ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

FINANCIAL SERVICES COMPANY

HIGHLIGHTS

Investment management firm: On-prem and Azure Cloud infrastructure; multiple locations

Project business driver: Insufficient threat detection controls

Key evaluation criteria: Rich and compelling deception palate; integrations & automation

Deployment: Multifaceted mix of server and endpoint decoys & breadcrumbs; CrowdStrike integration

Results: Azure Cloud deployment; threat hunting hypothesis testing

BACKGROUND

This New York-based investment firm manages over $20 billion in assets and commitments. Its IT estate includes satellite offices, on-premises and cloud-hosted applications and is currently executing a "lift and shift" strategy to expand its use of Azure Cloud.

PROBLEM STATEMENT

The firm recently hired a new Vice President of CyberSecurity, who was charged with conducting an evaluation of their security controls as part of an overall business risk analysis. He determined that the firm lacked sufficient internal threat detection controls, and decided to evaluate deception solutions, as he had seen their value demonstrated at a previous employer. He felt deception was a particularly appropriate choice given the lack of Security staff and the limited capabilities of their (outsourced) SOC.

Based on previous experience and a review of relevant standards and best practices (in particular the NIST CyberSecurity Framework and MITRE ATT&CK), the team felt that the highest priorities were rapid, accurate detection of the following behaviors:

- Reconnaissance
- Lateral Movement
- Data Exfiltration
- Ransomware

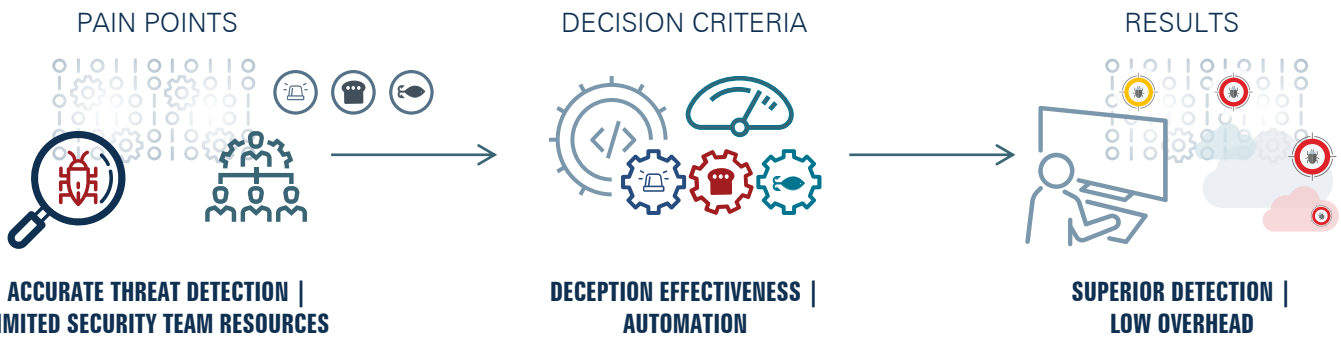
SOLUTION SELECTION CRITERIA

Because the critical use case was detection and the security team capabilities were limited, the following two criteria were rated highest:

Quality and Richness of Decoys and Breadcrumbs: The ability to deploy and maintain credible deception assets was seen as essential, as otherwise the solution would be unlikely to entice and deceive a sophisticated attacker.

Integrations and Automation: The solution had to be highly automated, as the firm simply didn't have the staff for anything less. Integrations into their IT and Security architectures were therefore mandatory.

Following a brief market scan and vendor evaluation, Acalvio was invited to conduct a proof of concept, involving a ShadowPlex deployment in the New York office. During the evaluation, the company brought in their third-party penetration tester to conduct an annual exercise. As the pentesters executed their methodology, ShadowPlex reliably detected their activity. At the same time, the SOC didn't report anything out of the ordinary. An investigation discovered that some IOCs were being sent to the SOC, but they didn't trigger any sort of notification or action at all. This experience, coupled with the firm's positive evaluation of the ShadowPlex administrative interface, led to a decision to move to a production deployment.



DEPLOYMENT

The initial production deployment was in the New York headquarters, and includes the following decoy types across Microsoft Windows, Linux, and MacOS:

- Databases (e.g. MySQL, SQL Server)
- Active Directory Domain Controllers
- SMB (Windows) file shares
- End user workstations

The deployment also makes heavy use of a variety of breadcrumb types to lead adversaries to the decoys, including:

- Browser cache entries
- RDP connection profiles
- Database configuration files
- Active Directory object definitions

For automation, ShadowPlex was integrated with CrowdStrike Falcon to support three use cases:

Endpoint Discovery: As the firm implements a "zero-trust" network paradigm with heavy use of internal firewalling, Falcon is used to help populate the endpoint database;

Breadcrumb Deployment: Falcon deploys breadcrumbs on production systems, eliminating the need to provision and manage a parallel set of privileged access across the environment;

Endpoint Response: If ShadowPlex detects a compromised endpoint, it signals Falcon to implement the response policy, which can include isolation and process termination.

NEXT STEPS

With ShadowPlex in production and returning high fidelity results, the firm plans to expand their use of the solution in two ways:

- Decoy deployment in Azure Cloud
- Azure Sentinel alert management integration

Looking further ahead, the firm intends to start a Threat Hunting program within a year, and will use ShadowPlex for hypothesis testing in support of the program.

Acalvio is a leading provider of Deception Technology for Advanced Threat Protection. With over 26 issued patents, Acalvio has integrated Deception technology with advanced AI to provide autonomous deception solution that is effective, easy to use and can be deployed at enterprise-scale with minimal overhead. Acalvio ShadowPlex reduces attacker dwell time by early detection of advanced threats and increases SOC efficiency by sophisticated investigation and active threat-hunting capabilities. Extensive partner integrations allow ShadowPlex to leverage customer's ecosystem for rapid and comprehensive threat containment.

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