ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

CONSUMER SERVICES

HIGHLIGHTS

Consumer Services firm: multiple sites and big push to AWS cloud

Project business driver: protection of member and credit card information

Key evaluation criteria: Lateral movement detection, high fidelity alerts, hybrid cloud; MSSP option

Deployment: Acalvio ShadowPlex; single Deception Farm projects decoys across 100 subnets and AWS VPCs; breadcrumbs on servers

Results: 2 years in production; Ops outsourced to MSSP; effective detection of abnormal behavior

BACKGROUND

This US-based consumer services company serves millions of members, maintains dozens of offices, and its IT team supports thousands of staff and volunteers. A registered non-profit, the organization is active in many areas, including lobbying, insurance, and education.

PROBLEM STATEMENT

The organization has limited IT staff, but handles sensitive member data and credit card information, as well as crucial information that supports its lobbying efforts. This makes it an obvious target. The SOC was overwhelmed by the "noise" of thousands of low-fidelity alerts, particularly those generated by endpoint security. It also lacked tools to detect suspicious lateral activity, both on-premises and in its cloud environments. Lastly, the organization was about to embark on a major effort to move workloads from their data center to Amazon AWS.

SOLUTION SELECTION CRITERIA

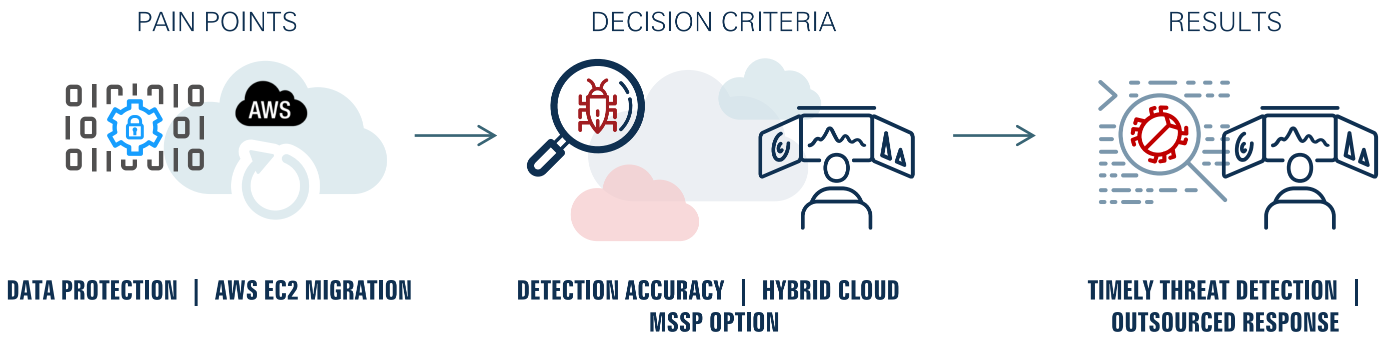
In its RFP, the organization focused on the following key criteria

- General visibility, and in particular lateral movement analysis
- Low volume, high fidelity alerts
- Hybrid cloud support
- Ability to be run by the internal team, or by a managed security service provider (MSSP)

Acalvio ShadowPlex Deception was chosen because it evaluated well on these criteria, including a demonstration of hybrid cloud support from a single administrative interface.

DEPLOYMENT

ShadowPlex was deployed as a single Deception Farm that projected sensors across two physical sites in the eastern US, followed by a migration of assets to a large Amazon AWS EC2 estate. In total almost 100 subnets and AWS VPCs are populated with Deception decoys, including DMZs, data center and access VLANs, and cloud instances that host sensitive data and support external access. Breadcrumbs deployed on servers augment the decoys and are based on a combination of ARP entries, SSH registry entries, and RDP shortcuts. The solution was deployed in just 30 days, and is operated by an MSSP.



PAIN POINTS

DATA PROTECTION | AWS EC2 MIGRATION

DECISION CRITERIA

DETECTION ACCURACY | HYBRID CLOUD
MSSP OPTION

RESULTS

TIMELY THREAT DETECTION |
OUTSOURCED RESPONSE

RESULTS

The solution has been effective in identifying compromised endpoints with high fidelity, and the ShadowPlex AI component modifies decoys and breadcrumbs to maintain “freshness” and credibility within the environment. In one case an Apple device started transmitting abnormal P2P packets indicating compromise, leading the SOC to decide to simply wipe the device to mitigate the risk. By keeping the operational requirements low, the SOC is able to focus their efforts on proactive projects, and partnering with the MSSP when needed to collaborate on incident response. They also report a high degree of satisfaction with Acalvio’s Customer Support team whenever needed for escalations.

Acalvio is a leading provider of Deception Technology for Advanced Threat Protection. With over 25 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/