ACALVIO

CASE STUDY

ACALVIO SHADOWPLEX PROACTIVE DEFENSE STRATEGY

AIRPORT FACILITY ORGANIZATION

HIGHLIGHTS

Airport Management Services

Protect critical assets in Airport Operations network

Project Business Driver

Protect unmanaged endpoints, direct financial and reputation loss from breaches and disruption

Key Evaluation Criteria

Ease of deployment

Comprehensive deception coverage

Agentless Solution

Deployment

Decoys representing important IT assets in airport network

Decoys in Unmanaged & IoT networks

Baits in data repositories

Results

Protection across multiple networks of the large airport network

Rapid deployment of deception strategy

Detection of lateral movement and exploit attempts by stealthy threats

ShadowPlex provides advanced deception technology to protect financial services infrastructure from cyber threats.

BACKGROUND

This airport facilities organization serves as a bustling hub for international travel, overseeing the management and development of the airport to ensure smooth operations and a seamless passenger experience. As such, cybersecurity is a top priority due to the escalating volume of advanced threats targeting the IT and IoT assets that are critical for seamless airport operations.

THE CHALLENGE

The airport operations organization manages a wide range of critical systems, including Ground Support Network (GSN), Parking Control Systems (PCS), ETAM, airport terminal, HVAC systems, operational technology (OT), and IT workstations, making it a prime target for sophisticated cyberattacks.

Despite investments in security solutions like firewalls, IAM, AV, EDR, SIEM, and SOAR, security reviews and red team assessments revealed significant detection gaps, such as:

- Securing OT and engineering workstations essential for airport operations
- Emerging ransomware targeting ground support and OT systems
- Attacks on GSN, VOIP and PCS networks from unmanaged endpoints
- Credential-based attacks on employee systems and IT applications

With attacker breakout times averaging 62 minutes, the organization needed to enhance threat detection and response speed. Recognizing that AI-driven threats would only become more sophisticated, the security team sought a solution beyond traditional anomaly detection.

A prototype deployment of cyber deception targeting IT and OT systems, along with a red team exercise, demonstrated its effectiveness in addressing detection gaps. This success led the team to evaluate a full-scale distributed deception platform to improve threat visibility and detection for the SOC.

SOLUTION SELECTION CRITERIA

The key success criteria for selecting a deception solution included:

- Packaged solutions for threats targeting Airport Infrastructure
- Enterprise-wide deployment with minimal administrative effort
- No impact on production infrastructure and endpoints
- Interoperability with existing security solutions
- Compatibility with existing SOC workflows

THE SOLUTION

The initial production deployment was in the Datacentre and DMZ network segments, and includes deceptions to protect the important servers and data repositories.

- **Rich Deception Set:** Protection for datacenter and IoT networks including SIEM, IoT applications, VoIP and Ground Support Network (GSN)
- **Prepackaged Solutions:** Deception playbooks for Airport infrastructure assets that can be deployed with minimal administrative effort.
- **Agentless Architecture:** Scalable deployment across the enterprise without resource utilization overhead on the endpoints, which was a crucial requirement for the endpoint team.
- **Zero Disruption & AI Automation:** Automated and auto-scaled deceptions, saving administrative time. The airport operations required zero disruption deployment.
- **Prebuilt Integrations:** Seamless onboarding with existing EDR, SIEM, and SOAR solutions, reducing integration time and cost.

The security team deployed Acalvio's Advanced Threat Defense to cover critical use cases and protect assets in airport management services, including deceptions to protect IT, IoT and airport terminal network.

> "Cybersecurity is of paramount importance to us as a financial services organization. With the rapid escalation in breaches, strengthening our cyber defenses and accelerating our threat detection and response is an important priority. We have added cyber deception to strengthen our detection capabilities and defend against identity threats, ransomware, and insider threats."
>
> — CISO of the enterprise

RESULTS AND BENEFITS

Acalvio ShadowPlex delivered the following outcomes:

- ✓ **Protected key assets:** Flight info and, reservation systems, SIEM, Parking Control, HVAC
- ✓ **Expanded detection** coverage, filling gaps in traditional security
- ✓ **Support for multiple use cases**: Early threat detection, key asset protection, insider threat detection
- ✓ **Protection of airport infrastructure** by diverting attacks from real assets
- ✓ **Protect passenger data, flight info**,: Detect data breaches, detect unauthorized access
- ✓ **Detection of vulnerability exploit attempts**
- ✓ **Enhanced defense against attacks**, targeting unmanaged IT and IoT assets
- ✓ **Precision in detecting insider threats**
- ✓ **Improved Zero Trust maturity** through enhanced cyber visibility

CONCLUSION

The deployment of Acalvio ShadowPlex has significantly strengthened the airport management organization's cybersecurity posture, closing critical detection gaps and providing robust protection against sophisticated cyber threats. By incorporating deception technology into their security strategy, the organization has greatly improved both threat detection and response times while enhancing resilience against evolving attacks. The successful implementation of Acalvio's solutions underscores the essential role of advanced cyber deception in safeguarding critical airport systems, ensuring the continuity of operations, and maintaining the trust of passengers and staff.

ACALVIO

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy on-premises, in the cloud or via marquee managed service providers. For more information, please visit www.acalvio.com.