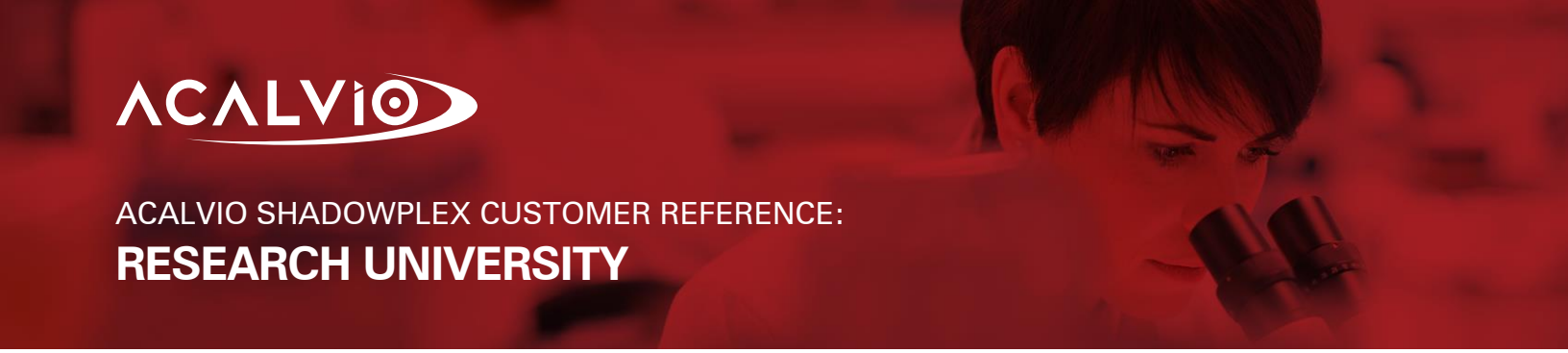


ACALVIO SHADOWPLEX CUSTOMER REFERENCE:

RESEARCH UNIVERSITY

HIGHLIGHTS

Australian research university: Over 75,000 staff and students; multiple locations

Project business driver: Protection of medical and technology research data

Key evaluation criteria: Low-false positives, agentless, scale and integrations

Deployment: Acalvio ShadowPlex across AWS and on-prem including vSphere/NSX; DMZ and general VLANs; integrated with device whitelisting

Results: Threat intelligence from Internet probing; ransomware and Active Directory defenses; high operational efficiency

BACKGROUND

This research university, one of the largest in Australia, has over 75,000 faculty, staff, and students spread across multiple locations and international satellite campuses. It has a particular emphasis on medical and technology research, which generates considerable revenue and enhances the reputation of the institution. The university's IT environment is a hybrid cloud that includes multiple IaaS providers and VMware based software-defined datacenters running vSphere and NSX. They continue to migrate applications and infrastructure to the cloud, and to move workloads between clouds to take advantage of differences in cost and capabilities.

PROBLEM STATEMENT

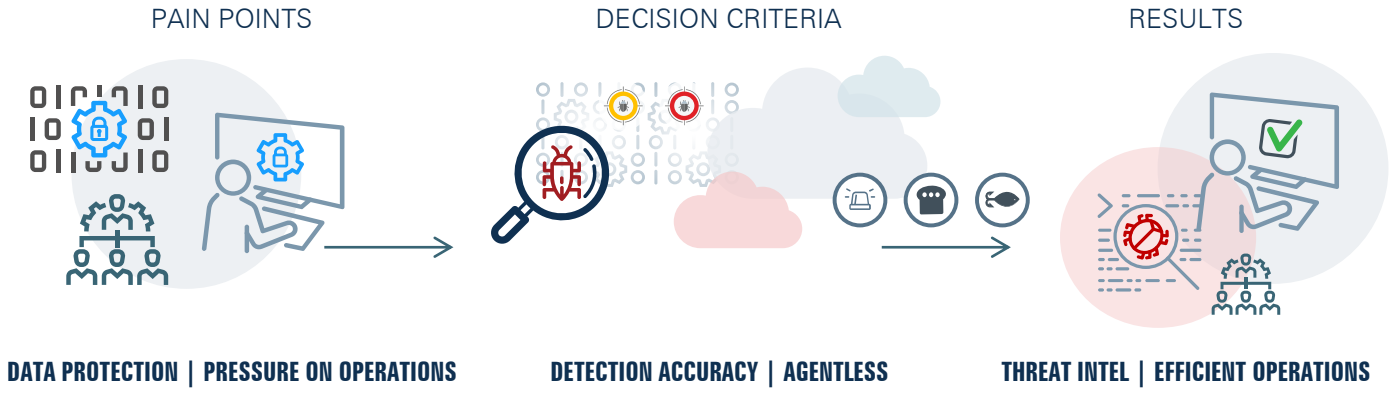
The university conducts high-value research that is an obvious target for theft. While they have EDR and a SIEM, they are struggling to deal with the volume of events and alerts being generated. Therefore, they needed a complementary solution for breach detection that would immediately identify intrusions in the research facilities with a high level of accuracy. This requirement led them to conduct an RFP for Deception solutions.

SOLUTION SELECTION CRITERIA

Beyond the core requirement for detection accuracy and low noise, the university's selection team required an agentless solution, as they didn't want to have to manage additional endpoint software. Ease of scalability and hybrid cloud (IaaS and VMware) support were essential given the size and breadth of the IT environment. The university also prioritized integrations with their Splunk SIEM and CrowdStrike EDR solution for remediation. After reducing their RFP response from six to three vendors, they selected Acalvio primarily based on these criteria, but also because they appreciated Acalvio's focus on Deception. They felt the closest alternative was spreading themselves too thin with multiple solution areas and preferred a vendor that was totally committed to Deception.

DEPLOYMENT

The initial ShadowPlex deployment was across three environments: AWS, vSphere/NSX, and on-premises traditional VLANs that host the research assets. Web server decoys were deployed on DMZs to detect scanning from the Internet, while up to ten Windows Server, Linux, and NAS decoys were deployed on internal networks for breach and lateral movement detection. In the highest value VLANs, the university integrated the decoys with their MAC whitelisting solution. The operational model is to push ShadowPlex alerts to Splunk, and then use the ShadowPlex UI to investigate and resolve the alert.



RESULTS

Immediately following deployment, the ShadowPlex DMZ decoys started reporting incoming sweeps from the Internet. This generated a list of public IPs that was used for threat intelligence and blacklisting purposes. Because of the ease of deployment and lack of false positives, the university added ransomware and Active Directory threat detection, and scaled up the solution to the other parts of the IT estate. They completed the CrowdStrike integration for threat response, deployed baits in cloud file shares, and leveraged the solution to gather more advanced threat intelligence, in particular information about the threat actors targeting the university. Overall the entire process from RFP to deployment took under four months, and has met the project objectives without requiring specialized staff training.

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/