ACALVIO

CASE STUDY

ACALVIO SHADOWPLEX PROACTIVE DEFENSE STRATEGY

FINANCIAL SERVICES ORGANIZATION

HIGHLIGHTS

Financial Services

Protect assets in financial services

Project Business Driver

Ransomware payments reaching an all-time high, direct financial and reputation loss from breaches

Key Evaluation Criteria

Ease of deployment with minimal manual effort and time involvement

Comprehensive deception coverage

Deployment

Decoys representing important assets in financial services

Honeytoken accounts in identity stores

Honeytokens on endpoints

Baits in data repositories

Results

Protection across multiple locations of the large financial services institution

Detection of lateral movement attempts by stealthy threats

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

BACKGROUND

This financial services organization serves its members across multiple geographies, managing significant financial holdings. As such, cybersecurity is a top priority due to the escalating volume of advanced threats targeting the organization.

THE CHALLENGE

The organization manages a vast set of financial data, attracting a constant avalanche of cyberattacks, including those specially crafted for this entity. Despite investing in various cybersecurity solutions like firewalls, IAM, AV, EDR, Log Analytics, SIEM, and SOAR, periodic security reviews and red team assessments revealed detection gaps.
These gaps included:

- Protecting financial services infrastructure (SWIFT, ATMs)
- Novel ransomware variants from RaaS affiliates
- Threats targeting unmanaged endpoints
- Identity-driven attacks leveraging cached credentials and exploits

With adversaries' breakout times dropping to an average of 62 minutes, the organization needed to accelerate its threat detection and response strategies. Recognizing that AI-driven adversaries would continue to gain sophistication, the security team sought an additional defense layer beyond anomaly or behavior-based detection to address existing gaps.

Access to cyber deception via a remote workforce protection offering highlighted its potential. The security team conducted a prototype deployment of deceptive artifacts and a controlled red team exercise, which demonstrated the benefits of cyber deception. This led to an evaluation of distributed deception platforms to enhance threat detection and SOC visibility.

SOLUTION SELECTION CRITERIA

The key success criteria for selecting a deception solution included:

- Packaged solutions for threats targeting financial services
- 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 New York headquarters, and includes deceptions to protect the important servers and data repositories.

- **Rich Deception Set:** Protection for SWIFT payment systems, ATM, and POS devices.
- **Prepackaged Solutions:** deception playbooks for financial services 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.
- **AI Automation:** Automated deception configuration, saving administrative time.
- **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 and Identity Protection products to cover critical use cases and protect assets in financial services, including deceptions to protect payment infrastructure, sensitive payment data.

> "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, including payment infrastructure and sensitive data
- ✓ Expanded detection coverage, filling gaps in traditional security
- ✓ Support for multiple use cases: early threat detection, identity protection, insider threat detection
- ✓ Protection of financial infrastructure by diverting attacks from real assets
- ✓ Prevention of sensitive data exfiltration
- ✓ Detection of zero-day ransomware attacks
- ✓ Enhanced defense against identity-driven attacks, providing an effective ITDR layer
- ✓ Precision in detecting insider threats
- ✓ Improved Zero Trust maturity through enhanced cyber visibility

CONCLUSION

The deployment of Acalvio ShadowPlex has significantly improved the organization's cybersecurity posture, addressing critical detection gaps and providing comprehensive protection against sophisticated threats. By integrating deception technology into their security strategy, the organization has not only uplevelled their threat detection and response times but also enhanced their overall resilience against evolving cyber threats. The successful implementation of Acalvio's solutions showcases the vital role of advanced cyber deception in protecting financial services organizations, ensuring the safety of sensitive financial data, and maintaining trust with their members.

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.