SentinelOne®

Identity Threats Detection and Response – the new buzz word for 2023?

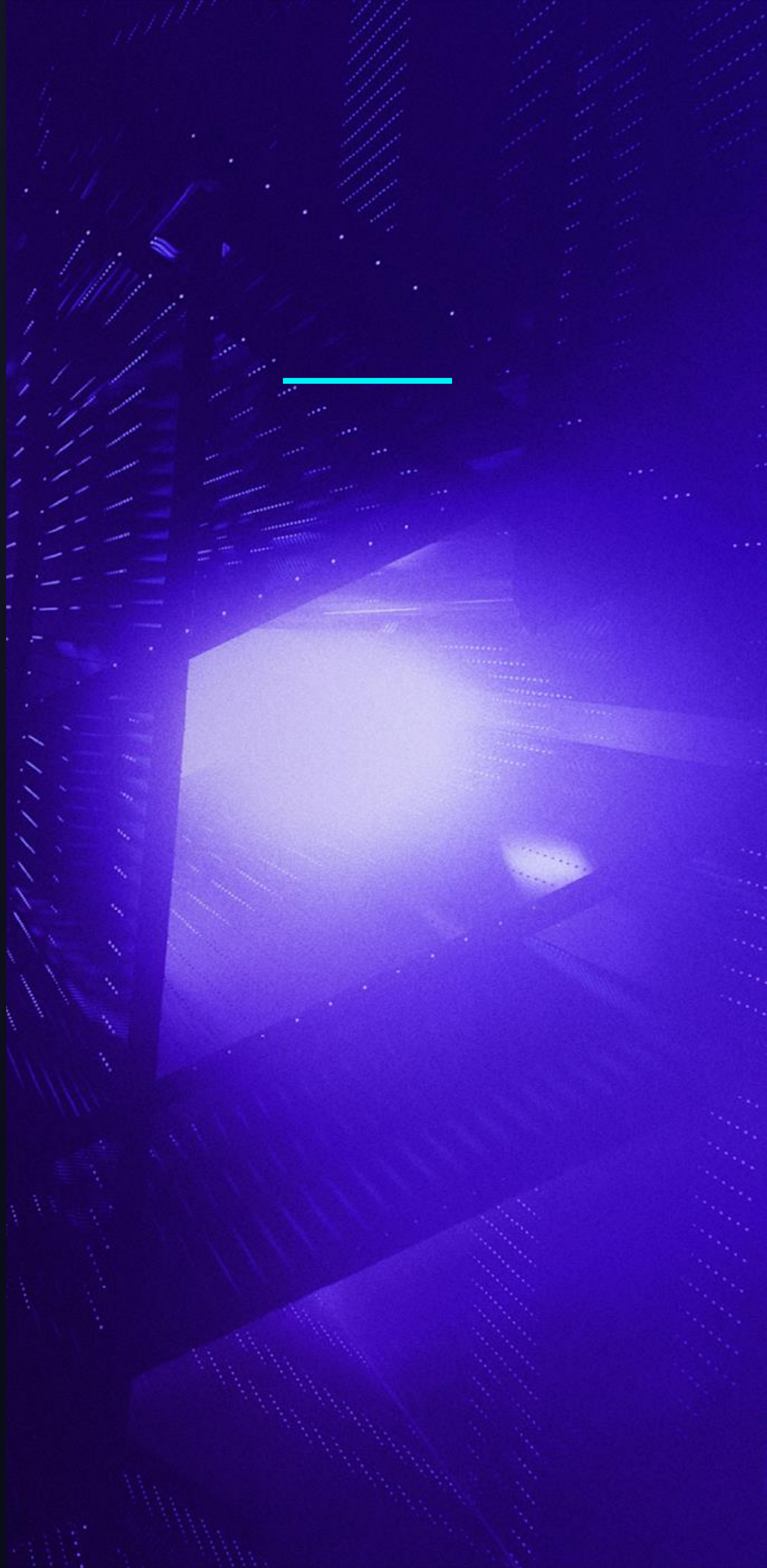
Milad Aslaner

Agenda

- Identity Security Challenges
- Limitation Of Today’s Security Controls
- How We Need To Evolve Our Security Controls

SentinelOne®

Identity Security Challenges



The Elephant In The Room

90%

Organizations use Microsoft Active Directory

3%

Organizations fully migrated from legacy on-premises AD to a cloud identity service

50%

Organizations see the need to protect AD with additional security measures

SentinelOne

Identity Security Challenges

78%

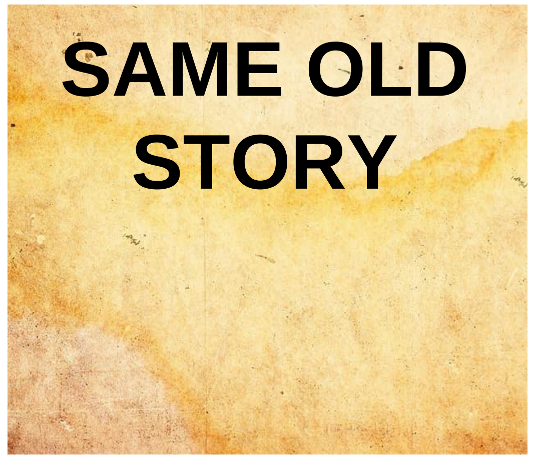
Organizations experienced direct business impacts due to identity-related breaches

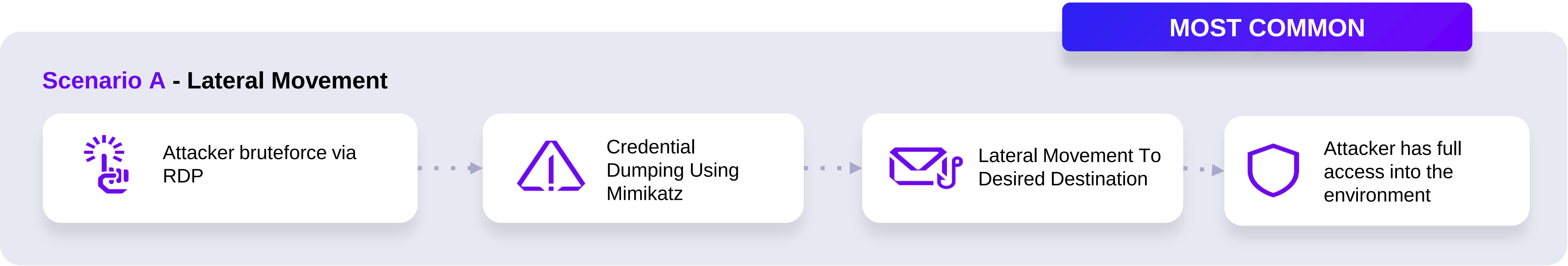
96%

Organizations confirmed they have prevented or minimized the breach by implementing better security outcomes

- Exponential increase of managed identities in a enterprise (B2B, B2C, etc.)
- Cloud environments vulnerable for identity-based attacks
- living off the land (LotL) techniques increasingly leveraged by attackers
- Poor identity security hygiene (MFA, password policies, etc.)
- Inadequate Management Of Privileged Identities

Identity Based Threatpaths

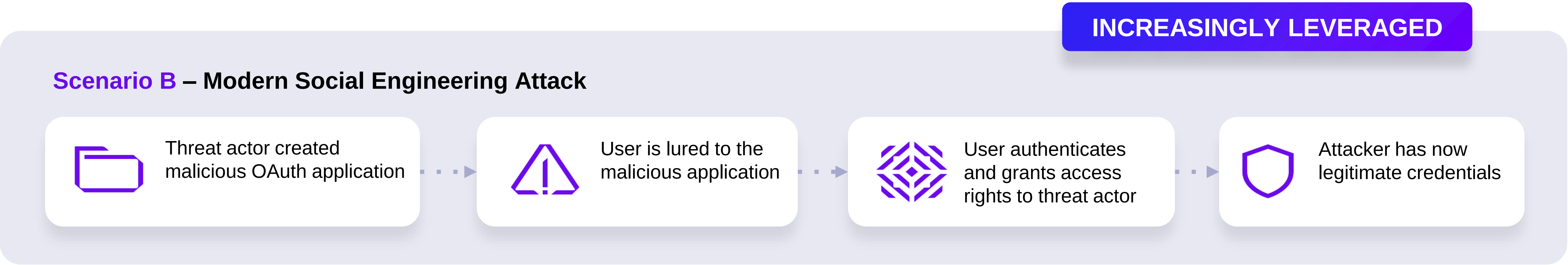




MOST COMMON

Scenario A - Lateral Movement

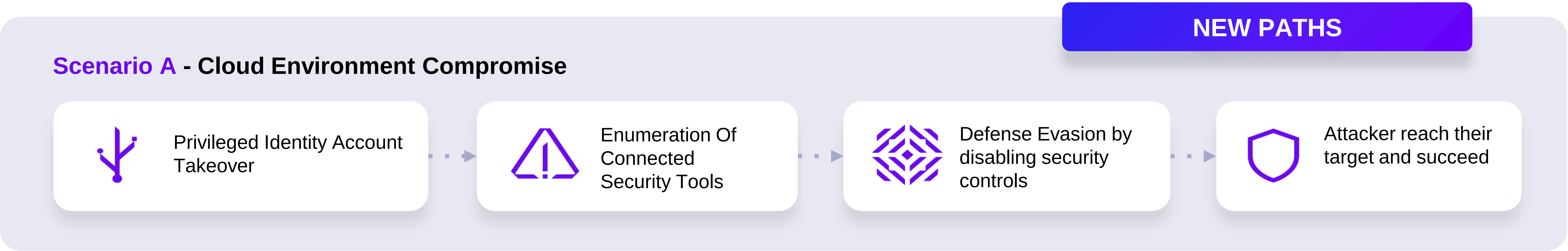
Attacker bruteforce via RDP → Credential Dumping Using Mimikatz → Lateral Movement To Desired Destination → Attacker has full access into the environment



INCREASINGLY LEVERAGED

Scenario B – Modern Social Engineering Attack

Threat actor created malicious OAuth application → User is lured to the malicious application → User authenticates and grants access rights to threat actor → Attacker has now legitimate credentials



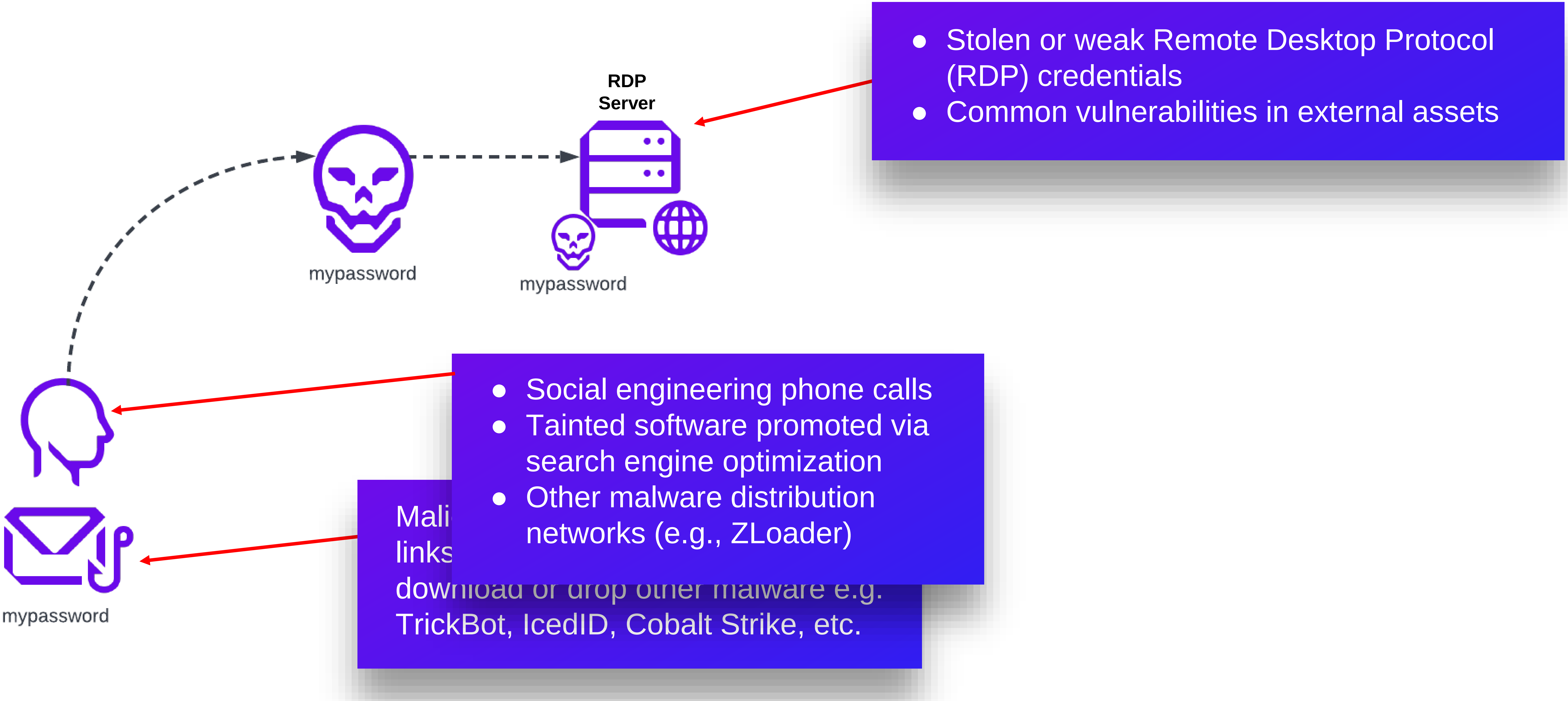
NEW PATHS

Scenario A - Cloud Environment Compromise

Privileged Identity Account Takeover → Enumeration Of Connected Security Tools → Defense Evasion by disabling security controls → Attacker reach their target and succeed

Using Active Directory to Spread Ransomware

Example Attack Anatomy



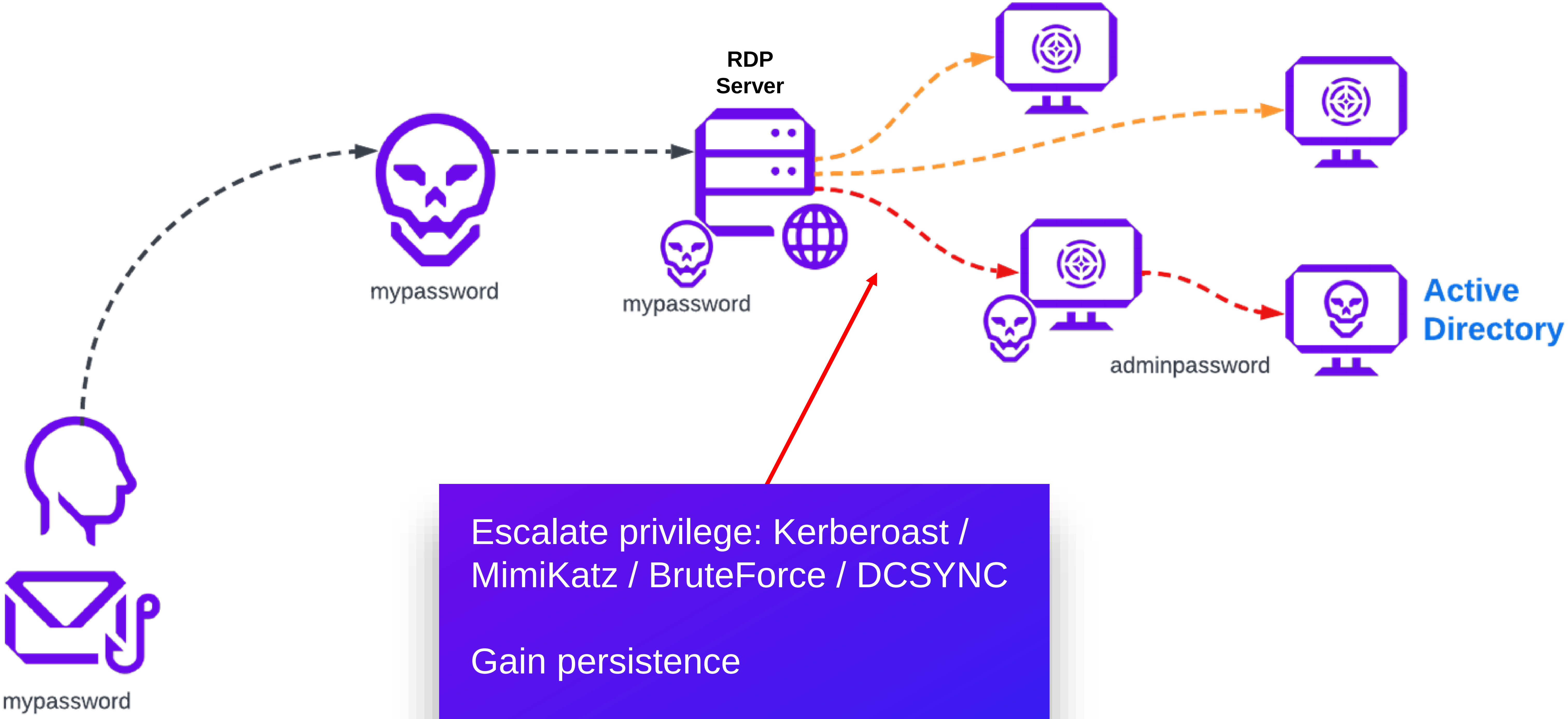
- Stolen or weak Remote Desktop Protocol (RDP) credentials
- Common vulnerabilities in external assets

- Social engineering phone calls
- Tainted software promoted via search engine optimization
- Other malware distribution networks (e.g., ZLoader)

Mali
links
download or drop other malware e.g.
TrickBot, IcedID, Cobalt Strike, etc.

Using Active Directory to Spread Ransomware

Example Attack Anatomy



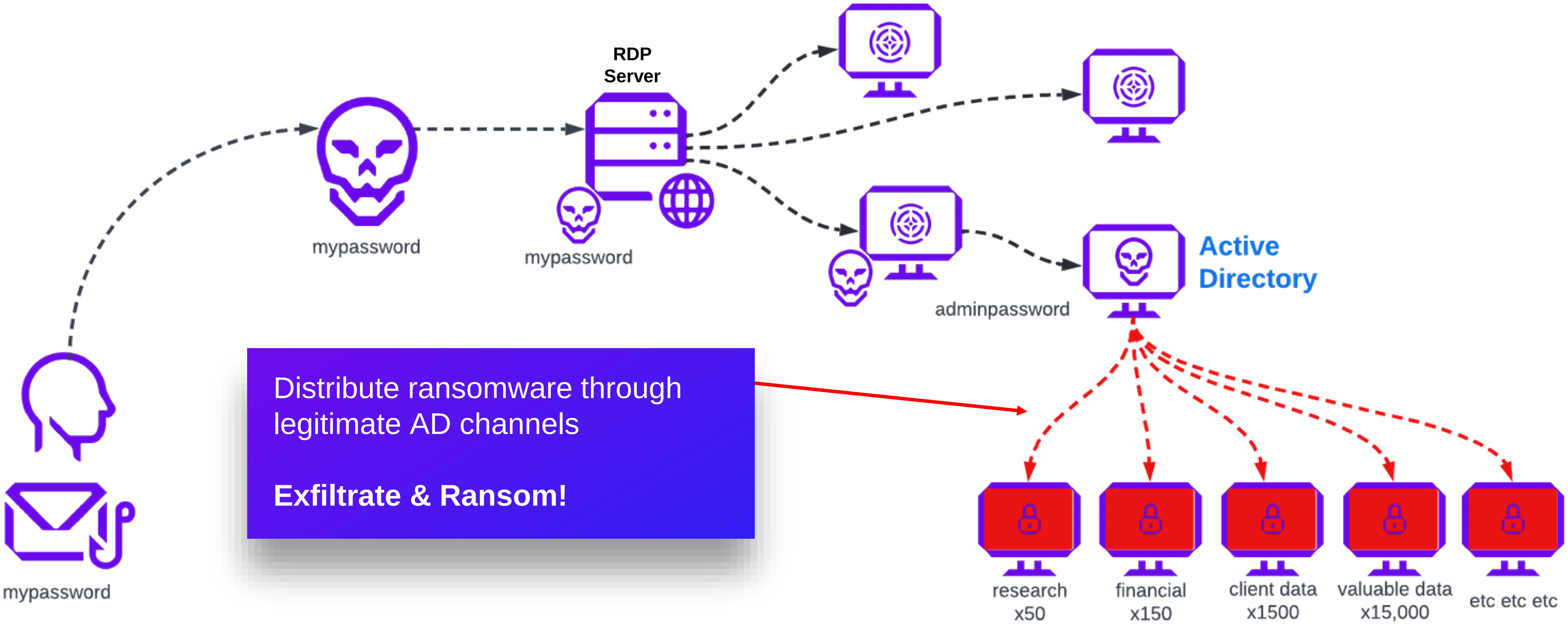
Escalate privilege: Kerberoast / MimiKatz / BruteForce / DCSYNC

Gain persistence

Move laterally…..

Using Active Directory to Spread Ransomware

Example Attack Anatomy

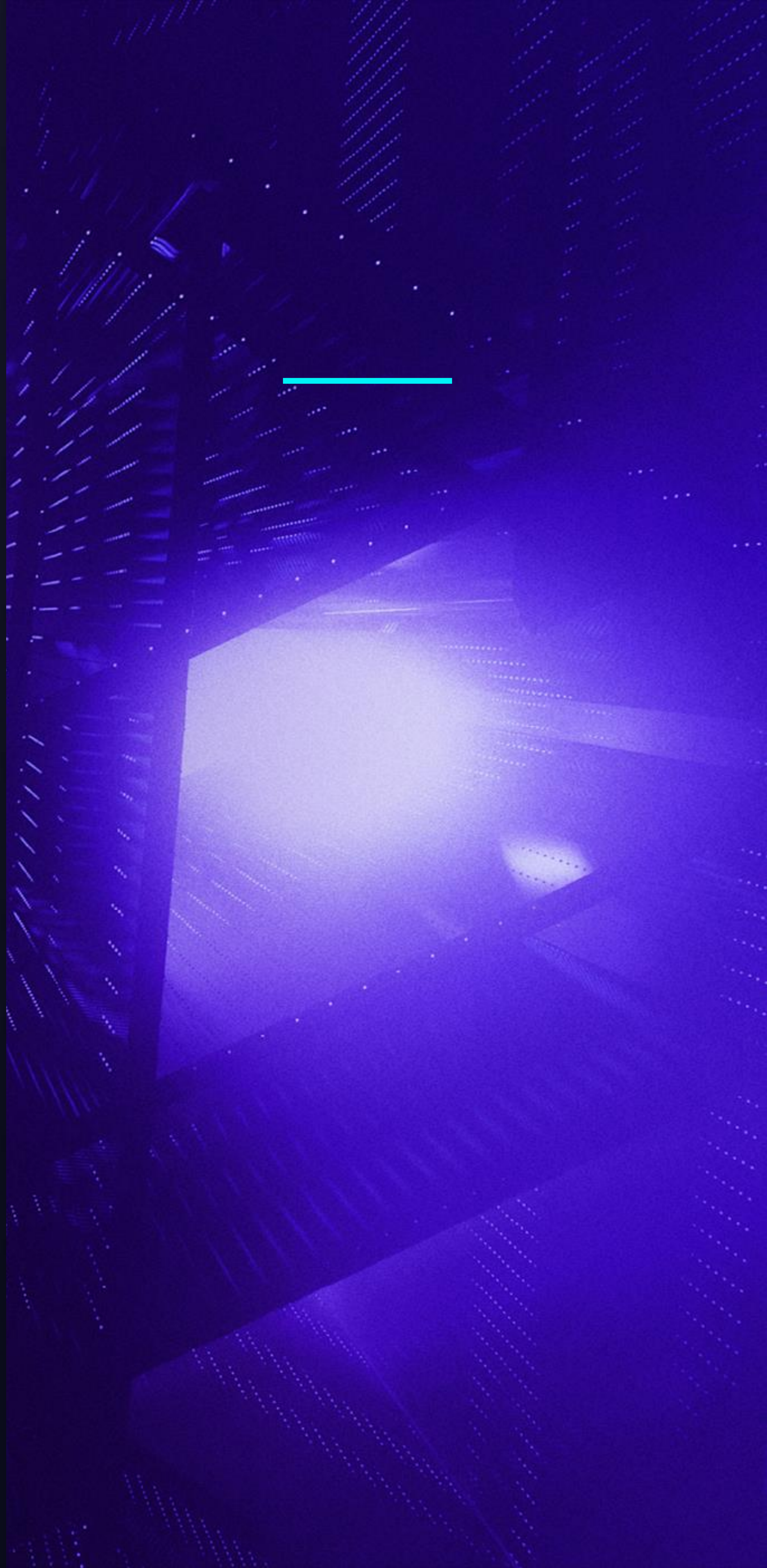


Distribute ransomware through legitimate AD channels

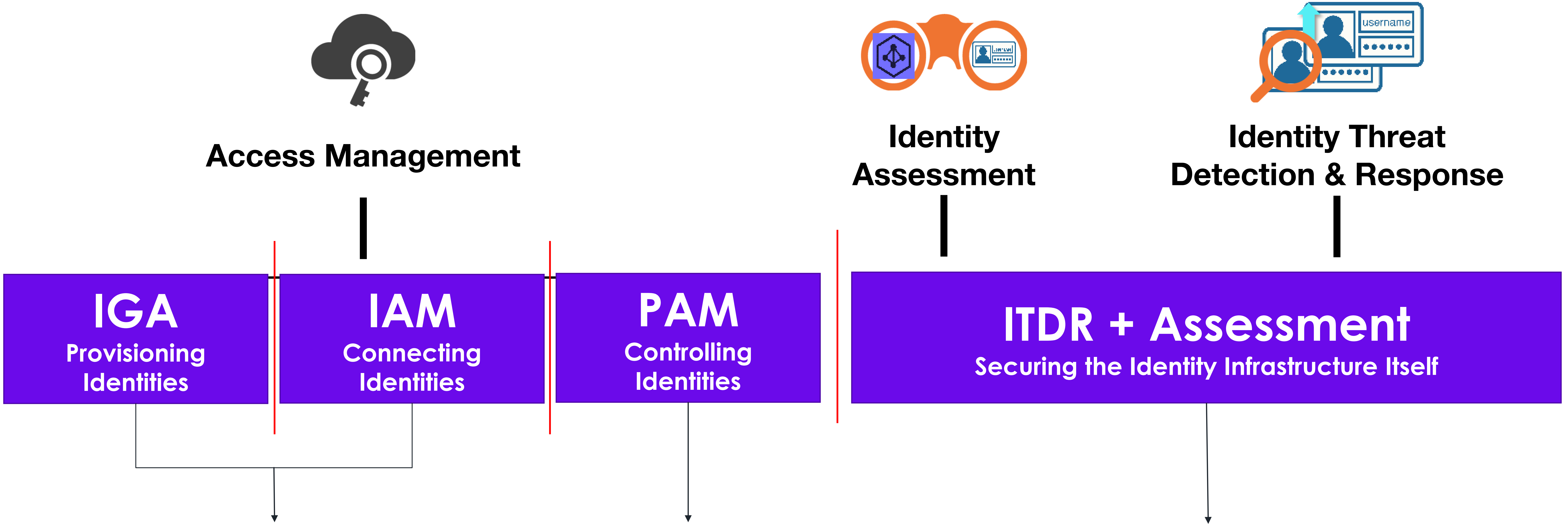
Exfiltrate & Ransom!

SentinelOne

Limitation of today's security controls



Journey Of Identity Security



Access Management

Identity Assessment

Identity Threat Detection & Response

IGA
Provisioning Identities

IAM
Connecting Identities

PAM
Controlling Identities

ITDR + Assessment
Securing the Identity Infrastructure Itself

Majority of organizations completed the adoption of IGA and IAM.

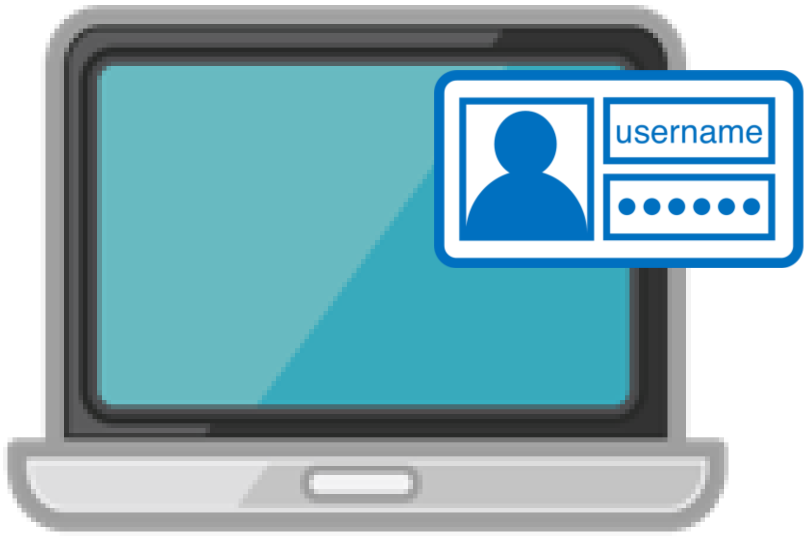
Subset of organizations adopted PAM.

Most organizations have an EDR, some also have real-time assessment capabilities but very few organizations adopted ITDR just yet.

The Gap in Traditional Defenses

1

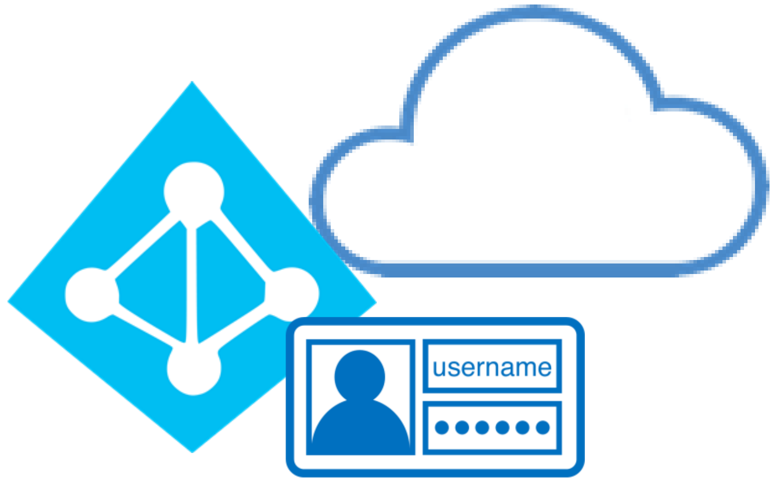
Endpoint



Prevent, Detect, Respond To Endpoint-Centric Alerts

2

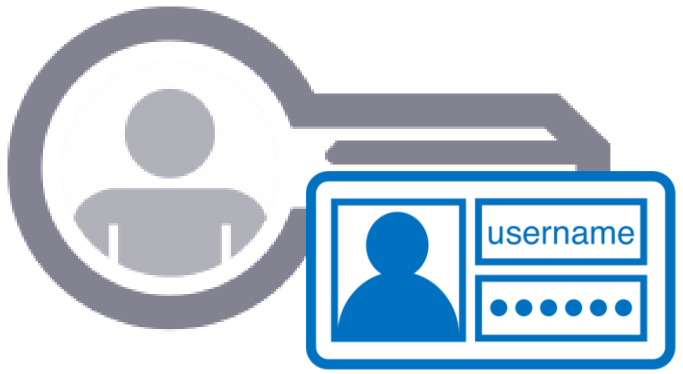
Identity



Prevent, Detect, Respond To Identity-Centric Alerts

3

Access Management

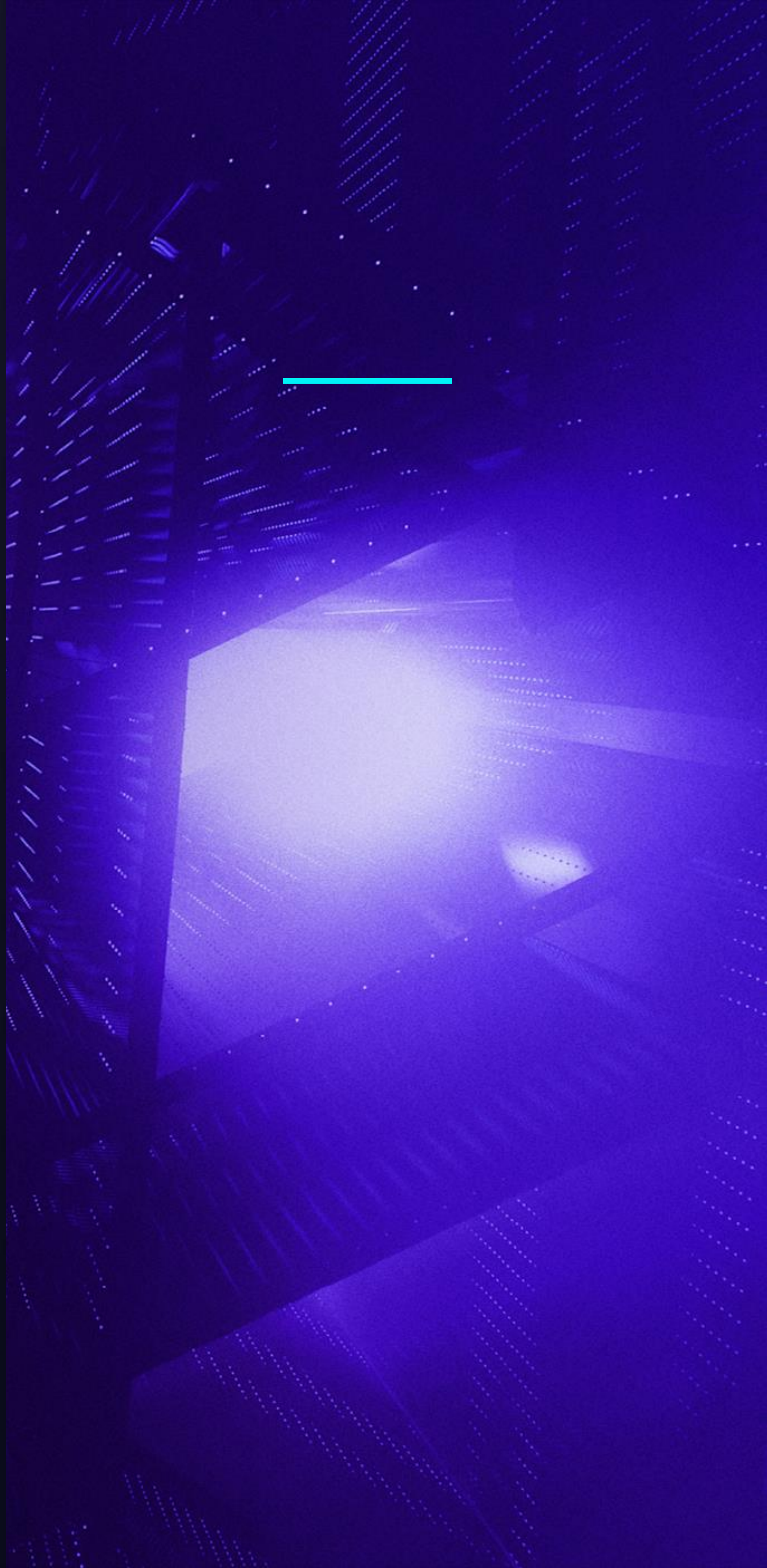


Ensure Right Access Is Granted To Right People

Detection Gaps + Operational Complexity

SentinelOne®

How We Need To Evolve Our Security Controls



Identity Security Challenges and Requirements

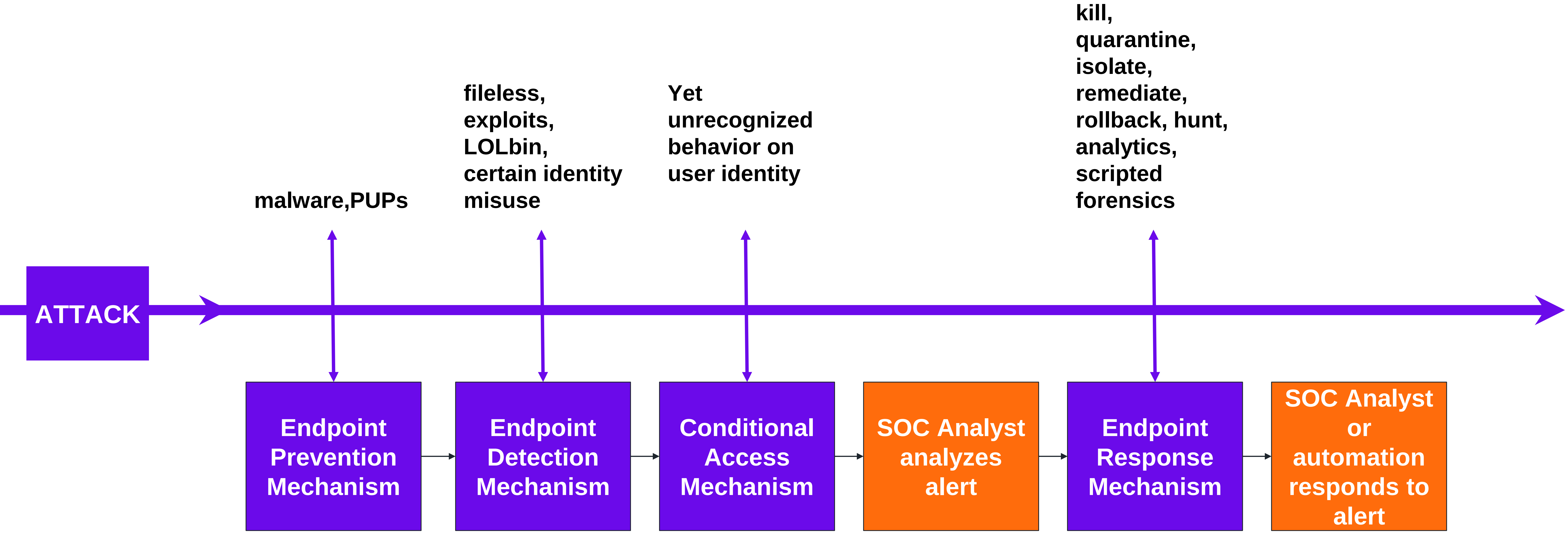
	Challenge	People	Process	Tech
IDENTITY POSTURE	Exponential increase of managed identities in a enterprise (B2B, B2C, etc.)	Drive awareness that it's no longer just employee identities we need to worry about	Managing B2B and B2C user identities	Identity and Access Management (IAM) solution
CLOUD ENVIRONMENT	Cloud environments vulnerable for identity-based attacks	Adequate training to understand cloud security threats and impact to user identities	Defined roles and responsibilities between cloud and identity teams	Cloud Security Posture Management (CSPM)
COMPLEX ATTACKS	Living off the land (LotL) techniques, zero days, and cloud vulnerabilities increasingly leveraged by attackers	Security awareness training for end users and IR training for security professionals	Incident response playbooks beyond the endpoint-centric surface.	Deception, Detection, and Response Across Identity and Endpoint
SECURITY HYGIENE	Poor identity security hygiene (MFA, password policies, etc.)	Educate on adoption of MFA, strong password/no password auth	Identity security best practices outlined as procedures.	Attack Surface Management (ASM) and Cloud Identity Entitlement Management (CIEM)
PRIVILEGED IDENTITY	Inadequate Management Of Privileged Identities	Ensure employees and contractors are comfortable with operating priv. identities	Defined RACI model for user identities in and outside organization	Modern Privileged Identity Management (PIM)

Rethinking Our Attack/Security Chain

Post-Breach

Tech

People



ATTACK

malware,PUPs

fileless, exploits, LOLbin, certain identity misuse

Yet unrecognized behavior on user identity

kill, quarantine, isolate, remediate, rollback, hunt, analytics, scripted forensics

Endpoint Prevention Mechanism

Endpoint Detection Mechanism

Conditional Access Mechanism

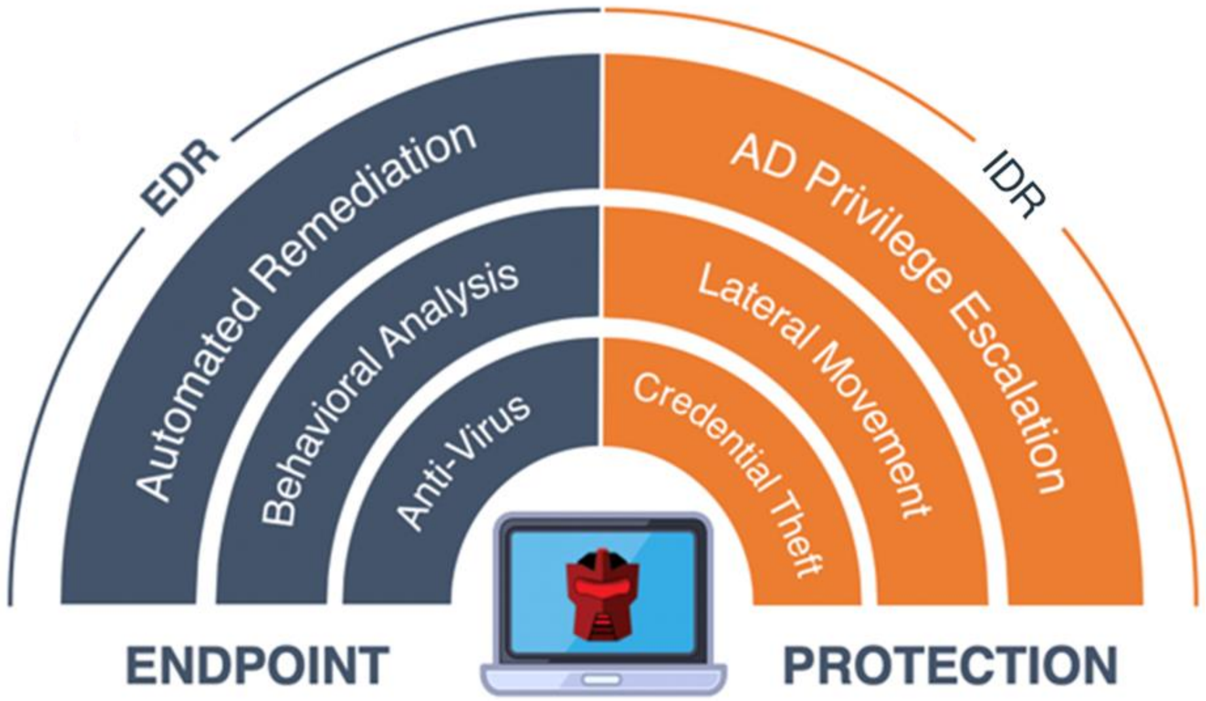
SOC Analyst analyzes alert

Endpoint Response Mechanism

SOC Analyst or automation responds to alert

Organizational Cyber Threats Requires Convergence

Endpoint-Centric
Protect, Detect, and
Respond



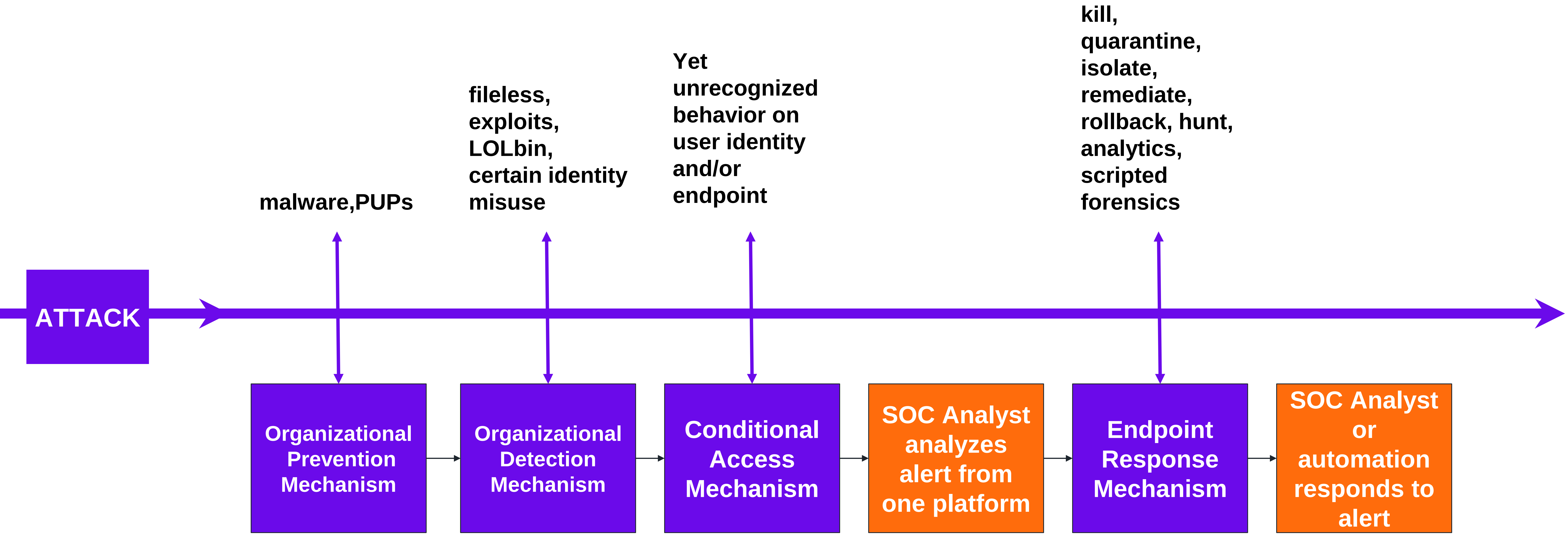
Identity-Centric
Protect, Detect, and
Respond

CONVERGENCE OF ENDPOINT+IDENTITY SECURITY CONTROLS

ORGANIZATIONAL SECURITY CONTROLS

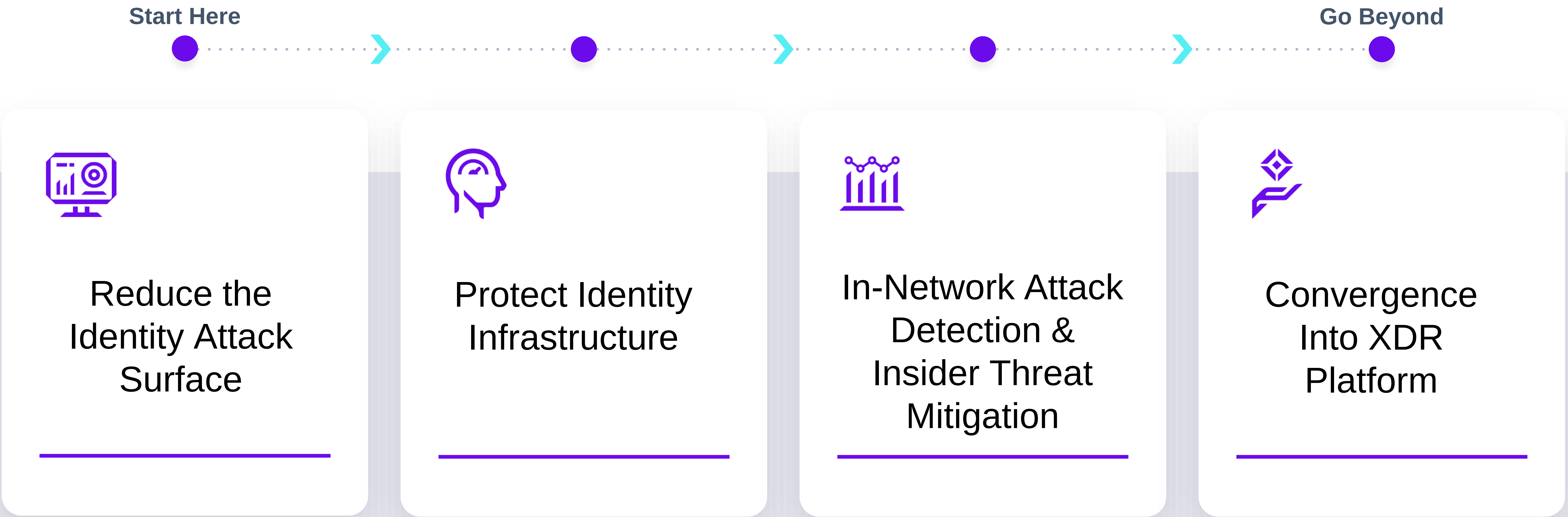
Rethinking Our Attack/Security Chain

Convergence Post-Breach



Tech
People
malware,PUPs
fileless, exploits, LOLbin, certain identity misuse
Yet unrecognized behavior on user identity and/or endpoint
kill, quarantine, isolate, remediate, rollback, hunt, analytics, scripted forensics
ATTACK
Organizational Prevention Mechanism
Organizational Detection Mechanism
Conditional Access Mechanism
SOC Analyst analyzes alert from one platform
Endpoint Response Mechanism
SOC Analyst or automation responds to alert

So What’s Next?



Start Here

Go Beyond

Reduce the Identity Attack Surface

Protect Identity Infrastructure

In-Network Attack Detection & Insider Threat Mitigation

Convergence Into XDR Platform

SentinelOne®

Thank You