ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

SEMICONDUCTOR MANUFACTURER

HIGHLIGHTS

Semiconductor Manufacturer: Global footprint; 10K+ employees

Project business driver: IP protection; business continuity including SaaS

Key evaluation criteria: Hybrid cloud, scalability, low operational overhead, agentless

Deployment: Acalvio ShadowPlex; single Deception Farm covering 100+ VLANs in 10+ countries

Results: 3 years in production; multiple threats detected and mitigated per month via standard SOC workflow

BACKGROUND

This Fortune 250 manufacturer is a leader in semiconductor and systems technologies, with a worldwide footprint and over 10,000 employees. It has an aggressive acquisition strategy, meaning it has to manage a very dynamic, heterogeneous IT environment. Research and Development labs pose particular challenges, because of the wide variety of embedded devices running non-standard or older operating systems. While the majority of the applications and data is either on-premises or in IaaS (AWS), they do store some important data in SaaS-based content management services.

PROBLEM: IP PROTECTION

The manufacturer has a large amount of widely distributed intellectual property that it needs to protect. It is a frequent target of attacks seeking either IP theft or disruption to business processes. Besides the primary need to detect and mitigate such attacks, it also sought attack surface visibility, and to closely monitor the DMZ that hosts Internet facing commercial services, as this was an obvious vector for compromise.

SOLUTION SELECTION CRITERIA

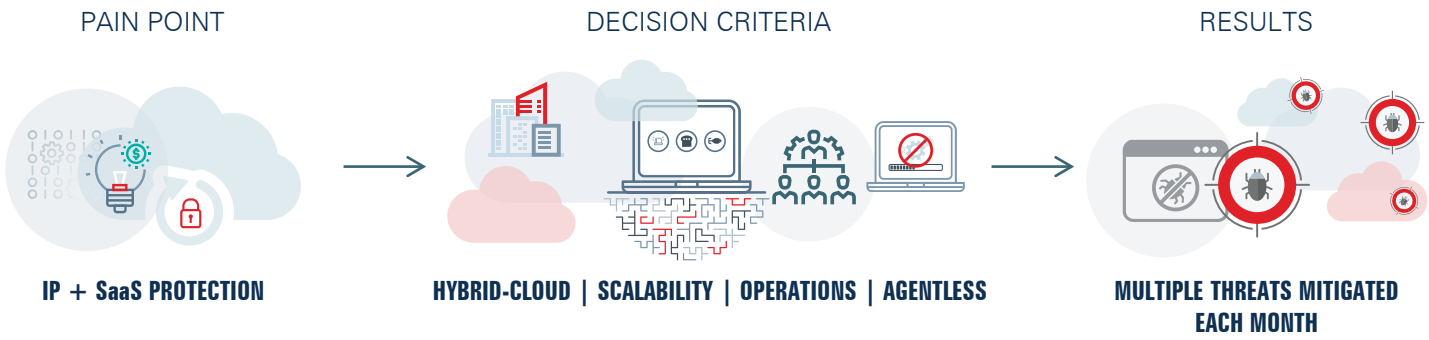
The organization settled on the following criteria for its evaluation of potential internal threat detection solutions:

- Support for on-prem, IaaS, and SaaS environments
- High scalability
- Ability to operate with low-false positives in a dynamic, heterogeneous environment
- Agentless deployment, in particular, for R&D locations
- Low staff requirements and training for both solution maintenance and alert management

Acalvio ShadowPlex Deception was chosen based on an evaluation of two vendors that focused on the five core solution criteria, plus an evaluation of the vendor's track record of execution.

DEPLOYMENT

ShadowPlex was initially deployed across over 100 VLANs and 10 countries. When M&A events occur either additional VLANs are on-boarded to ShadowPlex, or the devices are simply added to the existing VLANs (which are configured with very large address spaces). Deception assets are centralized in a single Deception Farm, projected across the network automatically by ShadowPlex, and self-configured to blend with the local network environment. This greatly reduces the time and staffing required to support changes and keeps the deception assets credible as the environments change. This is a crucial capability because the Security team isn't always informed of changes by the lines of business, and in any case isn't in a position to thoroughly analyze modifications to connected systems. Breadcrumbs and baits (which consume virtually no system resources) are deployed on small footprint and legacy devices. The initial deployment required less than 0.5 full-time staff (FTE), while ongoing operations require almost no support at all, as the solution is integrated into the SOC's standard incidence response workflow.



RESULTS AND NEXT STEPS

After over three years in production, ShadowPlex has proven its ability to detect threat actors both within the perimeter and in the SaaS-based content management system. Multiple high- fidelity alerts are generated each month and handled by the SOC, in the same manner as they handle the rest of the security events. These alerts are usually the result of the detection of host compromise or attempted lateral movement. The information about attacker TTPs (tactics, techniques and procedures) informs proactive threat hunting. Because ShadowPlex is largely self-managing and full integrated into existing security processes, the additional staff overhead is minimal.

ShadowPlex also proved its value during the acquisition and integration of a very large firm into the parent. The team didn't have the time, WAN bandwidth, or business insights to perform an audit of the acquired firm's environment. Instead, they just deployed an additional virtual sensor as an extension of their existing ShadowPlex system. ShadowPlex's ability to discover the target environment, classify assets, and deploy credible deceptions enabled the Security team to extend the Deception coverage to the acquired company in a few days. The Security team at the acquired company did not need to perform any manual steps or provide data to the parent company.

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/