Solution Brief

Complexity is inevitable, but Manageable

Shattering asset management challenges in FIS

Financial Institutions, or FIS organizations have always been a lucrative target for potential adversaries for obvious reasons. Adversaries have spent years identifying the hardware assets that offer the path of least resistance. This is especially true when internal threat actors are involved, or when these adversaries want to execute hardware supply chain attacks. The proliferation of connected devices in financial institutions infrastructures brings an increased level of uncontrolled risks, presenting global regulatory compliance, audit, and security challenges if left unchecked. Visibility is the foundation for tackling such challenges. Unhindered asset visibility eliminates network and asset blind spots and provides organizations with an accurate accounting of every connected asset and its corresponding attributes. FIS organizations lack of asset visibility is further exacerbated by the siloed approach, which manages assets based on legacy categories of IT/OT/IoT. While FIS entities are primarily perceived as IT organizations, they hold considerable OT/IoT assets. This approach is a sure recipe for blind spots and policy enforcement inconsistency. This process of attaining comprehensive visibility is the basis for a reliable assessment of an asset's risk level. In such a process, in addition to asset visibility, security hygiene data is incorporated and the appropriate policies and controls are enforced to meet regulatory standards. Yet, existing solutions such as XDR device control, NAC, and IDS still fail to provide adequate visibility and protection against hardware-based attacks that spoof legitimate devices (using network-connected and USB peripherals as their attack vehicles). As such, financial organizations are unable to fully control their asset risks, leaving them in a vulnerable position that undermines their regulatory compliance.

True asset identity

Sepio analyzes the physical layer of every asset to generate an AssetDNA profile. This brings a new dimension of visibility to the organization's security management processes that ensures security teams can determine the true nature of the assets - legitimate or rogue - and close any security vulnerabilities or policy gaps. The physical layer includes electrical and functional characteristics, which provide agnostic visibility and objective truth. By assessing these physical properties, Sepio is not subject to misleading profile perceptions or behavioral assumptions. Every asset, no matter its functionality, operability, or location, is detected and identified for what it truly is, eliminating blind spots and offering greater reliability.

Sepio and Axonius 'Power boost'

Sepio and Axonius together support FIS organizations in their quest for a complete and comprehensive asset inventory. Axonius aggregates, normalizes, deduplicates and correlates data from Sepio and other customer-owned tools to deliver full asset visibility across their environment- including visibility into OT and IT, under a single pane of glass. By seamlessly connecting Sepio to Axonius via a simple API key, organizations can easily manage all CPS assets on the same risk scale, providing a unified view and consistent granular policy enforcement. Additionally, with this integration, customers can gain deeper insights and contextualization into asset-related data- including detection of rogue assets never before identified - such as passive taps, HID scripting tools, MiTM attacks (over network and USB), keyloggers and many more. With ease of deployment, enhanced visibility, enriched context and granular policies, true asset management at scale is now achievable.

Visibility. Security. Trust. Control.

Complete Asset Visibility

Unify external and internal assets for a holistic view of the attack surface. Connecting the Sepio adapter in Axonius gives organizations visibility into all assets, including OT and IoT devices. Alongside over 750 additional data sources on the Axonius platform, Sepio and Axonius deliver a credible and comprehensive inventory of all IT assets, making it easier to identify and mitigate potential security risks across the entire attack surface.

Mitigating Attack Tools

Mitigate hardware based attacks (introduced by internal threat actors or externally-initiated hardware supply chain attacks), removing the so-called path of least resistance. Eliminate the ability for attackers to obtain user credentials through keyloggers, preventing them from carrying out network/USB MiTM attacks or manipulating the internal hardware modules..

Granular Controls

Enforce specific controls based on organizational preferences. Today's controls are like a light switch: they're either all on or all off. With Sepio and Axonius, organizations can set granular level controls based on preferences. Whether it's for a specific vendor, model, set of users, or specific PCs, organizationsnow have the flexibility to provide a better employee experience while still protecting the organization.

Sepio & Axonius Benefits

Sepio and Axonius together deliver not only a complete and comprehensive inventory of all assets in your environment, but also deeper insight and contextualization into asset-related data.

Protect your private data and prevent breaches caused by malicious hardware attack tools.

Enforce granular entitlement at scale. Easily meet regulatory compliance requirements.

Better budget and resource planning.

Reduce clutter and improve your ESG scores.