TAG CYBER

# UNDERSTANDING ZERO TRUST HARDWARE ACCESS: AN INTRODUCTION TO THE SEPIO PLATFORM

DR. EDWARD G. AMOROSO

Zero trust security is an important concept in cybersecurity but has not been examined thoroughly in the context of underlying hardware platforms. This report explains hardware security for zero trust and illustrates the concept using the Sepio commercial solution.

## INTRODUCTION

The cybersecurity industry occasionally identifies a general protection concept that appears to meet the needs of all participants in an effective manner. Multifactor authentication, least privilege access, segregation of authorized duties, and automated correlation of indicators of compromise (IOC) are all examples of principles that collectively comprise the foundational base of the cybersecurity discipline.

Another generally accepted protection concept has emerged known as *zero trust*. Originally introduced in an industry analyst report,[1] zero trust helps to drive enterprise network designs that are free of a firewall-protected perimeter. Specifically, the idea of zero trust explains the condition that results for end users with devices accessing workloads hosted in public clouds. Neither entity can fully trust the other, which drives security controls for the session.

One aspect of the zero trust model that has received relatively little attention is the hardware aspect of its practical implementation. That is, where most zero trust architectures emphasize software controls for endpoints, networks, cloud infrastructure, and containerized applications, the role of the hardware in assuring the integrity of endpoints, servers, and other devices has been less examined by the cybersecurity community.

In this report, we discuss the zero trust model in the context of underlying hardware, with emphasis on endpoint protection and monitoring. We explain how hardware security can help avoid rogue or fake devices, and how this supports a zero trust implementation. Finally, the hardware security concept is instantiated using the *Sepio HAC-1* platform[2] to demonstrate how practitioners can take advantage of a commercially available solution.

## ZERO TRUST MODEL

It helps first to review the zero trust model in more detail. The concept emerges primarily with the dissolution of the enterprise perimeter as a primary control for cybersecurity. In traditional enterprise computing environments, any access or interaction between two entities, such as a client and server, required no mutual authentication because local trust was implied by the local area network (LAN) proximity enforced by the perimeter firewall.

A common way to represent this traditional set-up is to depict two entities inside a firewall perimeter which can share data freely in a bidirectional manner. Since the entities are locally connected inside a common boundary protection, no mutual one or two-factor authentication (1FA, 2FA) would be used. The security weakness in such a configuration is that malware which enters either entity can then freely traverse to the other entity across the unsecured access.

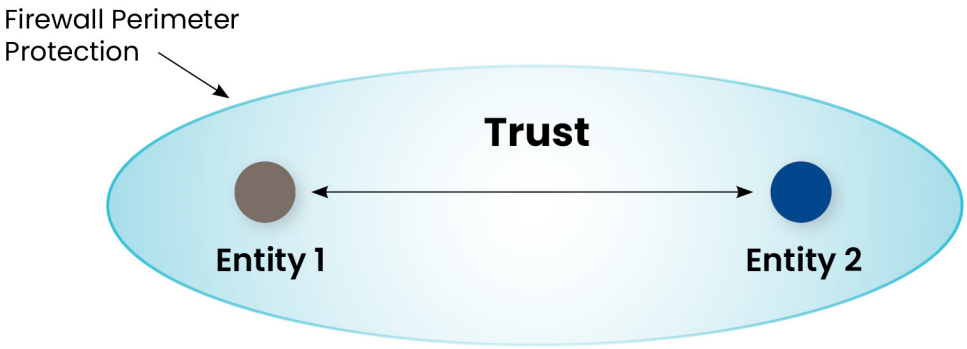


**FIGURE 1.** Traditional Local Trust Within a Perimeter

As mentioned above, the firewall perimeter has been replaced with a more open, virtualized architecture characterized by public cloud-hosting and SaaS usage. Work-from-home initiatives have also helped to drive this transition to more open arrangements. For example, employees working outside the office desiring some action, such as checking their paycheck stub, will prefer to do so directly, using a mobile app versus a clumsy VPN connection to the corporate LAN.

The representation of this open access is the essence of zero trust security. That is, two workloads – which can be apps, users, software, devices, or any other computing component that can initiate or accept a session request – will no longer benefit from a shared perimeter. Instead, a local protection scheme, often referred to as a *microsegment*, is required to enforce security policies for each of the entities. This can include 2FA or other requirements for access.

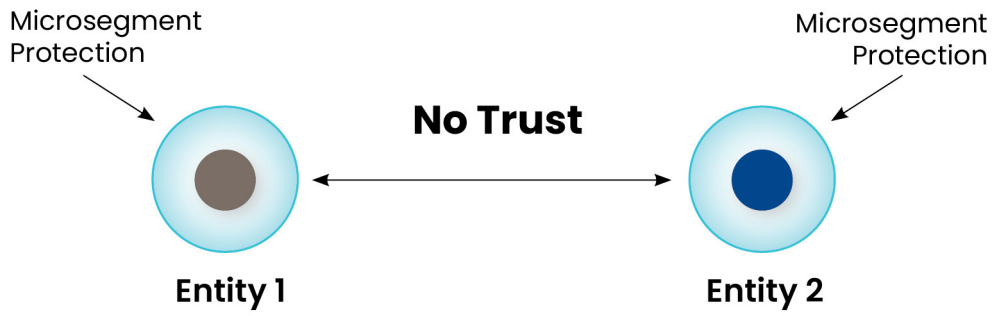


**FIGURE 2.** Zero Trust Access Without a Boundary Perimeter

The practical implementation of zero trust has, traditionally, required several security and compliance functions and components, all of which are best arranged in an orchestrated manner to simplify access and maintain protection. These control components typically include a focus on the device, network, cloud hosting environment, and the application. This common enterprise security arrangement for zero trust is depicted in Figure 3.

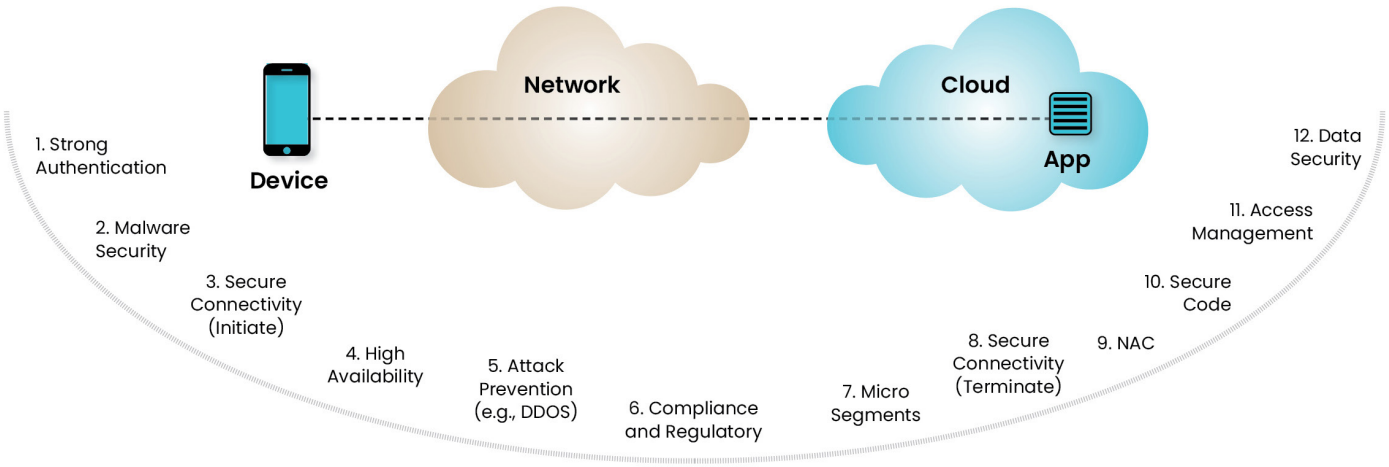


**FIGURE 3.** Traditional View of Zero Trust Components to Support Zero Trust

What's missing from this traditional view is the essential role that *hardware security* plays for all physical devices used in any zero trust architecture. This is most evident in an end user device, but it can also be true for physical computing hosts or Internet of Things (IoT) devices used to implement any aspect of the zero trust session. Servers, network devices, and any other computers will all benefit from additional underlying hardware security, as depicted in Figure 4.

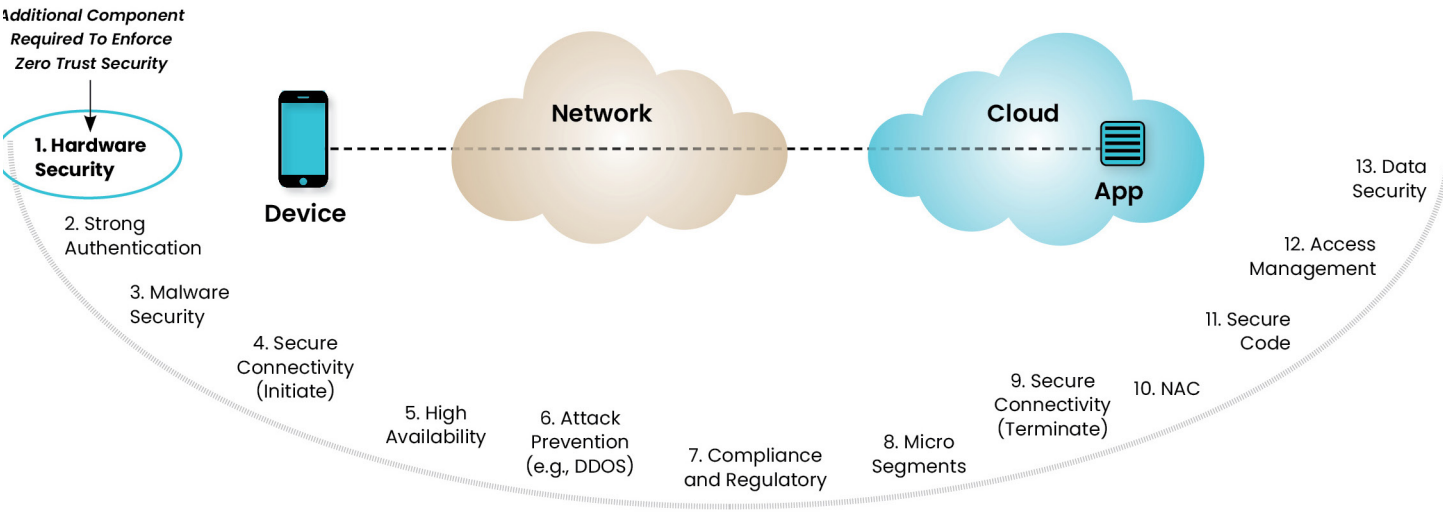


**FIGURE 4.** Adding Hardware Security for Zero Trust

The specific hardware security control that applies most directly to zero trust architectures involves policy enforcement at the hardware level. The resulting cybersecurity control, which can be described as *hardware access control (HAC)*, provides an important and missing element in the vital goal of improved threat visibility, security policy enforcement, and rogue device detection in any modern zero trust environment.

## APPLYING ZERO TRUST TO HARDWARE

The introduction of hardware security to an enterprise zero trust plan is driven by the need to protect endpoints and other tangible computing systems from the direct network accessibility that zero trust creates. The specific functional requirements that hardware security must address to effectively secure physical layer protection for zero trust can be grouped into three primary areas:

- *Hardware-Level Visibility* – This first goal is to improve the accuracy and coverage of the relevant metadata available to make determinations about the hardware involved in a zero trust session Such asset visibility helps to ensure that only known, acceptable devices can participate in business activity in a zero trust network. This requires Layer 1 data collection from all known and unknown peripherals in a target environment.
- *Hardware Identity Management* – The second goal is to use collected metadata about hardware devices to make identity-related decisions about any accessing entities. The underlying hardware includes important information collected at the physical and electrical levels that can help to uncover identity. Unique identifiers, such as fingerprints, are required to determine the identity of devices and peripherals.
- *Hardware Access Control* – The third goal is to make cyber risk-based access control decisions about whether a given hardware device should be allowed to access a given workload. Such access decisions should include determining whether a given device might be a rogue or impersonating system. This is often implemented using machine learning-based analysis on centralized management servers.

When attention to hardware is missing from zero trust implementations, important metadata is ignored. Obviously, the full equation on zero trust will include many other (mostly software) considerations, but there is no downside to introducing hardware visibility, identity management, and access control to any network implementation. In the next section, we review how Sepio Systems provides a commercial platform that addresses these objectives.

## CASE STUDY: SEPIO PLATFORM

The commercial Sepio HAC-1 platform supports a range of hardware device and Internet of Things (IoT) cybersecurity functions, with emphasis on improved asset visibility for enterprise teams and any other organizations operating a network. Typical Sepio customers include banks, insurance companies, critical infrastructure operators, government agencies, Internet service providers, and many other organizations of varying size and scope.

The Sepio platform supports the provision of Hardware Access Control (HAC) in a zero-trust environment. This capability drives deeper visibility into deployed hardware assets, which is essential for mitigation, policy enforcement, third party integrations, and other zero trust controls. Specifically, the HAC-1 platform focuses primarily on *physical layer visibility, hardware access* control support, and *rogue device protection*. These are discussed below.

*Hardware Visibility and Zero Trust*
Sepio's commercial HAC-1 platform meets the objective of accurate, real-time visibility into deployed hardware devices using a unique fingerprinting algorithm based on the physical layer characteristics that can be observed. These physical and electrical signals are collected and processed using machine learning models to develop a device fingerprint, which thus creates a unique identifier for that specific hardware device.

The device fingerprints that are calculated and maintained thus create a collective view of the deployed hardware that is in-scope for the organizational mission. Such visibility adds considerable value, because most existing organizations rely on IT inventories, which do not differentiate between devices, or they use software-based information, such as MAC addresses and device names, which can be unreliable (see Figure 5).

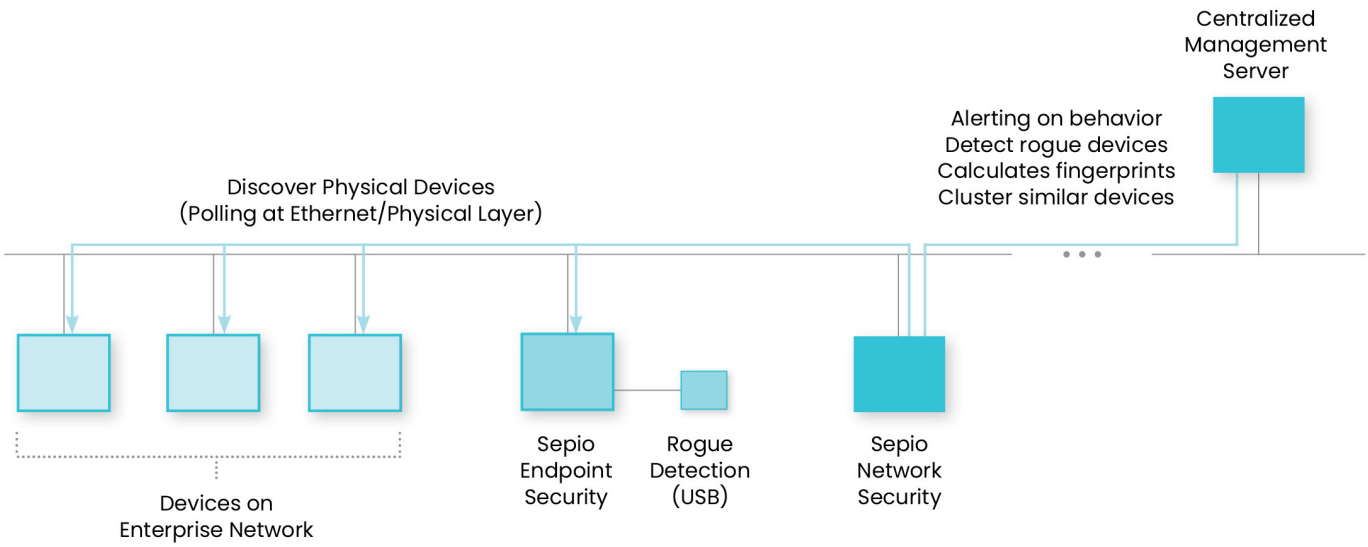


**FIGURE 5.** Sepio Platform Deployment

The Sepio solution includes discovery of devices on a network that are hidden at the physical layer, as well as special endpoint protection for devices with USB-connected peripherals to identify spoofed or vulnerable peripherals. The platform reports collected information to a server that calculates fingerprints, alerts on behavior, clusters similar devices, maintains a threat database, and serves as the focal point for enforcement of the hardware access decisions defined by the enterprise.

*Hardware Access and Zero Trust*

By maintaining physically grounded, fingerprint-based identities for devices, an organization can enforce zero trust access policies that do not require dependence on a perimeter. Instead, the inventory of machine identities serves as a policy base and can be combined with a threat database offered by Sepio to detect when a given device should not be granted access based on its posture.

The security policies used to enforce access based on hardware fingerprints are dynamic, which means that they can be adjusted based on real-time visibility into a given zero trust session. In addition, such policies are based on the well-known principle of least privilege, which minimizes access for any requesting entity to only those resources that are necessary and consistent with the overall mission.

*Rogue Devices and Zero Trust*

One benefit of the hardware-oriented visibility and policy enforcement offered by Sepio is that rogue devices can be more easily identified in a network. Specifically, if the fingerprint of a device does not register or make sense in the context of a given deployment, then access can be denied until additional information can be obtained. This is a unique mechanism that can significantly reduce risk associated with peripherals on a network (see Figure 7).

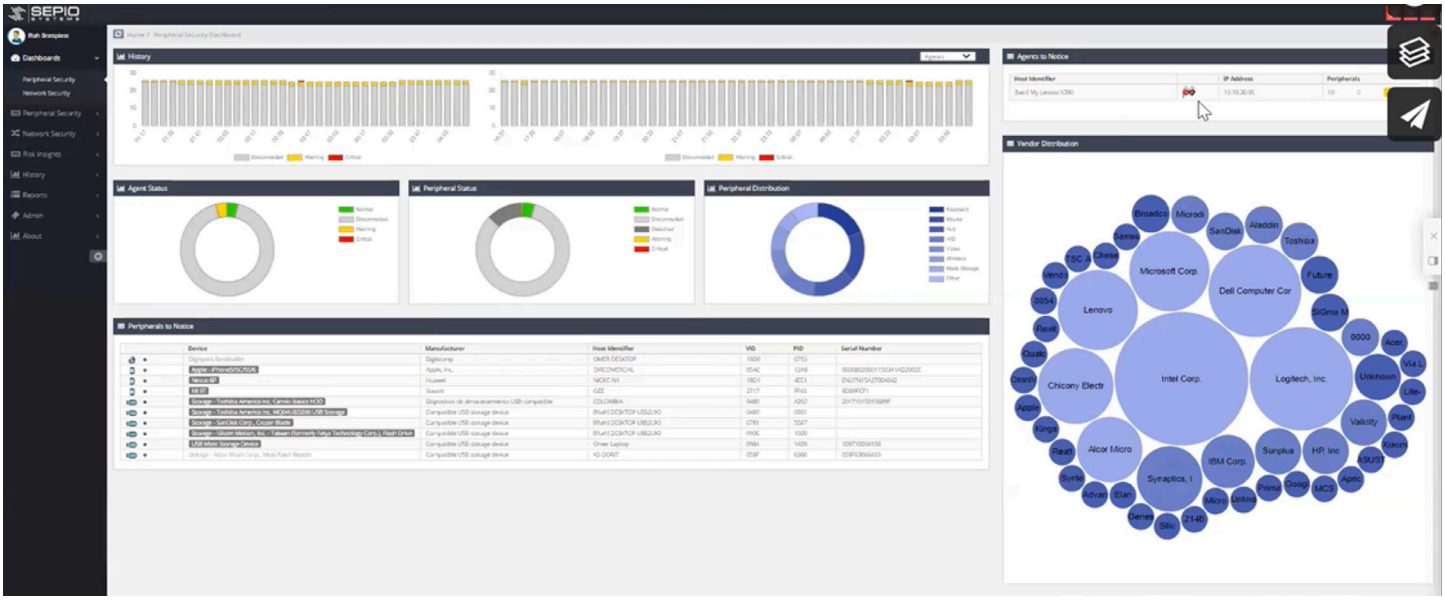


**FIGURE 6.** Sepio Peripheral Device Display

Such automatic rogue detection should be the front-end component of any organizational process designed to keep rogue devices off the network and away from essential resources. Enterprise teams should be focused on blocking rogue devices presumably controlled by malicious actors from attempts to bypass controls such a microsegmentation or to initiate some other attack on resources.

## ACTION PLAN

Every enterprise security team is encouraged to improve their hardware access control by taking immediate steps. While every organization is different, and while the current security and situational posture will vary between circumstances, we can offer below a generic methodology that can be tailored and customized. Specifically, we recommend that teams initiate the following steps to address hardware access security:

*Step 1: Inventory of Access Policies*
*Organizations should review their existing policies, which will likely involve identity-based mediation. These policies should be examined for uniformity across the enterprise, consistency of identity-based information, and suitability for both zero trust and least privilege.*

*Step 2: Define Functional and Policy Requirements*
A set of functional requirements for access policies should be developed – and we encourage inclusion of hardware access control. Even if the organization just desires identification of rogue devices, inclusion of full hardware access support should be included.

*Step 3: Scan Vendor Landscape*
Team should review vendor offerings, including Sepio's HAC-1, and to initiate proof of concept testing with local devices. The TAG Cyber team offers tailored portfolio management through its research support offering (see https://www.tag-cyber.com/ for details).

## REFERENCES

https://sepio.systems/blog/zero-trust-hardware-access/

## ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

Copyright © 2021 TAG Cyber LLC. This report may not be reproduced, distributed, or shared without TAG Cyber's written permission. The material in this report is comprised of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.

[1] https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
[2] https://sepio.systems/