

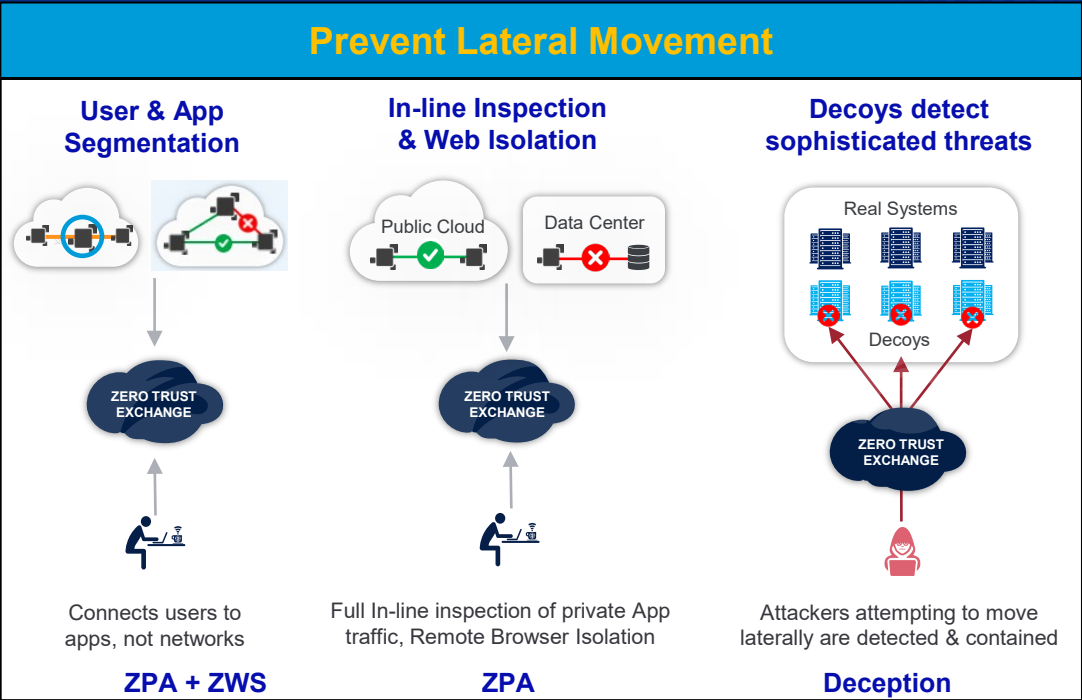
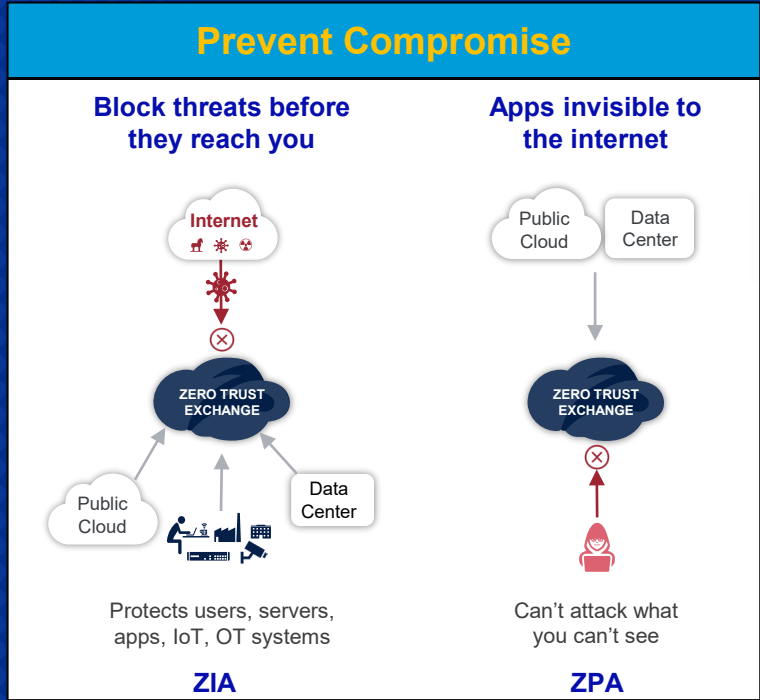


ZSCALER DECEPTION

Experience your network, Secured

Fernando Cruchaga
Sr Solutions Engineer, Zscaler Deception

Zero Trust Security: Cyber Threat Protection



What sets Zscaler Cyber Threat Protection apart?

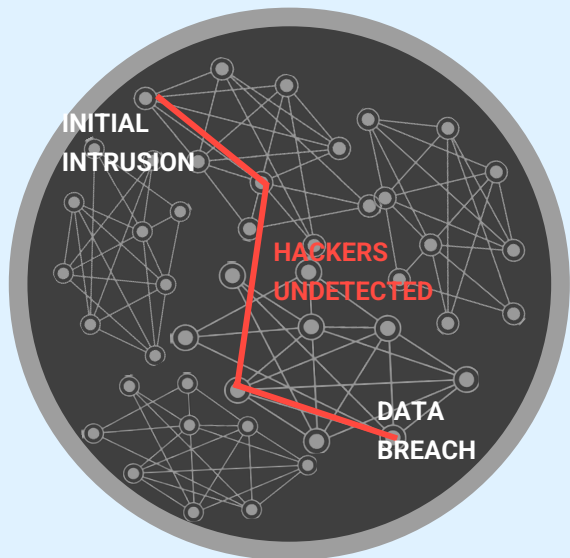
Zero Passthrough Connections

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.”

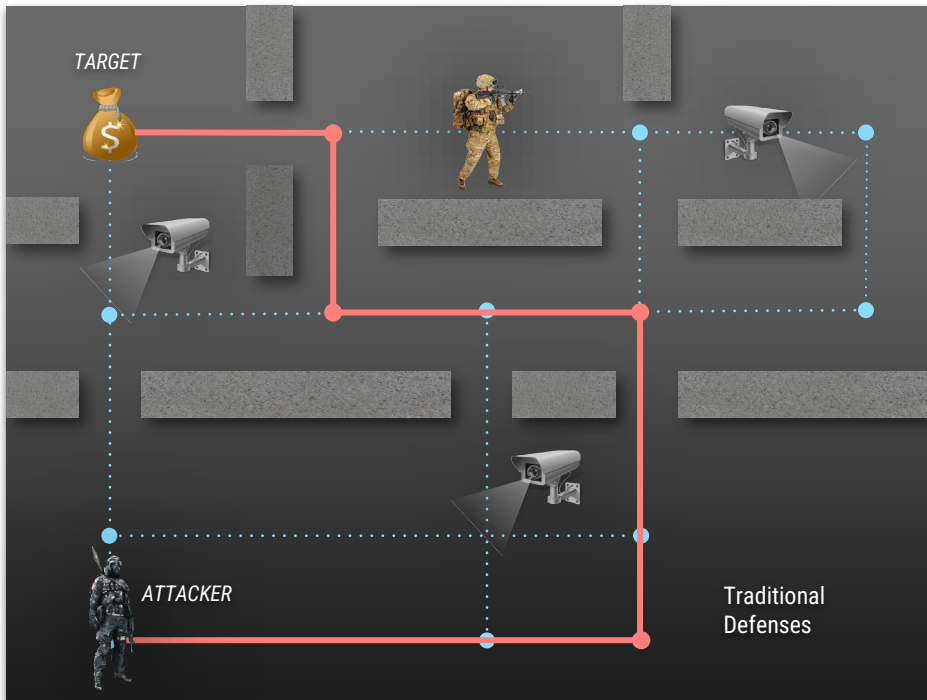
“Security leaders looking to build or expand their threat detection function should include deception tools in their stack.”

MITRE Engage

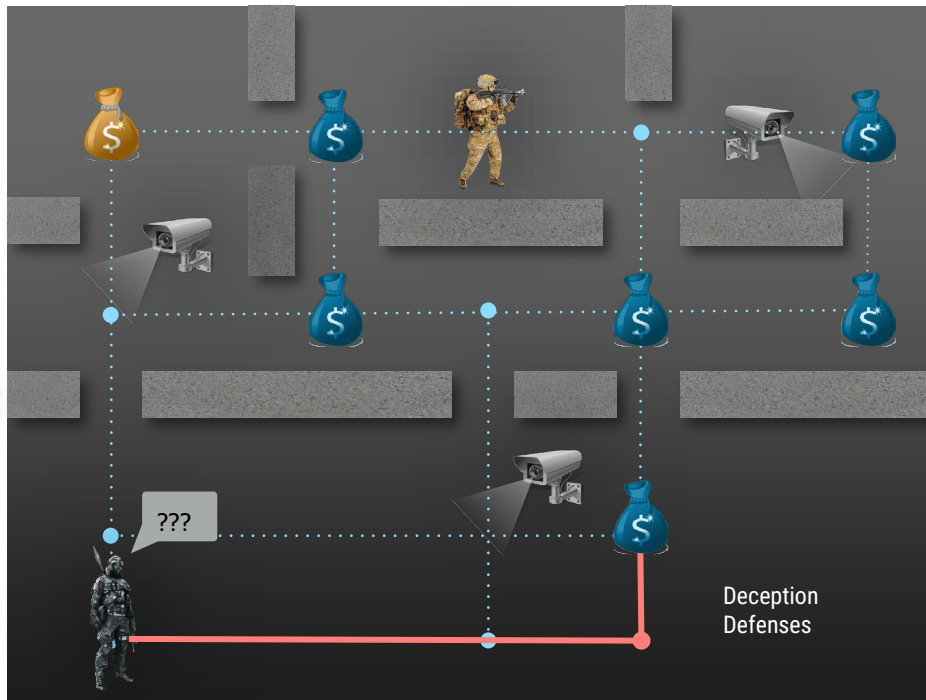
Launched Framework for planning adversary engagement, deception and denial activities in order to help execute strategies and technologies

Changing the game

Deception disrupts advanced attacks



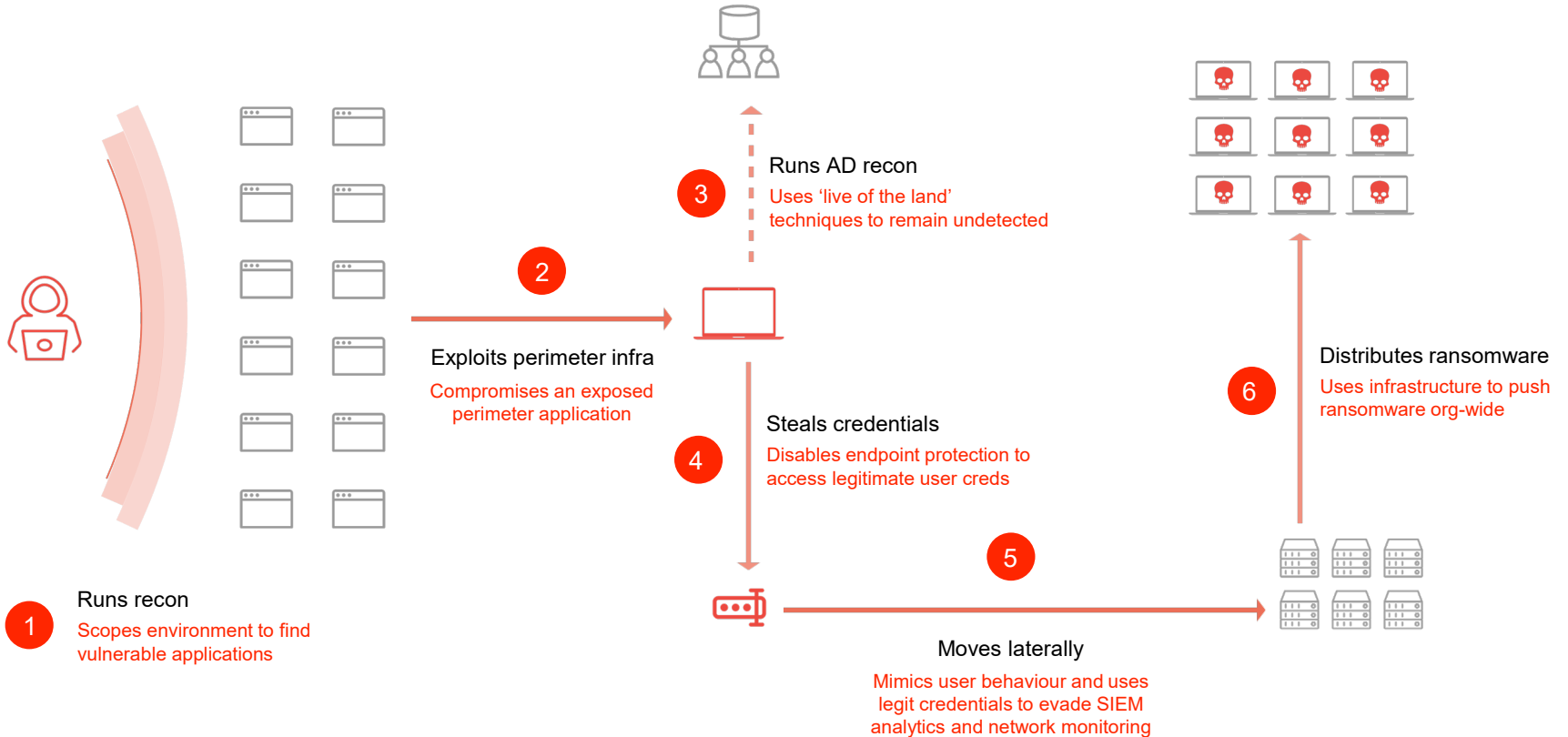
Attackers know your strategy. Predictable defenses are easily bypassed



Decoys and traps make your environment unpredictable, disrupt attacker playbooks

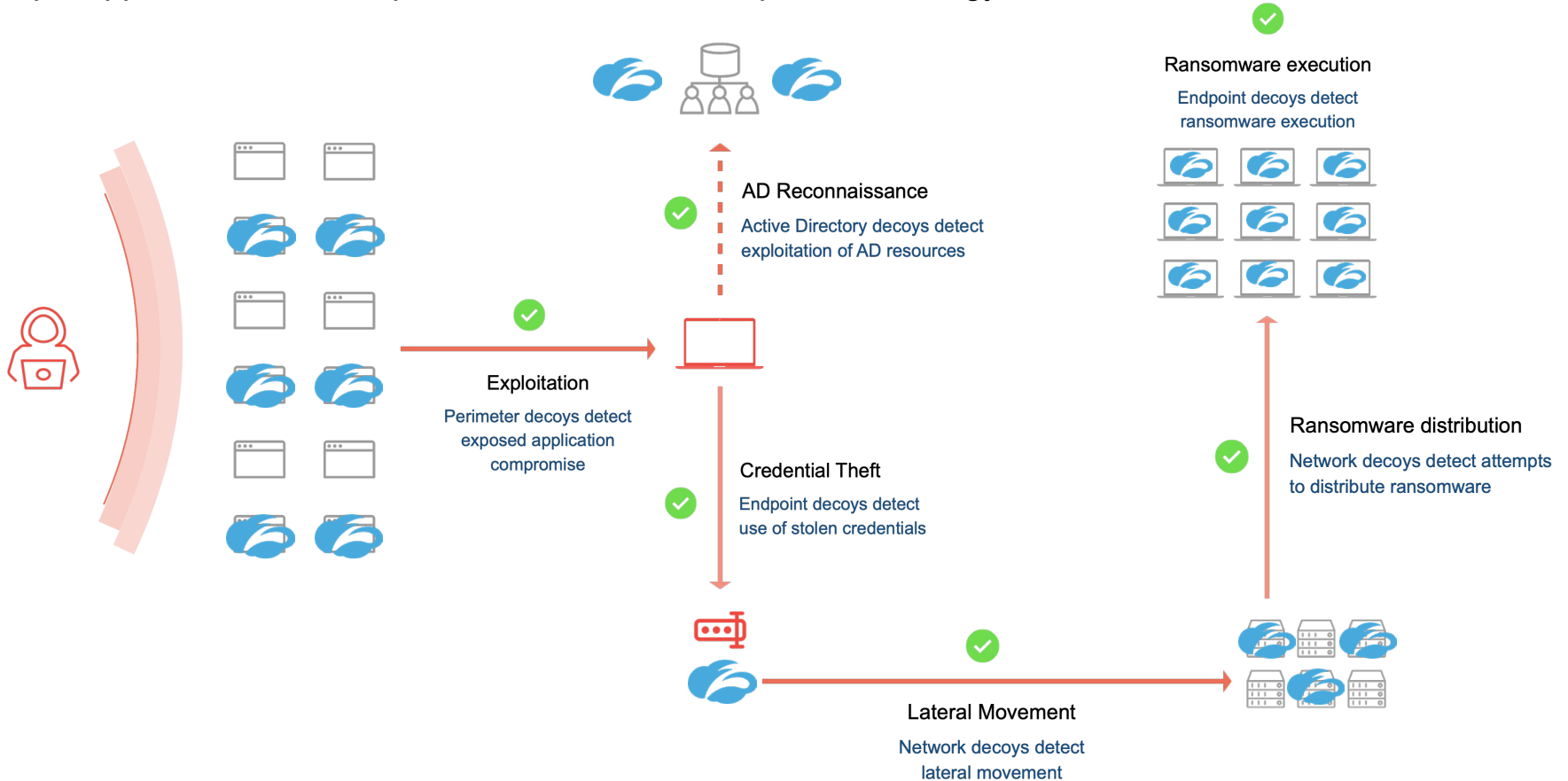
The anatomy of an advanced attack

How and why ransomware succeeds



The anatomy of an adversary engagement

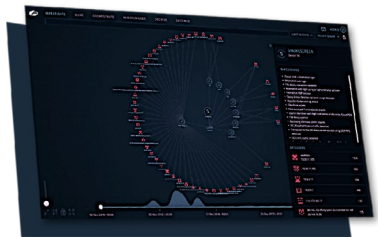
Multiple opportunities to disrupt ransomware with deception technology



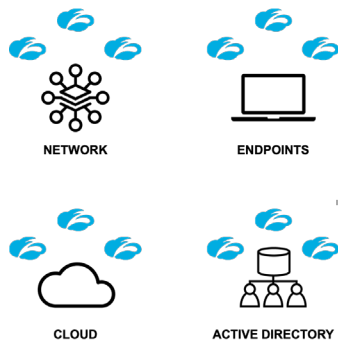
The solution

Zscaler Deception

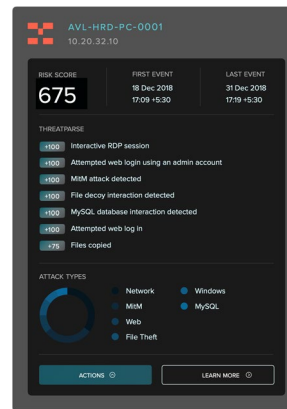
Configure and Deploy



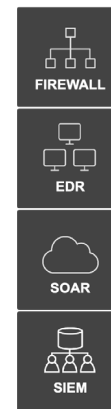
Detect threats



Investigate



Contain



Active Directory Risk

Zscaler Deception

Identity Posture - Active Directory

Result for: choicecorp.net | Scanned on: 11 Jan 2023 | 07:02

6 users and 2 computers assessed on choicecorp.net

Risk Score

DOMAIN RISK IS CRITICAL

DOMAIN RISK **100**

Your first Active Directory assessment risk score has been generated. Review this dashboard and analyze the report to learn what's contributing to the risk and what you can do to improve your score.

Focus Areas

- 1 user accounts don't require Kerberos pre-authentication leaving them vulnerable to AS-REP Roasting attacks
- 1 user accounts have the SPN attribute configured leaving them vulnerable to Kerberoasting attacks
- 5 user accounts have never-expiring passwords exposing them to prolonged access in the event of a compromise
- 2 computers are running an obsolete version of Windows OS leaving them vulnerable to exploitation
- 6 user account passwords are older than the recommended time period making them vulnerable to password-guessing attacks

Top 10 Users & Computers

NAME	Type	RISK
Fernando	User	Vulnerable to AS-REP Roasting + 4
Administrator	User	Passwords don't expire + 2
WIN2012R2D3	Computer	Obsolete Operating System
FILESRVW55	Computer	Obsolete Operating System
hellah	User	Passwords don't expire + 2
thor	User	Passwords don't expire + 2
lali	User	Passwords don't expire + 1
Odin	User	Passwords don't expire + 1

What is the impact?

Accounts without Kerberos PreAuth are vulnerable to a Kerberos attack that allows the extraction of password hashes from the Kerberos ticket. These hashes can then be cracked offline. The success of the cracking exercise is dependent on the strength of the password. The problem compounds when this attribute is set on accounts that are members of privileged groups. If the password has not been changed in a long time, it increases the likelihood that the password may be compromised.

Who is affected?

Name	Critical Group Membership	Password Last Set
Fernando (CN=Fernando,CN=Users,DC=choicecorp,DC=net)	CN=Domain Admins,CN=Users,DC=choicecorp,DC=net	3rd February, 2023
Choicecorphel (CN=Choicecorphel,CN=Users,DC=choicecorp,DC=net)		3rd February, 2023

Total: 2 Page 1 of 1

Identity Posture - Active Directory

Issues by Severity

All Critical High Medium Low

1 user accounts don't require Kerberos pre-authentication leaving them vulnerable to AS-REP Roasting attacks

Issue: Vulnerable to AS-REP Roasting
Type Of Risk: Kerberos Abuse
Severity: **Critical**
Remediation: **Easy**
MITRE ATT&CK ID: **T1080**

MITRE ATT&CK TACTICS: Credential Access

What is the issue?
The initial phase of Kerberos authentication is pre-authentication, which is designed to avoid password-guessing attacks. Accounts with the "Kerberos PreAuthentication Not Required" attribute can ignore this phase making it vulnerable to AS-REP Roasting attack.

1 user accounts have the SPN attribute configured leaving them vulnerable to Kerberoasting attacks

5 user accounts have never-expiring passwords exposing them to prolonged access in the event of a compromise

2 computers are running an obsolete version of Windows OS leaving them vulnerable to exploitation

6 user account passwords are older than the recommended time period making them vulnerable to password-guessing attacks

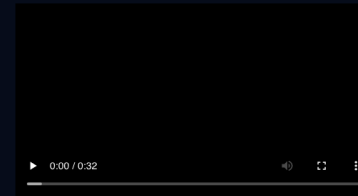
LAPS is not installed in the domain making password reuse possible. This makes it easier for adversaries to compromise the domain.

What is the impact?

Remediation

1. REMOVE THE "DO NOT REQUIRE KERBEROS PREAUTHENTICATION" FLAG FROM USER ACCOUNTS **EASY**

Accounts that do not use Kerberos Preauthentication are vulnerable to ASREP Roasting. This setting puts the credentials of these accounts at risk and should be revoked.



How to fix?

1. Open **Active Directory Users and Computers**
2. Select the user, right-click and open **Properties**
3. Open the **Account** tab
4. In the **Account options** panel, uncheck the **Do not require Kerberos preauthentication** checkmark and click **OK**

Commands

Set-ADAccountControl -Identity "UserName" -DoesNotRequirePreAuth \$False

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%

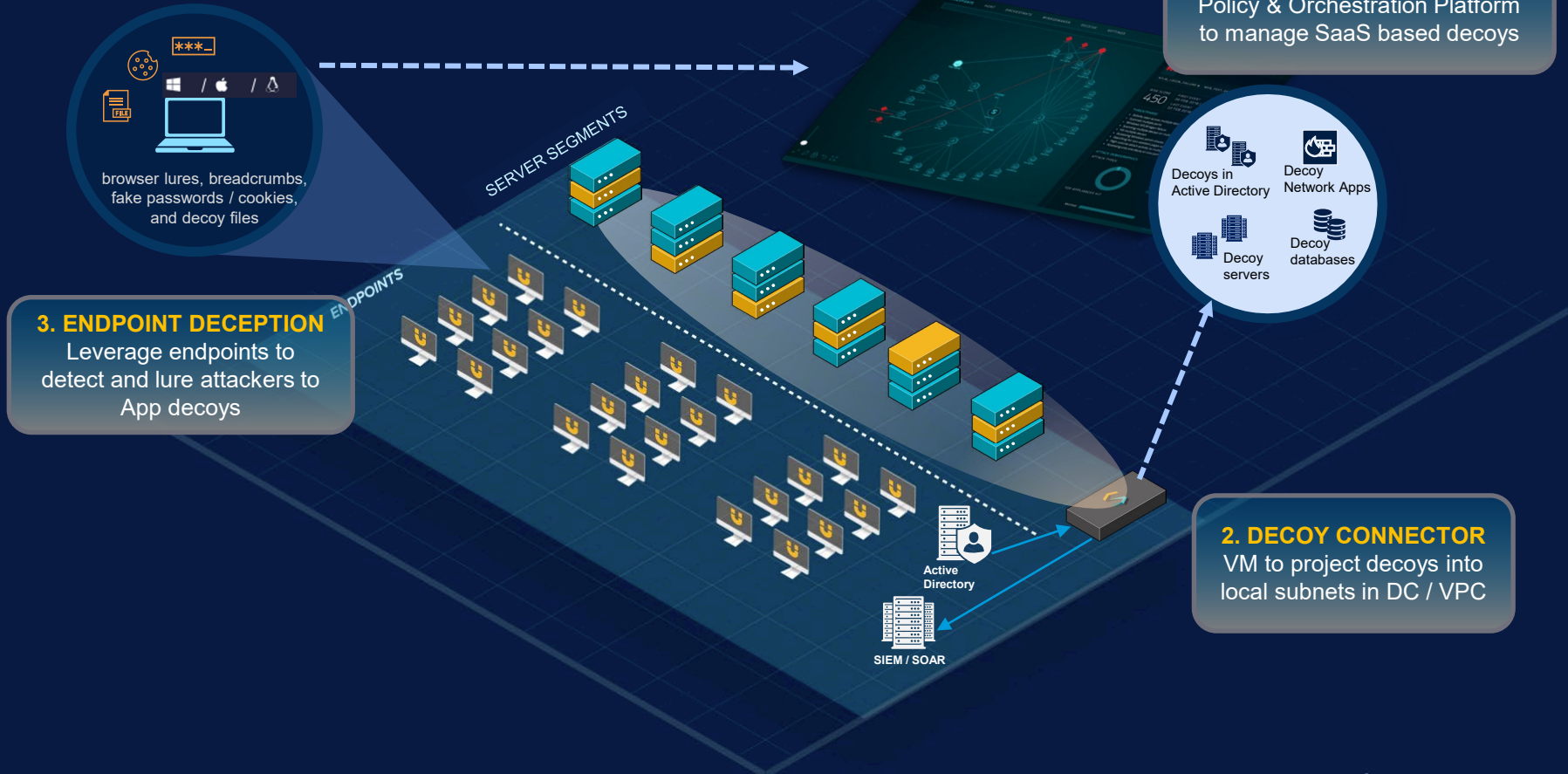
Average improvement in ability to detect an advanced threat in the early stages of an attack

98%

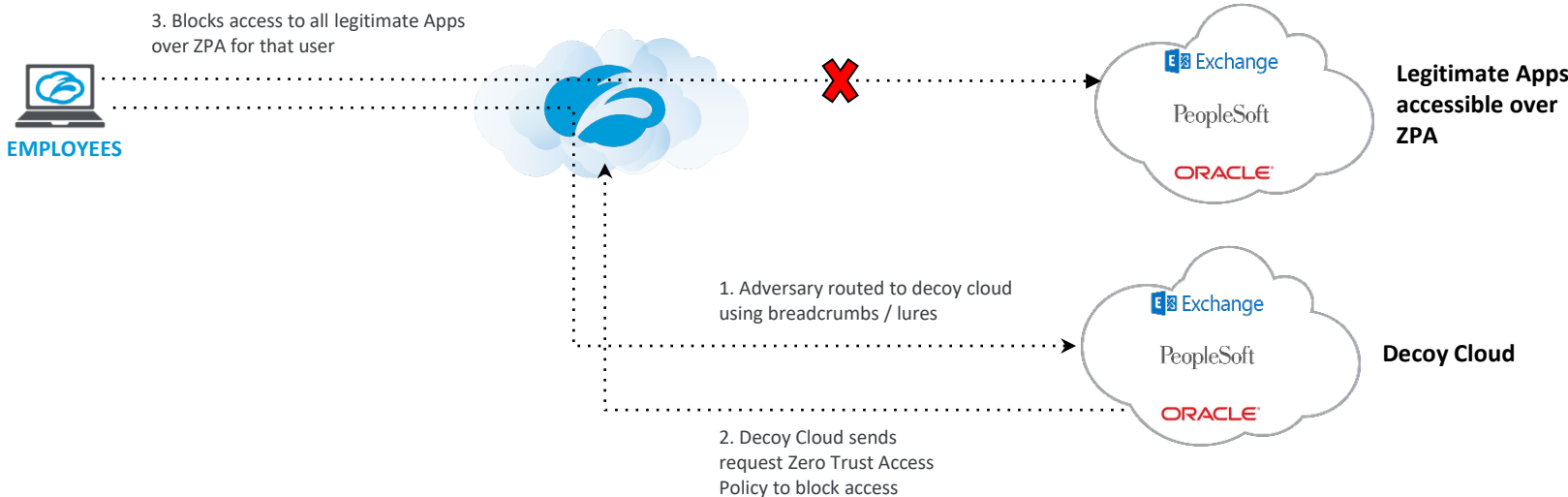
Average lesser alert volume than traditional detection controls

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

PREPARE	EXPOSE		AFFECT			ELICIT		UNDERSTAND
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and systems	Baseline	Decoy Artifacts and systems	Decoy Artifacts and systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Redefine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

 Coverage VIA On-boarding Training and services
 Out-of-the-box Solution Capabilities
 Use case not covered



Thank you!