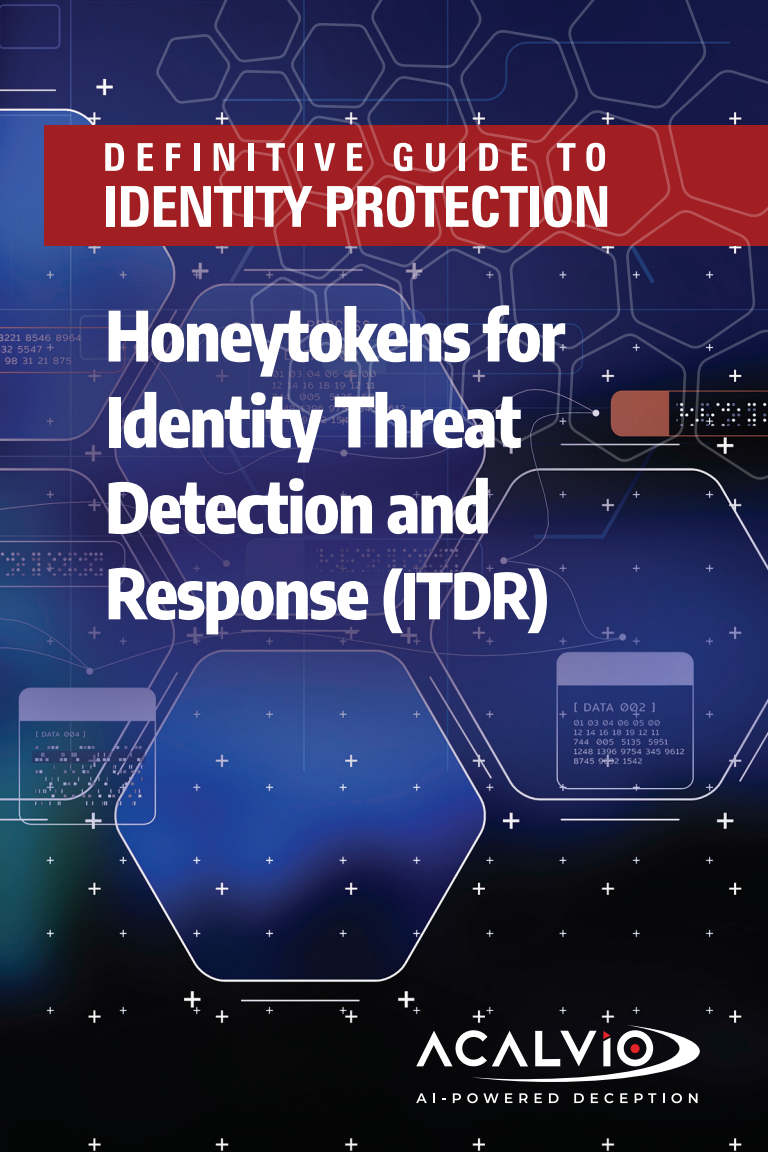
DEFINITIVE GUIDE TO

IDENTITY PROTECTION

Honeytokens for Identity Threat Detection and Response (ITDR)



ACALVIO

AI-POWERED DECEPTION

Overview

Identity-driven attacks are a prominent threat, with a staggering over 80% of breaches involving compromised identities. Adversaries increasingly exploit sophisticated methods to gain trusted access to identities, facilitating lateral movements and undermining traditional security measures. Conventional solutions struggle to differentiate between legitimate and malicious identity use, leaving significant vulnerabilities exposed. This guide introduces identity honeytokens and deception technology as a pivotal Identity Threat Detection and Response (ITDR) mechanism, offering an innovative layer of protection to fortify identities and pave the way toward a zero-trust architecture.

As we navigate through the chapters of this guide, we'll gain a deeper understanding of the current identity threat landscape and how to leverage cyber deception to mitigate these threats effectively. Adding cyber deception to identity security offers a proactive stance against adversaries so that organizations can protect their most valuable digital assets in an increasingly hostile cyber environment.

DEFINITIVE GUIDE TO IDENTITY PROTECTION:
Honeytokens for Identity Threat Detection and Response (ITDR)

DEFINITIVE GUIDE TO IDENTITY PROTECTION

Chapter 1

Understanding the Identity Architecture Landscape

Dive into the complex world of identity architecture, which spans on-premises stores like Active Directory and cloud-based solutions such as Microsoft Entra ID to hybrid connectors and SaaS providers like Okta. Uncover the nuances of various identity types, including privileged vs. regular user accounts and non-person entities, which can significantly outnumber user accounts, presenting unique security challenges.

Chapter 2

The Evolving Identity Threat Landscape

Explore the driving forces behind the surge in identity-driven attacks, from the dilution of traditional perimeters due to cloud adoption and remote work to advanced persistent threats and polymorphic ransomware. Analyze real-world breach scenarios and understand adversaries' tools and tactics, including Kerberoasting, MITM attacks, and exploitation of unpatched vulnerabilities.

Chapter 3

The Limitations of Traditional Security in Identity Protection

Discover the shortcomings of prevention-based security controls within the identity security ecosystem. Examine how adversaries circumvent measures like IAM, IGA, and MFA and the inherent risks associated with service accounts and non-person entities. Understand the challenges of misconfigurations, shadow admins, and legacy protocols that leave identity stores vulnerable.

Honeytokens for Identity Threat Detection and Response (ITDR)

Chapter 4

Bridging the Detection Gap with ITDR

Introduces ITDR as the missing piece in the identity security puzzle, designed to detect and respond to identity-driven attacks that elude prevention-based controls. Learn how deception-based ITDR leverages identity honeytokens to create a proactive defense mechanism capable of detecting sophisticated attacks agnostic to traditional detection methods.

Chapter 5

Implementing Deception for Robust Identity Protection

Details the application of deception-based ITDR, including the creation and management of deceptive user and service accounts, cloud IAM accounts, as well as credential profiles. It highlights cyber deception benefits and the subsequent response actions that can be taken to mitigate attack propagation and safeguard critical assets.

Chapter 6

The Role of Identity Protection in Zero Trust

Positions identity protection as a cornerstone of the Zero Trust Architecture (ZTA), emphasizing the shift from network-centric to data-centric security paradigms. Explore ZT's CISA and DOD pillar models and how deception-based ITDR aligns with the visibility and analytics capability, providing a necessary detection layer to complement a comprehensive ZTA strategy.

1 Understanding the Identity Architecture Landscape

Dive into the complex world of identity architecture, which spans on-premises stores like Active Directory and cloud-based solutions such as Microsoft Entra ID to hybrid connectors and SaaS providers like Okta. Uncover the nuances of various identity types, including privileged vs. regular user accounts and non-person entities, which can significantly outnumber user accounts, presenting uniquesecurity challenges.

Overview

The identity architecture of an organization is the framework that defines how individual identities are managed, secured, and utilized to access resources. This framework is crucial for establishing trust and managing risks associated with identity and access in a digital environment. This chapter will cover the components of identity architecture, exploring on-premises and cloud-based solutions, the nuances of various identity types, and the challenges associated with managing them effectively.

Understanding the Identity Architecture Landscape

On-Premises Identity Stores

Active Directory (AD): AD is a directory service developed by Microsoft for Windows domain networks. It is the cornerstone of identity services for most organizations, providing a centralized location for network administration and security. Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use.

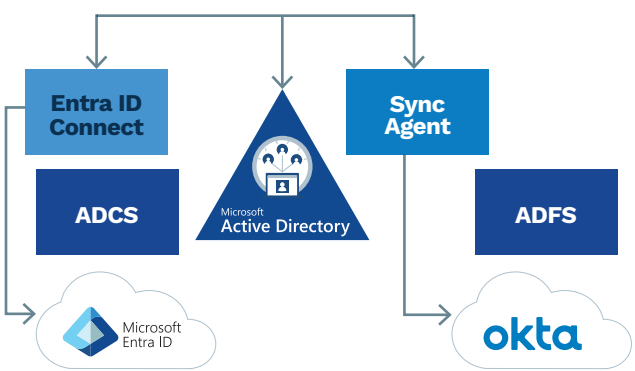
Active Directory Certificate Services (ADCS): ADCS provides customizable services for creating and managing public key certificates used in software security systems employing public key technologies. Organizations use ADCS to enhance security by binding the identity of a person, device, or service to a corresponding private key.

Active Directory Federation Services (ADFS): ADFS is a Single Sign-On (SSO) solution that provides users with streamlined access to systems and applications located across organizational boundaries. ADFS achieves this by securely sharing digital identity and entitlement rights, known as 'claims,' across security and enterprise boundaries.

Cloud Identity Stores

Microsoft Entra ID: This is a comprehensive identity and access management cloud solution by Microsoft that manages and secures user identities and access permissions across a wide range of environments, from on-premises to cloud-based applications.

IAM stores for PaaS/IaaS platforms: These are identity repositories specifically designed for Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) environments. They play a critical role in managing identities and permissions for services and resources hosted on the cloud, ensuring that only authorized entities can access your cloud resources.



Identity Stores (on premises and cloud)

Understanding the Identity Architecture Landscape (Continued)

SaaS Identity Providers

Okta: Okta is an independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers, and customers.

Ping: Ping Identity provides cloud-based, single sign-on (SSO), and identity management solutions with its PingOne and PingFederate platforms. It offers flexibility across hybrid IT environments and secure and seamless user experiences for access control.

Hybrid Identity Synchronization

Sync Agents: These agents connect hybrid identity stores by synchronizing identity information between on-premises AD and cloud-based solutions like Microsoft Entra ID, ensuring consistency and enabling unified identity management across diverse environments.

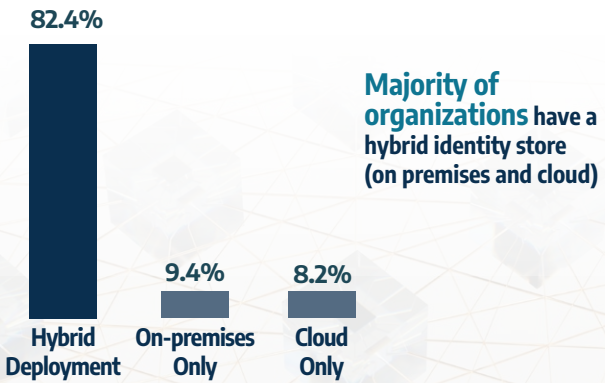
Identity Storage Locations

Credentials on Endpoints: These are authentication details stored directly on devices such as laptops, desktops, and mobile phones, enabling the device to authenticate the user or itself in various services.

Credentials in Applications: Applications often store credentials internally to interact with other services or databases, which can include hard-coded credentials in the application's code or stored in configuration files.

Identity Infrastructure Distribution: On-Premises, Hybrid & Cloud Only

Percentage of Respondents

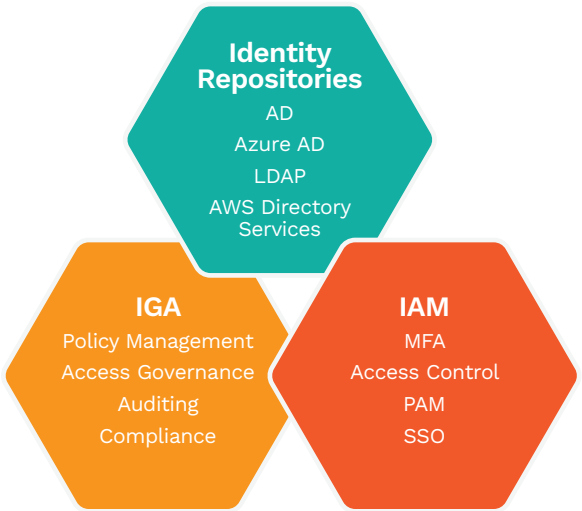


Understanding the Identity Architecture Landscape (Continued)

Identity Security Infrastructure

Privileged Access Management (PAM) and Identity Governance (IGA): PAM and IGA solutions provide prevention and policy-based security controls. PAM solutions manage credentials for privileged accounts and perform automated rotation of the credentials and keys. IGA solutions ensure conformance of identity security controls with governance policies. PAM and IGA solutions are a part of the identity architecture.

Multifactor (MFA) authentication and Single Sign-On (SSO): MFA solutions enforce strong authentication of the user, involving the use of additional factors beyond the password. SSO solutions enable the user to gain access to resources without requiring individual authentication when accessing each resource.



Identity Security Architecture (Identity and Access Management IAM, Identity Governance IGA)

Types of Identities

User Accounts

These are digital identities used by human users to interact with the system. They can be categorized into two:

1 **Privileged Users:** These accounts have elevated rights and permissions and are typically used by system administrators to manage IT systems.

2 **Regular Users:** These accounts have standard access rights necessary to perform regular job functions.

Types of Identities (Continued)

Non-Person Entities (NPEs):

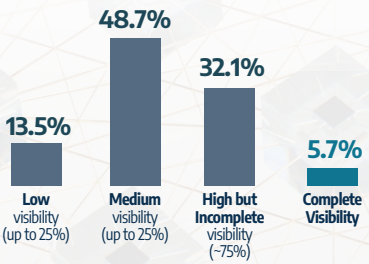
NPEs are identities that represent services, applications, or IoT devices rather than individual people. They are often used for automated processes and can outnumber human user accounts by a large margin, sometimes up to a 45-to-1 ratio.

Types of NPEs include:

1. **Service Accounts:** These are specialized user accounts for running applications or services on the network, with permissions limited to what the service requires to operate.

Level of Visibility Into Service Accounts

Percentage of Respondents



Only 5.7% of organizations have complete visibility into all service accounts in their environment.

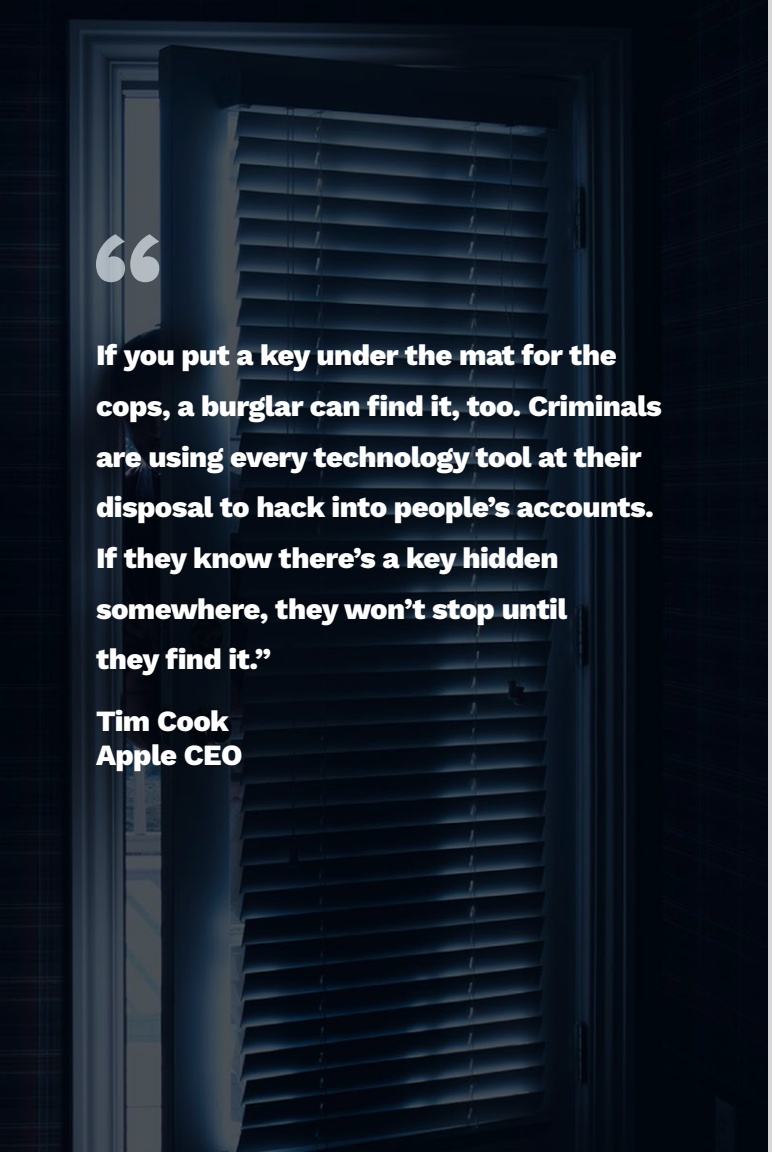
2. **API keys and tokens:** These are access keys and tokens that enable secure access to APIs. With modern applications leveraging a micro services architecture, API keys and tokens are increasingly adopted for interoperability.

3. **Certificates:** These are Public Key Infrastructure (PKI) certificates and keys that are used to establish the identity using strong forms of authentication.

4. **Application Accounts:** Similar to service accounts, these are used by applications to access databases, run jobs, or perform other tasks.Application Accounts: Similar to service accounts, these are used by applications to access databases, run jobs, or perform other tasks.

5. **Accounts in IT/Automation Tools and Scripts:** These accounts are used within automation tools and scripts for performing batch jobs, scheduled tasks, or other automated activities without human intervention.

Machine Identities outnumber human identities by a factor of 45 to 1



“If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people’s accounts. If they know there’s a key hidden somewhere, they won’t stop until they find it.”

Tim Cook
Apple CEO

Summary

Identity architecture forms the backbone of an organization’s security posture, and an in-depth understanding of its components and risks is vital for developing robust defense mechanisms against modern identity threats. By recognizing and effectively managing the complexity and interconnectivity of these components, organizations can better safeguard against identity-related breaches and ensure secure and efficient operations in today’s interconnected world.

The Evolving Identity Threat Landscape

Explore the driving forces behind the surge in identity-driven attacks, from the dilution of traditional perimeters due to cloud adoption and remote work to advanced persistent threats and polymorphic ransomware. Analyze real-world breach scenarios and understand the tools and tactics adversaries employ, including Kerberoasting, MITM attacks, and exploitation of unpatched vulnerabilities.

Overview

The identity threat landscape is rapidly changing, shaped by a variety of factors that make traditional security perimeters less effective and create new vulnerabilities. This chapter explores these factors, the methods attackers use to exploit them, and the far-reaching implications of such attacks.

The Evolving Identity Threat Landscape

The Porous Perimeter

The concept of a defined network perimeter is becoming obsolete due to the cloud adoption and the rise of remote work. Employees now access corporate resources from anywhere, often using personal devices that may not be as secure as those managed by the organization. This erosion of the traditional perimeter requires a new approach to security where identity becomes the new boundary.

Cloud and SaaS Adoption

Cloud services and Software as a Service (SaaS) applications have increased the complexity of identity architectures. Each service has its own set of user accounts and permissions, multiplying the number of potential attack vectors. Often, these services are interconnected, allowing an attacker who gains access to one service to leverage it to access others.

In this observed Midnight Blizzard activity, the actor tailored their password spray attacks to a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures.
—Microsoft, Jan 2024

Remote Work

The increased adoption of remote work significantly increases the identity risk exposure and attack surface. Attackers that gain access to a laptop of an employee who is traveling or working remotely can leverage credentials stored on the laptop in configuration files and credential caches to gain access to enterprise resources.

Advanced Persistent Threats (APTs)

APTs are stealthy threats in which an unauthorized user gains access to a network and remains undetected for an extended period. APT actors often target identities to gain the privileges needed to move laterally within the network and reach valuable data.

Insider Threat

Insider threats range from compromised users, negligent employees, to malicious employees. Insiders have trusted access to resources and look for privileged identities to gain access to intellectual property and sensitive data.

Polymorphic Ransomware

Ransomware has evolved into polymorphic variants, which can change their identifiable features to evade detection by signature-based security tools. These variants often manipulate identities or exploit identity-related vulnerabilities to gain initial access to an organization's network.

Active Directory Attack Timelines

"The Wonder Years"
(2010-2014)

2010
March: Windows Credentials Editor (WCE) & RootedCon presentation by Hernan Ochoa

2011
May: First version of Mimikatz tool released by Benjamin Delpy

2012
Exploiting Windows 2008 Group Policy Preferences by Emilien Giraul

May: Chris Campbell's post on GPP

Passwords

October: Responder v1 tool released by Laurent Gaffie

2013
October: Invoke-Mimikatz PowerShell module released by Joe Bialek

2014
August: "Abusing Microsoft Kerberos sorry you guys don't get it" Black Hat presentation by Benjamin Delpy & Skip Duckwell

Golden Tickets

Overpass-the-hash

Pass-the-ticket

September: PAC Validation, The 20 Minute Rule and Exceptions (BHUSA 2014 part deux) blog post about Silver Tickets by Skip Duckwell

September: Kerberoast released by Tim Medin at DerbyCon

December: PowerView tool released by Will Schroeder

with MITRE ATT&CK

"The Golden Years"
(2015-2019)

Tools
DSInternals

Kekeo

PowerSploit (ID: S0194)
Impacket (ID: S0357)
PowerShell Empire (ID: S0363)

DCSync added to Mimikatz (ID: T1003.006)

CrackMapExec (ID: S0488)
Bloodhound (ID: S0521)
DeathStar.py

NTLMRelayX

SharpHound GhostPack

Rubeus (ID: S1071)

Privilege Escalation
DNSAdmin to Domain Admin

AD Permissions

"Printer Bug"

Resource-Based Constrained Delegation

Persistence
AD Permissions

DCShadow (ID: T1207)

"The Third Age"
(2020-2023)

Tools
RemotePotato0

PetitPotam Certify

Certipy

KrbRelayUp

CrackMapExec continues as NetExec (nxc)

Privilege Escalation
Certified Pre-Owned (ADCS Attacks)

Kerberos Relay Attack

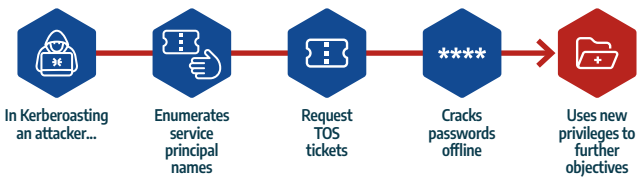
Persistence
Certified Pre-Owned (ADCS Attacks)

Attackers Have Evolved Multiple Avenues for Identity Exploits

Tools and Tactics Employed by Adversaries

Kerberoasting

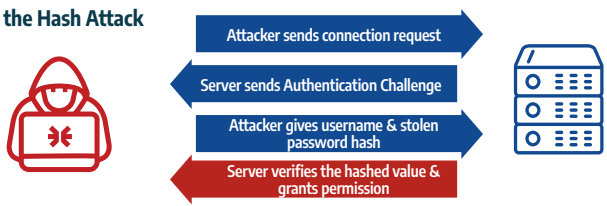
How Kerberoasting Attacks Work



This is a technique where attackers exploit the Kerberos ticket-granting service to crack the passwords of service accounts. It's particularly insidious because it can be performed without triggering many traditional security alerts.

Pass the Hash/Pass the Ticket attacks

Pass the Hash Attack



Attackers obtain access to a password hash or a stolen Kerberos ticket to gain access to a resource without requiring access to the actual password. It's challenging to detect as it involves abuse of Kerberos authentication workflows, resulting in logs and events that are not distinguishable from legitimate authentication activity.

Exploitation of Unpatched Vulnerabilities

Many identity-related attacks exploit known vulnerabilities that have not yet been patched. This could be due to legacy systems that cannot be updated or simply a lag in applying security updates.

Emerging Threats and Techniques

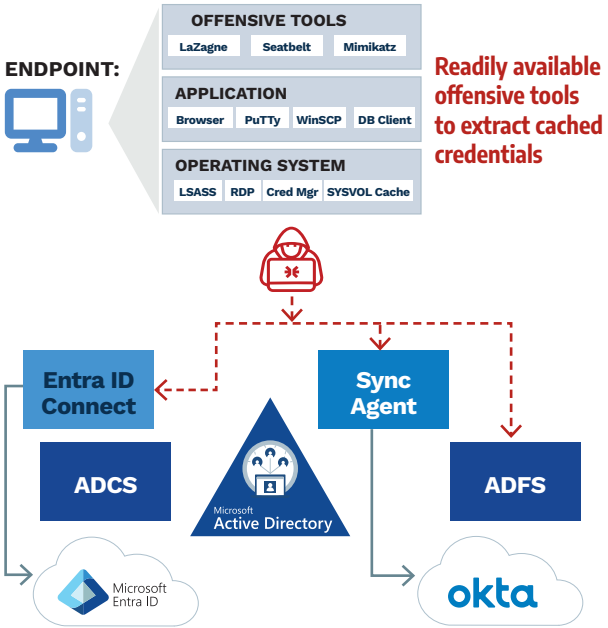
Attackers are constantly developing new methods to exploit identity systems. These include:

Attacks exploiting cached credentials: These attacks leverage readily available offensive tools that extract credentials from operating system caches and application caches on endpoints. These credentials include privileged user accounts and service accounts.

Attacks against sync agents: Attacks that target third party sync agents and perform in-memory exploits to gain access to credentials of privileged accounts and service accounts.

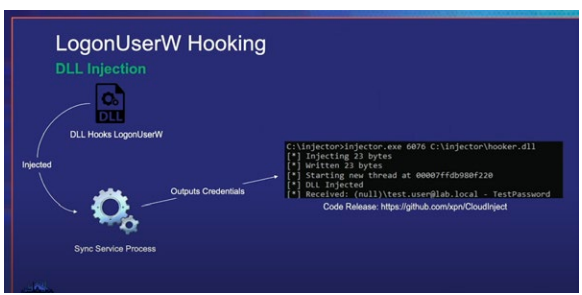
Session Cookie Hijacking: Tokens used in single sign-on (SSO) or multi-factor authentication (MFA) can be stolen, allowing attackers to impersonate legitimate users.

ADCS Attacks: These attacks target Active Directory Certificate Services (ADCS) by abusing certificate template misconfigurations to escalate privileges and maintain persistence.



Readily available offensive tools to extract cached credentials

Attacks against third-party sync agents to gain access to credentials



Stealthy identity attacks that bypass traditional defenses

Real-world Breach Scenarios

Understanding how attackers exploit identities requires a close look at real-world breach scenarios. Below are two illustrative examples of identity-driven attacks, showcasing the methods and impacts.

Example 1: The Phishing Infiltration and Lateral Movement

In a well-documented breach of a financial institution, attackers began with a targeted phishing campaign. They sent emails to employees with a malicious attachment that, once opened, installed credential-stealing malware on the endpoint. Using these stolen credentials, the attackers were able to masquerade as legitimate employees.

Capitalizing on the obtained credentials of an entry-level employee, they executed a lateral movement within the network. Utilizing a combination of privilege escalation techniques and exploiting weaknesses in the identity and access management controls, the attackers gained higher-level access. Eventually, they reached the domain controller, allowing them to issue requests for any user's credentials within the organization. The breach resulted in substantial data loss, including sensitive customer information.

Example 2: The Service Account Compromise

Another incident involved an attacker discovering an unprotected service account during reconnaissance activities. This service account was configured with high privileges for convenience, a common but risky practice. With this account, the attacker accessed the application to which the service account had access.

They used this foothold to install a backdoor that went undetected due to the legitimate appearance of the service account's activities. Over several months, the attacker extracted sensitive data from the corporate network, leading to a significant breach that exposed intellectual property and resulted in financial losses and reputational damage.

Both examples demonstrate how identities, whether of a human user or a non-person entity like a service account, can be leveraged to gain unauthorized access and move undetected within a network.

Service Accounts Blind Spots:

Detecting Active Directory compromises can be difficult, time-consuming, and resource intensive, even for organisations with mature security information and event management (SIEM) and security operations centre (SOC) capabilities. This is because many Active Directory compromises exploit legitimate functionality and generate the same events that are generated by normal activity."

— NSA and Five Eyes Intelligence Alliance
"Detecting and Mitigating Active Directory Compromises"

Summary

The identity threat landscape continuously shifts as attackers adapt their methods to the changing technological environment. Understanding these trends is crucial for organizations to develop strategies that protect against identity-driven attacks. As the security perimeter becomes less relevant, identity becomes the cornerstone of any robust security strategy, requiring vigilant management, constant evaluation, and proactive measures to ensure the integrity and confidentiality of organizational resources.

The complexity and fluidity of the identity threat landscape underscore the need for dynamic and adaptive security measures. Organizations must recognize the centrality of identity in modern cybersecurity and evolve their approaches to stay ahead of threats. In the next chapter, we'll examine how traditional security solutions are failing to meet these challenges and what can be done to address these gaps.

The Limitations of Traditional Security in Identity Protection

Discover the shortcomings of prevention-based security controls within the identity security ecosystem. Examine how adversaries circumvent measures like IAM, IGA, and MFA, and the inherent risks associated with service accounts and non-person entities. Understand the challenges posed by misconfigurations, shadow admins, and legacy protocols that leave identity stores vulnerable.

Overview

The traditional security measures within the identity ecosystem are primarily designed to prevent unauthorized access based on a set of rules or policies. These measures include Identity and Access Management (IAM), Identity Governance and Administration (IGA), Multi-Factor Authentication (MFA), and network segmentation for identity stores. However, the evolving sophistication of cyberattacks has exposed critical shortcomings in this prevention-centric approach.

> **“Attackers think in graphs; defenders think in lists. As long as this is true, attackers win.”**
>
> **— John Lambert**
> **Corporate Vice President,**
> **Security Fellow, Microsoft**

Inadequacies of Prevention-Based Controls

The Bypassing of Security Measures: Adversaries have developed numerous techniques to sidestep prevention-based security controls. They often target non-person entities (NPEs) and service accounts, exploiting the fact that these accounts are difficult to monitor and control with MFA and other standard security measures.

Challenges with Service Accounts: Service accounts, necessary for the operation of many IT processes, often possess high levels of access and are typically not subject to the same security measures as human user accounts. Limited visibility and oversight create significant onboarding challenges for Privileged Access Management (PAM) systems.

MFA Fatigue and Token Theft: Attackers exploit human psychology through MFA fatigue attacks, where they repeatedly request MFA authentication until the victim approves out of frustration. Additionally, session tokens and authentication cookies can be stolen, allowing attackers to impersonate legitimate users.

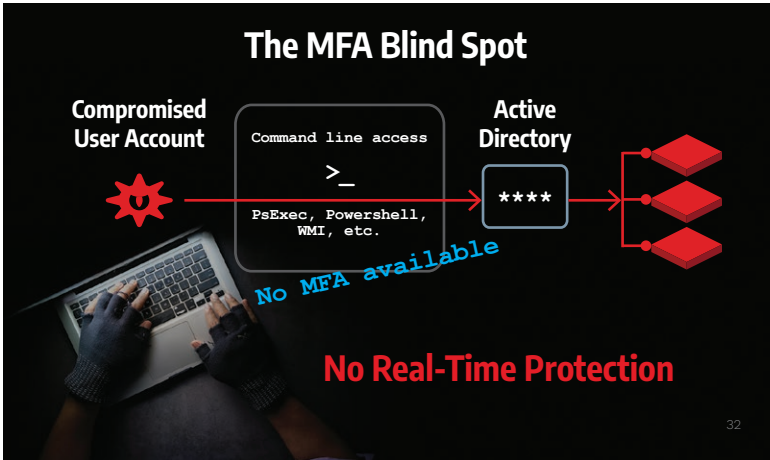
Helpdesk Accounts and Suppport Accounts Exploitation: Adversaries target accounts that have administrative access to Privileged Access Management (PAM) solutions and Identity Governance (IGA) solutions. This includes exploits against helpdesk accounts, support accounts and admin accounts to gain unauthorized access to the privileged identities protected by PAM/IGA solutions.

Misconfigurations and Shadow IT

Shadow Admins: These are accounts with administrative privileges that are not officially designated as administrators. They can create blind spots in security oversight, giving attackers a way to gain elevated access without detection.

Service Account Security Gaps: Many organizations have service accounts configured with more privileges than necessary, making them prime targets for attackers.

Unconstrained Delegations: In some configurations, like unconstrained delegation in Active Directory, systems can impersonate any user without authentication, presenting a significant security risk.



Vulnerabilities and Exploits

Unpatched Systems: Attackers continue to identify and exploit vulnerabilities in the identity architecture, ranging from exploiting any legacy settings that have not been hardened (such as SMBv1) to more recent exploits against the software and protocols that run the identity stores.

Identity Trust Exploitation: Components of identity infrastructure, such as connectors for hybrid environments or third-party sync agents, can become attack vectors if compromised.

What was theoretical years ago is often practical today or tomorrow

Attackers keep identifying novel techniques that are often new takes on old issues.

Key Facts & Figures at a Glance

62%
OF INTERACTIVE INTRUSIONS INVOLVING THE ABUSE OF VALID ACCOUNTS, WITH 34% OF INTRUSIONS SPECIFICALLY INVOLVED THE USE OF DOMAIN ACCOUNTS OR DEFAULT ACCOUNTS

160%
INCREASE IN ATTEMPTS TO GATHER SECRET KEYS AND OTHER CREDENTIAL MATERIALS VIA CLOUD INSTANCE METADATA APIs

583%
INCREASE IN KERBEROASTING ATTACKS (A SUB-TECHNIQUE OF STEAL OR FORGE KERBEROS TICKETS), WITH VICE SPIDER RESPONSIBLE FOR 27% OF ALL KERBEROASTING ATTACKS

Detection Deficiencies in Traditional Solutions

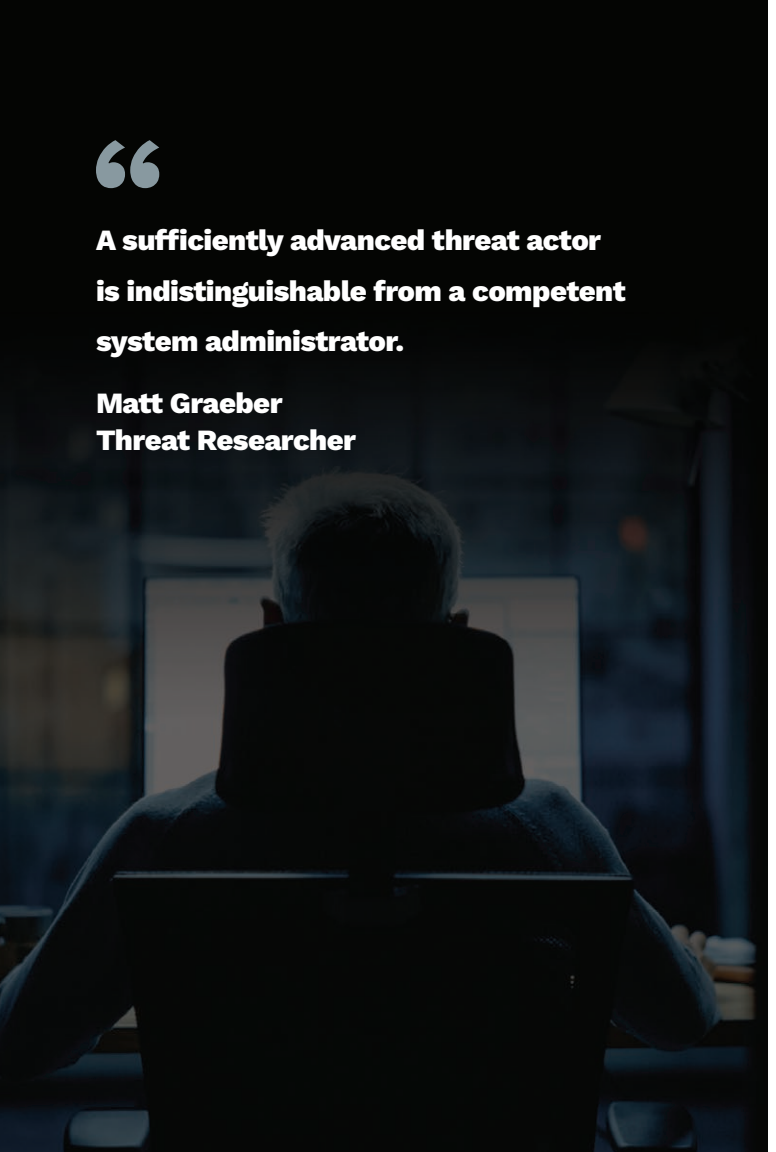
Traditional security solutions often fail to differentiate between legitimate and malicious use of credentials. This is evident from the surge in identity threats, including a 583% increase in Kerberoasting attacks and high-profile breaches in 2023 and 2024.

Client-Side and Offline Attacks: Adversaries perform attacks that are not logged, such as manipulating identity information on the client side or executing offline attacks against identity stores.

Cached credentials: Endpoints have credentials cached in the operating system and in installed applications, attackers leverage these to gain trusted access to resources through actions that appear legitimate to traditional security solutions.

Logs and Analytics Challenges: Many identity-related actions are not captured in logs, especially for cloud identity stores without premium subscriptions. Even when logs are available, analyzing them can be slow, and adversaries often move faster than they can be detected.

Unmanaged Endpoints: Over 25% of attacks originate from unmanaged endpoints, such as printers, IoT devices, and medical equipment. These devices are often overlooked and can provide an entry point for attackers.



A sufficiently advanced threat actor is indistinguishable from a competent system administrator.

Matt Graeber
Threat Researcher

Summary

Traditional identity security measures are struggling to keep pace with the innovative methods of modern cyber adversaries. As attackers become more adept at circumventing defenses, organizations must reassess their security strategies, particularly regarding identity management. The following chapters will explore the innovative solutions that address these shortcomings, including the emerging field of Identity Threat Detection and Response (ITDR).

Bridging the Detection Gap with ITDR

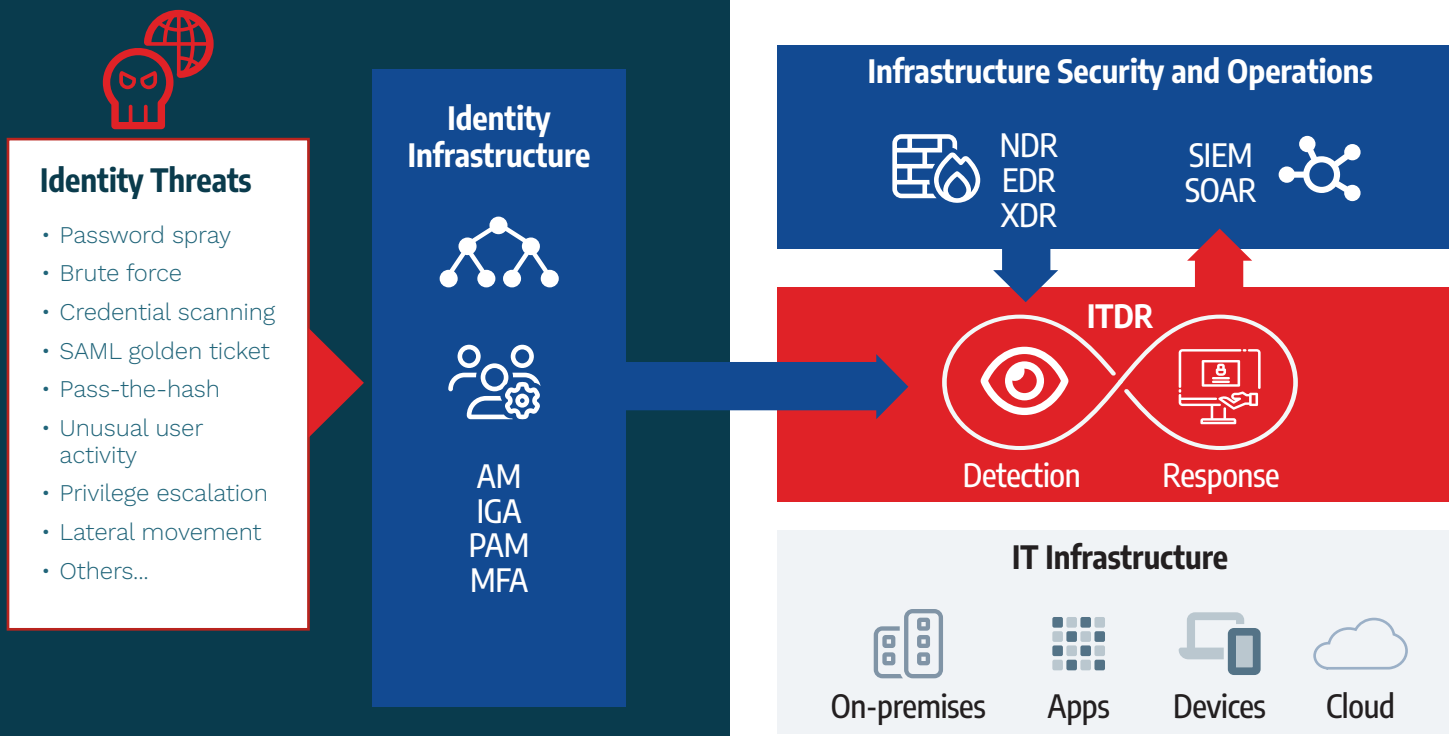
Introduces ITDR as the missing piece in the identity security puzzle, designed to detect and respond to identity-driven attacks that elude prevention-based controls. Learn how deception-based ITDR leverages identity honeytokens to create a proactive defense mechanism that can detect known and sophisticated attacks that bypass traditional detection methods.

Overview

The escalation of identity-driven threats necessitates an advanced approach to cybersecurity. Identity Threat Detection and Response (ITDR) emerges as the strategic response, targeting the detection of identity-based attacks that traditional prevention-based measures often miss.

How ITDR Works with Infrastructure Security to Detect and Respond to Identity Threats

ITDR solutions focus on threat detection and response to protect the identity infrastructure.



Gartner: ITDR reference architecture

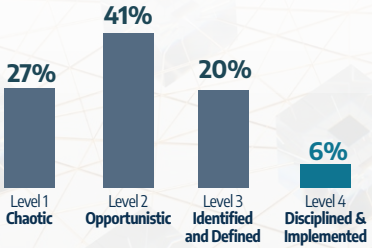
Defining ITDR

The Need for a Detection Layer: Identity security frameworks have historically emphasized prevention. However, as adversaries evolve, there is a glaring need for a dedicated detection layer that doesn't just block attempted exploits but actively seeks out and identifies incursions that have already occurred.

ITDR as a Solution: ITDR stands for Identity Threat Detection and Response. It is specifically designed to identify suspicious activity related to identity usage and respond to it in real-time, filling a crucial gap in the identity security landscape.

Identity Security Maturity: Confidence Against Identity Threats

Percentage of Respondents



Only 6% of organizations meet the requirements for the level of maturity against identity threats

The Role of Deception-Based ITDR

Deception technology is at the heart of ITDR. It extends beyond simply monitoring and incorporates proactive defense mechanisms that bait and trap attackers.

Identity Honeytokens: Honeytokens are deceptive accounts that are deliberately placed to mimic real user accounts or service accounts. They serve as a trap for attackers, to detect and divert attackers.

Honeytoken Accounts: These are deceptive user and service accounts seeded throughout the identity stores. They appear legitimate but are monitored for any access, which would be unauthorized and indicative of a breach.

Honeytokens on Endpoints: Deceptive credentials that are derived from honeytoken accounts, these profiles are established on endpoints. Any use of these credentials can trigger alerts, as there should be no legitimate activity involving them.

Honeytokens for proactive identity threat defense

Detecting the Undetected

Current and Evolving Threats: The strength of Deception-based ITDR lies in its capacity to detect both known threats and adapt to emerging ones, providing a dynamic and resilient defense system.

Agnostic Detection: Deception-based ITDR does not rely on log files, network traffic analysis, or signature-based detection. This makes it effective against attacks that evade traditional surveillance, such as zero-day exploits or advanced persistent threats.

Expert Validation: Cybersecurity experts, practitioners, and threat researchers contribute to the development and refinement of ITDR solutions, providing an expert layer of attestation to the effectiveness of these systems and the role of cyber deception in a robust ITDR strategy.

Attackers can do an *infinite* number of things.

However, they have a *finite* number of pathways.

Configure detection around these.

Sean Metcalf | Identity Security expert

Deception Tech – Necessary for Identity Protection

Traditional approaches to identity threat detection are:

- Capable of detecting **some known threats** with known attacker TTPs but **not all**
- **Challenged at distinguishing** between legitimate and malicious usage of valid and trusted identities
- **Blind spots: Offline, client-side attacks & new attack techniques**

Deception Technology can detect known and unknown (zero-day) identity threats

Deception-based detection is independent of logs, signatures, network traffic or known offensive techniques.

Deception technology for ITDR:

- **Deploy deceptive identity artifacts** that threat actors will try to exploit
- **Interaction with deceptive artifacts generates alerts** enabling identity threat detection with precision and speed

TAG: KERBEROAST HONEYPOT

FEB 08 2017

Detecting Kerberoasting Activity Part 2 – Creating a Kerberoast Service Account Honeypot

By Sean Metcalf in ActiveDirectorySecurity, Microsoft Security, Technical Reference

```
PS C:\Windows\system32>  $KerberoastEventData | where {$_.ServiceName -like "*Honeypot*"}
 | select EventID,Date,AccountName,ClientAddress,ServiceName

EventID       : 4769
Date          : 2/8/2017 7:54:21 AM
AccountName   : JoeUser@LAB.ADSECURITY.ORG
ClientAddress : ::ffff:10.100.10.110
ServiceName   : KerberoastHONEYPOT
```

In my previous post, "Detecting Kerberoasting Activity" I explain how Kerberoasting works and describe how to detect potential Kerberoasting activity. The trick to this is understanding what activity is normal in order to filter out the noise and increase the fidelity of the alert. This post describes how to filter from millions of events to ...

Continue reading

AP-REQ, Audit Kerberos Service Ticket Operations, Detect Kerberoast Activity, Detecting Kerberoast activity, Event ID 4769, Kerberoast honeypot, Kerberoasting activity, Kerberos RC4 Encryption, Kerberos Service Ticket, Kerberos TGS, Kerberos TGS Ticket, NTLM Password, RC4_HMAC_MD5, service account honeypot, TGS-REP, TGS-REQ

Identity security experts attest to the benefits of deception to detect identity threats

Detecting the Un-Detected

Examples include:

Cybersecurity Frameworks and Organizations:

NIST (National Institute of Standards and Technology) is known for its comprehensive cybersecurity framework, which is widely respected and followed.

MITRE is notably recognized for the MITRE ATT&CK framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Industry Consortia and Think Tanks:

Groups like the Cybersecurity Coalition or the Information Security Forum bring together industry experts to drive security innovation and develop best practices.

Cybersecurity Researchers and Academics:

Leading academics from institutions with strong cybersecurity programs, as well as independent researchers who publish peer-reviewed papers on security topics. As an example, the leading Active Directory security blog, adsecurity.org outlined the importance of deception for detecting stealthy identity threats such as Kerberoasting.

Practitioners and Experts:

Frontline cybersecurity professionals, consultants, and organizations who regularly engage with and implement ITDR solutions. Their insights are particularly valuable as they are based on practical, real-world experiences.

Regulatory Bodies:

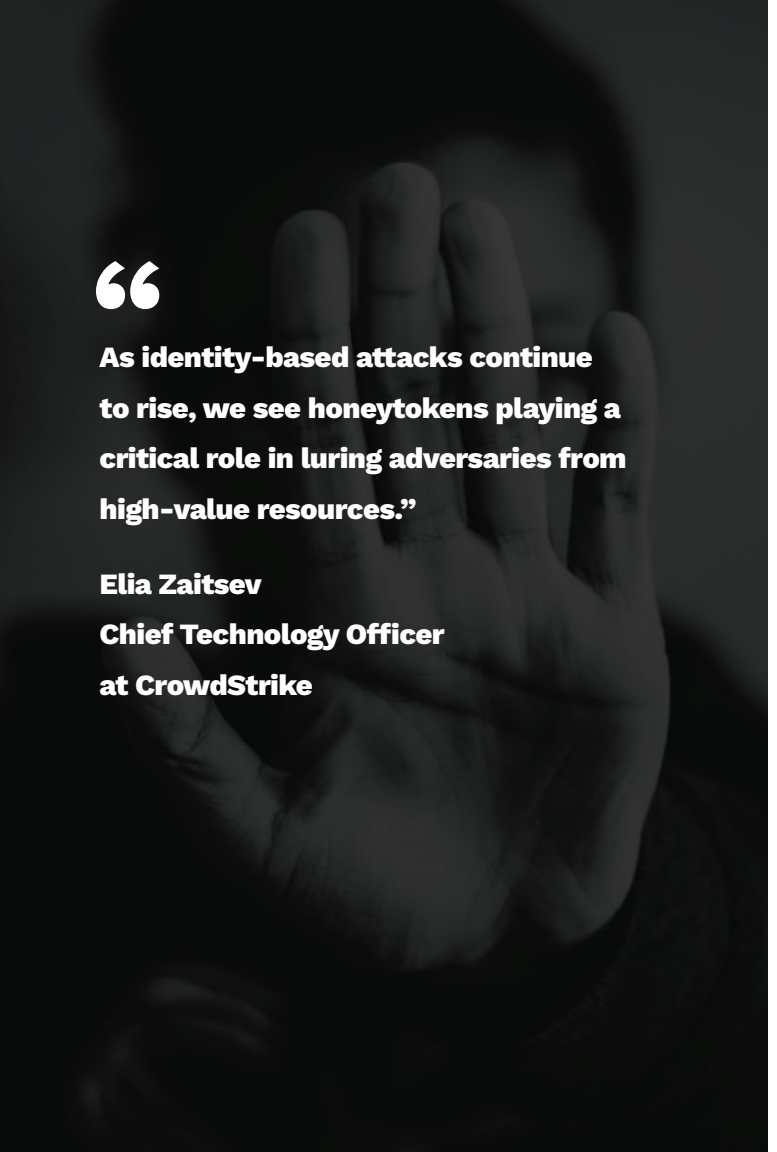
Agencies like the Cybersecurity and Infrastructure Security Agency (CISA) or the European Union Agency for Cybersecurity (ENISA) that provide guidance for cybersecurity practices.

Certifying Authorities:

Organizations that offer professional certifications, such as (ISC)for the Certified Information Systems Security Professional (CISSP) certification, may also provide expert opinions on ITDR effectiveness.

“Honeytokens are effective at helping organizations detect intrusions or malicious activities that other security products can’t stop.”

Kevin Mandia
CEO Mandiant, Google Cloud
at RSA Conference 2023



“As identity-based attacks continue to rise, we see honeytokens playing a critical role in luring adversaries from high-value resources.”

Elia Zaitsev
Chief Technology Officer
at CrowdStrike

Summary

Through ITDR, organizations gain a powerful ally in the fight against identity-related cyber threats. By adopting deception-based strategies and innovative detection technologies, they can turn their networks into environments where attackers are outsmarted at their own game. The next chapters will go deeper into the practical deployment of ITDR solutions and their integration into broader cybersecurity strategies.

Implementing Deception for Robust Identity Protection

Details the application of deception-based ITDR, including the creation and management of deceptive user and service accounts, as well as credential profiles. Provides a highlight of cyber deception benefits and the subsequent response actions that can be taken to mitigate attack propagation, safeguarding critical assets.

Overview

Deception technology is transforming the security landscape by offering an advanced set of tools designed to deceive and derail attackers. Implementing deception-based Identity Threat Detection and Response (ITDR) systems is a critical step in creating a robust security posture. This chapter outlines the application of such systems, the benefits they offer, and the response actions they enable to protect an organization's assets.

"The use of canary objects [honeytokens] in Active Directory is an effective technique to detect Active Directory compromises. The benefit of this technique is that it does not rely on correlating event logs, providing a strong indication a compromise has happened. Notably, this technique does not rely on detecting the tooling used by malicious actors ... but instead detects the compromise itself. As such, it is more likely to accurately detect compromises against Active Directory."

— NSA and Five Eyes Intelligence Alliance
"Detecting and Mitigating Active Directory Compromises"

Laying the Foundation for Deception-Based ITDR

Deception-based ITDR introduces a layer of security that uses deception technology to create traps, known as honeytokens, which are designed to mimic legitimate user and service accounts and credential profiles.

Identity Honeytokens:

Honeytokens are strategically placed in identity stores and on endpoints. These tokens are false credentials or digital artifacts that have no legitimate use, making any interaction with them inherently suspicious and indicative of malicious activity.

Honeytoken Accounts:

Within identity stores, deceptive user and service accounts are created. These accounts, if accessed, immediately alert the security team to potential unauthorized or malicious activity.

Honeytokens on Endpoints:

Credential profiles are established on endpoints to further lay the groundwork for detection. Attempts to use these credentials can trigger automated security protocols.

Deception Types

Honeytoken Accounts

Deceptive accounts added to identity stores

User accounts and service accounts

Detect identity threats

Honeytokens on Endpoints

Deceptive credential profiles deployed on endpoints

Derived from honeytoken accounts

Early detection of identity threats

The Cyber Deception Advantage

Comprehensive Threat Detection:

Deception-based ITDR is uniquely positioned to detect both known and emergent identity threats. It does so in a manner that is independent of the limitations associated with traditional detection methods, such as reliance on logs, network traffic monitoring, or signature-based detection.

High-fidelity Alerts for Security Operations Center:

Traditional security solutions are associated with a large volume of false positives, requiring security operations center (SOC) teams to perform manual correlation and confirmation. Deception technology is not used in legitimate workflows, any usage of the deceptions is an immediate indicator of malicious activity. SOC teams gain the benefit of high-fidelity alerts that can be acted on immediately, ensuring the attack is stopped prior to propagation.

Expert Validation:

The strategies and tools used in deception-based ITDR are validated by a community of cybersecurity experts, practitioners, and researchers. Their collective experience and expertise attest to the effectiveness of these solutions.

Divert and Slow Down Attackers

Attackers mount identity exploits against the deceptive targets, leading to slowing down the attacker and wasting their time and resources. Defense teams gain precious time to respond to the threat and prevent the attacker from compromising the critical assets.

Threat Hunting

Defense teams can deploy honeytokens as part of a threat hunting action to identify and confirm the presence of latent threats in the environment as a proactive measure.

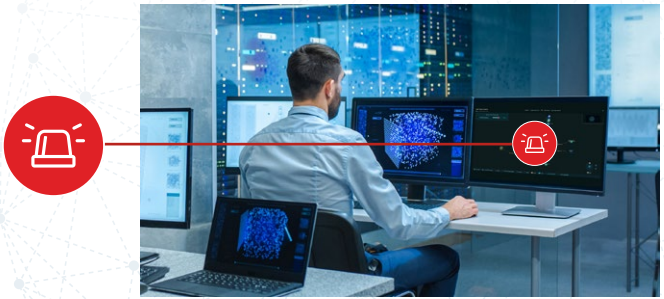
Precise and Early Detection

Early Warning System:

The early and precise detection of identity threats is paramount. Deception-based ITDR acts as an early warning system, identifying intrusions at the initial stages and allowing for immediate action.

Detection Agnostic to Logs or Network Traffic:

This detection does not depend on conventional security data, making it particularly effective against sophisticated attacks that typically bypass standard security monitoring.



Response Actions and Mitigating Attack Propagation

Automated Responses:

Upon detection of an interaction with a honeytoken, the system can initiate automated response protocols, such as isolating the affected system, alerting security personnel, or revoking access to halt the attack's progress.

Manual Interventions:

Security teams are also equipped to perform manual interventions, leveraging the intelligence gathered from the deception system to perform targeted countermeasures against an attacker.

Safeguarding the Identity Infrastructure

Building a Resilient Environment:

With deception-based ITDR, organizations can create an environment where attackers can never be sure if they are accessing legitimate resources or being lured into a trap. This uncertainty acts as a deterrent and can significantly reduce the success rate of attacks.

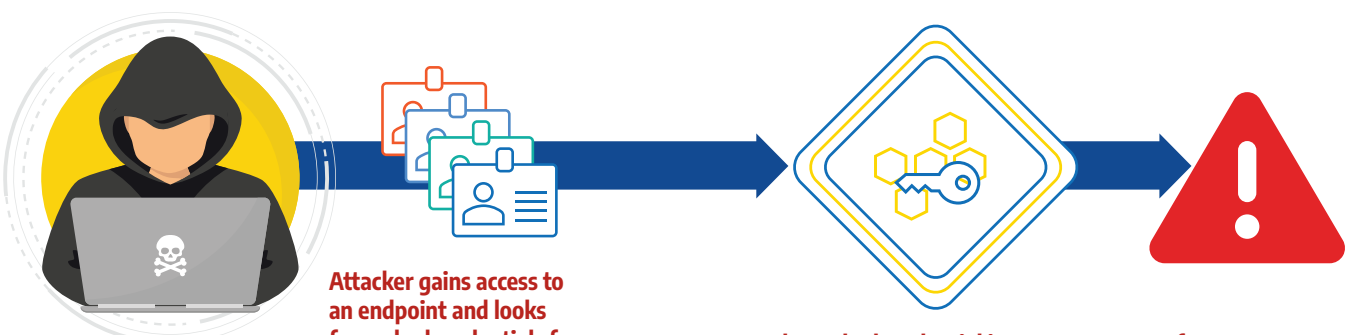
Deception-based ITDR represents a paradigm shift in cybersecurity, moving from reactive to proactive defense mechanisms. By integrating these strategies into their cybersecurity framework, organizations can enhance their ability to detect, respond to, and protect against identity-driven threats, ensuring the safeguarding of their most crucial digital assets.

Protection of Critical Assets:

Early detection and response capabilities make sure that identities and the assets they have access to are protected, significantly reducing the risk of data breaches and intellectual property theft.

Overcoming the Manual Challenges of Legacy Deception

While deception-based ITDR provides a strategic advantage in cybersecurity, its implementation can be complex and resource-intensive. Creating and managing honeytokens and deceptive accounts manually can also be fraught with challenges. This section will cover these difficulties and explore how innovations from companies like Acalvio are revolutionizing the field of cyber deception.



Manual Creation of Honeytokens: Challenges

Requires extensive domain knowledge:

Administrators that attempt to create honeytokens manually must grapple with challenges such as deciding the number, type, placement of the honeytokens. A single user account can have 100+ attributes, requiring the administrator to make lots of decisions, each of which involve deep domain knowledge of cyber deception and identity threats.

Complex Deployment:

Manually deploying honeytokens requires a detailed understanding of an organization's network and systems, as well as the creation of convincing but non-functional credentials that can lure attackers without disrupting legitimate operations.

Resource-Intensive Maintenance:

Maintaining the effectiveness of honeytokens requires continuous updates and management to keep up with the ever-changing network environments and sophisticated attack strategies.

Consistency and Scalability:

Ensuring consistency and scalability across large and diverse IT environments is challenging when deploying honeytokens manually, often leading to gaps in the deception strategy.

Manual deployment of Honeytoken Accounts and Honeytokens is fraught with challenges:

How do I deploy honeytokens to a large number of endpoints?

What values do I set for the 100+ attributes needed to create each user account?

How can we make them attractive to adversaries?

What types of accounts should we create as honeytokens?

What usernames should we give them?

Administrators grapple with finding answers to these questions for a manual deployment of honeytokens

Acalvio's Innovative Solutions

Acalvio Technologies, a leader in deception technology, addresses these challenges with automated solutions that simplify the deployment and management of deception campaigns by combining domain knowledge with AI.

Automated Recommendations:

Acalvio's platforms leverage AI for automated recommendations of realistic deceptions that are enticing for attackers to exploit, providing an effective approach to automate the deception placement, count, types at scale.

Automated Deployment:

Acalvio's platforms use automation to deploy honeytokens across an enterprise's network, significantly reducing the time and expertise required to implement effective deception.

Dynamic Adaptation:

Their solutions dynamically adapt to changes in the network, updating honeytokens and deceptive accounts to maintain the integrity of the deception environment.

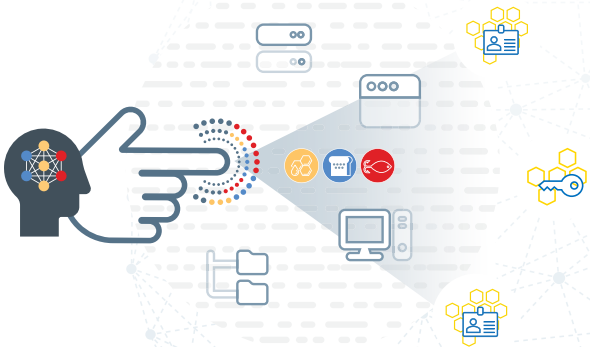
Agentless and Enterprise-Scale Deception:

Acalvio's systems are designed for scalability, ensuring that organizations of all sizes can implement a robust deception strategy without the limitations associated with manual deployment. The agentless solution eliminates management complexity associated with the deployment of additional agents.

Integration with Existing Infrastructure:

Innovation from Acalvio seamlessly integrates with existing security infrastructures, enhancing the capabilities of traditional security measures and filling in the gaps that manual processes may leave.

Predictive Analytics
AI-powered Platform



Integrations with Identity Protection Leaders

Acalvio's innovative deception platform integrates directly with leading identity protection platforms, including CrowdStrike Identity Protection and Microsoft Defender for Identity (MDI), providing an automated and scalable solution for honeytokens. This collaboration provides a powerful example of how the combination of deception technology and next-generation identity and endpoint security can simplify and automate the protection of digital identities.

Innovative platforms combine deployment automation with deception strategy to strengthen the cybersecurity posture

Identity Honeytokens

Automated recommendations across identity stores & endpoints

Example of Automated Deception:

Imagine an organization that utilizes CrowdStrike for its identity security. By integrating Acalvio's deception solutions, the organization can automatically deploy honeytokens that are pre integrated with CrowdStrike. If an attacker attempts to identify targets for identity exploits, the honeytokens are surfaced to the attacker and any usage results in an immediate alert in the CrowdStrike console, providing SOC teams with actionable intelligence through a single pane of glass.

Proof of Simplification and Automation:

This integration exemplifies the simplification and automation of creating a deceptive environment. There's no need for any software installation on premises and no need for security teams to manually configure honeytokens. Instead, the system gains visibility to the identity architecture, deploying honeytokens in an automated manner. This approach strengthens the cybersecurity posture without adding overhead to the infrastructure or the security teams, making the solution easy to adopt.

Made attractive for attackers to exploit

Placed strategically along attack pathways

Refreshed dynamically

The Resulting Advantages

Efficient Operation:

Automation reduces the operational burden on IT security teams, allowing them to focus on strategic initiatives rather than the tactical nuances of honeytoken placement and management.

Enhanced Detection:

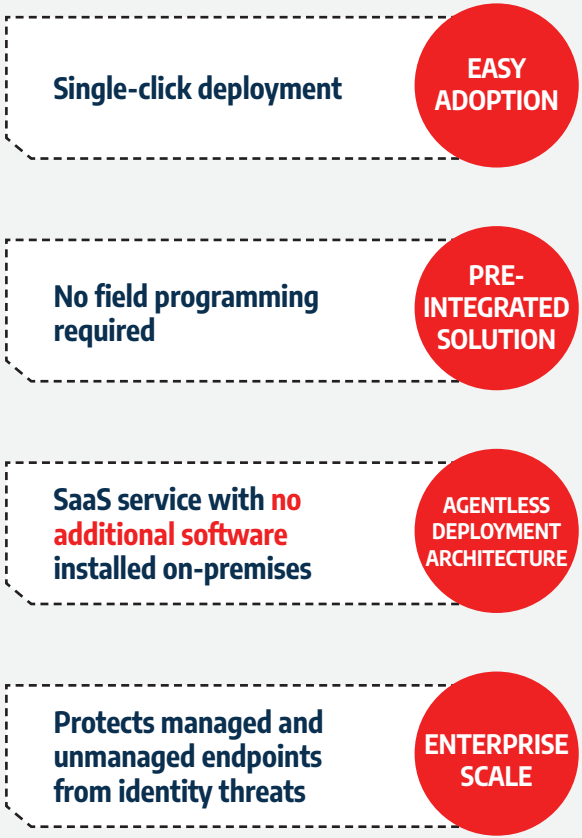
With automated deception, organizations benefit from an enhanced detection mechanism that is more responsive and less prone to human error.

Comprehensive Coverage:

Acalvio's technology provides comprehensive coverage across the entire network, ensuring that no asset is left unprotected due to scalability constraints.

By integrating automated deception solutions like those from Acalvio, organizations can overcome the manual challenges associated with creating honeytokens. This advancement not only streamlines the deployment process but also confirms that the deception is realistic, attractive to adversaries, and sustainable at scale, making it a potent tool in the arsenal of identity protection.

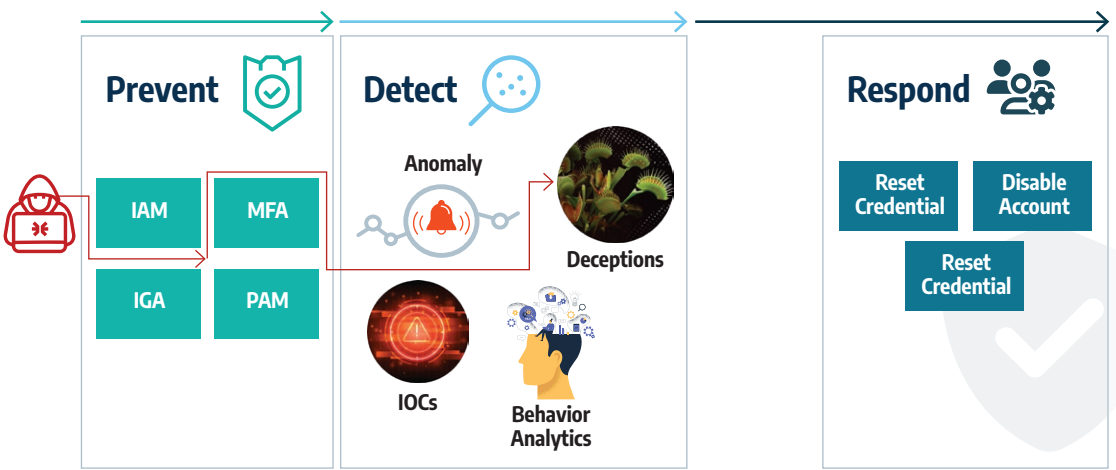
Advanced deception platforms provide ease of adoption and scale



Defense In Depth for Identity Protection

Defense in Depth is a cybersecurity strategy that involves a layered defense approach to provide comprehensive protection against the ever evolving threat landscape. The principle of defense in depth is based on the recognition that no single solution or approach can defend against all possible threat vectors. By combining prevention-based security controls with a layered detection approach, defense teams gain visibility to threats that exploit gaps in an individual layer.

Cyber deception is a necessary layer for a defense in depth approach to identity protection. By evolving the attack TTPs, adversaries bypass security solutions that are looking for “known bad” threats. Deception-based threat detection is agnostic to attacker TTPs, providing security teams with visibility to threats that have bypassed detection approaches that are looking for “known bad”.



Comprehensive identity protection involves a strategic combination of security layers to defend against current and evolving identity threats

Defense in Depth for Identity Protection

Automated Moving Target Defense Technology Innovators:

Acalvio — Advanced Threat Defense That Looks Too Real to Resist

Analysis by:
Mark Pohto and Carl Manion
Gartner® Emerging Tech — Security
June 2023

Summary

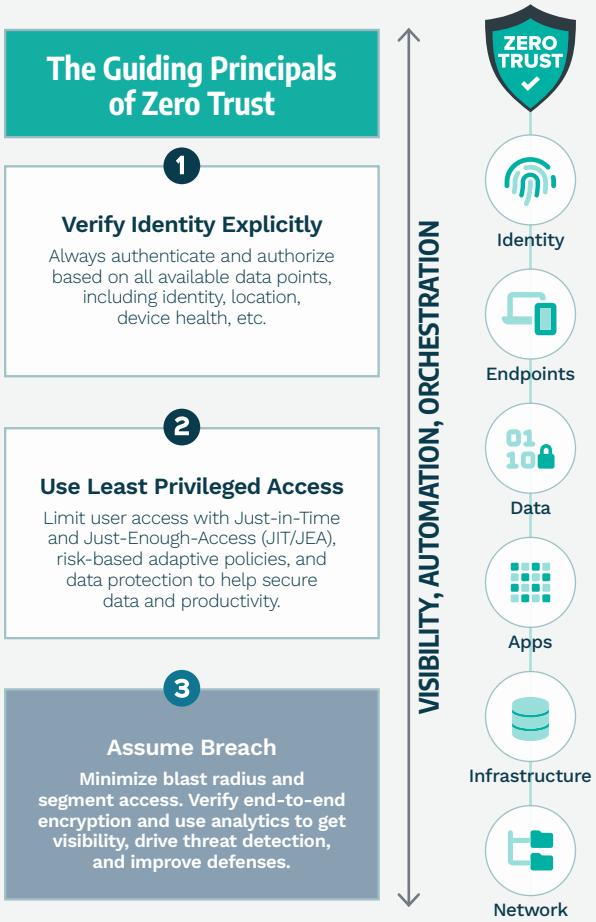
Through deception-based ITDR based on identity honeytokens, organizations gain the benefit of early and precise detection of identity threats. The high-fidelity alerts enable rapid response actions, preventing adversary breakout and protecting the critical assets of the organization. By adopting an enterprise-scale platform like Acalvio, cyber defense teams gain the benefit of automated deployment and refresh of honeytokens, freeing up the administrator from the need to make decisions that require domain knowledge of deception technology and identity threats. The agentless deployment architecture and the integrations with CrowdStrike and Microsoft enable rapid onboarding of the Acalvio platform to provide immediate value to the organization.

The Role of Identity Protection in Zero Trust

Identifies identity protection as a cornerstone of the Zero Trust Architecture (ZTA), emphasizing the shift from network-centric to data-centric security paradigms. Explore the CISA and DOD pillar models for ZT and how deception-based ITDR aligns with the visibility and analytics capability, providing a necessary layer of detection to advance the maturity of a ZTA strategy.

Overview

In the era of sophisticated cyber threats, traditional perimeter-based security models are no longer sufficient. The Zero Trust Architecture (ZTA) has emerged as a transformative approach, shifting the security focus from the network perimeter to a data-centric model. This final chapter discusses the critical role of identity protection within ZTA and how deception-based ITDR integrates into this framework to enhance visibility, analytics, and detection capabilities.



The Data-Centric Pivot of Zero Trust

Zero Trust is predicated on the belief that trust is a vulnerability. Rather than 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. This means that no user or system is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources.

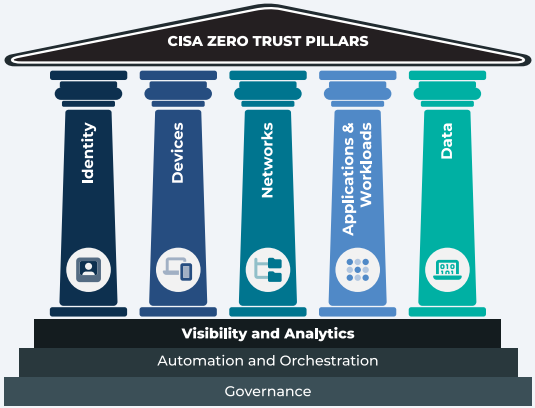
Zero Trust Anchored in Identity Protection

In the Zero Trust model, protecting critical assets and sensitive data is paramount. Identity protection is the cornerstone, ensuring that the right individuals have access to the right resources, at the right times, for the right reasons.

The CISA 5 Pillar Model for ZT

The Cybersecurity and Infrastructure Security Agency (CISA) outlines a five-pillar model for implementing Zero Trust, emphasizing the following components:

1. **Identity**
2. **Device**
3. **Network/Environment**
4. **Application/Workload**
5. **Data**

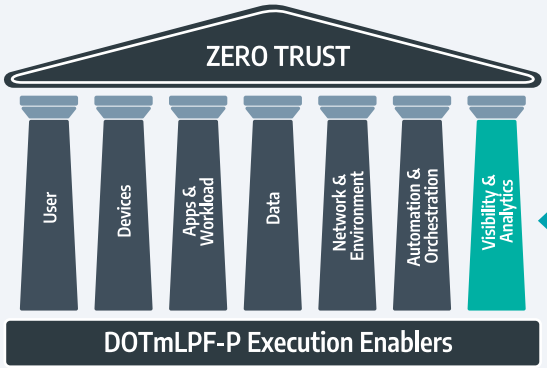


These pillars are supported by three cross-cutting capabilities: **Visibility and Analytics Automation and Orchestration and Governance.**

DoD's Zero Trust Pillar Model for ZT

The U.S. Department of Defense (DoD) also emphasizes a robust Zero Trust strategy, which aligns closely with the principles of CISA's model but is tailored to meet the unique requirements of national defense. **Their components include:**

1. Users
2. Devices
3. Applications & Workloads
4. Data
5. Networks & Environments
6. Automation & Orchestration
7. Visibility & Analytics



Visibility & Analytics: Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

In the DoD's implementation, the principles of Zero Trust extend across the entire spectrum of the defense information network. Given the critical nature of its mission, the DoD emphasizes the need to protect against state-sponsored cyber activities and advanced persistent threats (APTs). The DoD's model prioritizes advanced threat-hunting capabilities, real-time data analytics, and automated security responses to ensure that the network and its resources remain uncompromised.

The incorporation of deception-based ITDR into both the CISA and DoD models of Zero Trust demonstrates a cross-sector acknowledgment that adaptive, proactive security measures are vital. In environments ranging from civilian government to national defense, ITDR's role is clear: to provide a sophisticated layer of detection is foundational for a mature Zero Trust strategy.

Assume Breach Principle and Visibility

The 'Assume Breach' principle is a fundamental tenet of Zero Trust. It acknowledges the necessity of being able to quickly detect and respond to threats that have evaded initial defenses. Visibility and analytics are critical here, as they provide the intelligence necessary to detect anomalous behavior and potential threats.

Deception-Based ITDR as a Visibility Enhancer

Deception-based ITDR is foundational for Zero Trust's visibility and analytics capability by creating a responsive detection layer that identifies unauthorized identity use. It provides early warning signs of breach attempts, making it a valuable tool for the 'identity' pillar of ZTA.

Aligning Deception ITDR with ZTA

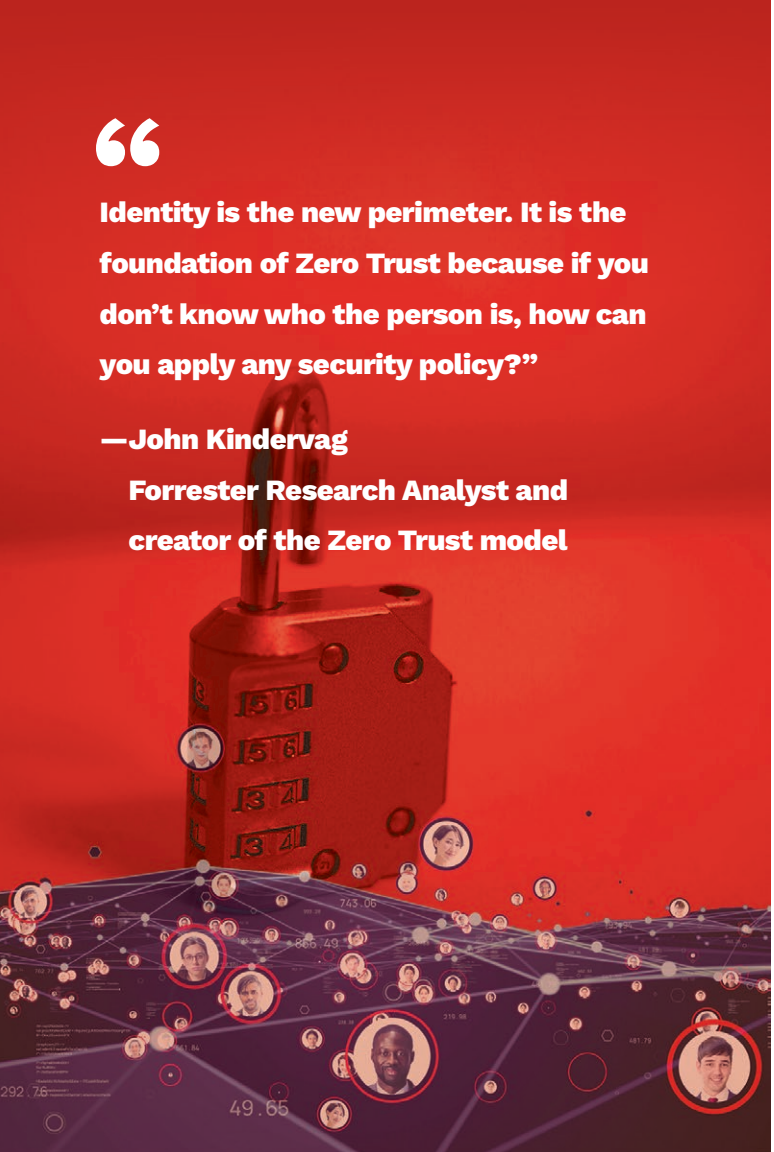
Deception-based ITDR seamlessly maps onto the visibility and analytics capability of ZTA. By creating deceptive accounts and honeytokens that integrate with real-time monitoring systems, ITDR provides a level of detection and response that is essential for a robust Zero Trust strategy.

Necessary Detection Layer for mature ZTA

In the dynamic landscape of Zero Trust, deception-based ITDR offers the necessary detection layer that adapts to the evolving threat environment. It enhances the analytical capabilities required for a mature ZTA, ensuring that every aspect of the system contributes to the security posture. Deception also supports the DoD's objective to outmaneuver adversaries in the cyberspace domain by delivering tactical and strategic advantages through superior cybersecurity measures.

Zero Trust is a STRATEGY

ASSUME BREACH is a fundamental principle of Zero Trust



Summary

As we close this exploration of identity security, it is evident that deception-based ITDR is a critical component that strengthens the very foundation of Zero Trust Architecture. It augments the model’s data-centric focus by ensuring that identity—often the first line of defense in a cybersecurity strategy—is protected with sophisticated, dynamic, and responsive measures. With ITDR’s integration into Zero Trust, organizations can confidently navigate the cybersecurity landscape, bolstered by a strategy that is as adaptive and resilient as the threats it aims to thwart.

10 ESSENTIAL REQUIREMENTS OF AN EFFECTIVE DECEPTION SOLUTION FOR ITDR

1 Deception must provide both SCALE AND COVERAGE.

Attackers can gain initial access from any part of the organization and pivot toward the identity architecture. Deception solutions must be scalable to deploy honeytokens across the enterprise environment.

2 Deception must include HONEYTOKENS on ENDPOINTS in addition to identity stores.

Attackers can gain initial access from any part of the organization and pivot toward the identity architecture. Deception solutions must be scalable to deploy honeytokens across the enterprise environment.

3 Deception must PROTECT on premises and cloud identity stores.

Organizations are adopting hybrid identity architectures, with increasing use of Cloud (IaaS, PaaS, and SaaS). Attackers can pivot from on premises to cloud or vice versa. Deception solutions must protect on premises and cloud environments to defend against identity threats targeting hybrid environments.

4 Deception must DETECT specific identity threats in addition to evolving threats.

Attackers leverage a set of identity exploits, such as Kerberoasting, Pass the Hash attacks to gain access to resources. Deception solutions must have awareness of identity threats to detect these exploits early in the attack lifecycle.

5 Deception must be ENTICING to the attacker.

Attackers look for targets that provide opportunities to elevate privileges and compromise critical assets. Deception solutions must deploy deceptions that are attractive for attackers to exploit, providing early warning of identity compromise.

10 ESSENTIAL REQUIREMENTS OF AN EFFECTIVE DECEPTION SOLUTION FOR ITDR (CONTINUED)

6 Deception must be REALISTIC and auto refreshed.

Attackers perform reconnaissance to identify targets for identity exploits. Deception solutions must deploy realistic deceptions that are believable to the adversary. Deceptions must be dynamic and refreshed automatically to keep the deceptions fresh and maintain their realism over time.

7 Deception must be deployed with a STRATEGY.

Attackers have specific goals and objectives. Attackers perform planning based on the characteristics of the environment. Deception solutions must have a strategy to automate the count, placement, type of deceptions to detect a wide variety of identity threats.

8 Deception must have the ability to CONTAIN THE ATTACKER.

Attackers can exploit targets and leverage these for further exploit activity. Deception solutions must have built-in attacker containment to restrict and deny attackers from continuing their exploit actions.

9 Deception must be PRE-INTEGRATED with existing identity security solutions.

Adoption of siloed security tooling results in gaps that are exploited by adversaries. Deception solutions must be pre-integrated with identity security solutions deployed at the enterprise to ensure interoperability and provide value to the enterprise.

10 Deception must be EASY TO DEPLOY AND ADMINISTER.

Security teams are faced with significant shortage of available skills and resources. Deception solutions must be designed for ease of deployment, avoiding deployment challenges associated with the rollout of additional agents and providing a high level of automation to reduce administrative effort.

In Closing

Through deception-based ITDR based on identity honeytokens, organizations gain the benefit of early and precise detection of identity threats. The high-fidelity alerts enable rapid response actions, preventing adversary breakout and protecting the critical assets of the organization. By adopting an enterprise-scale platform like Acalvio, cyber defense teams gain the benefit of automated deployment and refresh of honeytokens, freeing up the administrator from the need to make decisions that require domain knowledge of deception technology and identity threats. The agentless deployment architecture and the integrations with CrowdStrike and Microsoft enable rapid onboarding of the Acalvio platform to provide immediate value to the organization.

ACALVIO

AI-POWERED DECEPTION

Acalvio is the leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT, and Cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable Zero Trust security models. Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from Cloud, on-premises, or through managed service providers.

For more information, please visit www.acalvio.com

References

1. "Non-Person Entity" NIST https://csrc.nist.gov/glossary/term/non_person_entity
2. "MITRE ATT&CK" https://attack.mitre.org/
3. "Kerberoasting" "Attacking Kerberos: kicking the guard dog of Hades", Tim Medin, DerbyCon 2014
4. "LSASS" https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Serviceq
5. "LaZagne" https://github.com/AlessandroZ/LaZagne
6. "Seatbelt" https://github.com/GhostPack/Seatbelt
7. "Mimikatz" https://en.wikipedia.org/wiki/Mimikatz
8. "Session Cookie Hijacking" https://en.wikipedia.org/wiki/Session_hijacking
9. "ADCS", Active Directory Certificate Services https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview
10. "ADFS" Active Directory Federation Services, https://en.wikipedia.org/wiki/Active_Directory_Federation_Services
11. "Service Accounts" https://learn.microsoft.com/en-us/entra/architecture/service-accounts-on-premises
12. "Unconstrained Delegation" https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-unconstrained-kerberos
13. "IDTR" https://en.wikipedia.org/wiki/Identity_threat_detection_and_response
14. "Honeytokens" https://www.acalvio.com/resources/glossary/honeytoken/
15. "NIST" National Institute of Standards and Technology, https://www.nist.gov/
16. "CrowdStrike Identity Protection" https://www.crowdstrike.com/platform/identity-protection
17. "Microsoft Defender for Identity" MDI, https://learn.microsoft.com/en-us/defender-for-identity/what-is
18. "Defense in Depth" https://en.wikipedia.org/wiki/Defense_in_depth_(computing)
19. "Zero Trust" https://en.wikipedia.org/wiki/Zero_trust_security_model

References

20. "Visibility and Analytics" https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF

21. "CISA 5 Pillar Model" https://www.cisa.gov/zero-trust-maturity-model

22. "DoD Zero Trust Pillar Model" https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

23. "Privilege Escalation" https://attack.mitre.org/tactics/TA0004/

24. "Lateral Movement" https://attack.mitre.org/tactics/TA0008/

25. "NSA and Five Eyes Alliance Jointly Releases Guidance for Mitigating Active Directory Compromises" https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3917556/nsa-jointly-releases-guidance-for-mitigating-active-directory-compromises/

Acalvio Technologies
2520 Mission College Blvd, #110, Santa Clara, CA 95054
www.acalvio.com