Solution Brief

Navigate the growing complexity of connected assets and maintain regulatory compliance

Achieving complete asset visibility at scale

The proliferation of connected devices in financial institutions brings an increased level of uncontrolled risks, presenting global regulatory compliance, audit, and network security challenges if left unchecked. Visibility is the foundation to tackling such challenges. Complete asset visibility eliminates blind spots and provides entities with an accurate account of every connected asset and its corresponding attributes. This serves as the premise for a reliable assessment of an asset's risk level, whereby the appropriate policies and controls are enforced to meet regulatory standards.

Yet, existing solutions, such as NACs and IDSs, fail to provide comprehensive asset visibility. As such, financial organizations are unable to understand and control asset risks, leaving them in a vulnerable position that undermines their regulatory compliance.

Don't be fixated on legacy solutions

Legacy NAC solutions used by financial institutions do not provide visibility for a complete and accurate asset inventory. Rather, NACs "babysit" a predefined asset whitelist, only controlling what they already know. Establishing a whitelist is not only tedious and time-consuming, but is a never-ending project that demands frequent updates. These resource-heavy, labor-intensive set-up requirements make NACs unsuitable for largescale deployments, allowing for visibility gaps that prevent the tool from enforcing policies and controlling assets effectively.

Some financial entities turn to passive network probing tools, such as IDS, to overcome NAC limitations. However, these next gen solutions are an IT nightmare due to network dependencies and privacy issues, making them impractical to use at scale. In addition, the significant resource requirements and configuration changes cause cumbersome deployment challenges, hindering widespread application across the dispersed network, leaving parts of the enterprise unprotected due to visibility gaps.

NAC and IDS blind spots get exploited by rogue devices, which take advantage of the gaps in visibility; payment terminals and ATMs are particularly vulnerable to this threat. These malicious assets impersonate legitimate HIDs by manipulating physical attributes, and traffic-based security tools lack the visibility to differentiate between authentic and spoofed devices. As a result, rogue devices gain access to ATMs without raising any security alarms, leaving financial institutions vulnerable to costly attacks and in potential violation of regulatory compliance.

Sepio's Asset Risk Management Platform

A product not a project

Sepio's unique trafficless approach enables infinite scalability across the entire asset ecosystem by eliminating the need for resource draining analyses. With no IT nightmares, no privacy infringements, and no compliance issues, the platform is easy to deploy and run – it's a product, not a project.

True asset identity

Sepio analyzes the physical layer to generate a DNA profile for every known and shadow asset, bringing a new dimension of visibility that closes the gaps of current solutions. The physical layer includes electrical, mechanical, and functional characteristics which provide agnostic visibility and objective truth. Assessing these physical properties means Sepio is untainted by misleading profile perceptions or behavioral assumptions. Every asset, no matter its functionality, operability, or location, gets detected and identified for what it truly is, eliminating blind spots and offering greater reliability.

Actionable visibility

Sepio helps you instantly understand what needs attention by automatically generating a contextual Asset Risk Factor (ARF) score for every asset based on its DNA profile, regardless of how it is or isn't being used. The ARF score informs you of high-medium-low risks, eliminating noise to provide actionable visibility that expedites time to resolution, identifies regulation and control gaps, and prevents crises with automated mitigation. Further, the actionable visibility means you can control asset risks with regulation-based policy enforcement to maintain compliance.

Greater ROI

The platform integrates seamlessly with multiple cybersecurity solutions, such as NACs, EDRs, XDRs, Zero Trust solutions, and more, to bring them greater visibility and context. By radically augmenting the power of existing tools, Sepio gets you more value from your IT and security investments.

THE SEPIO PLATFORM:

Discover all known & shadow assets

Provide actionable visibility through contextual risk scores

Eliminate blind spots and regulatory gaps

Enforce regulation-based policies

Mitigate risks from uncontrolled assets

Fortify efficacy of existing security tools

About Sepio

Founded in 2016 by cybersecurity industry veterans, 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. The company's headquarters is in Rockville, Maryland with offices in Lisbon and Tel Aviv. Sepio operates globally through its vast channel partners' network. For more information,

Visit: www.sepiocyber.com