ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

CONSUMER PACKAGED GOODS COMPANY

HIGHLIGHTS

Consumer packaged goods (CPG) company: 100K+ staff; worldwide footprint

Project business drivers: Defense in Depth, Threat Hunting, Threat Mitigation

Key evaluation criteria: Flexible deployment, Integrations, Active Directory security

Deployment: 100+ VLANs, cloud and on-prem, SIEM, EDR, & Active Directory integrated

Results: Detected various types of malicious activity; Visibility of AD mis-configuration risk; Used for advanced threat hunting and artifact analysis.

BACKGROUND

This Fortune 500 company is a well-known food and beverage brand in the consumer packaged goods industry. It has an ongoing IT transformation program to move workloads from their data center to Azure Cloud, including rearchitecting Active Directory to leverage Azure AD and cloud and on-prem domain controllers.

PROBLEM STATEMENT

The company embraces a policy of Deception in Depth, and needed to evolve their security controls to cope with their constantly evolving hybrid cloud, IT/OT environment. They sought to fill gaps in their threat detection capabilities, in particular gaps in controls across the MITRE ATT&CK framework that needed to be addressed.

Active Directory risk management was a particular area of concern. The Security team did not have the authority to insist on a large scale re-configure of AD, and suspected that there were risks such as attacks leveraging Kerberos Unconstrained Delegations.

The firm also needed to improve their Threat Hunting capabilities. Their hunting tools were inflexible, and limited to using log analysis based on well-known IOCs. The enterprise was looking for better capabilities for analysis of memory snapshots and “living off the land” adversary techniques such as malicious PowerShell scripts.

Finally, threat mitigation was another weak area. Existing controls did not enable isolation of malicious host processes at scale. As a result, the enterprise was living with known malware within server environments where host quarantining could not be performed because of availability impacts. In summary, the goal was to close as many gaps as possible with as few products as possible.

SOLUTION SELECTION CRITERIA

The enterprise was already convinced that Deception was the most viable solution category, because of its flexibility, low risk to application availability, and high-fidelity alerts. They did a two month pilot running in Azure to validate their hypothesis and select a vendor. Acalvio ShadowPlex won the evaluation as it best supported the key use cases listed above, and scored well in these dimensions:

Flexibility: It was vital that the solution was flexible enough to protect a wide variety of high-value, off-the-shelf and custom applications. ShadowPlex's rich palette of decoys, breadcrumbs and baits, the ability to add new decoy types for custom applications, and AI-driven deployment automation, meant that all key assets could be obfuscated and protected.

Active Directory Security: ShadowPlex provided superior AD controls with its InSights package to surface AD attack surface, plus a rich palette of AD-specific deception artifacts.

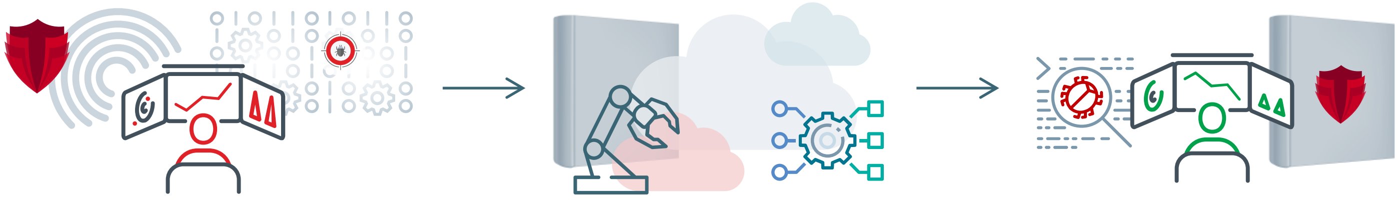
Threat Hunting: The offering gave the Threat Hunting team the ability to deploy deception assets to validate hypotheses, obfuscate key IT assets thought to be attack targets, and analyze artifacts such as PowerShell scripts and memory snapshots.

Integrations: ShadowPlex demonstrated built-in integrations with key security tools, including SIEM, EDR, and Sandbox solutions.

PAIN POINTS

DECISION CRITERIA

RESULTS



DEFENSE IN DEPTH | THREAT HUNTING | THREAT MITIGATION

ACTIVE DIRECTORY SECURITY | FLEXIBILITY | INTEGRATIONS

INTEGRATED THREAT DECTION | LOWER AD CONFIGURATION RISK | EFFECTIVE THREAT HUNTING

DEPLOYMENT

The initial ShadowPlex deployment spans roughly 100 VLANs and includes both on-prem and cloud. The focus is on protecting "crown jewels" such as SAP and Internet facing business critical applications. A wide variety of deception assets are placed within Active Directory, including Computer and User objects, SPNs registered to decoys, and more. The ShadowPlex Deception Farm is deployed in the cloud and projects decoys across the environment. ShadowPlex has been integrated into the SOC's Incident Response workflow, with the SIEM and EDR solutions tied into ShadowPlex for consolidated alert management and deception artifact deployment and process mitigation.

Crucial to the success of the deployment was the minimal support required from the IT team. The Security organization was able to perform the deployment on their own in less than a month with half an FTE of manpower.

RESULTS AND NEXT STEPS

ShadowPlex detected various types of malicious activity, including coin-mining malware and penetration attempts on SQL Servers, web front ends, and SAP decoys. The InSights capability has surfaced serious Active Directory mis-configuration risks, which are prioritized for remediation in partnership with the relevant operational team. On the Threat Hunting side, ShadowPlex is used to hunt for specific threat vectors, and to test for the presence of attackers looking for hosts with insecure SMB protocols enabled. This is done by deploying decoys with vulnerabilities and seeing if an adversary attempts to compromise them. The EDR integration is used not only to facilitate breadcrumb and bait deployments on hosts, but also to perform adversary traversal analysis, that is, to trace out the route an attacker has used during lateral movement.

Now that the SOC is comfortable handling ShadowPlex alerts, the company has the following priorities for extending the deployment:

- Scaling Deception to protect additional assets, including their large cloud-based VDI infrastructure;
- Integrating with their SOAR platform to automate response using pre-defined playbooks.
- Conducting a pilot deployment in an OT manufacturing environment.

Overall, the ShadowPlex solution has clearly satisfied the Security team's requirement to close a wide variety of risk management gaps with a small operational footprint, and without requiring significant support from the wider IT organization.

Acalvio is a leading provider of Deception Technology for Advanced Threat Protection. With over 26 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/