Acalvio ShadowPlex for Financial Services Organizations

Proactive defense to protect financial services from cyber threats

Financial services is a high-value target for cybercriminals and subject to heightened scrutiny

Financial services institutions not only face increased risks from cybercriminals targeting their vast monetary assets and large volumes of personally identifiable information (PII), but they are also under growing regulatory pressures. With regulatory bodies introducing stricter cybersecurity requirements, financial institutions must prioritize advanced defense mechanisms to stay compliant. As threat actors continue to evolve their tactics, strengthening the security posture is essential.

Threat vectors targeting financial services

Financial services are targeted by a wide variety of threats. The immediate action to protect their assets. **The top threat vectors targeting financial services include:**

Banking Trojans and Custom Malware: Financial institutions are targeted by trojans such as Emotet and IceID, which extract credentials and propagate within banking and financial systems. Additionally, adversaries develop custom malware like BlackPOS and vSkimmer to target ATM and POS devices, aiming to access payment information and financial data.

Ransomware: Ransomware threats target financial services for financial gain through ransom payments. Ransomware as a Service (RaaS) affiliates, such as Lockbit and Alphv, are particularly active in the financial services vertical. These groups engage in triple extortion, exfiltrating data and causing reputational damage to the organization.

Identity Threats: Threat actors target the identity architecture to gain access to admin and service accounts, escalate privileges, and gain trusted access to critical assets. Adversaries exploit identity-driven vulnerabilities to access payment infrastructure and important servers.

Insider Threats: Insider threats are of particular concern in financial institutions, as insiders have authorized access to financial infrastructure and payment systems. With increased adoption of cloud services and SaaS applications, insiders can exfiltrate sensitive financial information from these document repositories.

Supply Chain Attacks: Supply chain attacks have risen in prominence, exemplified by the SolarWinds breach that compromised financial institutions. With the increased adoption of open-source software, the risk from third-party software in supply chain attacks has significantly increased. Recent attacks leveraging supply chain compromises in popular NodeJS open-source software (Node Package Manager or npm) have targeted financial institutions, enabling subsequent attack payloads to compromise these organizations.

Cloud Attacks: Financial services institutions are increasingly adopting cloud environments and SaaS applications to provide improved availability and quality of service to their customers. This shift results in an increased attack surface, with cloud environments being targeted by threat actors using novel, cloud-specific exploits.

Regulations in financial services have implications on cybersecurity

Financial services organizations must comply with multiple regulatory requirements, such as PCI DSS, GDPR, SOX. These standards require institutions to retain data as a form of evidence, which introduces significant restrictions and, in some cases, increases the attack surface. Threat actors are acutely aware of the vast data archives financial institutions must maintain and frequently target these repositories to gain unauthorized access to critical financial data.

Why traditional approaches to cybersecurity are not sufficient to protect financial services

Financial institutions have traditionally relied on compliance and regulations to formulate their prevention-based security controls. However, these approaches face critical limitations, especially with the advent of sophisticated cyber threats. **The escalating cyber risk is resulting in increased emphasis for cyber defense teams to move beyond traditional security strategies:**

Incompatibility with Financial Services Infrastructure: Incompatibility with Financial Services Infrastructure: Agent-based security solutions are not compatible with specialized equipment such as SWIFT systems, ATMs, or POS devices, leaving these critical infrastructures exposed.

Unawareness of Financial Services Protocols: Traditional detection tools often do not understand proprietary financial protocols such as ISO 8583, ISO 20022, and FIX, which leads to significant detection gaps.

Advanced Adversary Techniques: Modern adversaries use AI-fueled polymorphic malware and Living off the Land (LotL) techniques to evade detection systems that rely on known tactics, techniques, and procedures (TTPs).

Overview of cyber deception

Cyber deception involves setting traps for attackers, placing these traps at strategic locations, and monitoring for any interactions with them. These deceptions are not used for legitimate activity, meaning that any interaction with them is an immediate indicator of malicious behavior. Deception technology is not reliant on traditional detection methods, such as logs, signatures, or network traffic, and is entirely agnostic to the attacker's tactics, techniques, and procedures (TTPs). This makes it possible to detect stealthy attacker actions that would evade traditional security solutions.

Cyber deception offers financial institutions a critical tool to fulfill regulatory requirements while strengthening defenses against sophisticated threats.

Deception technology for protecting assets in financial services

Deception is a proven, effective approach to protecting critical assets in financial services. By deploying decoys that represent enterprise assets and financial services infrastructure, defense teams can precisely detect threats targeting the sector. The beauty of deception is that it does not interfere with production assets or network traffic, ensuring no operational impact on the environment.

Early threat detection using deception technology

Defense teams aiming to detect threats early and reduce Mean Time to Detect (MTTD) can benefit significantly from deploying deception technology. By deploying deceptions across endpoints, identity stores, and networks, institutions can create a targeted set of traps for attackers. When an attacker gains initial access and begins performing offensive actions, these carefully laid out traps are triggered, providing immediate detection.

This early warning system gives defense teams the opportunity to respond swiftly, isolating the threat and preventing adversary breakout. Deception technology plays a critical role in accelerating threat detection and ensuring that institutions maintain robust cyber resilience.

Considerations for an effective deception strategy

An effective deception strategy for financial services must be tailored to the unique infrastructure and assets within the industry. Financial institutions have specific assets such as ATM devices, POS devices, and SWIFT payment systems. Attackers frequently target these assets to gain unauthorized access to sensitive financial data and critical systems.

A robust deception strategy combines protections for traditional IT assets with specialized deceptions designed for financial infrastructure. This dual-layered approach delivers comprehensive coverage and protection.

Improving security operations center (SOC) efficiency

Security Operations Centers (SOCs) are typically overwhelmed with alerts, often unable to investigate more than 5% of the incoming alerts. This creates a risk of missed signals and introduces vulnerabilities for financial services organizations.

Deception technology provides high-fidelity, actionable alerts that SOC teams can prioritize. By focusing investigations on alerts raised by deception solutions, SOC teams can quickly isolate threats and prevent adversary breakout. This approach improves SOC efficiency, reduces alert fatigue, and enhances overall protection of assets in financial services.

Acalvio ShadowPlex: packaged solutions to protect financial services

ShadowPlex provides advanced deception technology with a rich palette of deceptions specifically designed to protect assets in financial services organizations.

The ShadowPlex suite of advanced deception technology is tailor-made for the financial services sector. By utilizing this technology, financial institutions can not only meet regulatory requirements but also gain enhanced visibility into emerging and sophisticated threats targeting their assets.

Decoys Representing Financial Assets: ShadowPlex includes decoys representing crucial assets in a financial services environment, such as SWIFT systems, ATMs, and POS systems. It also supports IT and IoT decoys that mimic network assets, applications, and sensitive data. This ensures that financial institutions can detect and divert threats aimed at critical infrastructure, keeping real assets secure.

Identity Honeytokens: ShadowPlex deploys honeytokens within identity stores, representing deceptive user accounts and service accounts. These honeytokens detect a variety of identity-based threats, including insider threats, helping financial institutions secure critical systems in alignment with regulatory frameworks.

Honeytokens on Endpoints: ShadowPlex offers deceptive credential profiles that are designed to detect credential exploits on endpoints, which are critical in environments like financial services, where attackers often target endpoint credentials to access sensitive systems.

Baits to Detect Data Exfiltration: Given the sensitive nature of data in financial services, data exfiltration is one of the most critical risks. ShadowPlex deploys baits that represent deceptive data, enabling defense teams to detect and respond to exfiltration attempts early.

Pre-Packaged Playbooks: ShadowPlex provides pre-packaged playbooks specifically designed to protect financial institutions from a variety of threats. These playbooks include strategies to defend against identity threats, insider threats, ransomware, and specific playbooks to protect payment systems and critical infrastructure.

Advanced Deception Technology Combined with AI: ShadowPlex combines sophisticated deception technology with AI to deliver immediate value to organizations. By leveraging this combination, financial institutions can bolster their defenses against a wide variety of threats, ensuring compliance with regulatory frameworks and safeguarding critical assets.

Use cases for protecting Financial Services through Acalvio ShadowPlex

ShadowPlex has been successfully deployed across various financial institutions, ranging from banking organizations to payment processors and fintech companies. Key use cases where ShadowPlex excels include:

✓ Protect payment infrastructure (such as SWIFT systems)

Payment infrastructure, such as SWIFT systems, is frequently targeted by advanced persistent threats (APTs) and modern ransomware. ShadowPlex deploys decoys that mimic SWIFT servers, web access portals like Relationship Management Portal (RMA) for SWIFT, and honeytokens on jump servers and identity stores. This allows defense teams to detect threats targeting SWIFT systems, divert adversaries away from real assets.

✓ Protect payment terminals and devices (such as ATM, POS)

Banking trojans and malware target POS terminals and ATM devices to gain access to a financial services environment. The devices contain sensitive information, such as the authorization infrastructure for credit and debit card payment systems. By deploying decoys that represent ATM terminals and POS devices, defense teams can detect threats targeting these devices.

✔ Vulnerability exploits against payment protocols (such as ISO 8583)

Payment systems and authorization protocols like ISO 8583 form the backbone of the financial services infrastructure. Traditional security solutions are often unaware of the specific protocols and vulnerabilities. ShadowPlex deploys decoys to detect exploit attempts on these protocols, giving defense teams visibility into these stealthy threats and protect payment infrastructure.

✔ Protect cloud infrastructure in financial services

Financial services organizations increasingly rely on cloud workloads for elastic compute power and data storage, but traditional agent-based security controls often fall short in these environments. Adversaries exploit identity compromises — including Cloud Identity and Access Management (IAM) users and service accounts — to elevate privileges and gain unauthorized access to cloud resources.

By deploying honeytokens tailored for cloud workloads, such as deceptive IAM users, service accounts, and access keys, ShadowPlex enables defense teams to detect these compromises early. Any interaction with these deceptive assets provides immediate visibility into threats targeting sensitive financial data stored in the cloud. This proactive detection helps prevent privilege escalation and unauthorized access to critical systems. **ShadowPlex ensures financial institutions can effectively protect their cloud infrastructure while maintaining regulatory compliance.**

✔ Insider threats

Insider threats: Insider threats pose a significant risk in financial services, as insiders have trusted access to sensitive data and systems. ShadowPlex deploys identity honeytokens and baits in data repositories, enabling precise detection of insider threats and preventing unauthorized data exfiltration, a critical requirement for regulatory compliance.

✔ Ransomware

Ransomware poses a critical threat to financial services, with groups like Lockbit targeting institutions for large payouts. Attackers, including Ransomware-as-a-Service (RaaS) affiliates, often use insiders or compromised credentials to gain initial access, allowing them to escalate privileges, move laterally, exfiltrate data, and encrypt critical systems.
ShadowPlex counters these threats by deploying identity honeytokens, decoys, and tailored baits that detect ransomware activity early, even for zero-day variants. Any interaction with these deceptive assets alerts defense teams immediately, providing the time needed to isolate the attack and prevent data loss. By integrating ShadowPlex, financial institutions can safeguard against evolving ransomware tactics.

✔ Automated response actions

ShadowPlex includes built-in capabilities to execute automated response actions that isolate threats and prevent adversary breakout. These responses are triggered through integrations with security tools such as EDR and network management solutions. Security teams can configure automated response policies, ensuring that the high-fidelity alerts from ShadowPlex lead to swift, automated actions that neutralize threats before they spread. This approach provides an effective, hands-off method to isolate the threat and protect critical financial services infrastructure.

Summary: ShadowPlex provides a proactive approach to protect financial services

ShadowPlex delivers **proven deception technology**, tailored specifically to protect assets in the **financial services sector**. With its **AI-driven automation** and **pre-packaged deception playbooks,** ShadowPlex enables seamless deployment of deception across large financial organizations. By leveraging these capabilities, defense teams can strengthen their cybersecurity posture and safeguard **payment infrastructure** and **financial data** from a wide range of threats, including **ransomware, APTs**, and **insider threats**.

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**