation



Visibility Into Domain-Level Exposures



Visibility Into Device-Level Exposures



Visibility Into User-Level Exposures



Visibility Into Suspicious AD Events

Singularity | Identity for IdPs

AD Attack Surface Reduction + Real-Time Identity Attack Protection

Runs on Active Directory Server

- Small, Low-Impact Agent Footprint
- Deep Packet Inspection & Behavioral Analytics for All AD Activities

Enforce Conditional Access for Suspicious AD Transactions

- Force MFA Using Industry-Leading IAM Solutions

Detection of Advanced Identity-Based Attack Techniques

- ✓ Golden Ticket Attacks
- ✓ Silver Ticket Attacks
- ✓ Skeleton Key Attacks
- ✓ Pass-the-Ticket Attacks
- ✓ Pass-the-Hash Attacks
- ✓ Overpass-the-Hash Attacks
- ✓ Forged PAC Attack
- ✓ DCSync Attack
- ✓ DCShadow Attack
- ✓ AS-REP Roasting Attack
- ✓ Recon of Privileged & Service Accounts

DCSync Attack Detected

Alert ID: 0192d946-1610-74b8-83b6-ba79975422cc

Critical | Unknown | Oct 29, 2024 6:15 PM

Actions Event Search

Overview Indicators (1) Mitigation (0) Notes (0) History (0) Raw data

Alert Status: New Assigned To: - Analyst Verdict: Undefined

Alert Description and Recommendations
This event is generated when a DCSync attack is detected.

Detection Details

Confidence Level	Malicious
Detection Engine	ADSecure-DC
Detection Type	Rule
Vendor	SentinelOne
Product	Identity
First Event Time	Oct 29, 2024 6:15 PM
Last Event Time	Oct 29, 2024 6:15 PM
Domain	s1.lab
Attacker IP	10.0.0.5

Hide ^

Target Asset

Target Name	Ame-Dc16.S1.LAB
	IDP-POC-EU/Default site/Default Group
	Unknown
	10.0.0.4

Hide ^



Implements AD Security Best Practices



Single Device Installation



Visibility Into Domain-Level Exposures



Visibility Into Device-Level Exposures



Visibility Into User-Level Exposures

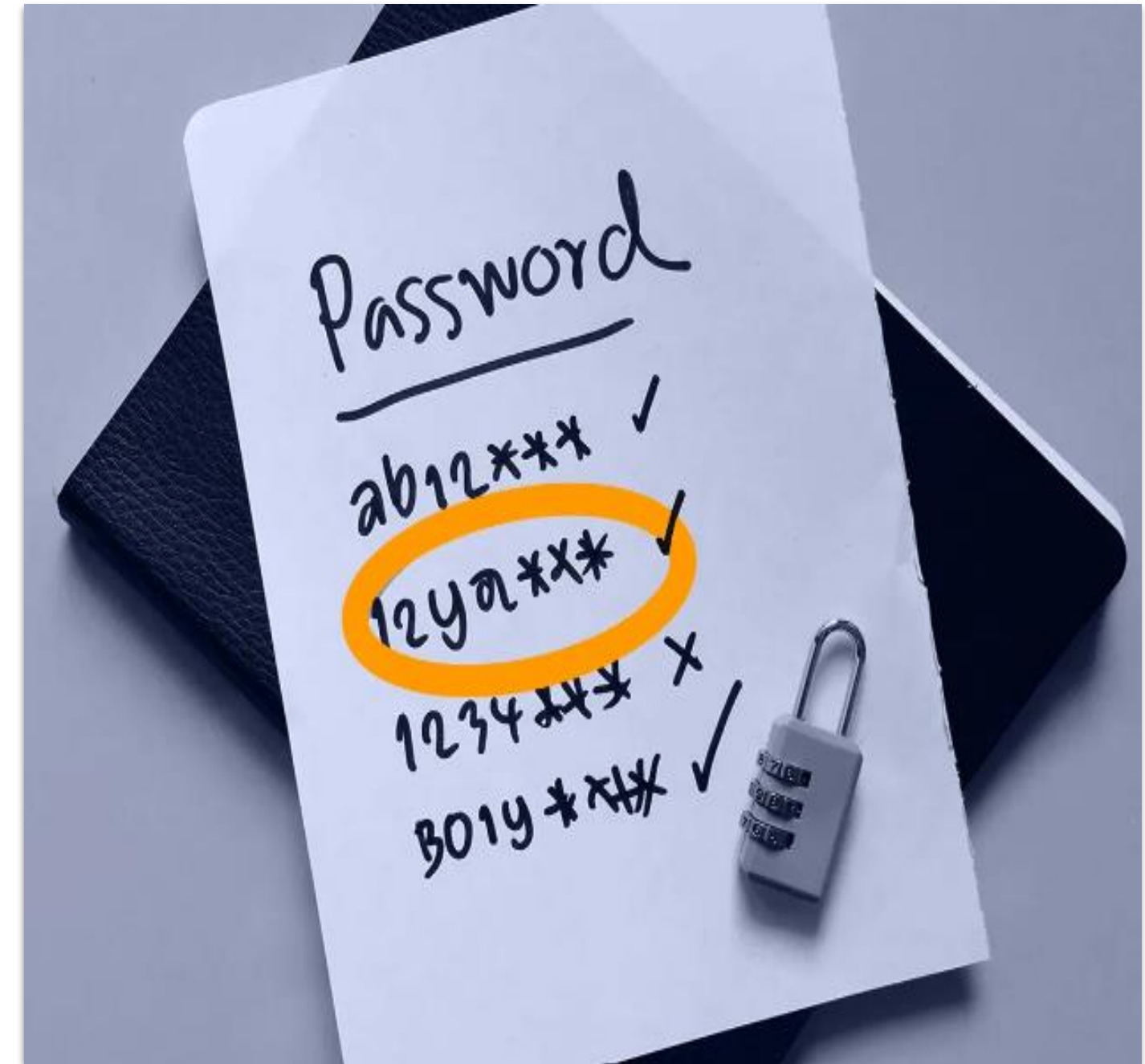


Visibility Into Suspicious AD Events

Singularity | Identity for IdPs

Compromised Credential Protection

- **Realtime protection** from creating or resetting compromised or weak credentials via policy
- **Automated response measures** such as changing passwords and disabling accounts for compromised passwords
- **Enhancing visibility** for users whose passwords have been compromised by adding a detect and protect mode
- **Enforce custom banned passwords** through a blocked list of easily guessed, commonly used passwords
- **Weekly security scans** to check if any credentials we are protecting have been disclosed on the dark web



Over 80% of data breaches are due to poor password security.

Singularity | Identity Detection and Response

Endpoint Identity Attack Detection & Misdirection

Defend Your Domain

Detect Active Directory attacks from any device type or OS.

Thwart the Adversary

Steer attackers away from AD crown jewels with misdirection down dead-end alleys

Deflect, Protect

Hide credentials and production data while making lateral movement difficult



Detection for
Identity-based
Attacks



On-prem AD, Entra
ID, and Multi-cloud
Environments



Technology to
Mislead Attackers






Identity Attack
Surface Reduction

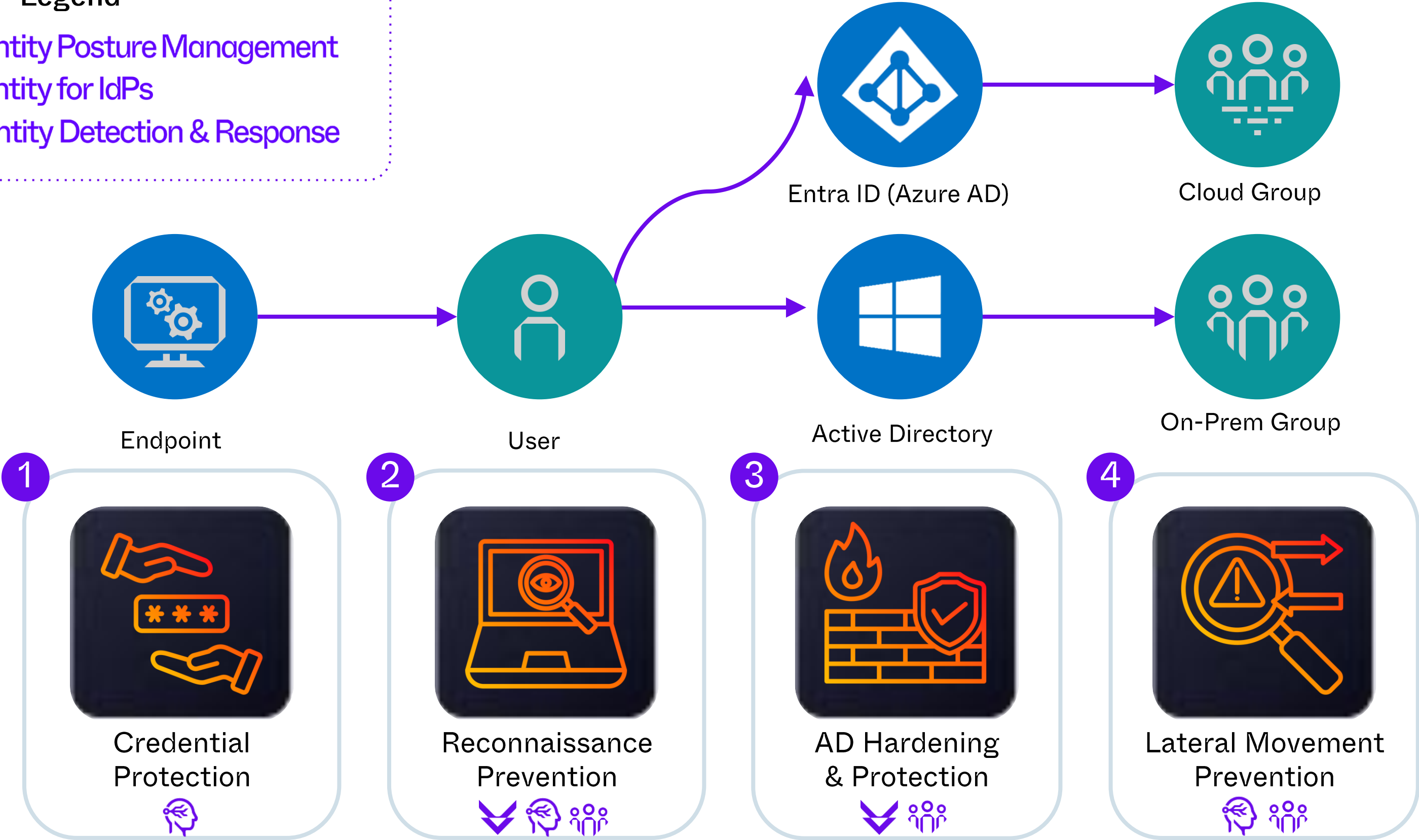


Zero Trust
Enforcement for
the Identity Layer

Comprehensive Identity Security

Legend

-  Singularity Identity Posture Management
-  Singularity Identity for IdPs
-  Singularity Identity Detection & Response



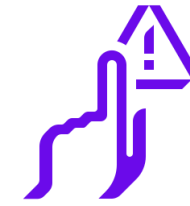
Identity Security Recommendations



Reduce the
Identity Attack
Surface



Protect the
Identity
Infrastructure



Disrupt
Attackers Early
in the Attack
Cycle



Incorporate
Identity into a
Holistic
Platform

NATIVE DATA



AI SIEM



Endpoint & Identity



Cloud



Exposure Management



Services

Singularity Platform

SUPERCHARGED BY Purple^{ai}

Singularity Data Lake

SECURITY & LOG ANALYTICS

INGEST DATA FROM ANY SOURCE

IDENTITY

EMAIL

CASB

SASE

WEB

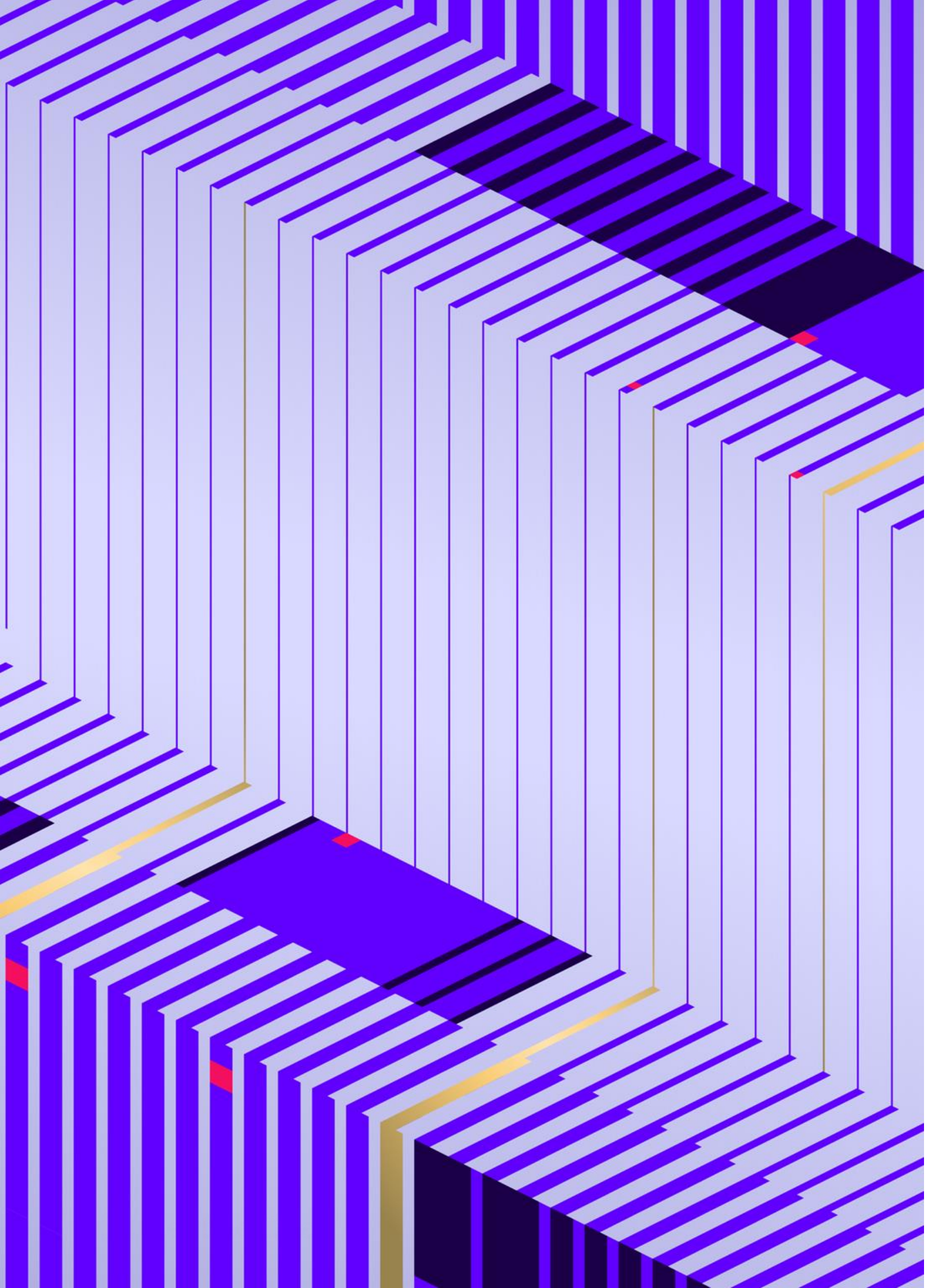
THREAT INTEL

SANDBOX

FIREWALL

CASE MGMT

LOG INGEST



Questions?