SEPIO

Zero Trust Hardware Access (ZTHA): Making Hardware Identity the Foundation of Zero Trust

A Sepio white paper

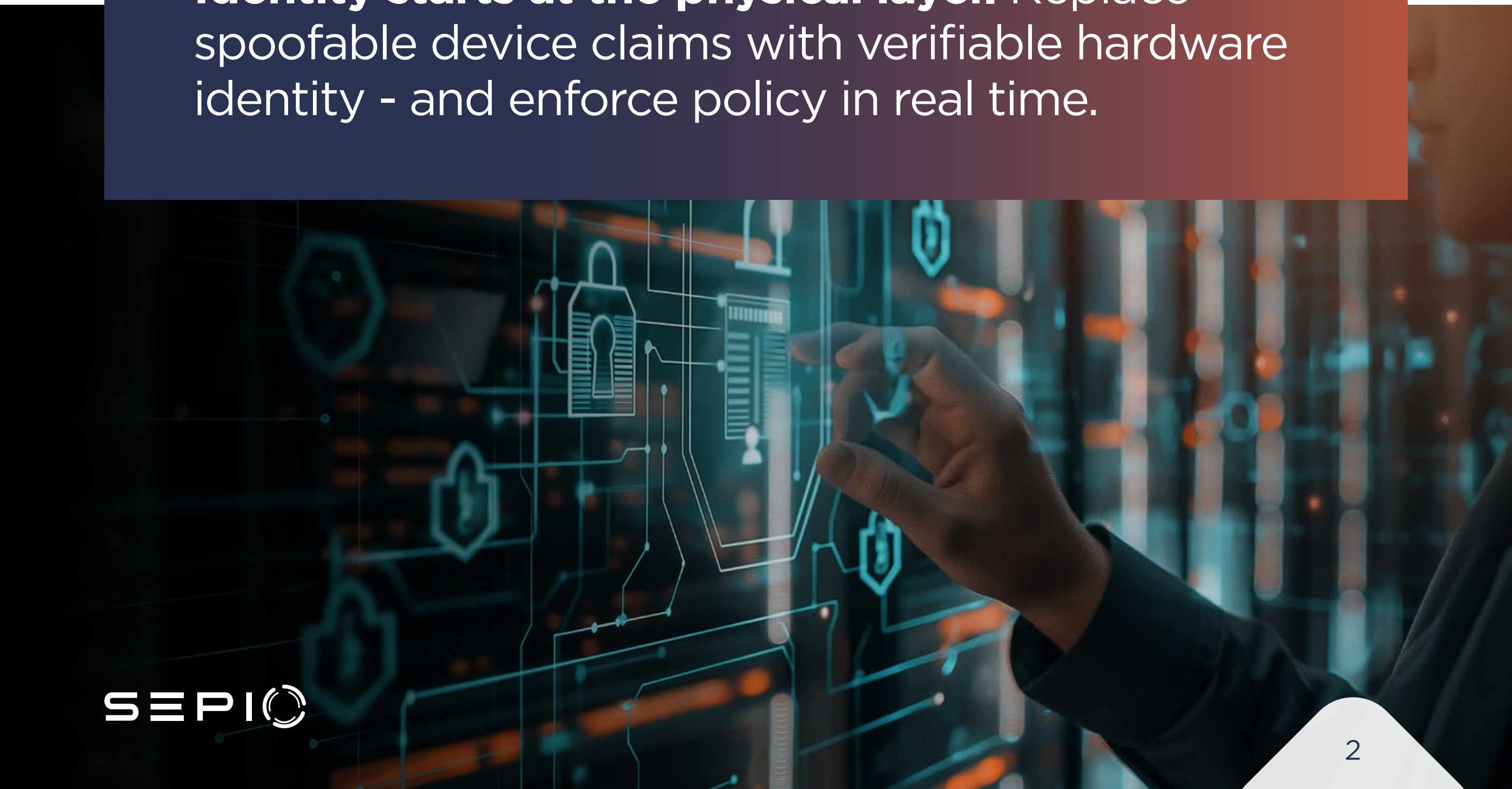
Introduction

Zero Trust's core principle - "Never Trust, Always Verify" - was built to eliminate implicit trust across users, applications, and networks. But in most environments, device identity is still assumed, based on identifiers that can be spoofed or misrepresented.

Zero Trust Hardware Access (ZTHA) extends Zero Trust to the foundation: the hardware that forms the network and every physical asset connected to it. ZTHA requires that a device is verified for what it is - before it is trusted to connect, communicate, or persist inside the environment.

Sepio's mission is to enable a Zero Trust solution that ensures that the foundation of the organization - the hardware that comprises the network and the physical devices that are connected to it - is unquestionably trustworthy.

> **Identity starts at the physical layer.** Replace spoofable device claims with verifiable hardware identity - and enforce policy in real time.



Why now: the case for ZTHA

There’s no better time to anchor Zero Trust in hardware:

- ✓ AI accelerates discovery of vulnerabilities and lowers the barrier to exploitation.
- ✓ Point solutions keep failing - fragmented tools create blind spots across IT/OT/IoT where exposure grows unnoticed.
- ✓ Hardware blind spots (Shadow IT, dormant implants, non-obvious rogue devices) persist because many controls focus on traffic, scanning, or assumptions - rather than presence and identity.

The result is simple: more complexity creates more opportunity for adversaries, and therefore higher risk.

Threat:
Likelihood a bad actor will attempt to compromise

Exposure:
The extent your environment is vulnerable/accessible

Risk:
Threat + exposure, prioritized by business context

The hardware gap in Zero Trust

Most security stacks verify users and applications well - but still inherit a critical assumption: a device is trusted because it appears legitimate. That creates blind spots for Shadow IT, spoofed assets, dormant implants, and dual-use devices.

While it is still necessary for enterprises to implement traditional security solutions as a form of tactical response, ZT provides a strategic framework that enables a shift to proactive security. As such, organizations can benefit from a hybrid environment that is both proactive and reactive, thus increasing the overall cybersecurity posture. With ZT, the concept of trust is eliminated from the organization's network architecture, thus providing more opportunities to identify threats and take subsequent action to avoid an attack. Importantly, ZT protects the enterprise outside its typical perimeters, which is especially relevant as telework, Bring Your Own Device (BYOD), and Internet of Things (IoT) devices become increasingly common "within" organizations. The ZT model ensures that network access is granted based on who, what, when, where, and how. However, to answer such questions, the enterprise must have complete device visibility.

ZT is based on the following three guiding principles:

1. Never trust, always verify

Enterprise network devices, and users, are typically assumed to be fully trusted as they are internal. However, both the device and the user's identity can be spoofed by a malicious actor. Furthermore, unmanaged and remote assets cannot be assumed as trusted since they are out of the enterprise's control, even though they are considered "internal". To eliminate the risks that come with trust, ZT eliminates the trust component itself; every user, device and application/workload must be treated as untrusted – every single time.

2. Verify explicitly

Access to resources is determined by a dynamic policy that relies on identity management and other data sources. Authentication and

authorization should always be based on all data points, including user identity, location, device health, data classification, and more, to comprehensively evaluate the device and user's identity. The evaluation should continue for as long as the session lasts to ensure maximum protection.

3. Assume breach

Under the ZT model, resources are defended by the assumption that there has already been a breach, meaning that devices and users are denied network access by default. Access can be blocked several ways, depending on the ZTA the organization decides to implement. An architecture based on identity means that the characteristics of all users, devices, data flows, and requests for access must be heavily scrutinized. Access to data is controlled, minimized, and monitored based on the principle of least privilege, meaning that users' network access is limited to the lowest level required to perform the task. An architecture based on micro-segmentation significantly reduces the user's ability to move laterally throughout the network by isolating workloads through granular segmentation policies. Essentially, the network splits into smaller parts, each of which requires separate access. Micro-segmentation is an effective ZT approach as, often, a perpetrator's point of infiltration is not the target of attack. Micro-segmentation prevents the lateral network movement that facilitates the actual attack. A strong ZTA will incorporate numerous aspects from various approaches to enhance the Assume Breach principle. Finally, all configuration changes, resource access and network traffic should be logged, inspected, and constantly monitored for suspicious activity.

The three components of Zero Trust

Comprehensive security monitoring for validation of users and their devices' security posture.

Granular, dynamic and risk-based access control through policy enforcement.

System security automation that protects data and resources.

The Zero Trust Hardware Access Framework

Zero Trust Hardware Access (ZTHA) extends the core Zero Trust principle - "never trust, always verify"- to the physical layer.

In modern environments, hardware is no longer a passive foundation; it is an active attack surface spanning IT, IoT, OT, peripherals, and "invisible" devices that evade network-centric tooling. ZTHA provides a structured way to move from knowing what is connected, to proving what it is, to ensuring it remains compliant, and finally to enforcing policy in real time when it is not.

This framework is built as five layers, progressing from foundational visibility to decisive control. Each layer includes:

- ✓ a ZTHA layer (what stage you're in),
- ✓ a key capability (what you must be able to do),
- ✓ a requirement (what "good" looks like operationally).

Layer #1 - Visibility

Key Capability: Comprehensive Asset Discovery
Requirement: Discover and map all connected devices (IT, IoT, Shadow IT, USB, etc.), including those invisible to network-centric tools.
Visibility is the non-negotiable foundation. If you can't reliably see what is connected, everything above it becomes guesswork.

ZTHA visibility is not limited to "managed endpoints" or "known MAC/IP" - it must capture:

- devices that are unmanaged (no agent, no MDM),
- devices that are silent/dormant (not actively generating traffic),
- devices that are non-traditional (USB peripherals, embedded systems, OT controllers),
- devices introduced as Shadow IT (brought in without process or approval).

Outcome: A continuously updated, normalized hardware inventory and connectivity map that reflects reality-not procurement records.

Layer #2 - Identification

Key Capability: Identity Verification
Requirement: Establish asset identity based on its own characteristics, registered information, and organizational context.

Zero Trust breaks if device identity relies on spoofable claims. Identification in ZTHA means moving from "what the device says it is" to "what evidence proves it is." Practically, identity verification combines:

- device characteristics (immutable or hard-to-fake traits),
- registered information (what the organization expects to be present),
- organizational context (where it is connected, which segment, which function, which owner, what role it should play).

Outcome: A defensible hardware identity record (high-confidence classification) that supports allow/deny decisions and downstream policy automation.

Layer #3 - Policy and Postures

Key Capability: Compliance Validation
Requirement: Continuous validation of the device's behavior, configuration, and compliance against a security policy.

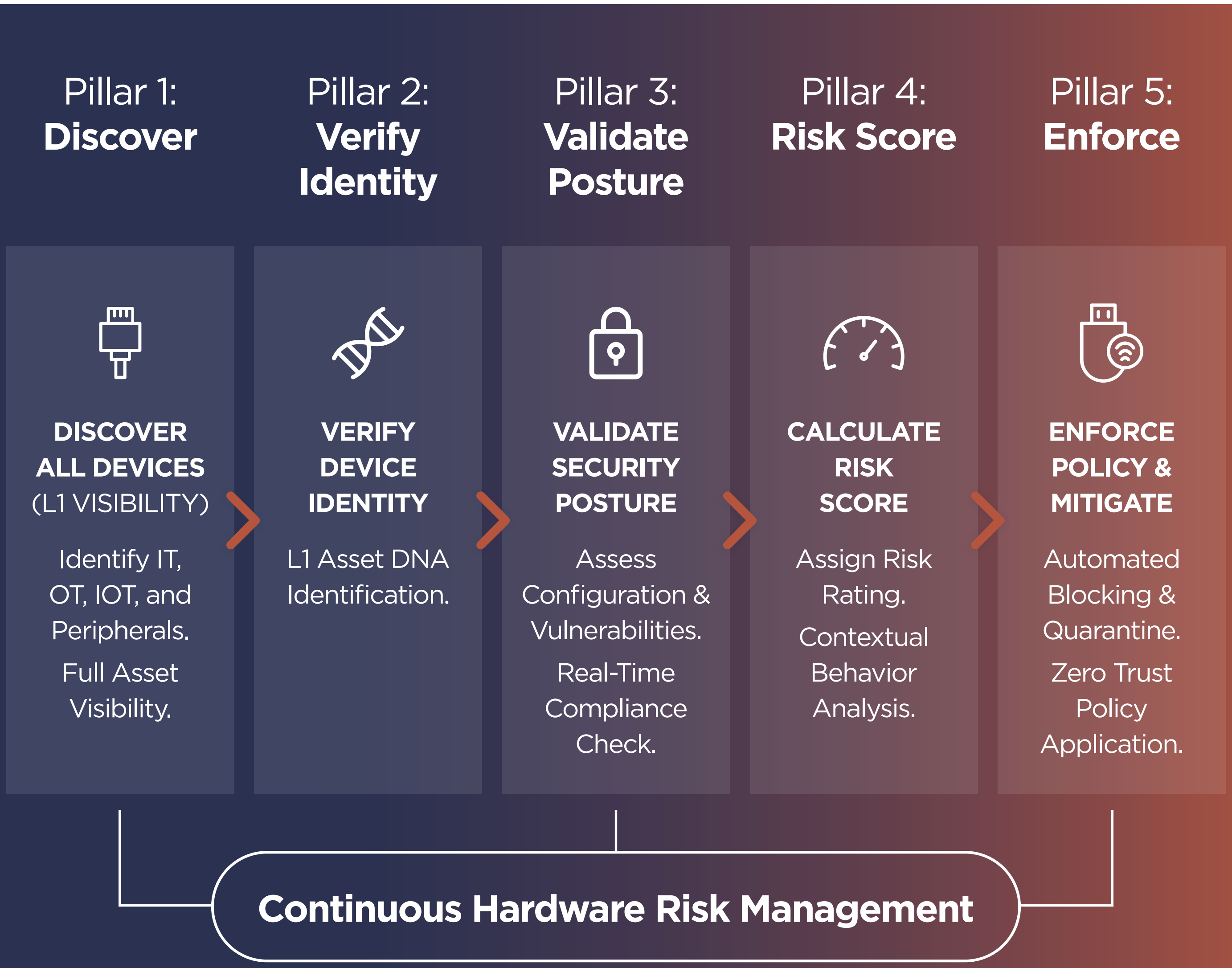
After you know what it is, you must determine whether it is allowed to be here and operate this way. “Posture” is the living state of the asset: how it is configured, how it behaves relative to its expected role, and whether it complies with defined policy.

This layer introduces continuous checks such as:

- Is the asset operating within its expected role and environment?
- Does it meet the required configuration baseline?
- Is it aligned with policy for location/zone/function?
- Has anything drifted (changes in posture over time)?

Outcome: A clear pass/fail (or graded) posture state per device, continuously refreshed—not an annual audit snapshot.

The Five Pillars Of Sepio Zero Trust For Hardware



Pillar 1: **Discover**

DISCOVER ALL DEVICES (L1 VISIBILITY)

Identify IT, OT, IOT, and Peripherals.

Full Asset Visibility.

Pillar 2: **Verify Identity**

VERIFY DEVICE IDENTITY

L1 Asset DNA Identification.

Pillar 3: **Validate Posture**

VALIDATE SECURITY POSTURE

Assess Configuration & Vulnerabilities.

Real-Time Compliance Check.

Pillar 4: **Risk Score**

CALCULATE RISK SCORE

Assign Risk Rating.

Contextual Behavior Analysis.

Pillar 5: **Enforce**

ENFORCE POLICY & MITIGATE

Automated Blocking & Quarantine.

Zero Trust Policy Application.

Continuous Hardware Risk Management

Layer #4 - Risk

Key Capability: Risk Assignment and Scoring
Requirement: Continuous validation of the device's behavior, configuration, and compliance against a security policy (used as the evidence base for risk).

ZTHA treats risk as more than a vulnerability list. Risk scoring prioritizes what matters now, based on the evidence collected in layers 1–3 plus business impact. Risk should reflect:

- likelihood (how exposed / suspicious / non-compliant),
- impact (criticality of location, function, and dependencies),
- confidence (how strong the identity/posture evidence is),
- urgency (how quickly it could enable compromise).

Risk scoring is what transforms ZTHA from "visibility" into defensible operational prioritization: what must be remediated first, where enforcement must be immediate, and what can be handled through workflow.

Outcome: A ranked, explainable risk list that drives response actions and resource allocation.

Layer #5 - Control & Enforcement

Key Capability: Access Control and Active Remediation
Requirement: Notify, alert, and actively deny unauthorized/non-compliant devices in real-time.

This is where ZTHA becomes a true control plane: not just identifying problems, but reducing exposure. Enforcement must be actionable and timely, ranging from low-friction workflows to hard blocks.

Typical enforcement modes include:

- Notify / alert (security operations awareness and triage),
- Quarantine / restrict (limit access pending investigation),
- Deny (block connectivity for unauthorized or non-compliant assets),
- Active remediation workflows (tickets, playbooks, automated actions through integrations).

A key ZTHA principle: enforcement should be based on verified identity + posture + risk, not on unreliable assumptions.

Outcome: Real-time exposure reduction—unauthorized or non-compliant hardware is prevented from operating inside the environment.

How the layers work together

The framework is designed as a continuous loop:

1. Visibility ensures nothing is missed.
2. Identification turns inventory into trusted identity.
3. Policy & posture defines what "good" is and checks it continuously.
4. Risk turns evidence into prioritization.
5. Control & enforcement reduces exposure and closes the loop with measurable outcomes.

eliminates the trust component itself; every user, device and application/workload must be treated as untrusted – every single time.

Zero Trust Hardware Access With Sepio

With a lack of device visibility limiting the ZTA's efficacy, enterprises are beginning to focus on applying ZT to the hardware level. Starting at the first layer of defense ensures that a more comprehensive ZTA is in place to provide a stronger overall ZT approach.

42%

Organizations adopting a ZT approach on the hardware level due to an inability to identify, classify & monitory endpoint and IoT devices.

33%

Organizations adopting a ZT approach on the hardware level due to insufficient visibility into endpoint & IoT activity.

The ZT model grants access based on who, what, when, where, and how. If the organization cannot answer these questions accurately, then the ZTA is essentially ineffective. To answer such questions and have a strong ZTA, enterprises must have complete asset visibility. With Zero Trust Hardware Access, the focus is on all hardware assets operating within the enterprise's infrastructure – including remote assets – as this is where access requests originate from, as well as being able to answer the critical questions of "who, what, when, where, and how".

Concentrating on hardware improves the overall efficacy of the enterprise's ZTA, especially micro-segmentation efforts, as the PE can make accurate access decisions through deep visibility into a device's characteristics. Furthermore, enabling Hardware Access Control through policy enforcement stops a hardware attacker at the first hurdle, not even giving them the opportunity to cause damage or infiltrate the network.

Sepio's Hardware Access Control solution enables Zero Trust Hardware Access through a comprehensive approach to Hardware Access Control. sepio provides enterprises with complete device visibility by using Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices. By validating devices' Physical Layer information, sepio verifies the device's true identity – not simply what it claims to be. Comparing a device's digital fingerprint with the extensive built-in threat intelligence database for known-to-be vulnerable devices allows Sepio to instantly detect when a vulnerable or malicious device is present within the organization's infrastructure.

The comprehensive policy enforcement mechanism of Sepio allows the system administrator to define a strict, or more granular, set of rules for the system to enforce that controls hardware access based on device characteristics. As such, Hardware Access Control policies support PLP, which is integral to ZT. More importantly, when breached, Sepio automatically instigates a mitigation process to instantly block unapproved or Rogue hardware. Hardware Access Control policies provide actionable support to Zero Trust Hardware Access and prevent malicious devices from bypassing traditional ZT security policy measures, such as identity-based approval and micro-segmentation.

The three components of Zero Trust enhanced by Sepio

COMPREHENSIVE SECURITY MONITORING FOR VALIDATION OF USERS AND THEIR DEVICES' SECURITY POSTURE.

Sepio's ultimate visibility capabilities enable the most comprehensive approach to device monitoring.

GRANULAR, DYNAMIC AND RISK-BASED ACCESS CONTROL THROUGH POLICY ENFORCEMENT.

Sepio allows organizations to implement strict, or more granular, hardware access control rules.

SYSTEM SECURITY AUTOMATION THAT PROTECTS DATA AND RESOURCES.

Sepio allows organizations to implement strict, or more granular, hardware access control rules.

Conclusion

As it can no longer be assumed that internal users and devices can be trusted, ZT is an attractive security model being adopted by many organizations. Based on the principle of "never trust, always verify", organizations adopt ZT to enhance their security by treating every user and device – internal or external – as a potential threat and eliminating any automatic trust given to those requesting network access. Additionally, with ZT, users and devices are only provided with the necessary network access to perform the task, reducing the possibility of malicious lateral movement.

However, a ZTA relies on numerous data sources for the PE to make an accurate decision. The lack of visibility and access policy challenges put the efficacy of the ZTA at risk. Such challenges allow Rogue Devices to bypass identity-based authentication and micro-segmentation, providing an attacker with unauthorized network access – without the enterprise even knowing. To mitigate the risk, organizations must focus on Zero Trust Hardware Access. Doing so means that ZT applies to the first layer of defense and can therefore better protect the organization from intruders.

With SEPIO, a Zero Trust Hardware Access approach can be achieved through complete device visibility and a policy enforcement mechanism that, when combined, also enable Rogue Device mitigation. As a result, the enterprise benefits from a stronger overall ZTA as hardware attack tools can no longer bypass the ZT model.

SEPIO