ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

HEALTHCARE PROVIDER

HIGHLIGHTS

Healthcare provider: Multiple Data Centers and requiring protection for specialized workloads

Project Business Driver: Insufficient threat detection controls for the specialized workloads

Key evaluation Criteria: Rich and compelling deception palette for specialized workloads.
Key detection capabilities across the sites of the healthcare provider

Deployment: A multifaceted mix of server, endpoint, and healthcare asset decoys, breadcrumbs, and baits.

Results: After a year in production, ShadowPlex has proven its ability to detect threat actors effectively across IT and Healthcare devices via standard SOC workflow.

BACKGROUND

This healthcare provider operates multiple hospitals, emergency departments and health centers throughout the country which serve more than 300,000 patients. The healthcare provider system has more than 600 doctors, 1700 nurses and 7800 employees.

PROBLEM

The operations of a healthcare facility are critical and time-sensitive because they deal with human well-being. Any delay or disruption to these operations could be catastrophic, and hence the security of such processes is critical.

This healthcare system approached Acalvio to secure from a variety of threat vectors, primarily

- Ransomware
- Protection from unauthorized access to protected health information
- Detection of threat activity in networks containing sensitive medical devices
- Detection of threats in the networks containing IT assets

SOLUTION SELECTION CRITERIA

To protect against a variety of threat vectors, this healthcare system used the following evaluation criteria to select a deception solution:

•Early and high-fidelity detection against Ransomware

•Protection from unauthorized access to protected health information

•Availability of decoys of assets typically found in a specialized workload containing healthcare devices, built-in

•Detection of threat activity in the networks containing IT assets

Acalvio ShadowPlex and its sophisticated, but easy-to-deploy deceptive artifacts demonstrated to achieve fast and early detections in all the scenarios and threat vectors mentioned above. The solution also provided out-of-the-box decoys for healthcare assets typically found in a healthcare facility, which the customer was looking for.

DEPLOYMENT

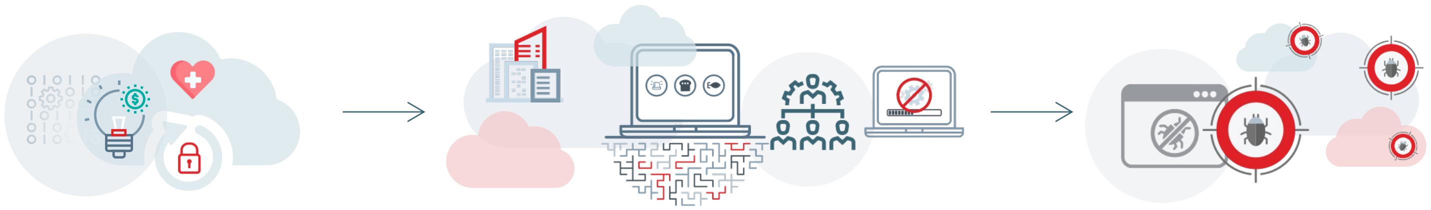
ShadowPlex was deployed across three data centers, ten medical assets networks, and one Head Office network. The deployment was done using a single on-premises deception server that gave centralized management capabilities in terms of strategizing and managing deceptions, which significantly improved the ease of operation.

The overall deployment was completed within 30 days.

PAIN POINT

DECISION CRITERIA

RESULTS



Ransomware, Healthcare Asset Protection

IT & OT Threat Detection, Solution for Healthcare Devices, Optimized SOC bandwidth

Advanced Threat Detection, Zero False Positive Alerts, Fast Deployment

RESULTS AND NEXT STEPS

After a year in production, ShadowPlex has proven its ability to detect threat actors effectively across IT and Healthcare devices via standard SOC workflow. Here are the summary of results:

- Best practice deception deployment, guided by Acalvio's customer success team, detected threats in critical VLANs, which would've otherwise gone unnoticed.
- High fidelity, and zero false positive alerts provided by ShadowPlex benefited the SOC in saving bandwidth spent analyzing incidents which provided a great return on investment.
- Through AI/ML capabilities, ShadowPlex simplified operations and deployment which made designing and implementing deception quick and easy
- As alerts are fully mapped to the MITRE ATT&CK Framework, the customer's SOC could easily classify, separate, and build use cases.

As next steps, this customer plans to enable their SOC team to use ShadowPlex for advanced threat hunting and identity threat detection and response (ITDR) use cases.

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