Microsoft

ACALVIO
AI-POWERED DECEPTION

# Accelerating Zero Trust through Deception and AI

## Microsoft and Acalvio partner to deliver State-of-the-Art Identity Protection

Threat actors are evolving their strategies to align with a Zero Trust approach. As Zero Trust gains prominence, attackers are increasingly shifting to identity exploits. Zero Trust is built on Identity as a key pillar. Authentication and Access Management are necessary but are of little benefit if the identity itself is stolen. Any Zero Trust Architecture (ZTA) must include identity protection as a foundational technology.

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 to perform Lateral Movement and Privilege Escalation. When the threat actors obtain access to valid enterprise identities, their activities and movement within the network are masked as legitimate traffic. Additionally, identity threats are evolving to leverage novel techniques such as offline attacks, client-side attacks and zero days that are designed to evade detection by identity access management controls.

## Identity Threat Detection & Response (ITDR) – Next Generation

Honey accounts and Honeytokens are a class of advanced deception techniques that are proven to be extremely powerful and efficient in detecting a wide variety of identity threats with precision and speed. Honey accounts are deceptive accounts (representing user and service accounts) created in Active Directory (AD) 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 on endpoints and cloud workloads. Any usage or manipulation of these deception artifacts is a very reliable indicator of an identity threat.

Microsoft has recently introduced Honeytoken Entity tags in Microsoft Defender for Identity. Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert in Defender.

Acalvio built the industry-first enterprise-scale honeytoken solution by leveraging deep expertise in cyber deception and combined it with advanced AI techniques to make it completely autonomous. This partnership adds cutting-edge honeytoken technology to the power of Microsoft Defender and provides the most comprehensive Identity Threat Detection & Response for Microsoft Defender customers.

### Key Solution Benefits

- Deception based detection of a wide variety of identity threats, including zero days, offline and client-side attacks that bypass existing detection mechanisms.
- Identity threat detection and response as a new layer for identity protection.
- Complete control on types and counts of honeytoken accounts being created for customers.
- Powerful capability to detect identity threats from both managed and unmanaged endpoints

## Microsoft and Acalvio Integration Overview

Acalvio has built integrations with Microsoft Defender and Microsoft Sentinel to enable customers deploy honeytokens at enterprise-scale. Figure 1 shows the high-level integration architecture. Integration with Defender for Endpoint (MDE) allows discovery of network assets for automatically configuring effective honeytokens, and autonomous deployment and management of honeytokens across a large number of endpoints, both on-premises and in cloud. The integrated solution leverages MDE and does not need to deploy any additional agents.

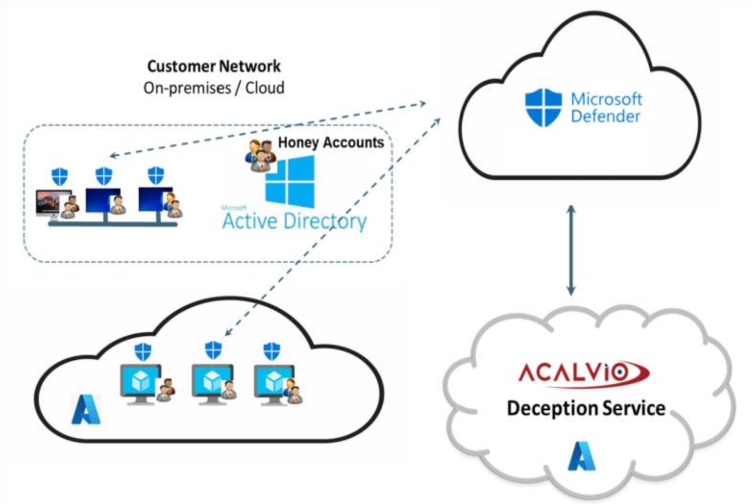

*Figure 1: Integration Architecture*

Acalvio has also built integration with Microsoft Sentinel to send identity compromise alerts for further investigation and response. If the customer has deployed Microsoft Defender for Identity (MDI), Acalvio can leverage Honeytoken entity capability by tagging honey accounts. The alerts are generated by MDI, enabling a single pane of glass.

**Delivered from Azure:** Honeytokens are delivered as a SaaS service and require no new agents to be deployed on the endpoints.

**Ease of Use:**

- Pre-integrations with Microsoft Defender and Microsoft Sentinel enable immediate time to value with no additional integration or field programming.
- A fully automated, robust platform for operationalizing honeytoken accounts for Identity Protection.

**Enterprise Scale:** Honeytokens capability seamlessly extended to 100's of thousands of enterprise endpoints managed by Defender, including deployment and refresh lifecycles.

**Effective:** Advanced AI-based recommendation engine for automatically blending of Honeytokens across multiple AD domains and each endpoint.

## Summary

**Zero Trust depends on Identity being secure. Microsoft and Acalvio partnership brings innovative honeytoken technology to protect against identity compromise. The integrated solution is scalable and supports the ability to deploy across multiple AD domains and a large number of endpoints. The solution is easy to adopt, built on Defender and protects both managed and unmanaged endpoints from identity threats.**