ACALVIO HONEYTOKENS SOLUTION CUSTOMER REFERENCE:

HEALTHCARE SERVICE PROVIDER

HIGHLIGHTS

Healthcare Service Provider
Multiple AD domains in need of identity protection

Project Business Driver
Protecting identities from a variety of threats and staying ahead of evolving identity-driven attacks

Key Evaluation Criteria
Automated honeytokens capability
Agentless deployment design
Native integration with CrowdStrike

Deployment
Honey accounts across multiple AD domains
Honeytokens across tens of thousands of endpoints
No requirement for additional software installation

Results
Scalable Deployment of Deception-Based Identity Threat Detection and Response (ITDR) across all healthcare organization member bodies

BACKGROUND

This organization is a prominent player in the healthcare industry, operating within the ever-evolving and critical healthcare services. They are a network of independent acute healthcare providers.

This sector is characterized by constant advancements in medical technology, growing patient demands for top-quality care, and an unceasing commitment to improving public health outcomes. They are increasingly vulnerable to a growing array of cyber attacks posing serious risks to confidential data, critical medical infrastructure, and the overall integrity of healthcare services.

PROBLEM

The organization had expressed significant concerns regarding identity protection, given the substantial increase in identity-driven attacks and breaches. The organization manages multiple large Active Directory domains, assigning one domain for each member body. While preventive measures like MFA and PAM have been implemented, notable identity threat surface remains exposed to potential attackers. Consequently, the organization made the decision to adopt CrowdStrike Identity Protection and was actively seeking to implement honey accounts and honeytokens to safeguard against both known and unknown identity threats.

SOLUTION SELECTION CRITERIA

The organization attempted to deploy honey accounts manually. This experiment was fraught with multiple challenges, from naming the honey accounts appropriately to blending in with the AD domain and making it attractive to attackers.

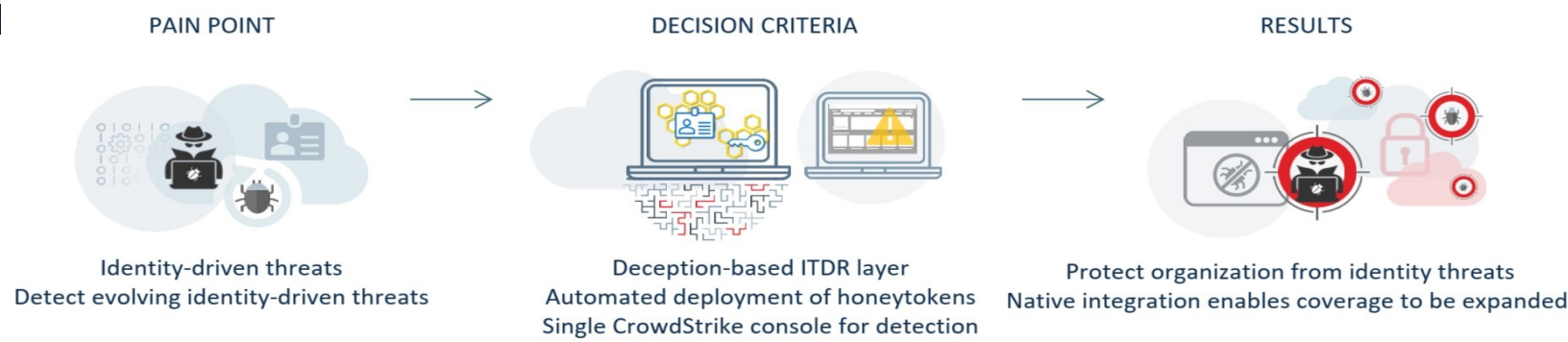
The organization recognized the need for a deception platform to automate the process of deploying honeytokens at scale. Acalvio ShadowPlex was selected for its proven and scalable honeytoken offering and the native integration with CrowdStrike. Their primary selection criteria included:

- ❑ Recommendation of honey accounts that blend with the AD domain and are attractive to attackers
- ❑ Automated honeytoken recommendation and deployment to identity caches on endpoints
- ❑ Agentless deployment architecture to avoid compatibility challenges associated with agents on endpoints
- ❑ Single CrowdStrike console for identity threat detection

DEPLOYMENT

ShadowPlex was successfully deployed within just one week on the organization's network. The deployment process was straightforward, involving a one-step activation of permissions within CrowdStrike for the Acalvio integration. There was no need for any on-premises Acalvio software installation.

The administrator granted approval for the honey account recommendations within ShadowPlex, leading to the automated deployment of honey accounts and honeytokens across multiple AD domains and endpoints.



RESULTS AND NEXT STEPS

"Identity-driven attacks are an important priority for us. We were looking to deploy honeytokens but were unable to get past the first one or two due to the manual steps involved. We evaluated Acalvio ShadowPlex and were impressed by the elegance of the integration with CrowdStrike, with no Acalvio components to be deployed in our networks and honeytoken alerts showing up in the CrowdStrike console."

-CISO of the organization

The honey account and honeytoken deployment in this extensive healthcare organization has yielded significant benefits:

- ✓ High fidelity identity threat detection that is agnostic to attacker TTPs
- ✓ Detection of a wide variety of identity threats, including client-side attacks, offline attacks, zero-day attacks
- ✓ Early threat detection through honeytokens on endpoints, to protect the organization's assets
- ✓ Protection of both managed and unmanaged endpoints against identity threats
- ✓ Diversion of the attacker away from the real assets and toward the deceptive honey accounts and honeytokens
- ✓ Security Operation teams successfully utilized their established SOAR platform to effectively manage and respond to honeytoken detections initiated by Acalvio and CrowdStrike
- ✓ Effective deception-based ITDR layer for protecting identities, forming the foundation for Zero Trust design

In the next phase, the organization plans to onboard additional Active Directory domains into the CrowdStrike identity solution as they welcome new healthcare member bodies to the parent organization. The seamless Acalvio integration simplifies the deployment of honeytokens in the newly onboarded domains through an uncomplicated approval process, ensuring that the organization remains shielded against identity-driven attacks as they continue to expand their services.

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced IT and OT Threat Detection, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy on-premises, in the cloud or via marquee managed service providers.

Acalvio Technologies| 2520 Mission College Boulevard, Suite 110, Santa Clara, CA 95054, USA | www.acalvio.com