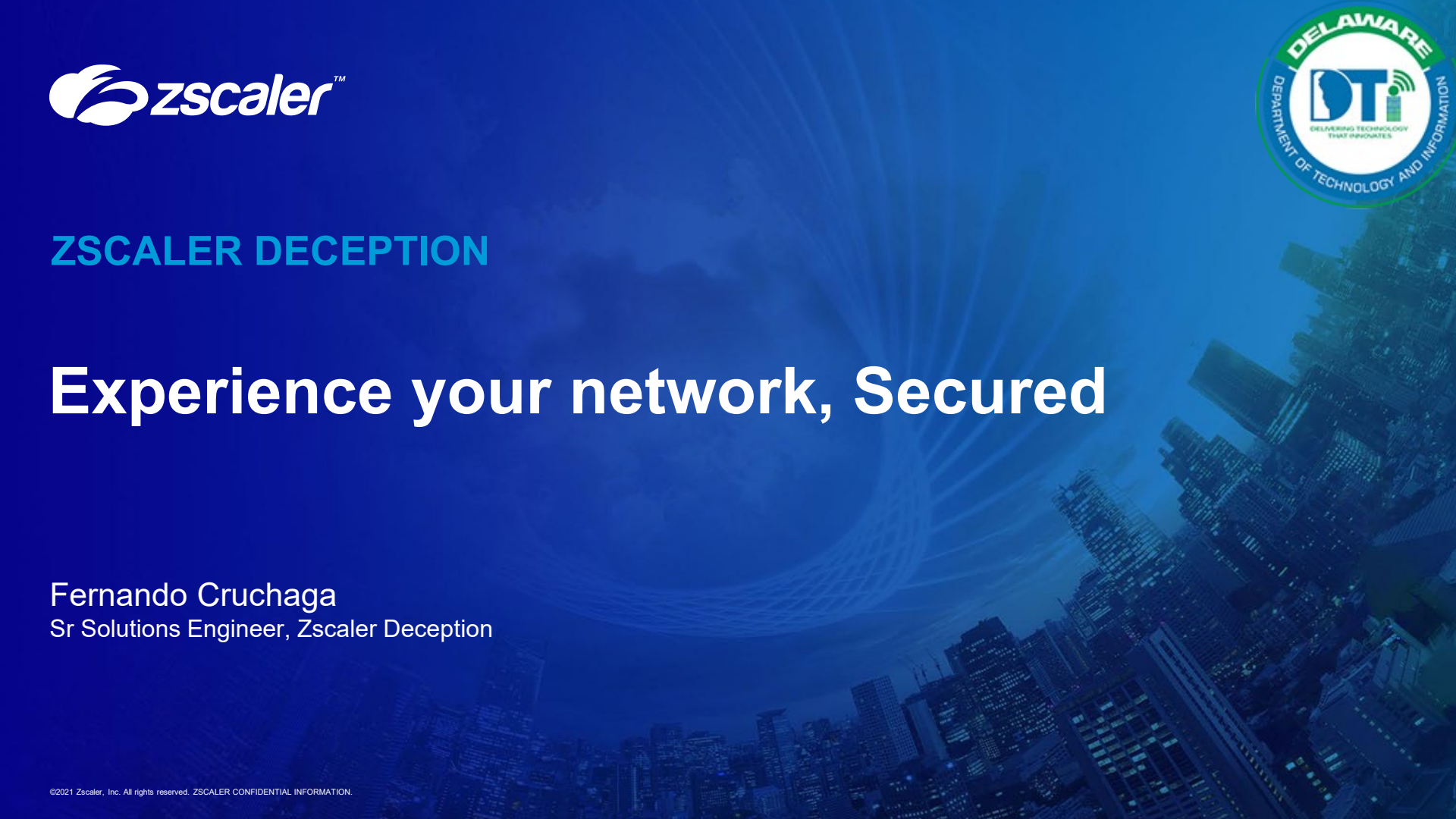
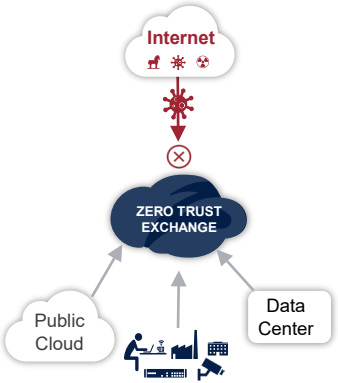


Zero Trust Security: Cyber Threat Protection

Prevent Compromise

Block threats before they reach you



Protects users, servers, apps, IoT, OT systems

ZIA

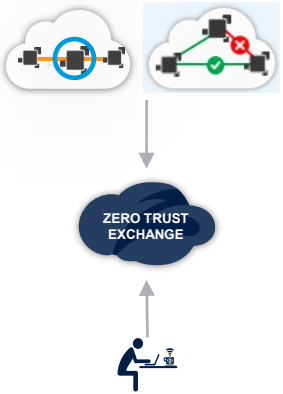
Apps invisible to the internet

Can't attack what you can't see

ZPA

Prevent Lateral Movement

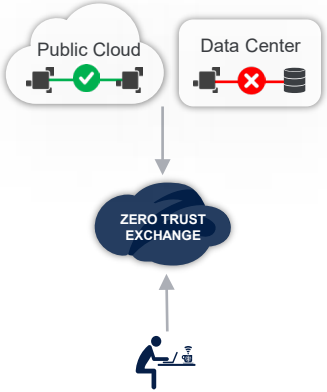
User & App Segmentation



Connects users to apps, not networks

ZPA + ZWS

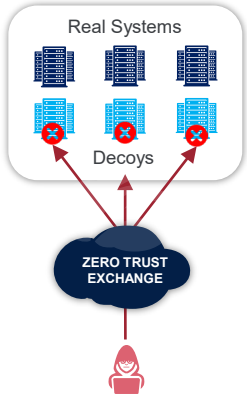
In-line Inspection & Web Isolation



Full In-line inspection of private App traffic, Remote Browser Isolation

ZPA

Decoys detect sophisticated threats



Attackers attempting to move laterally are detected & contained

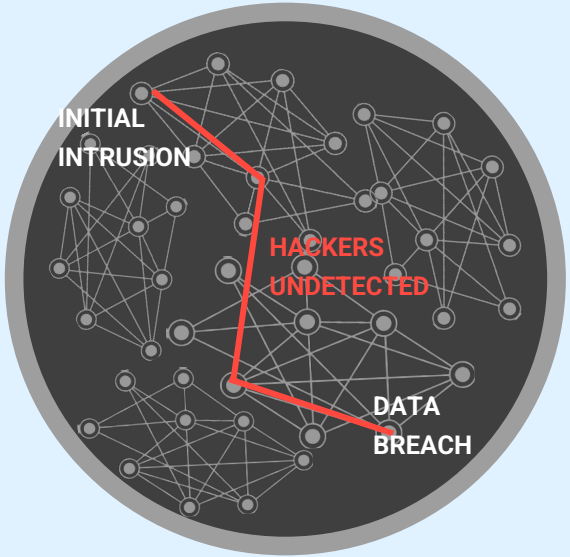
Deception

What sets Zscaler Cyber Threat Protection apart?

Zero Passthrough Connections **Zero Attack surface** **Zero Lateral Movement**

The Problem

Sophisticated attackers are stealthy



91% of attacks don't even generate a security alert.

SOURCE: MANDIANT

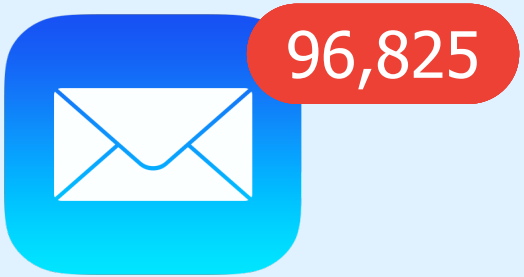
Advanced attacks are human-operated

- Use active reconn / discovery
- Clone normal behavior
- Make real-time judgements

68% of attacks are not malware-based.

SOURCE: CROWDSTRIKE

Security analysts chase ghosts and burn out



Monitoring team faces

- Event fatigue
- Data paralysis
- Missed alerts

45% of alerts are false positives.

SOURCE: ESG

Current approach puts the burden on the defenders who are stretched thin

Use Cases

Where is Deception being used

What are experts saying

Gartner On Deception

"Prioritize alerts from the deception platforms as high-priority, high-fidelity alerts that need immediate attention."

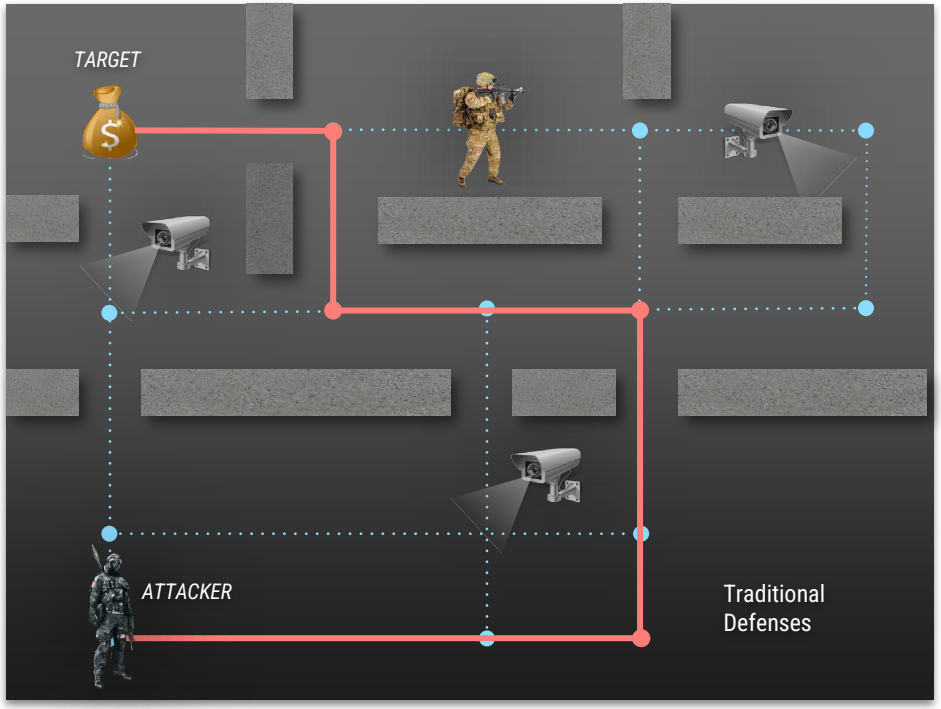
"Security leaders looking to build or expand their threat detection function should include deception tools in their stack."

MITRE | Engage

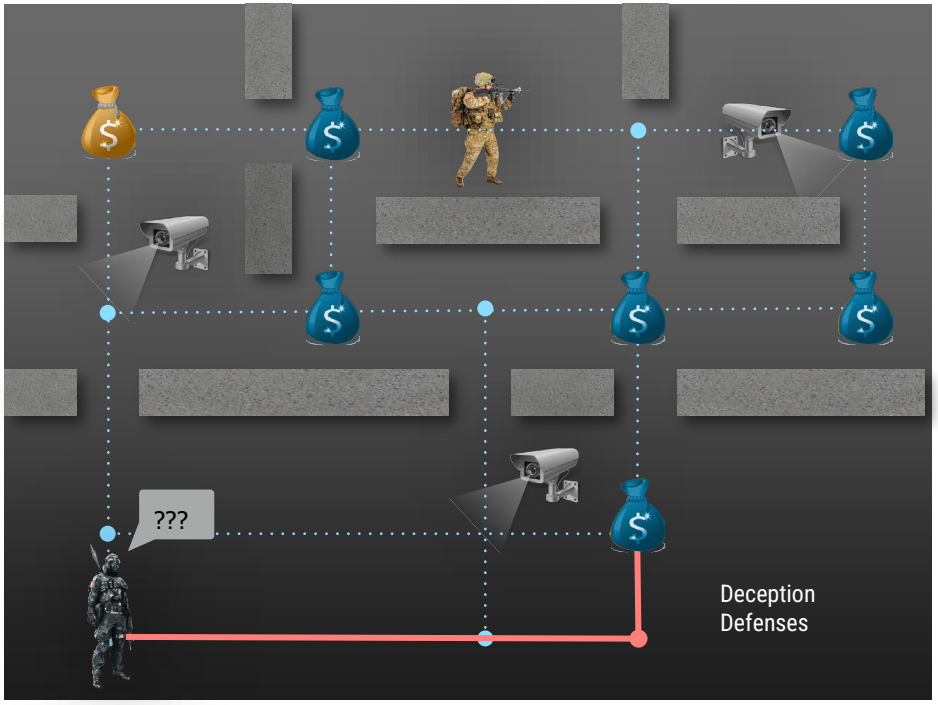
Launched Framework for planning adversary engagement, deception and denial activities in order to help execute strategies and technologies

Changing the game

Deception disrupts advanced attacks



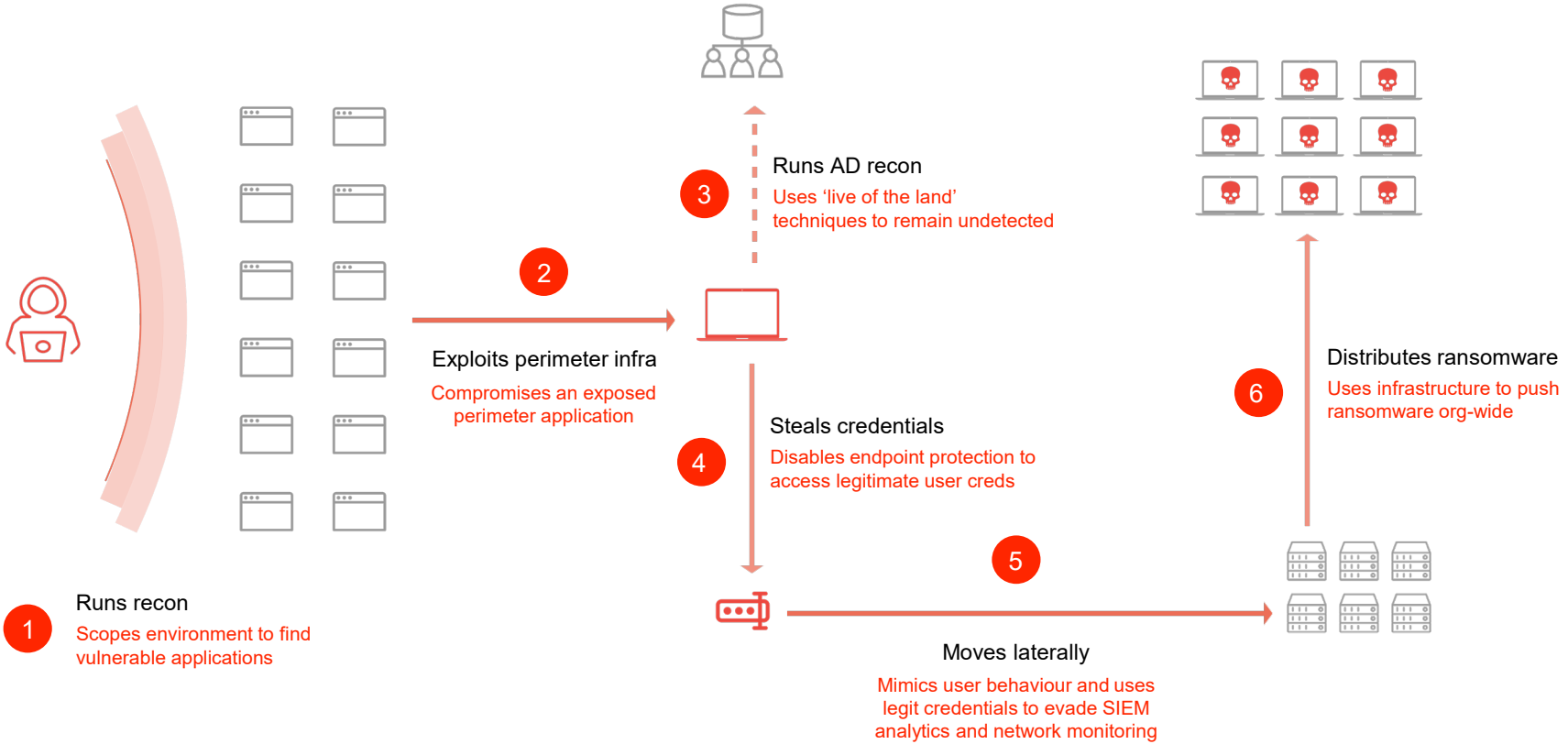
Attackers know your strategy. Predictable defenses are easily bypassed



Decoys and traps make your environment unpredictable, disrupt attacker playbooks

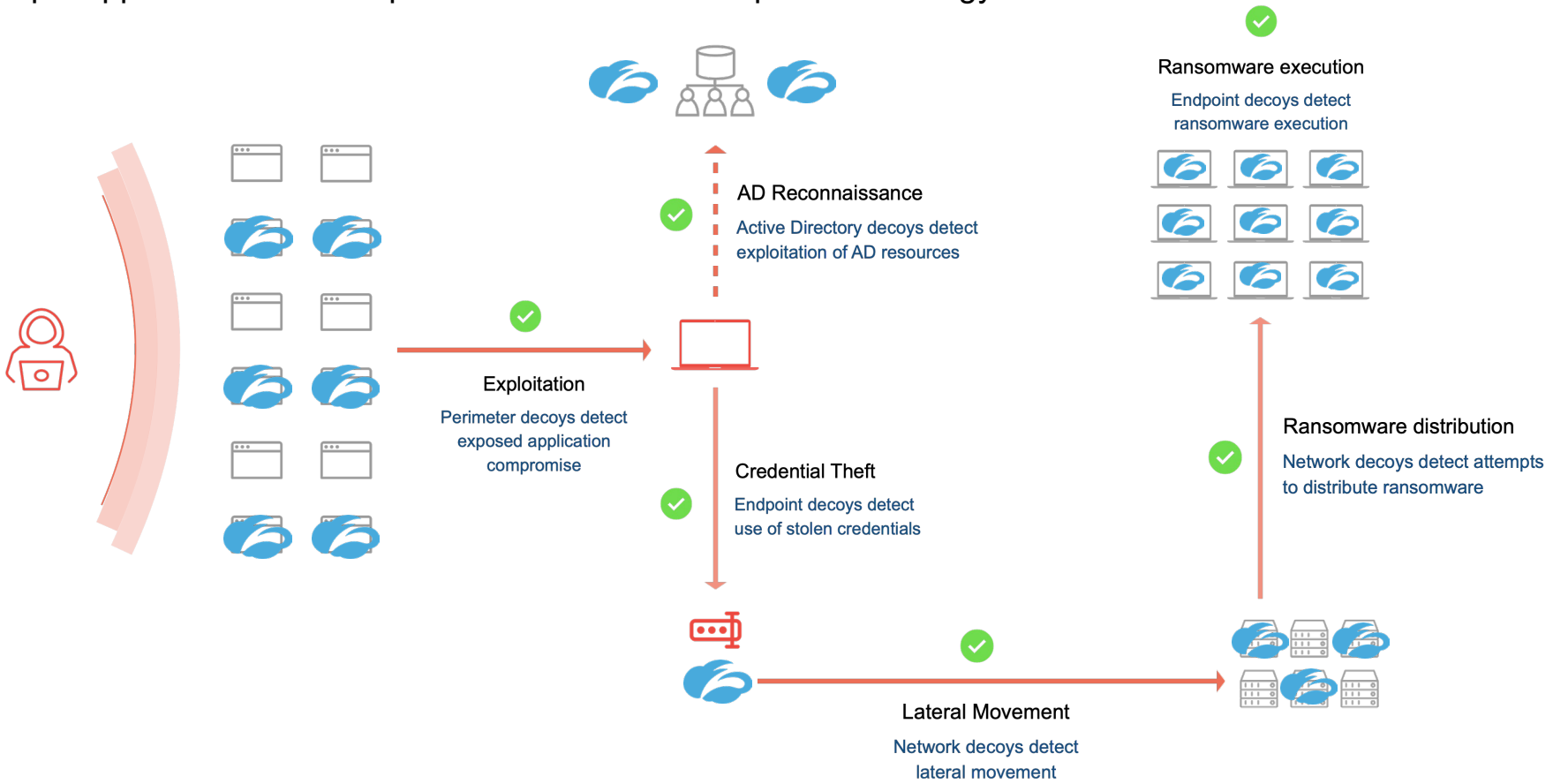
The anatomy of an advanced attack

How and why ransomware succeeds



The anatomy of an adversary engagement

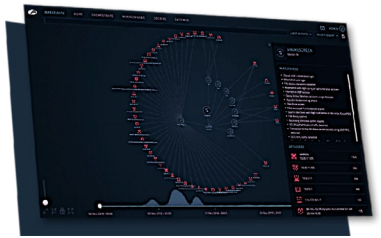
Multiple opportunities to disrupt ransomware with deception technology



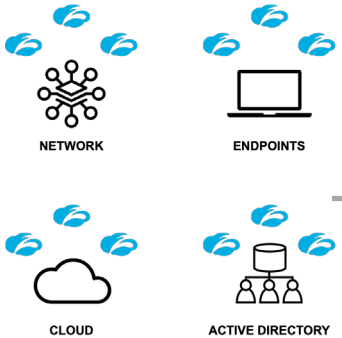
The solution

Zscaler Deception

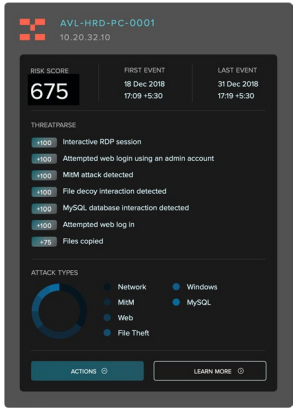
Configure and Deploy



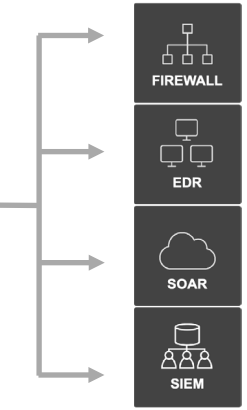
Detect threats



Investigate

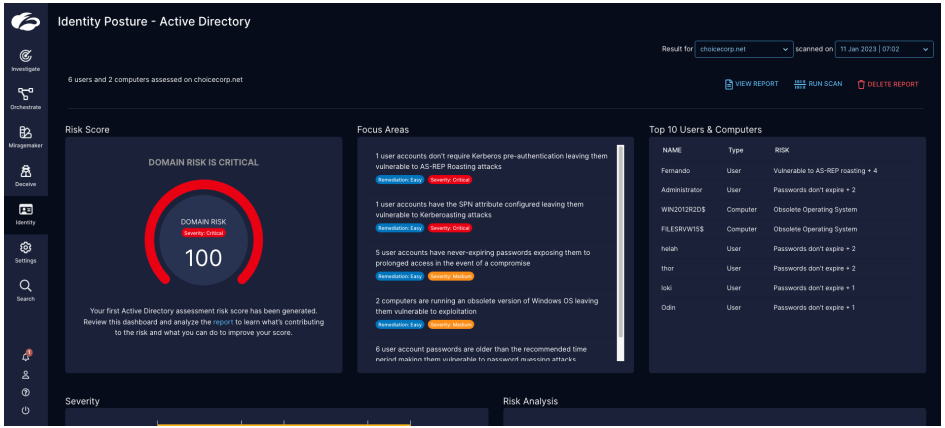


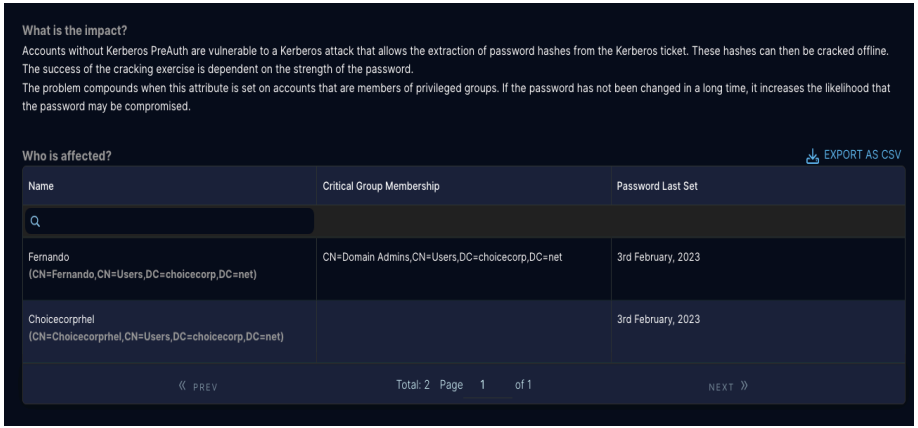
Contain

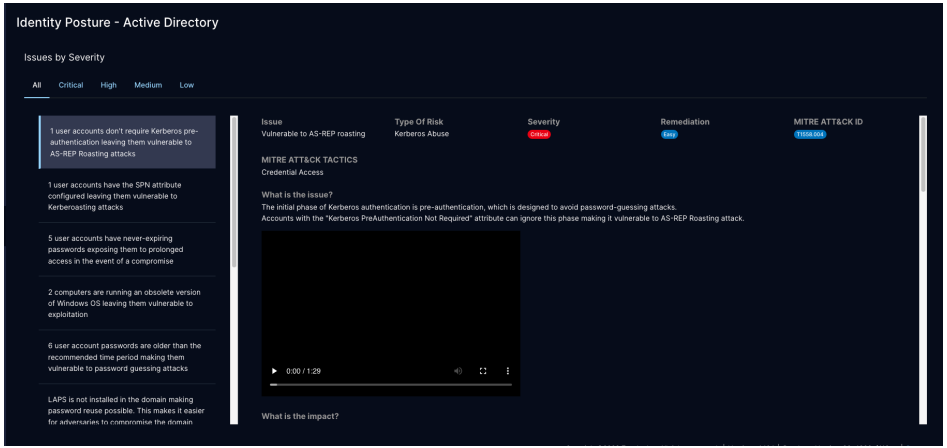


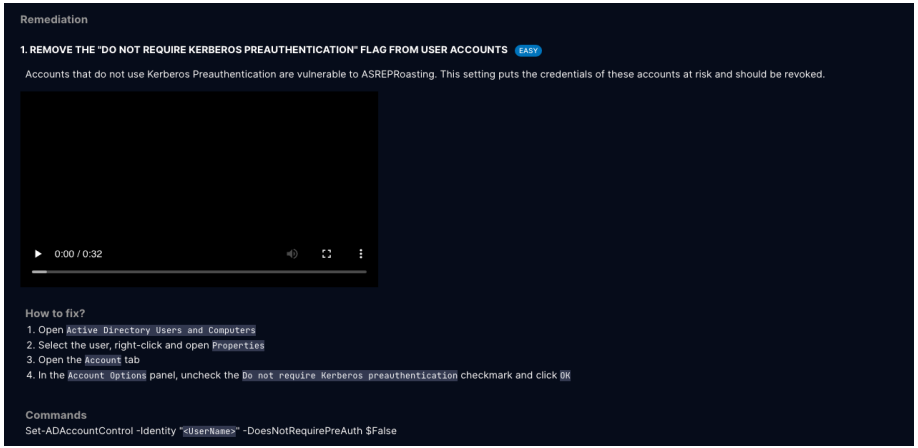
Active Directory Risk

Zscaler Deception









Why Zscaler Deception

Benefits of integrated Deception and Adversary Engagement

+167%

Average increase in ‘Opportunity to Detect’ advanced attacks like ransomware

+50%

Average increase visibility for targeted threats not found in threat intel feeds

+90%

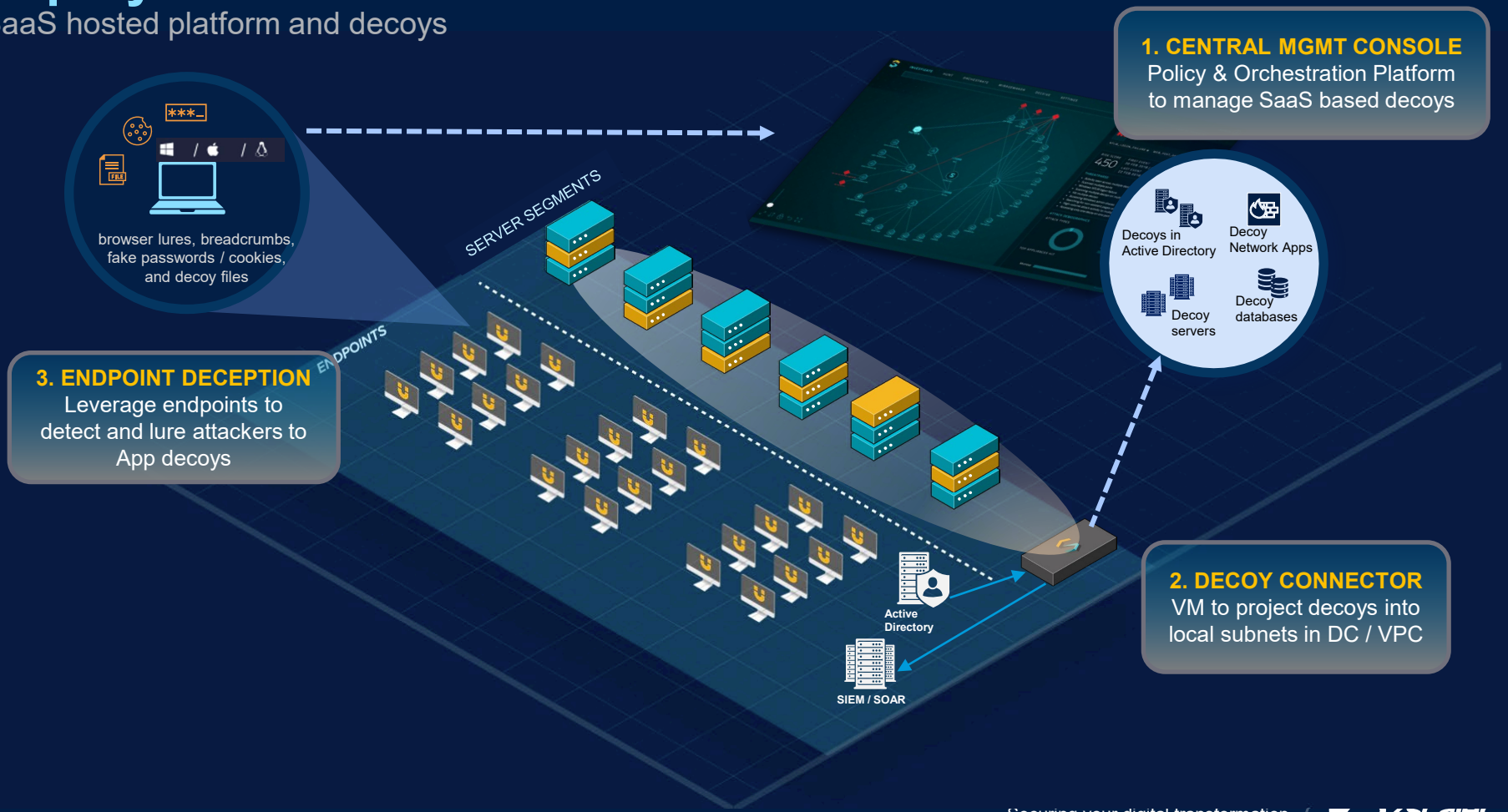
Average improvement in ability to detect an advanced threat in the early stages of an attack

98%

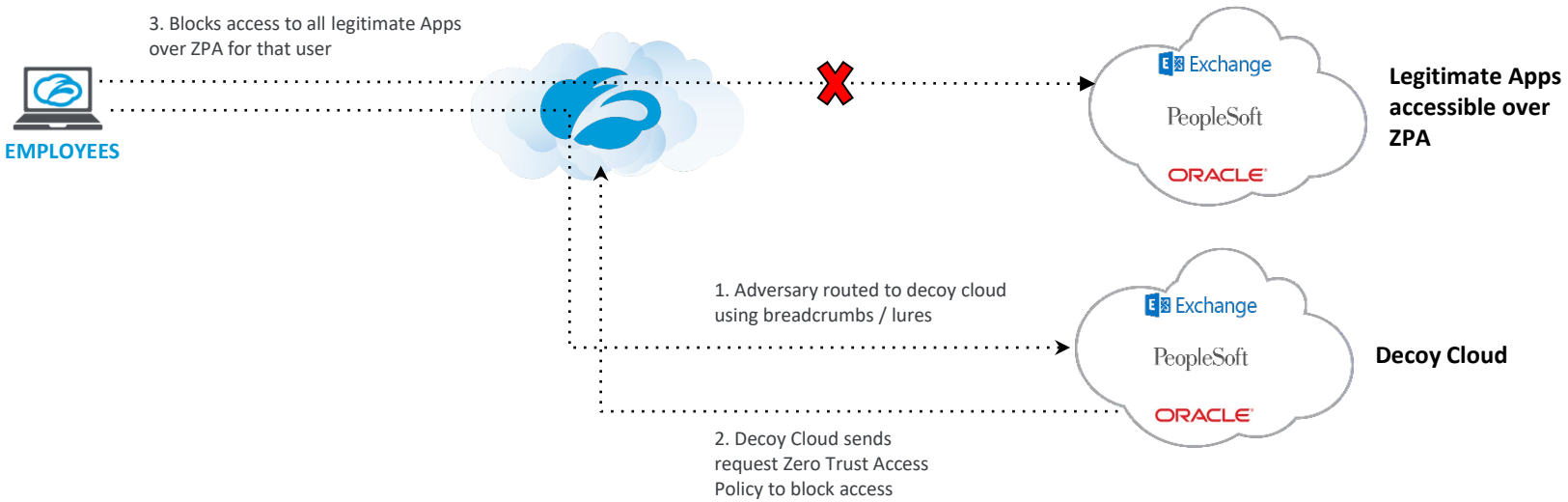
Average lesser alert volume than traditional detection controls

Deployment Architecture

SaaS hosted platform and decoys



Use cases - Native containment



Operationalize your MITRE ENGAGE Framework

Zscaler Deception provides coverage for 99% capabilities for strategic deception and denial activities