ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

# DEPLOYMENT FOR DIGITAL MULTIMEDIA COMPANY

## HIGHLIGHTS

**Digital Media firm:** 5,000 users; thousands of servers

**Project business driver:** Ransomware & APT risk mitigation

**Secondary drivers:** General threat detection & Active Directory protection

**Key evaluation criteria:** Scalability & low operational overhead

**Deployment:** Acalvio ShadowPlex in two data centers with centralized Deception Farm

**Results:** Detected malware missed by other security tools; facilitated complete removal

**Looking ahead:** Additional Threat Hunting use case under consideration

## BACKGROUND

This digital media company has dozens of properties and brands including video and music streaming, news, sports, real estate, and more. Their IT infrastructure supports over 5,000 users and hosts a wide variety of customer and internally facing applications, hosted on thousands of VMware servers in two data centers. They had basic security controls in place, including firewalls, endpoint protection, and vulnerability scanning.

## PROBLEM: RANSOMWARE AND APT RISK MITIGATION

The firm was particularly concerned about attacks on the data center assets, in particular ransomware, APTs, and malware in general. Any such attack could cause significant downtime and reputational loss, which was deemed an unacceptable level of business risk. The existing security controls were deemed insufficient to detect such an attack in time to mitigate it. Furthermore, the Security team struggled with a lack of visibility: given the nature of digital media, the IT environment was very dynamic, making it impossible to keep track of business-critical data and applications. Trying to instrument the applications and databases for threat detection was simply not an option.

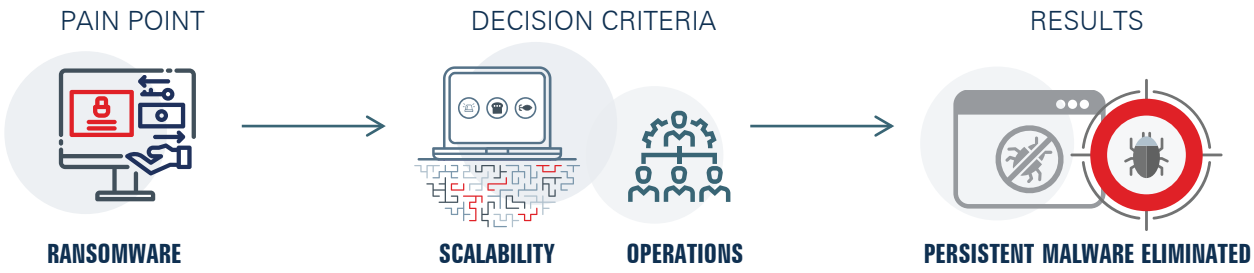
## SOLUTION SELECTION

The Security team researched the types of solutions available (e.g. UEBA) and decided on Deception as the best approach, in particular because of the "light touch" low-risk deployment model and the high fidelity, low-false positive output. In their formal evaluation and procurement process the key decision criteria were scalability, and minimizing operational overhead and staff training. After evaluating three vendors on their pre-production network, Acalvio ShadowPlex was selected because of its ability to scale via its Deception Farm architecture and Fluid Deception capability. Ease of operations was also demonstrated, in particular the ability to easily deploy deception artifacts to match the environment.

## DEPLOYMENT

ShadowPlex was installed in both data centers. Two ShadowPlex sensors per data center are able to blanket the environment by projecting dozens of decoys (centrally hosted in the Deception Farms) across hundreds of VLANs. The IT Operations team was trained to do initial triage of ShadowPlex alerts, with more serious events escalated to Security.

In addition to the primary threat detection use case, ShadowPlex is also protecting Active Directory. The firm deployed breadcrumbs (in the form of fake AD objects such as privileged user credentials and network objects) that motivate malicious actors to move laterally towards the decoys where they can be detected and monitored.




## RESULTS AND NEXT STEPS

ShadowPlex has proven its ability to detect threats. The firm's network is connected to that of its parent organization via firewalls, and the parent had a malware incident that they thought they eliminated. However it transpired that the attacker had a deeper footprint than originally believed, and compromised devices started to probe across the firewall into the media company's network. ShadowPlex detected the probing, helped identify the compromised devices, and allowed the firm to tighten their firewall policy to prevent future attacks.

Looking ahead, the Security team is exploring using ShadowPlex to help with proactive threat hunting by providing environmental visibility, and using it to deploy lures to test for specific threat actors and methods. In the meantime, the solution is the performing well as the primary control for internal threat detection, and has not imposed a significant operational burden on the team. Furthermore, the firm has adopted a ransomware mitigation workflow based on ShadowPlex, so that in the event of such an attack, the team has a well-defined process it can execute.

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/