ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

TELECOMMUNICATION SERVICE PROVIDER

HIGHLIGHTS

Telecommunication Service 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 distributed sites of the telecommunication company

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

Results: ShadowPlex detected numerous threats with high-fidelity alerts. It also provided visibility into Active Directory attack surface and secured it against cyber threats.

BACKGROUND

This telecommunications service provider is the leading mobile phone operator in its country and has 50 million subscribers worldwide. From an operations perspective, the company has 6 sites, 2500+ networks and nearly 25,000 employees.

PROBLEM

Threat vectors in the telecommunications industry range from automated malware like Ransomware to targeted espionage operations by Advanced Persistent Threat (APT) groups. APT-driven attacks against telecommunications companies have specific motives:

- Gather Call Data Records (CDR) of high-profile individuals
- Install malicious tools that monitor network connections to extract message data like IMSI numbers, source & destination phone numbers and SMS message contents.
- Cyber security tools that detect all types of attacks that target telco enterprises are hard to find, especially those that offer protection for core telecommunications and custom workloads.

SOLUTION SELECTION CRITERIA

The customer identified deception as a solution to detect malicious activity across their diverse and distributed workloads, shortlisted multiple deception vendors and passed them through a rigorous evaluation process. ShadowPlex was selected for following reasons:

•The scalability offered in terms of deploying deception best practices through thousands of deceptive artifacts within the enterprise.

•The distributed architecture makes it easy to deploy deception into the geographically spread operations.

•The built-in telecommunications workload protection decoys for
- Home Subscriber Server
- Home Location Register
- Mobility Management Entity
- Signaling Gateway
- Packet Gateway

•The specialized decoy services
- Session Initiation Protocol (SIP)
- Diameter

DEPLOYMENT

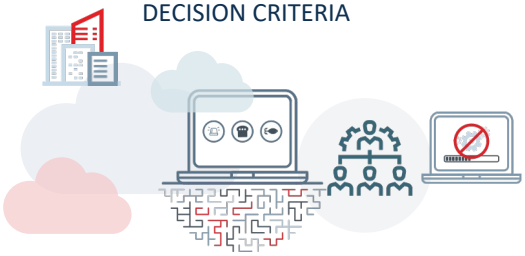
ShadowPlex was deployed in the 6 distributed sites across 2500+ subnets. Comprehensive protection was rolled out to the end-user networks, critical server segments, DMZ zones, and the networks with customer's specialized workloads.

ShadowPlex's distributed architecture, which uses a centralized Acalvio Deception Center (ADC) and multiple sensors to provide visibility into the enterprise network, ensured that the deployment, management and strategizing of deception were extremely simple. ShadowPlex also secured the Active directory (AD) of the customer with its innovative AD protection capability.

PAIN POINT

Ransomware, Telecommunication Asset Protection

DECISION CRITERIA



Protection for Telecommunication Workloads, Optimized SOC bandwidth

RESULTS

Advanced Threat Detection, Zero False Positive Alerts, Fast Deployment

RESULTS AND NEXT STEPS

After 4 years in production, ShadowPlex has proven its ability to detect threats effectively across their IT and specialized workloads in distributed datacenters via standard SOC workflow. Here are the summary of results:

- ShadowPlex detected numerous threats in the network which included the activity of a remote access trojan (RAT) and an early detection of an attempt at Ransomware detonation.
- ShadowPlex assessed the enterprise's Active Directory and identified misconfigurations, which would've otherwise gone unnoticed. Acalvio's customer success team provided guidance in remediation of these misconfigurations to help reduce the attack surface in the customer's AD.
- Purpose-built deceptions for Active Directory were registered using ShadowPlex into the enterprise AD of the customer, to ensure high-fidelity detections against AD enumeration and attack attempts.
- High-fidelity alerts with zero false positives provided by ShadowPlex helped reduce SOC bandwidth in analyzing incidents that ultimately resulted in a great return on investment.

As next steps, the customer was in the process of migrating some of their workloads to the cloud and plans to use the cloud protection package of ShadowPlex to secure cloud operations.

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