SEPIO

M&A Cybersecurity Due Diligence

USE CASE

Overview

In mergers and acquisitions, buyers inherit more than revenue, operations, and customers. They also inherit cyber risk. That risk becomes more significant when due diligence relies on policies, questionnaires, software posture, and declared inventories, but lacks a reliable way to validate the real hardware environment. Unknown devices, unmanaged peripherals, spoofed assets, shadow IT, and legacy hardware can remain hidden before close and become inherited exposure after close.

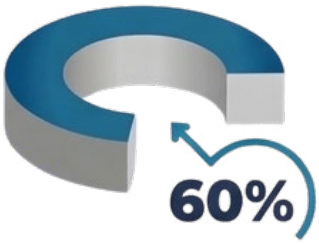
Sepio helps organizations apply Zero Trust Hardware Access to M&A cyber due diligence by validating connected assets based on their physical truth, not only on what they claim to be. This gives acquiring organizations deeper visibility before, during, and after integration.

The challenge

During an acquisition, the target environment may contain rogue network-connected devices, unmanaged USB peripherals, spoofed or mislabeled assets, shadow IT, dormant implants, legacy hardware missing from the CMDB, and third-party or remote assets outside normal inventory controls. If these assets are not discovered before close, they can become inherited exposure after close. This risk becomes more significant during integration, when systems connect, trust boundaries expand, and previously isolated issues can affect the broader enterprise.

The M&A cyber evolution: 2022 to 2026

2022 Gartner Metric



Cybersecurity considered a critical factor

2026 Realities (Today)

95% OF STRATEGIC DEALS
include mandatory, deep-dive technical cyber audit.

73% OF DEALMAKERS
view undisclosed data breach as immediate deal-breaker.

NIS2 COMPLIANCE IS PERSONAL LIABILITY FOR BOARDS

NIS2

2022

Why this use case matters now

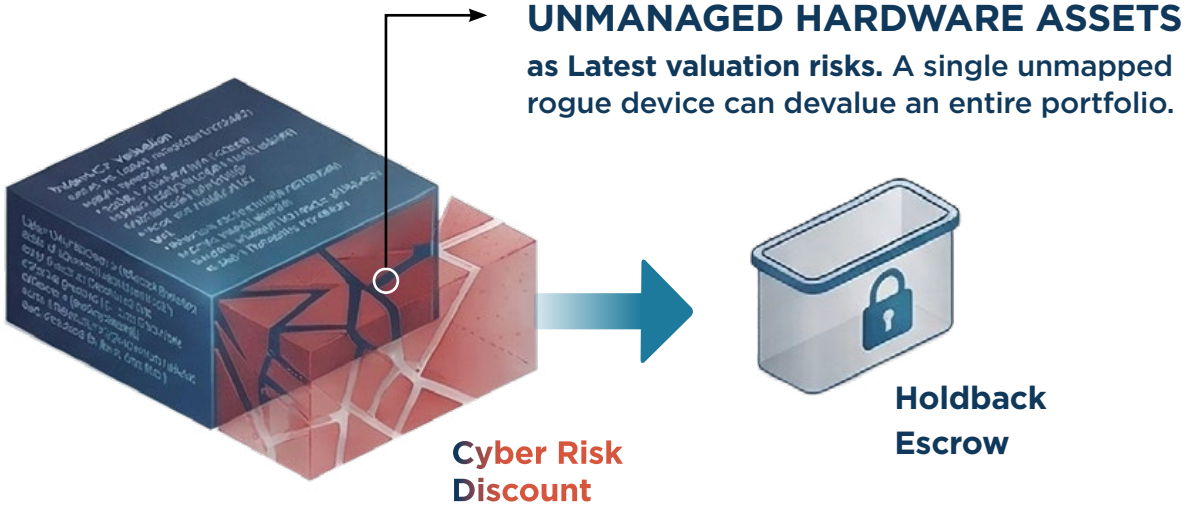
In mergers and acquisitions, trust assumptions change quickly. Networks are connected, endpoints are onboarded, third-party infrastructure is evaluated, and previously separate environments begin sharing access and data. Buyers often rely on declared inventories, software-reported identity, and point-in-time assessments. That creates a dangerous blind spot: the hardware itself may still be unknown, unmanaged, spoofed, or simply missing from the record. This is exactly where Zero Trust Hardware Access becomes critical.

Zero Trust strategies are designed to continuously verify users, applications, and sessions, but they often still assume the device is what it claims to be. During an acquisition, that assumption becomes even riskier. If the acquiring organization cannot validate the real identity and trustworthiness of connected hardware, it may inherit hidden exposure before integration is complete.

Where conventional diligence falls short

Most tools still trust what a device says it is. They rely on declared identity, software agents, asset records, or traffic-based assumptions. In M&A scenarios, that is often not enough. A device may appear legitimate while actually being unmanaged, unauthorized, spoofed, repurposed, or completely unknown. If the acquiring organization cannot verify the hardware itself, then the due diligence process may miss a meaningful source of inherited cyber risk. That is why Zero Trust cannot be complete if hardware identity is assumed.

Cyber value at risk (CVAR) impact



Latest Vulnerabilities cost > Remediation costs.

New escrow standard for cyber remediation.

25% Valuation adjustment standard.

How Sepio helps

Sepio applies Zero Trust Hardware Access to M&A cybersecurity due diligence. Using physical-layer intelligence and AssetDNA, Sepio helps organizations validate the real hardware environment across network and USB-connected assets.

This gives acquiring organizations deeper visibility into known, unknown, unmanaged, and suspicious devices and helps reduce uncertainty throughout the transaction lifecycle.

Before close

Uncover hidden assets not reflected in standard inventories. Identify unmanaged or suspicious hardware. Improve confidence in the target's actual security posture. Support more accurate remediation and integration planning. During integration Maintain visibility beyond a one-time diligence snapshot. Detect newly introduced hardware risk. Identify unknown devices and policy violations early. Reduce the chance that inherited exposure moves silently into the combined estate.

After close

Strengthen Zero Trust programs with verified hardware identity. Improve risk prioritization for connected assets. Support enforcement through existing security workflows. Increase trust in the integrity of the combined infrastructure.

Business value

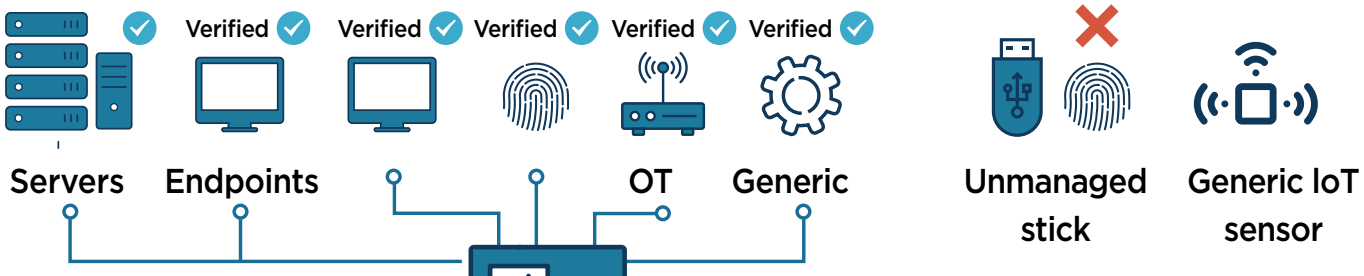
Applying Sepio to M&A cyber due diligence can help organizations reduce uncertainty before acquisition, improve cyber risk visibility during underwriting, support negotiation and remediation planning, accelerate safer post-merger integration, reduce the likelihood of inherited hidden exposure, and strengthen the foundation for Zero Trust initiatives.

Who this use case is for

This use case is especially relevant for financial institutions, healthcare organizations, manufacturers, critical infrastructure operators, government environments, and large enterprises with complex distributed asset environments.

These organizations often face higher integration complexity, stronger governance requirements, and greater exposure to hidden hardware risk during M&A.

2026: The foundation of zero trust hardware access

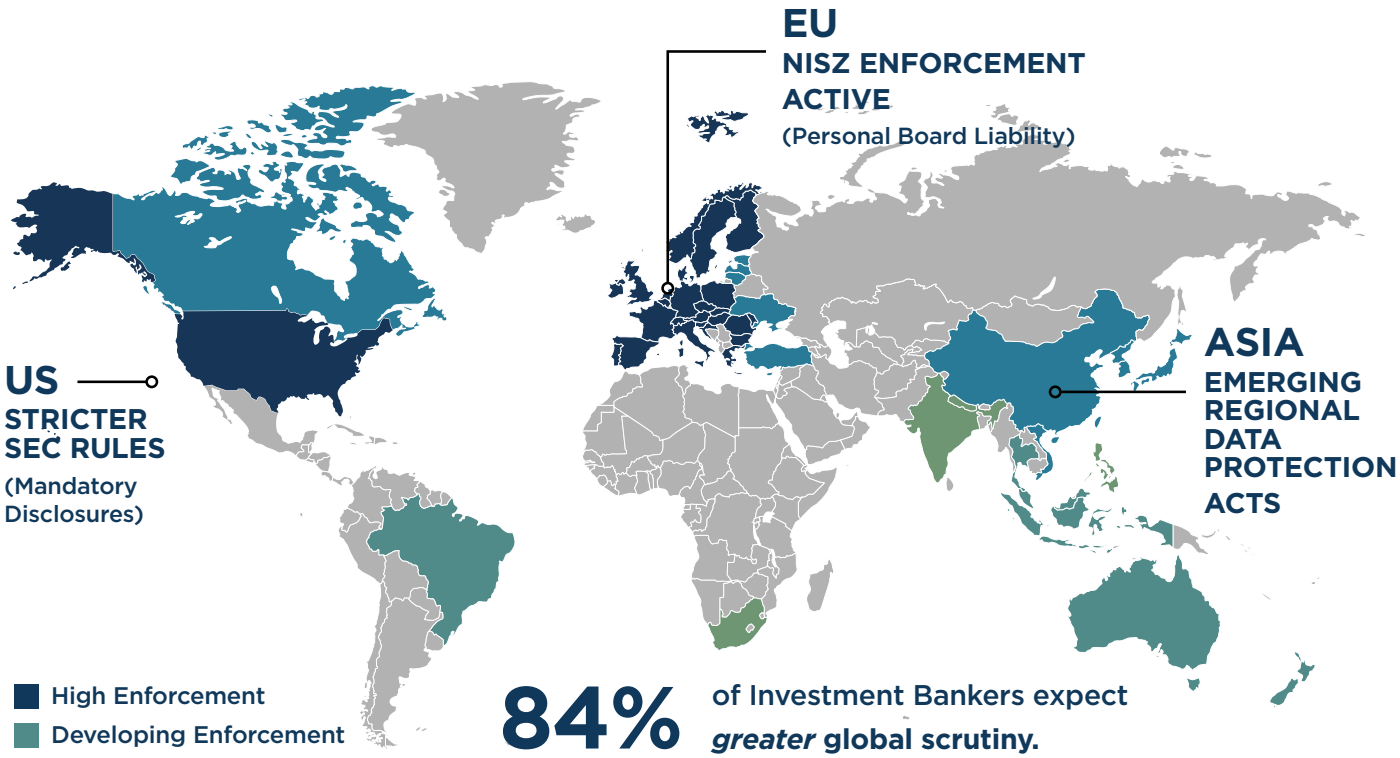


CONTINUOUS HARDWARE DISCOVERY & FINGERPRINTING:
Mapping the complete attack surface.

INSTANT IDENTIFICATION OF ROGUE & UNMANAGED DEVICES:
Denying untrusted hardware access at the physical layer.

68%
of post-closing breaches originate from unmanaged hardware.

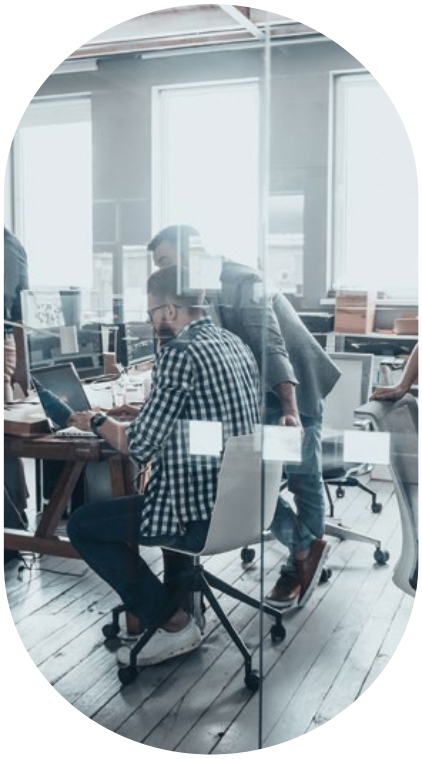
Global M&A cyber regulation landscape 2026



84% of Investment Bankers expect ***greater*** **global scrutiny.**

Key takeaway

The core M&A cybersecurity challenge is not only known vulnerabilities. It is also the possibility of inheriting hidden exposure from devices and assets that were never properly identified during diligence. Sepio helps reduce that risk by exposing the real hardware truth behind connected assets. With Zero Trust Hardware Access, acquiring organizations can move from assumed trust to verified trust throughout the transaction lifecycle.



See what conventional M&A cyber diligence may be missing

Sepio helps organizations apply Zero Trust Hardware Access to mergers, acquisitions, and post-close integration by exposing the real hardware truth behind connected assets.

SEPIO