ACALVIO
AI-POWERED DECEPTION

DATASHEET

Enterprise-scale Honeytokens for Identity Protection

With Deep Integration into CrowdStrike and Microsoft Security Ecosystem

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. Agentic AI attacks are automating credential-related exploits at machine-speed. Traditional security controls are unable to differentiate between normal and malicious use of legitimate 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 for CrowdStrike Identity Protection and Microsoft Defender 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 also leverages CrowdStrike Identity Protection and Microsoft Defender for Identity Honeytoken Tags for monitoring and alerting to provide a scalable and effective deception-based identity threat detection solution.

KEY BENEFITS

- Preemptive security to detect Agentic AI attacks targeting identities during the reconnaissance phase
- 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 CrowdStrike Identity Protection and Microsoft Defender. No Acalvio software to install in customers' on-premises networks.
- Administrative policies for 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
Agentic AI attacks are moving at machine-speed, targeting identities for lateral movement and privilege escalation	Acalvio ShadowPlex deploys honey accounts and honeytokens that are tailored to detect threats during the reconnaissance, credential access, and lateral movement stages of the attack.	Agentic AI attacks move at machine-speed, dramatically shrinking the time window for detection. Honeytokens provide early and high-fidelity detection to find and stop agentic AI attacks prior to propagation.
Attackers use a wide variety of identity attack techniques, 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.	Detect identity threats that bypass traditional security controls.
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.

TECHNICAL SOLUTION

CrowdStrike Identity Protection and Microsoft Defender for Identity 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 CrowdStrike and Microsoft platform.

"The use of honeytokens is an effective technique to detect identity compromise. The benefit of this technique [...] providing a strong indication that a compromise has happened."

Detecting and Mitigating Active Directory Compromises

—NSA and the Five Eyes Intelligence Agencies

Acalvio is an AI-powered preemptive cybersecurity company focused on countering AI-driven identity and infrastructure intrusion. Its 360 Deception platform combines Dynamic Deception, evolving HoneyPaths, and cloaking of production assets within deception fabric to disrupt automated reconnaissance, credential abuse, and lateral movement across identity systems, endpoints, cloud, network, and cyber-physical environments. By altering what attackers can perceive and trust, Acalvio shifts detection from post-compromise analysis to pre-impact exposure, enabling organizations to detect, delay, disrupt, and deny malicious activity at machine speed. The company serves enterprise and government organizations determined to break automated intrusion at its source. https://www.acalvio.com/