Where there's a breach, there's an identity compromise: What is your counter move?

Yiftach Keshet, VP Product Marketing, Silverfort

SILVERFORT

Would these past attacks work today?

2013: CryptoLocker
Ransomware payload

2011: 'Night Dragon'
Lateral movement techniques

Global Energy Cyberattacks:
"Night Dragon"

By McAfee® Foundstone® Professional Services and McAfee Labs™

February 10, 2011

The dropper will be copied over network shares to the compromised computer and remotely execute with psexec or via Windows Terminal Services (RDP). In some cases, an "AT.job" or "SchTasks" entry

- Using password cracking and pass-the-hash tools, attackers gain additional usernames and passwords, allowing them to obtain further authenticated access to sensitive internal desktops and servers

✔ **Attack fails**

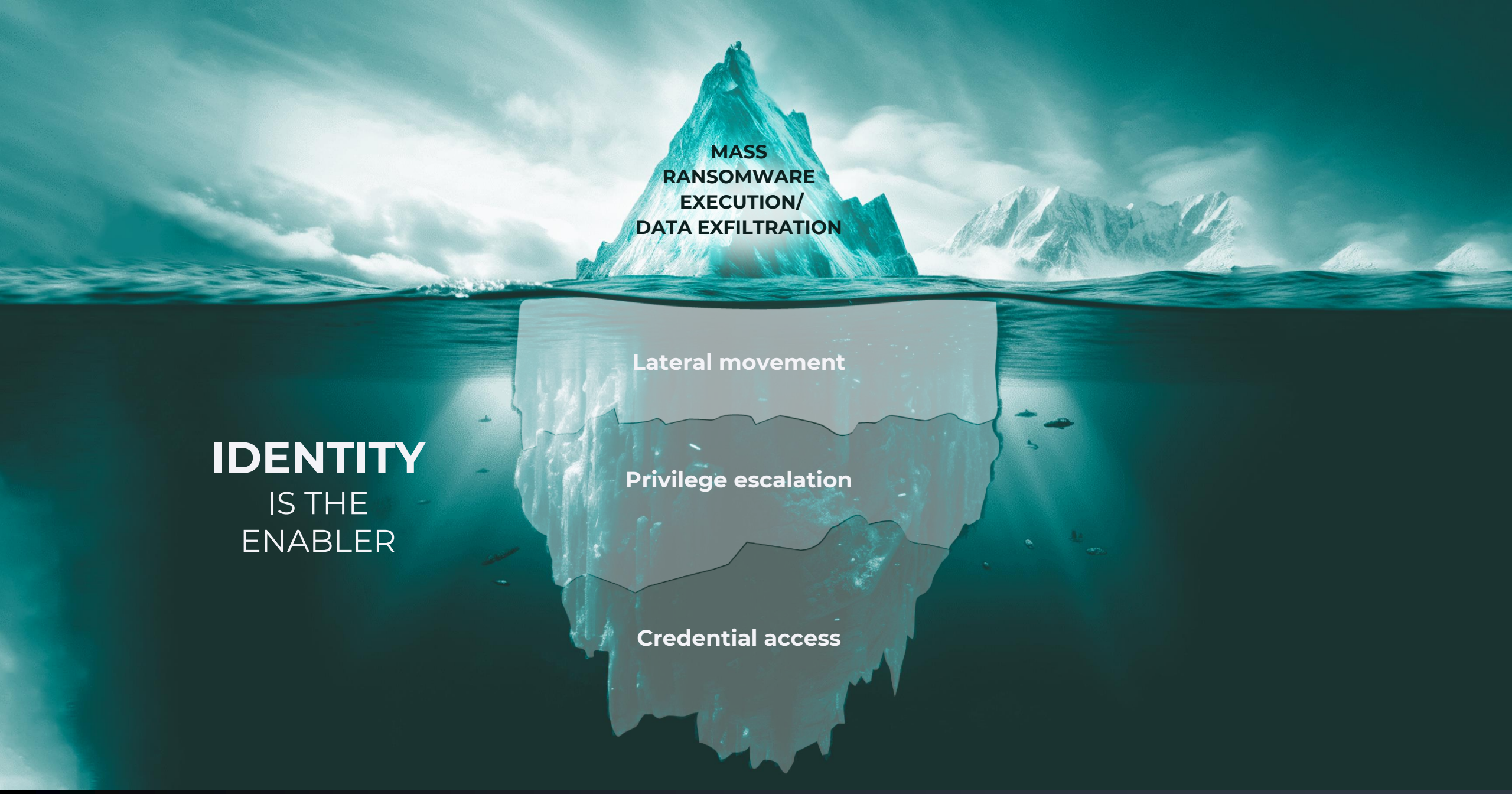
⚠ **Attack succeeds**

Identity security challenge zoom-in

Malicious access with a user account's **compromised credentials** is the **weakest link** in our security stack today

Today’s session:

- **Why are identity threats a blind spot?**
  - Identity attack surface management: threat exposure
  - Identity threat protection: absence of real-time controls against malicious access
- **The unified identity security approach**
  - Native integration with all IAM infrastructure components
  - Continuous monitoring, risk analysis and enforcement on every access attempt
  - Essential capabilities: ISPM, authentication firewall, privileged access, MFA, non-human identities, ITDR



IDENTITY
IS THE
ENABLER

The identity threat exposure gap

2/3 of user accounts authenticate **with NTLM protocol.** → **Credential access**

109 **new shadow admins** are created with a single Active Directory misconfiguration. → **Privilege escalation**

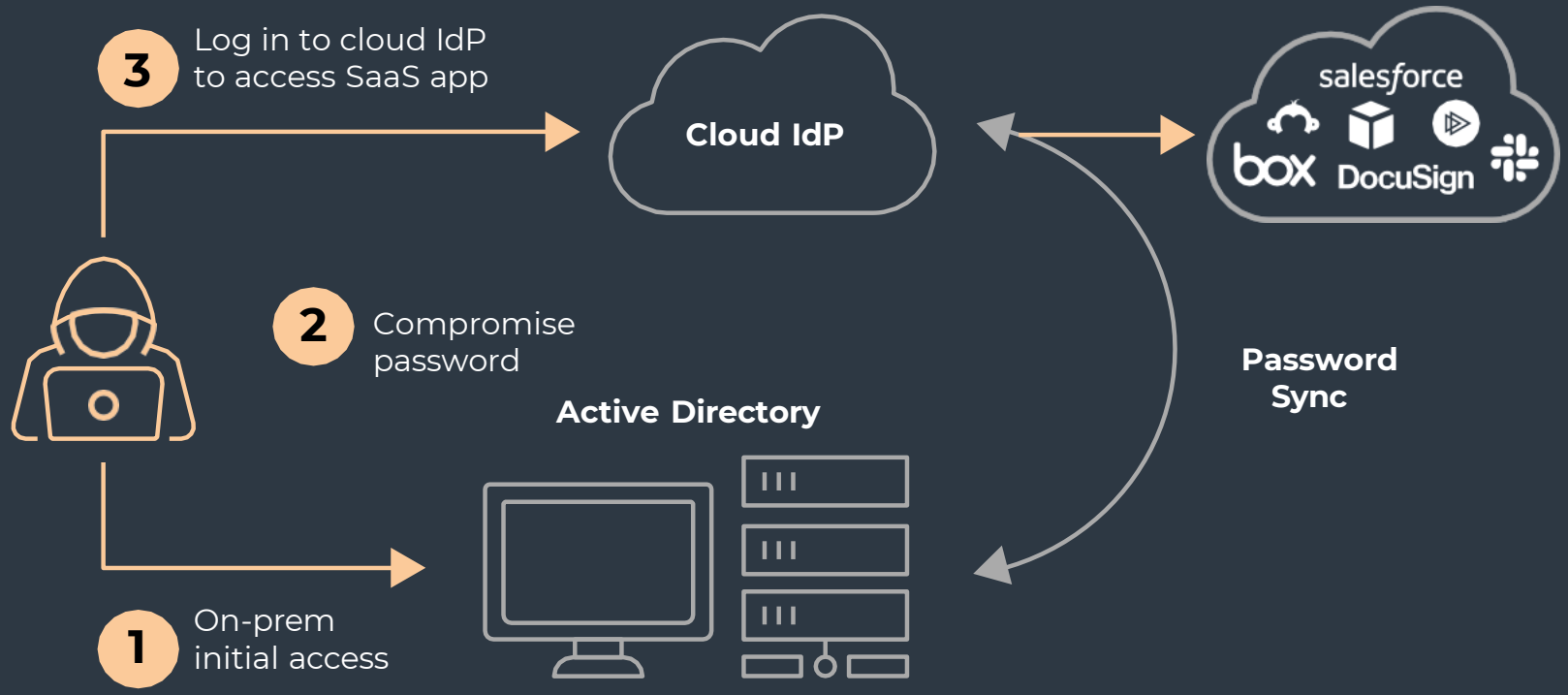
31% of all users are **service accounts,** which are often used by attackers to move laterally. → **Lateral movement**

Source: The Identity Underground Report, 2024

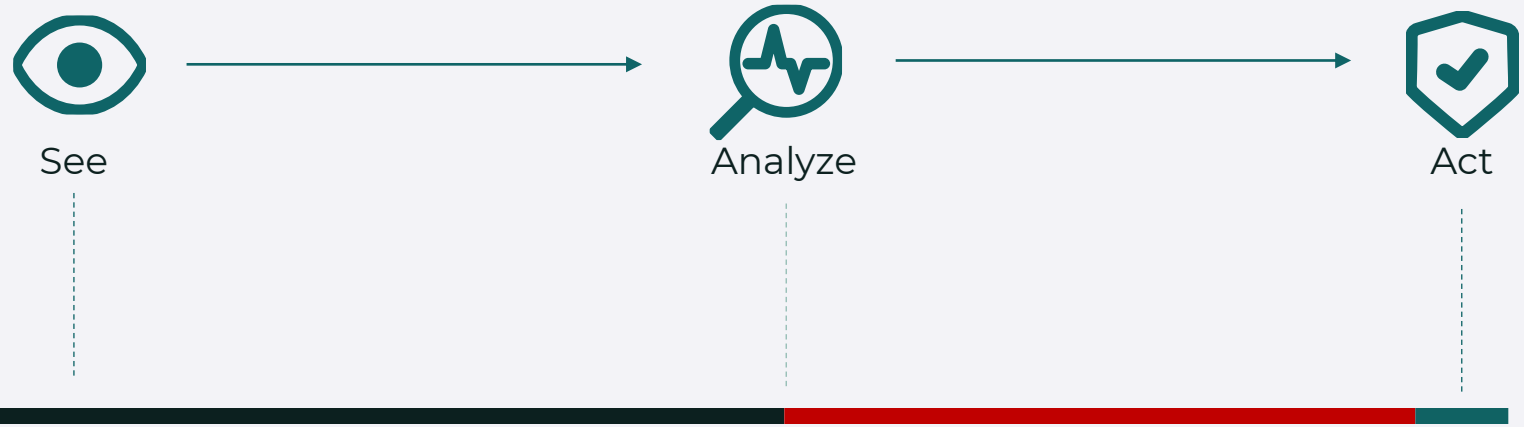
On-prem exposure to identity threats also endangers SaaS

67%

of businesses sync on-prem passwords to the cloud in an insecure manner



Threat protection generic flow



EDR\EPP	Processes/files	Malware	Terminate process/ delete file
Firewall\SSE	Network traffic	Data exfiltration/ insecure destination	Block traffic

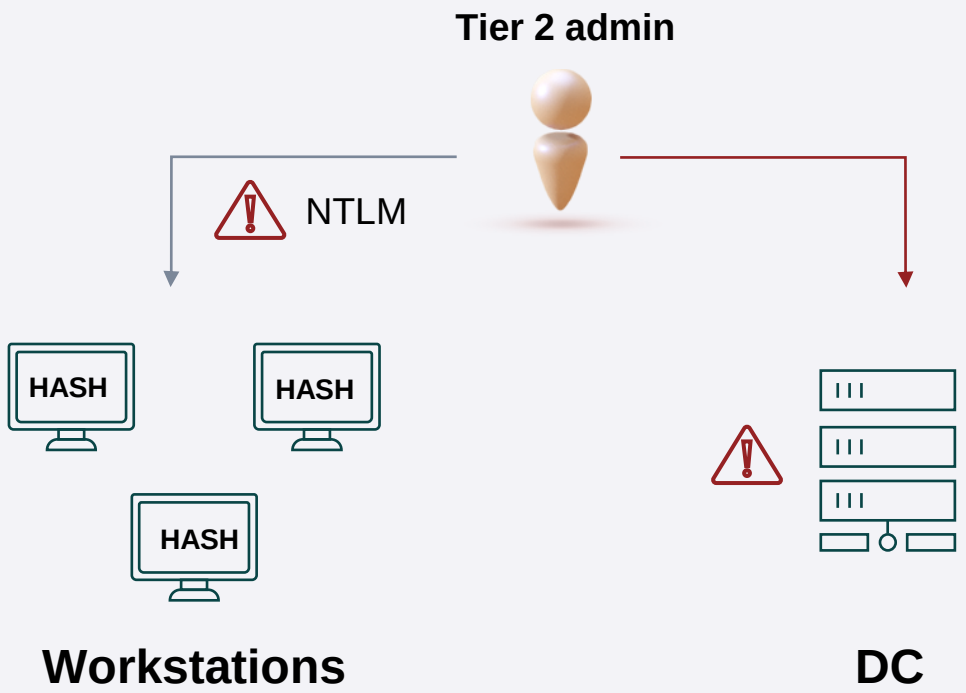
The identity threat protection gap

All human and machine accounts. All on-prem and cloud resources. All access protocols and methods.

Case study: Joe the helpdesk guy

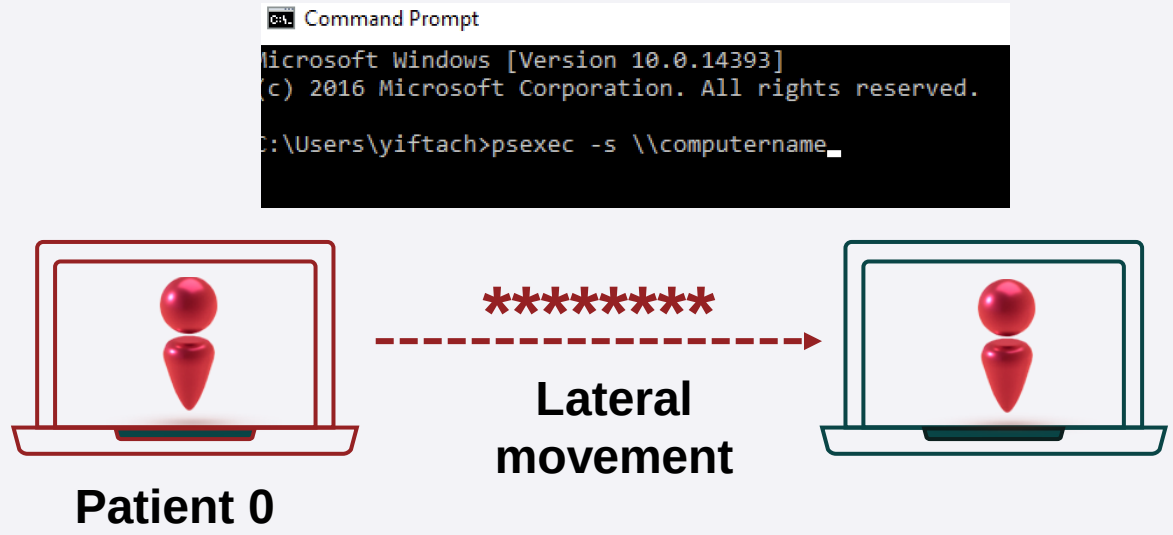
Identity threat exposure

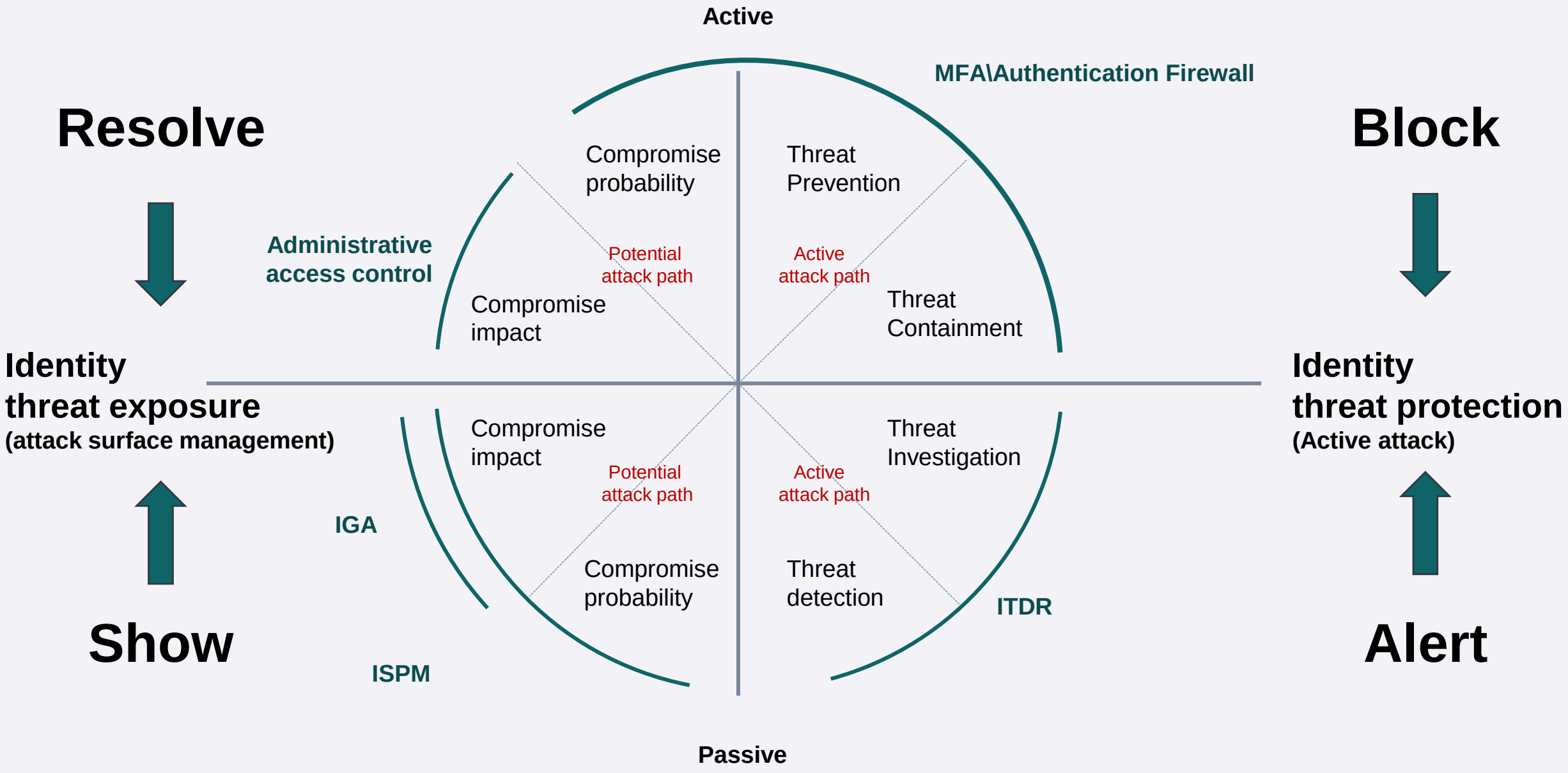
Can you see and resolve?



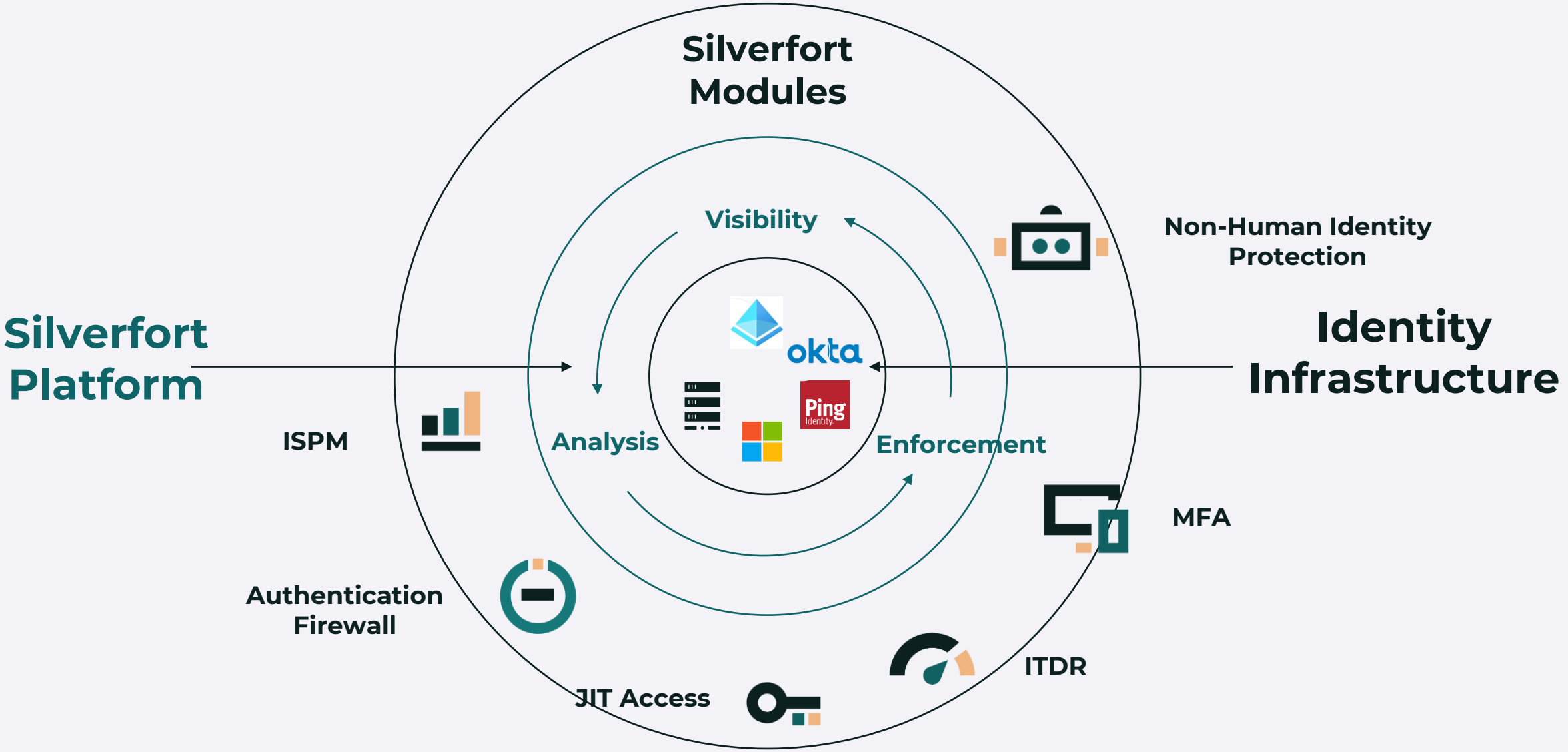
Identity threat protection

Can you detect and block?




Active
MFA\Authentication Firewall
Resolve
Block
Compromise probability
Threat Prevention
Administrative access control
Potential attack path
Active attack path
Compromise impact
Threat Containment
Identity threat exposure
(attack surface management)
Identity threat protection
(Active attack)
Compromise impact
Threat Investigation
Potential attack path
Active attack path
IGA
Compromise probability
Threat detection
ITDR
Show
Alert
ISPM
Passive

Unified Identity Security Platform



Identity Security in Action

Reduce identity threat exposure

Security Posture Monitoring & Hardening

Analyze every access attempt as it happens

Anomaly Detection

Verify detected threats by challenging the user with MFA

Verification

Block access attempts that were verified as malicious in real time

Protection

All users. All resources. All on-prem and cloud environments.

SILVERFORT

Thank You