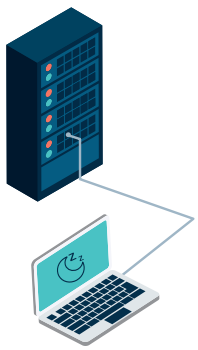
Solution Brief

Advanced Threats in Network Security: A Guide for Financial Institutions

Introduction

In the digital age, financial institutions face escalating threats that jeopardize their operational integrity, client trust, and regulatory compliance. As guardians of sensitive financial data, it is crucial for these organizations to understand and combat advanced threats that can infiltrate network security systems.



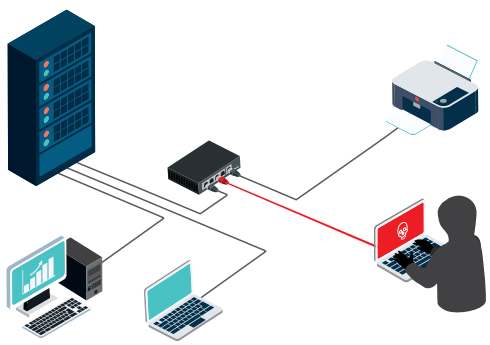
1 | Network Device Dormancy Risks

Issue: Devices like PCs and network printers often go dormant due to inactivity or power-saving settings, making them invisible to network management tools (turning into "MACless" assets).

Impact: Dormant devices miss critical security patches and updates, leaving them vulnerable to exploitation. This oversight can lead to significant security breaches and non-compliance with financial regulations.

Mitigation Strategies:

- **Deploy Sepio's Zero Trust Hardware Access solution:** Utilize Sepio's advanced hardware security management to gain visibility into all hardware devices, including those that have become dormant. Sepio's technology can detect and manage 'MACless' assets, ensuring they remain visible and monitored.
- **Integrate continuous monitoring with Sepio's solution:** Implement Sepio's continuous hardware monitoring solution that track both active and dormant devices. This solution ensures all devices are accounted for and receive necessary updates to maintain security integrity.
- **Enforce rigorous update policies using Sepio's automated compliance checks:** Leverage Sepio's capabilities to enforce policies that mandate regular checks and updates for all devices, regardless of their operational state, to prevent vulnerabilities and ensure compliance with financial regulations.



2 | Man-in-the-Middle (MiTM) Attacks on Network Printers

Issue: MiTM attacks involve intercepting and altering communications between networked devices, such as modifying the content sent to network printers.

Impact: These attacks can lead to the unauthorized alteration of printed documents, potentially causing misinformation(i.e., altered IBAN codes), financial discrepancies, and legal issues.

Mitigation Strategies:

- Implement Network Protection with Sepio's Zero Trust Hardware Access: Utilize Sepio's solution to ensure that all network printers and other hardware devices are authenticated, verified and trusted before they are allowed to communicate within the network. This reduces the risk of MiTM attacks by preventing unauthorized devices from intercepting or altering communications.
- Regular Device Integrity Checks with Sepio's Security Suite: Use Sepio's unique capabilities to perform checks ensuring they are not compromised and used as vectors for MiTM attacks. This helps maintain the security and authenticity of communications to and from these devices.
- Enhanced Visibility and Monitoring of Hardware Assets: With Sepio's comprehensive monitoring solutions, gain full visibility into all connected hardware devices, including network printers. This allows for the early detection of any anomalous or unauthorized activity, contributing significantly to mitigating the risks associated with MiTM attacks.

3 | Preventive Measures and Best Practices

- **Sepio's Hardware Vulnerability Assessments:** Leverage Sepio's solutions to conduct thorough assessments of all hardware devices within the network. This specialized scrutiny helps identify and rectify vulnerabilities specific to hardware, enhancing overall network security and resilience against cyber threats.
- **Education and Awareness with Sepio's Insights:** Utilize Sepio's detailed reporting and insights to continually educate employees about the latest cybersecurity threats, particularly those targeting hardware components. This education empowers employees to recognize and mitigate risks more effectively.
- **Ensuring Regulatory Compliance with Sepio:** With Sepio's robust hardware security management, ensure that your network adheres to the latest financial regulations. Sepio's solution helps maintain compliance by providing detailed visibility and control over all hardware devices, ensuring that they meet legal and security standards.

Conclusion

Financial institutions must prioritize vigilance and proactive management in network security to effectively guard against sophisticated threats. By integrating Sepio's patented security solution, which specialize in identifying dormant devices and mitigating Man-in-the-Middle (MITM) network attacks based on their physical layer characteristics, these institutions can enhance their defensive postures significantly. Sepio's unique capabilities in uncovering hidden risks and providing robust protection ensure that financial operations are not only compliant with stringent regulations but also secured against the most elusive threats, thereby maintaining and strengthening the trust of their clients.

Discover and accurately detect all hardware assets

Enforce flexible, scalable policies and meet regulatory requirements

Mitigate risks from rogue assets

Reduce hardware clutter and optimize budget spending

Integrate seamlessly with your existing security solutions

Certified - SOC 2 Type II, ISO/IEC 27001 and ISO/IEC 27017

About Sepio

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any scale. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical layer source, reflecting actual business, location, and rules. Sepio radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust solutions that simply see only the assets they are there to protect.

Visit: www.sepiocyber.com