ACALVIO
AI-POWERED DECEPTION

Enterprise-scale Honeytokens for Identity Protection

With Deep Integration into CrowdStrike and Microsoft Security Ecosystems

CHALLENGES

Identity threats are involved in over 80% of all cyberattacks (including APT threats, Ransomware attacks, and Advanced malware). Attackers harvest identities from endpoints, applications, and identity stores in the enterprise. Attackers target identities to perform Lateral Movement and Privilege Escalation. Traditional security solutions are unable to distinguish between legitimate and malicious use of credentials. In any organization, the identity attack surface can be large, and eliminating all the identity attack surface is challenging for security teams.

SOLUTION

ShadowPlex Honeytokens provides a necessary layer of Deception Technology-based defense-in-depth for Identity Protection.

Honeytoken accounts and honeytokens are a class of Deception Technology techniques that are proven to be extremely powerful and efficient in early detection of a variety of identity threats. Honeytoken accounts are deceptive accounts (representing user accounts and service accounts) created in Active Directory (AD) and Entra ID that are specifically designed to lure attackers and deflect them away from real identities. Honeytokens are deceptive credentials and data that are embedded in legitimate assets such as endpoints and cloud workloads. Any usage or manipulation of these deception artifacts is a reliable indicator of an identity threat.

Acalvio ShadowPlex leverages CrowdStrike Identity Module and Microsoft Defender for Identity Honeytoken Tags for deception monitoring and alerting to provide a scalable and effective deception-based identity threat detection solution.

KEY BENEFITS

- A fully automated, robust platform for operationalizing honeytokens for Identity Protection, both on-premises and in cloud.
- Honeytokens capability seamlessly extended to endpoints protected by Microsoft Defender for Endpoint, including deployment and refresh lifecycles.
- Advanced AI-based recommendation engine for honeytoken accounts.
- Pre-integration with Microsoft Defender and no Acalvio software to install in customers' on-premises networks.
- Complete control over types and counts of honeytoken accounts being created for customers.
- Powerful capability to detect identity threats from managed and unmanaged endpoints to strengthen Zero Trust environments.

Enterprise-scale Honeytokens for Identity Protection

ACALVIO
AI-POWERED DECEPTION

BUSINESS VALUE

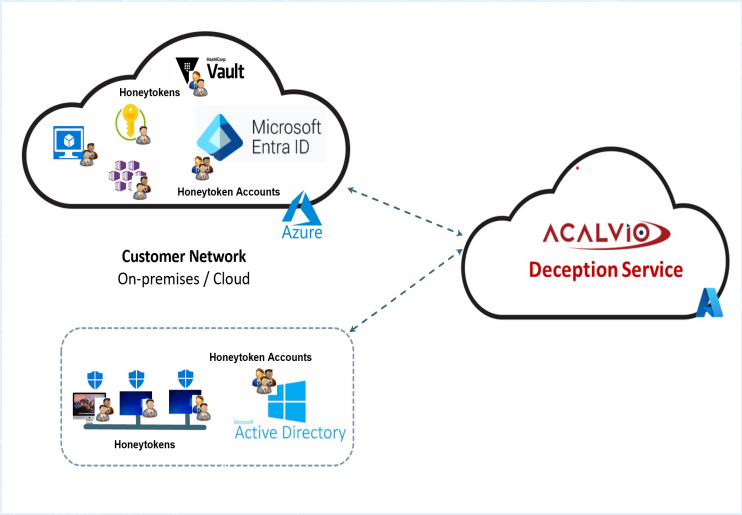
Challenge	Solution	Benefits
Customers are looking to gain the ability to detect a wide variety of identity threats, including client-side attacks, offline attacks, and zero days that evade traditional security solutions	ShadowPlex Honeytoken Accounts and Honeytokens provide a rich and mature set of capabilities for enterprises. The pre-integrated solution is completely automated for recommendation, deployment and management of honeytokens at scale.	Early and high-fidelity detection of identity threats
Deception-based detection of Identity threats on both managed and unmanaged endpoints	ShadowPlex Honeytoken Accounts added to the identity stores and made attractive for attackers to exploit.	SOC teams gain the benefit of detecting identity threats originating from unmanaged endpoints. Provides improved visibility to these threats.
Ability to extend Identity protection across the enterprise network, both on-premises and in Azure	Acalvio ShadowPlex is a scalable offering that enables deployment across a large hybrid enterprise network with multiple Active Directory domains, Entra ID and a large number of endpoints.	Attackers can target any identity store or endpoint and use it to pivot to other identity stores and endpoints. Comprehensive coverage across on-premises and cloud workloads is essential to avoid detection gaps.

TECHNICAL SOLUTION

Microsoft Defender for Identity and CrowdStrike Falcon Identity platform has built-in support for monitoring honeytoken accounts. Any access or alteration of a honeytoken triggers a dedicated detection, giving SOC analysts visibility into the adversary.

Manually creating honeytoken accounts and honeytokens is a laborious process, and it is extremely challenging to make them attractive to attackers.

The Honeytoken fulfilment capability from Acalvio is completely automated and pre-integrated into the Microsoft Defender and CrowdStrike Falcon platforms including EDR components for deception deployment.



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. **www.acalvio.com**