ACALVIO

ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

INDUSTRIAL MANUFACTURER

HIGHLIGHTS

Industrial Equipment Manufacturer:
Global footprint, 3,000 employees

Project business driver:
IP and customer data protection; OT network availability

Key evaluation criteria:
Lateral movement detection; low-false positives; OT network support

Deployment:
Acalvio ShadowPlex; single Deception Farm projects 4K decoys globally across VLANs in DMZs, enterprise and OT networks

Results: 1.5 years in production; detected unauthorized legacy gear; Email, SIEM, and reporting integrated to risk management processes focusing on lateral movement

BACKGROUND

This manufacturer of industrial equipment has over 25 offices and manufacturing plants in the US and abroad, 3,000 employees, and a very broad distribution channel. It operates in a very competitive product space, with numerous domestic and international competitors, and continuous pressure on operating margins.

PROBLEM STATEMENT

The organization found itself the frequent target of attacks seeking to obtain intellectual property related to its products, or to steal customer data. A consequence of such attempted penetrations was the loss of employee productivity caused by compromised endpoints. Like most IT and SOC teams, they struggled to obtain sufficient timely, accurate visibility into their environment, and there was no method of lateral movement anomaly detection. This meant that hacked endpoints were hard to identify, and could probe the rest of the network at will. Furthermore, they were concerned that the lack of security controls in their OT (manufacturing) environment constituted an unacceptable business risk.

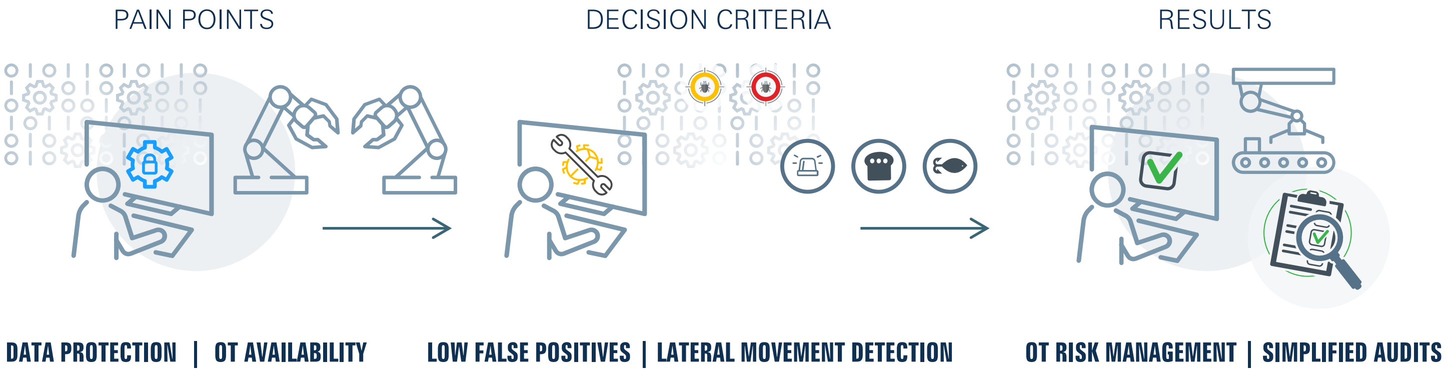
SOLUTION SELECTION CRITERIA

The security team decided to not conduct a product bake-off, but instead move directly to a pilot installation. They identified Deception as the preferred approach, mainly because of the desire to keep spurious alerts to an absolute minimum and not require agent software, but also because the focus of the project was to detect attacker lateral movement. Acalvio ShadowPlex was selected because of its degree of automation, in particular for customizing deception artifacts, and ability to engage with adversaries to retard their efforts to find and compromise high value servers. It also can be deployed in OT environments without risk to production systems due to its passive approach.

DEPLOYMENT

ShadowPlex was initially deployed in three access network VLANs, where it demonstrated its ability to automatically mimic the surrounding environment, and to not generate false positive alerts. Subsequently, the full deployment was executed: A single ShadowPlex Deception Farm in the US now supports locations all over the world. Eight sensors project roughly 4,000 decoys onto dozens of VLANs, including DMZs, enterprise internal networks, and OT networks in the manufacturing plants. The ShadowPlex automatic blending capability analyzes the network segments and customizes the decoys so that they appear similar to their environment. Elements of this process includes hostnames, MAC addresses, operating systems, services and active ports.

A key aspect of the deployment is its integration with the overall security architecture. Because Deception alerts have very high fidelity, when something is detected it usually requires a robust response. To that end, the SOC decided to use both email alerts to the SOC service alias, and events sent to the SIEM. Those events are collected into incidents and alerts are triggered on the SIEM. Lastly, weekly reporting is used to send interested stakeholders' information on host changes and incidents.


PAIN POINTS

DECISION CRITERIA

RESULTS

DATA PROTECTION | OT AVAILABILITY

LOW FALSE POSITIVES | LATERAL MOVEMENT DETECTION

OT RISK MANAGEMENT | SIMPLIFIED AUDITS

RESULTS

Once ShadowPlex was deployed, within a couple of days it identified legacy devices that were supposed to have been removed from the network but were not. A compromise of any of its 3,000 endpoints can now be quickly detected and mitigated when lateral movement is detected. The combination of ShadowPlex and the EDR solution acts as the primary control for insider threat management, and it is easy for auditors to verify the consistency of the control process during audits. While scanning for hosts is not allowed on the OT networks, lateral movement does trigger alerts to the SIEM, and this process acts as a compensating control for OT risk management.

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/