ITDR and where It fits in your identity security stack

Brian Freedman

CISSP | WW Director Solutions Architecture
QOMPLX
brian.freedman@qomplx.com

Agenda

1. **Common problems**
   Identity is a main vector for attackers and bypasses legacy solutions
2. **ITDR and how does it apply**
   Identity is the common factor in every large-scale cyber breach
3. **ITDR solutions**
4. **Q & A**

Identity is the main target for attackers

Verizon DBIR:

Stolen credentials led to nearly **50%** of attacks

Active Directory proven to be target of attacks

FireEye Analysis of SolarWinds Attack Code

“The backdoor also determines if the system is joined to an Active Directory (AD) domain and, if so, retrieves the domain name. ***Execution ceases*** *if the system is* ***not joined to an AD domain.”***

Identity is common attack vector with most common attacks

RANSOMWARE ATTACKS MOST PROMINENT IN JAN 2023 – TARGETED IDENTITIES

LockBit

Hive

Black Basta

Vice Society

ATTACKS LEVERAGING IDENTITIES

In 2022 hackers stole about 26 million user login credentials

Unauthorized access via default, shared, or stolen credentials constituted more than 1/3 of the entire hacking category

Far and away the most common action in this pattern is privilege abuse

System intrusion, social engineering and privilege misuse represent 9% of breaches

Cloud Identities are perfect target

94% OF ALL ENTERPRISES USE CLOUD SERVICES

88% OF CLOUD BREACHES ARE DUE TO HUMAN ERROR

75% OF ENTERPRISES CLAIM CLOUD SECURITY IS TOP CONCERN

AD Identities are primary target

90% OF INVESTIGATED ATTACKS BY MANDIANT INVOLVES AD IN SOME FORM

50% OF ORGANIZATIONS EXPERIENCED AN ACTIVE DIRECTORY ATTACK IN THE LAST TWO YEARS

40% OF THOSE ATTACKS WERE SUCCESSFUL BECAUSE ADVERSARIES EXPLOITED WEAK AD HYGIENE

Source: 26 Cloud Computing Statistics, Facts & Trends for 2023 (cloudwards.net) / 2022 Cyber Attack Statistics, Data, and Trends | Parachute / 2022Verizon-data-breach-investigations-report-dbir.pdf

QOMPLX:

Zero Trust starts with Identity

Zero Trust according to Microsoft:

Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to “never trust, always verify.” Every access request is fully authenticated, authorized, and encrypted before granting access.

Micro segmentation and least-privilege access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time.

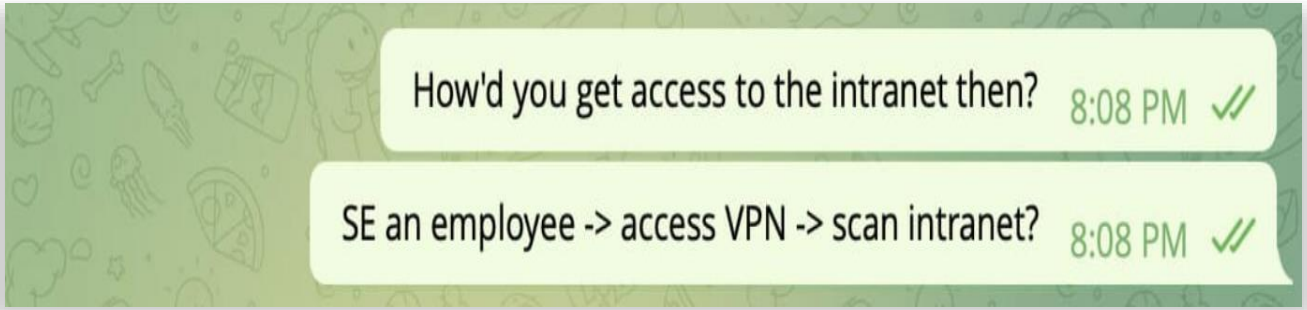
Three Zero Trust principles

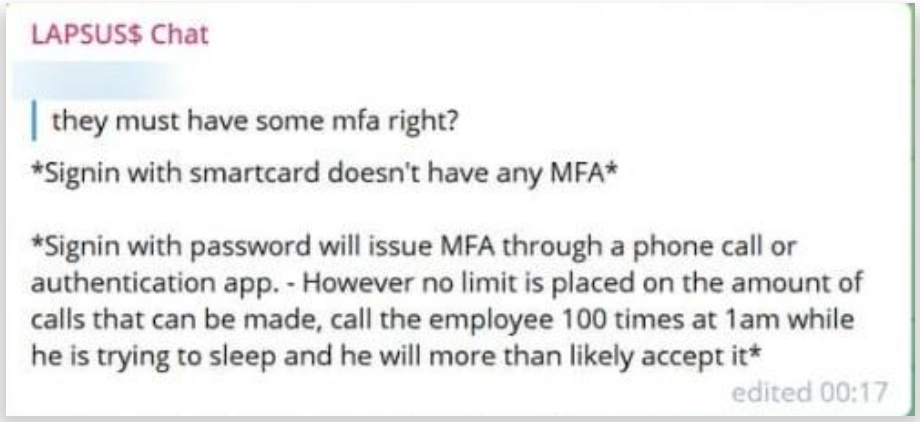
1. **VERIFY EXPLICITLY**
   Always authenticate and authorize based on all available data points

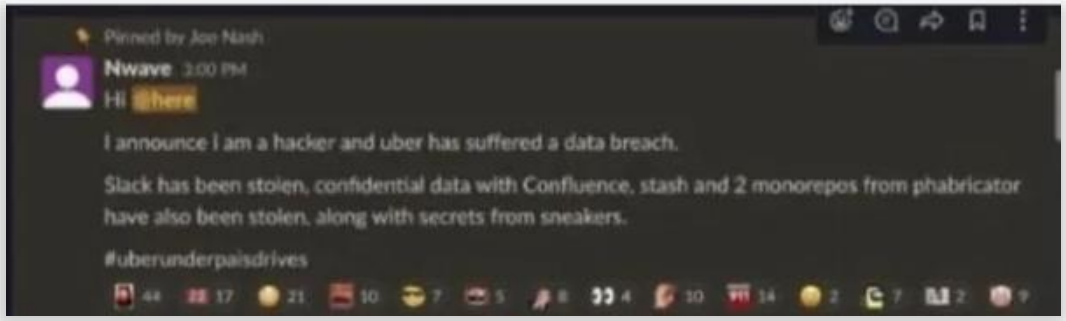
1. **USE LEAST PRIVILEGE ACCESS**
   Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection

2. **ASSUME BREACH**
   Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses

Why MFA is no longer enough







Active Directory Proven to be Target of Attacks

Lapsus$

On March 22, 2022, Microsoft stated

"DEV-537 (LAPSUS$) used DCSync attacks and Mimikatz to perform privilege escalation routines. Once Domain Admin access had been obtained,.."
THE defining step in LAPSUS$'s methodology is "Active Directory Privilege Escalation"

MSFT also said

"They (LAPSUS$) have been CONSISTENTLY observed to use AD Explorer, to enumerate all users and groups in the said network... this allows them to understand which accounts might have higher privileges" <to escalate privilege to in AD.>

*Source: lnkd.in/guca2AAp

Identity is a key target

Attack surface expansion

- Move to a hybrid environment
- Hybrid identities (AD, AAD, Okta, AWS, etc.)
- Work from home

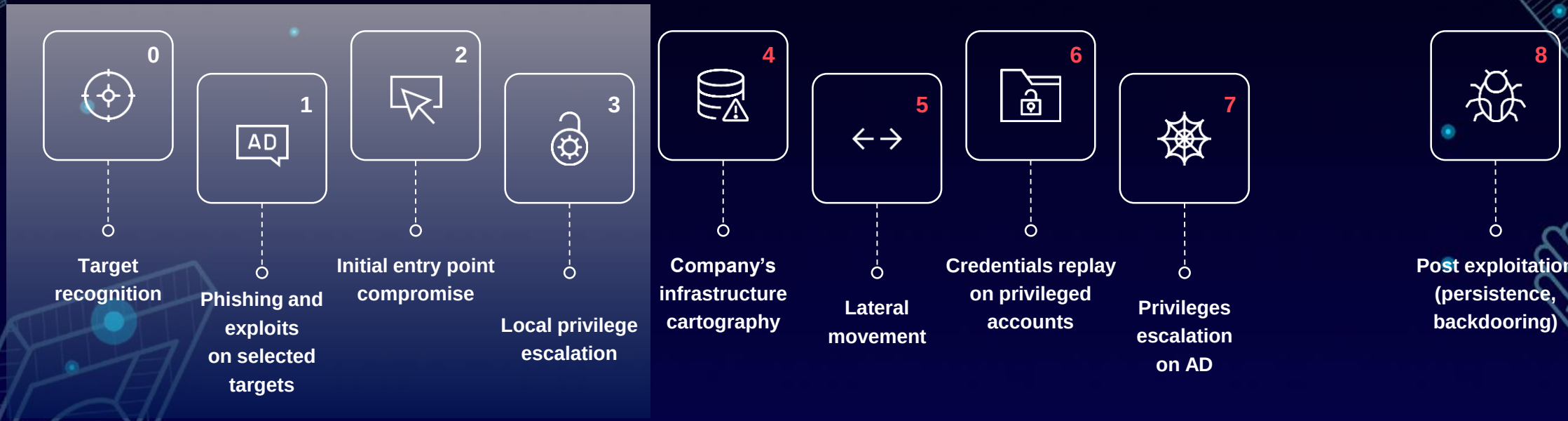
Identity system defense

- Layering of security solutions is essential
- PAM, MFA - needed, but don’t secure the identity itself
- Identity security hygiene
- Identity security attack detection (ITDR)
- Identity security attack response (ITDR)

Current identity solutions

SECURITY TECHNOLOGIES:

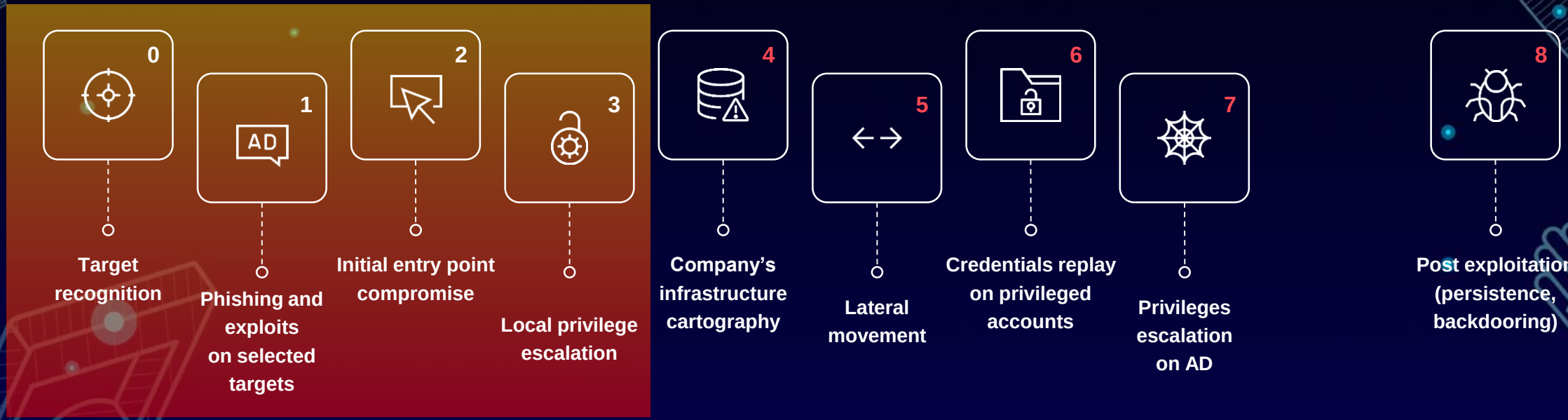
PAM / MFA / IGA / AM / CIEM



Current identity solutions

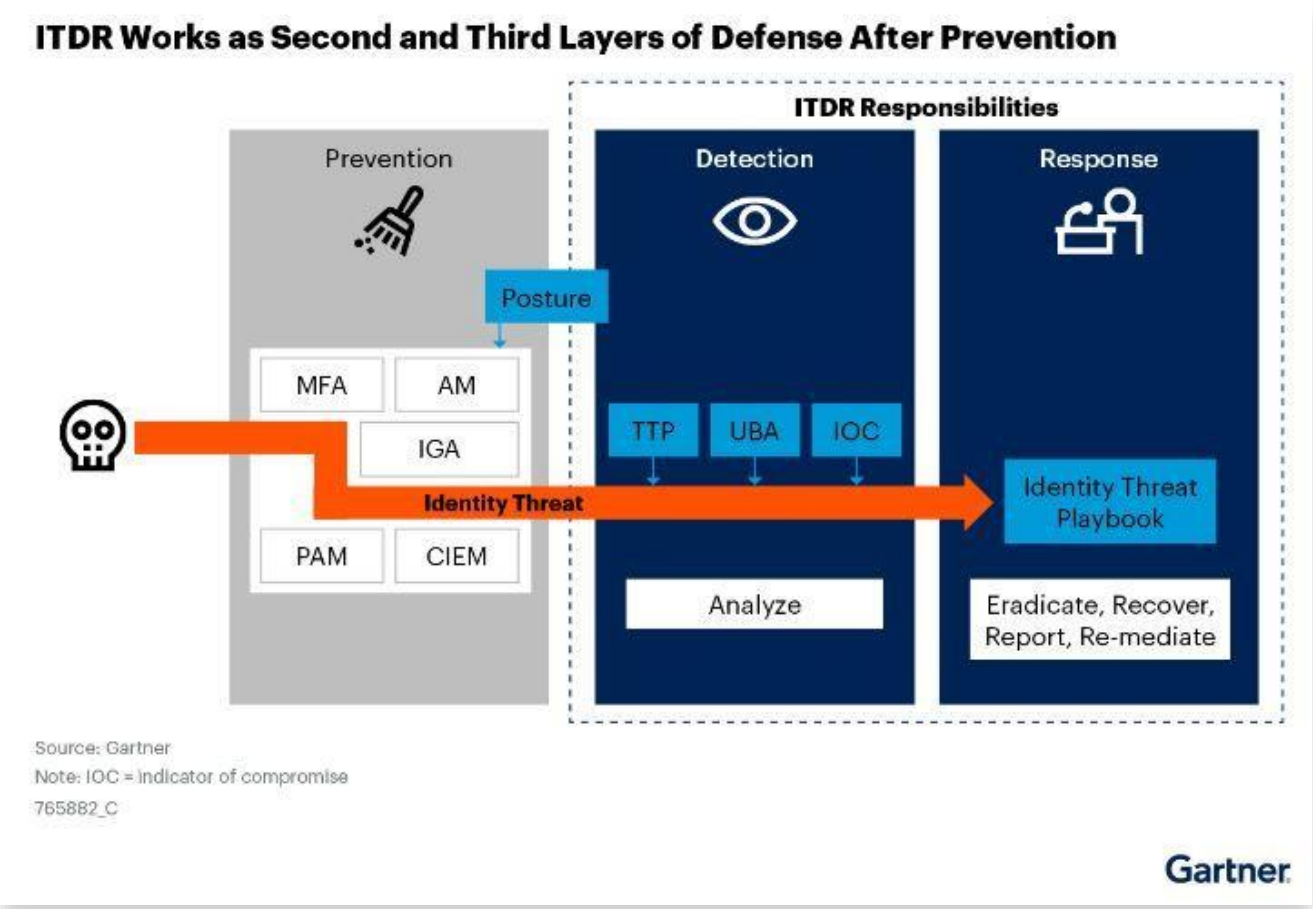
SECURITY TECHNOLOGIES:

PAM / MFA / IGA / AM / CIEM

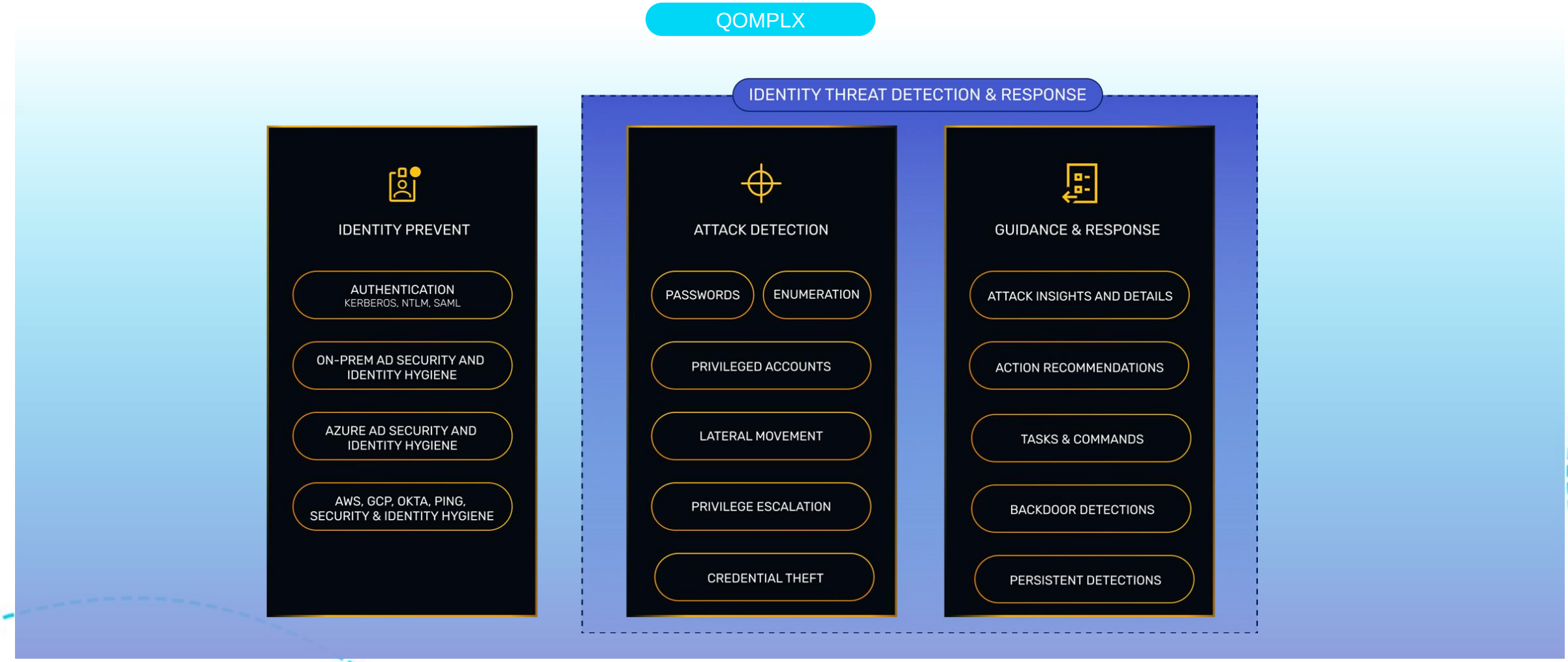


Identities not secured

Gartner – Identity Threat Detection & Response (ITDR)



Comprehensive Identity Security: Prevent, Detect & Respond



Identity Security - Prevent

On-prem identity

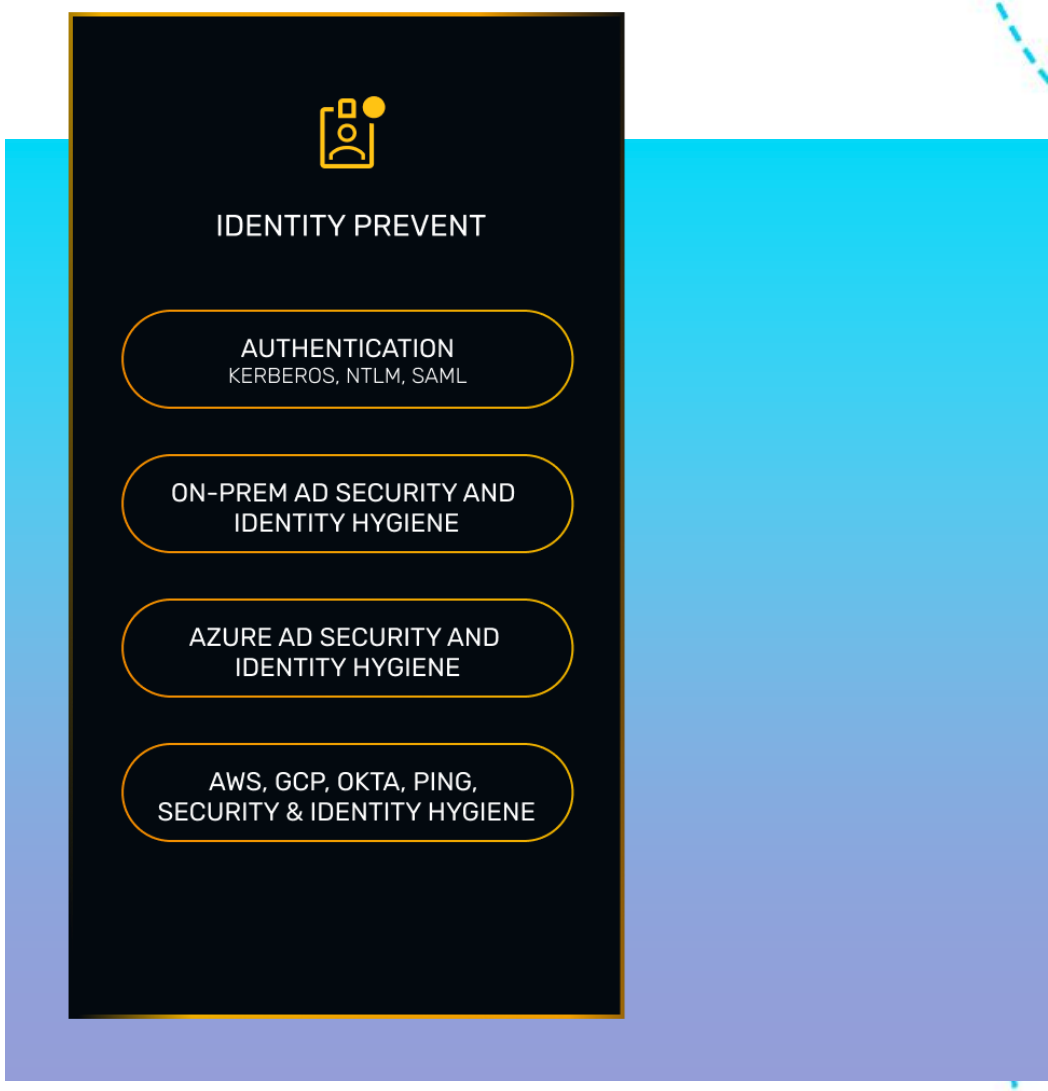
- Visibility of existing AD security issues
- 24x7 real-time and automatic analysis of every AD change for new security issues

Cloud identity

- Visibility of existing cloud identity security issues
- 24x7 real-time and automatic analysis of every change for new security issues

Guidance and remediation

- Insights and summaries of issues
- Contextual guidance for remediation



Identity Security - Detect

Assume breach

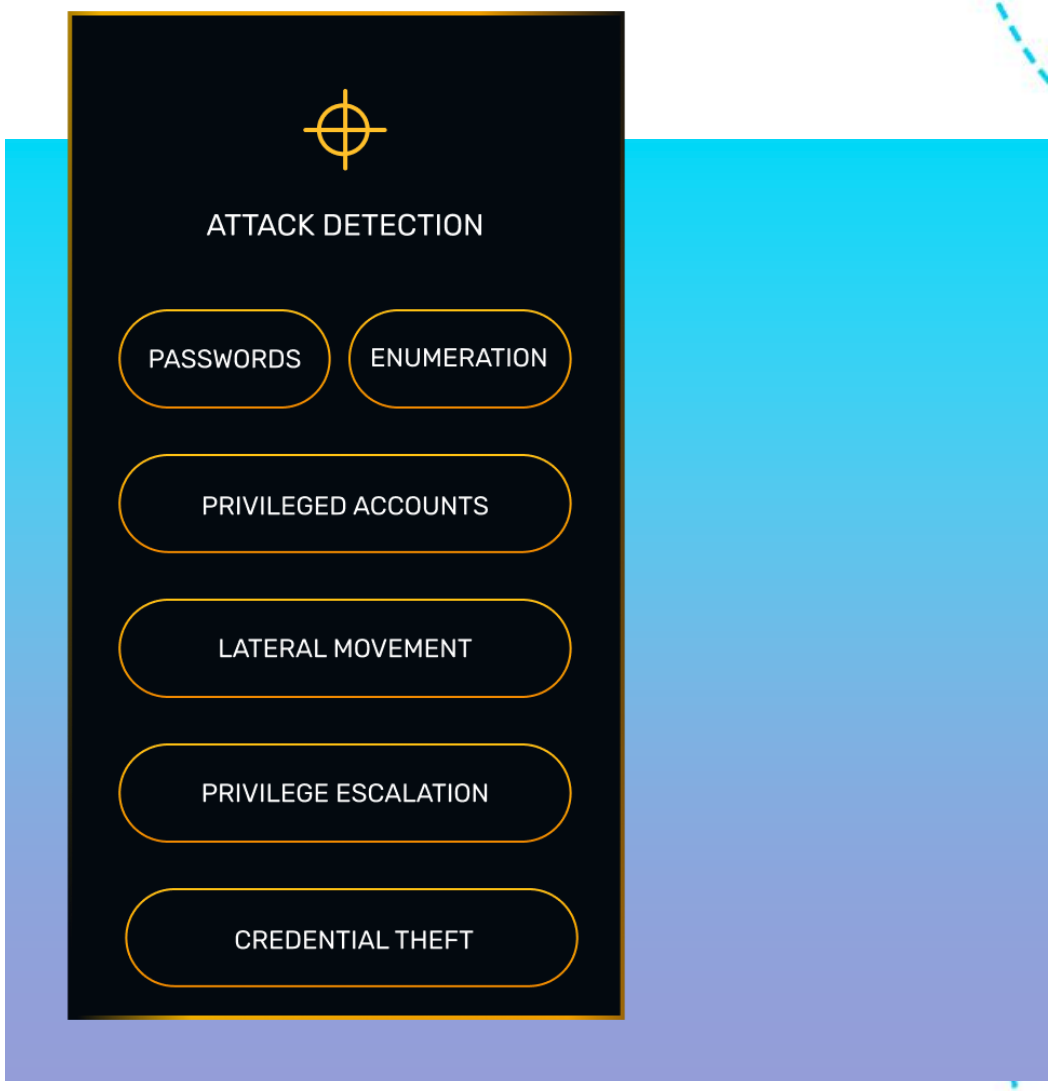
- Must take the approach that the network is already breached
- Basic and complex attacks must be detected where identities reside (on-prem and cloud)

Deep and wide attack detections

- Password attacks, lateral movement, privilege escalation, etc.
- Object, attribute, kerberoasting, impersonation, etc

Zero Trust related attack detections

- On-prem credential abuse and forgeries (Golden Ticket, Silver ticket, Diamond ticket, Sapphire ticket, etc.)
- Cloud credential abuse and forgeries (SAML and AAD Kerberos)



Identity Security - Response

Guidance and insights

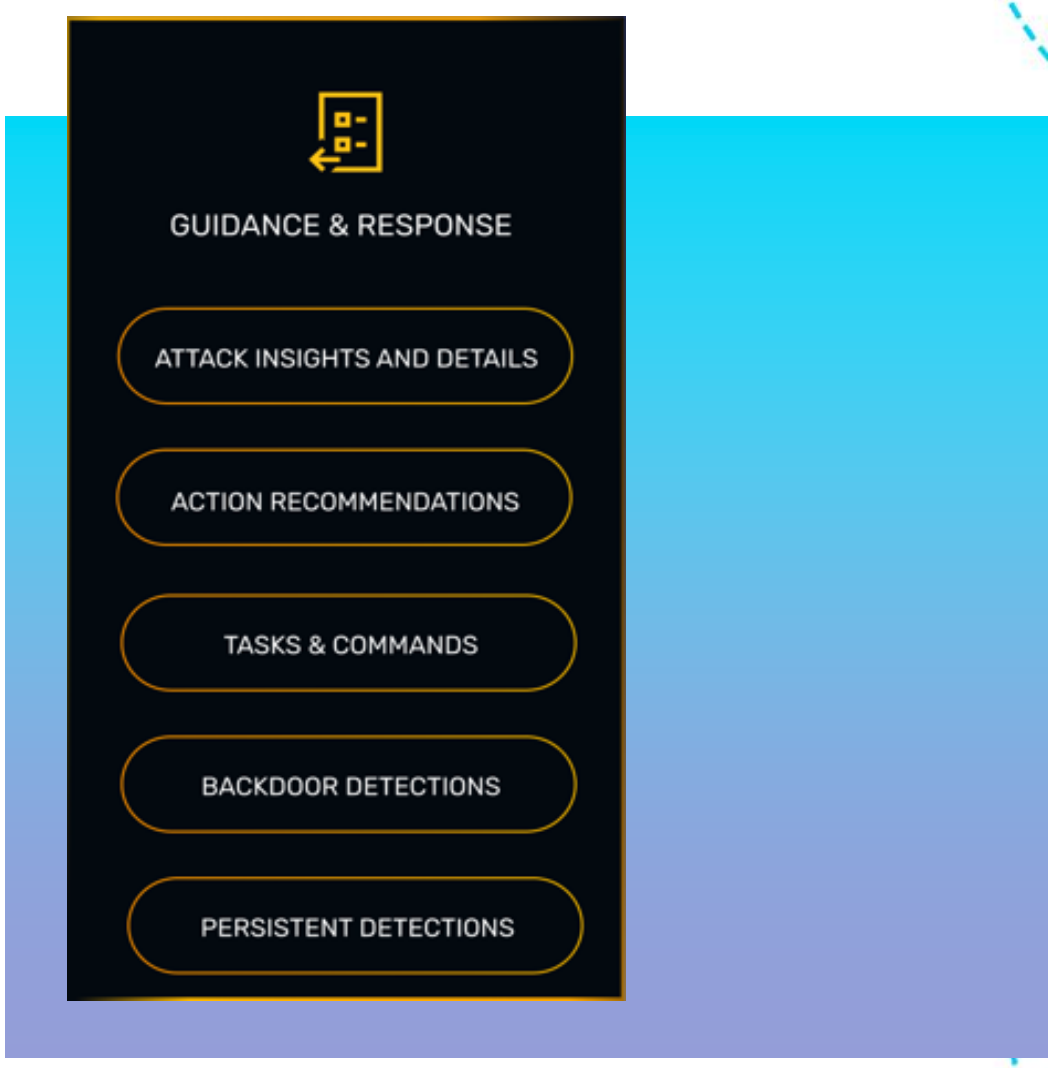
- Not everyone understands the technical aspects of an attack
- Time is of the essence… no time to research

Direction and examples

- Attacks can be complicated - knowing where to go in GUI is key
- PowerShell is powerful, but also complicated – examples make a difference

Playbooks for attack response

- Overview of the attack and consequences
- Step-by-step incident response tasks



Next steps – securing identities!

Summary

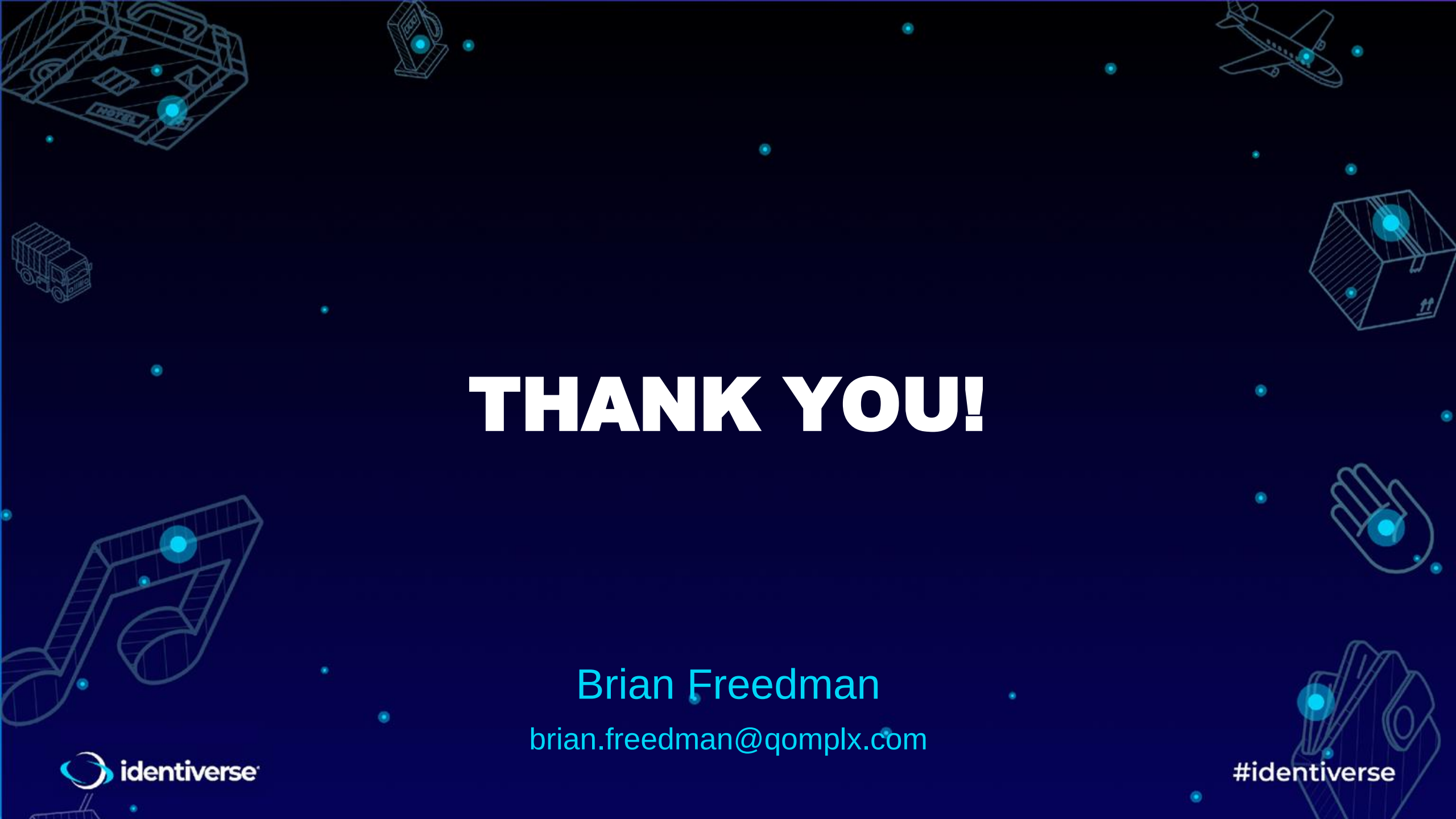
- Attackers are focusing on identities
- Current identity solutions are leaving an identity security gap
- Expand ITDR to include: Prevent + Detect + Response

Get visibility into all identity configurations

- Find and fix existing identity configurations that can be exploited
- Know when identities have new configurations that can be exploited

Realize that no matter what you do to secure identities – attacks can still occur

- Be able to detect simple attacks – password and privilege impersonation
- Be able to detect identity attacks – abusing identity attributes/properties
- Be able to detect identity credential attacks – modification and creation of identity credentials



THANK YOU!

Brian Freedman

brian.freedman@qomplx.com

identiverse

#identiverse