SEPIO

Gartner COOL VENDOR 2020

FROST & SULLIVAN 2019 BEST PRACTICES AWARD
EUROPEAN ROGUE DEVICE MITIGATION ENABLING TECHNOLOGY LEADERSHIP AWARD

Embracing a Zero Trust Hardware Access Security Model

Never Trust, Always Verify

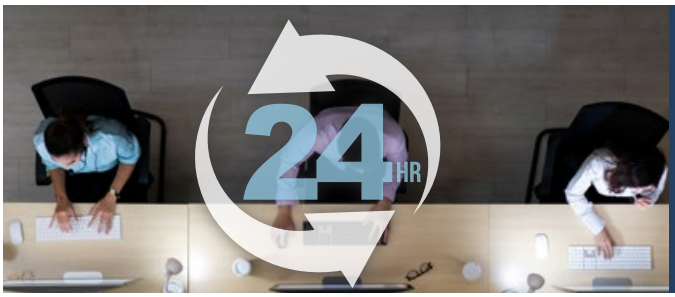
- Enterprise network devices and users are assumed to be trusted as they are internal.
- But this presents risks to cybersecurity as the device or user's identity can be spoofed by a malicious actor.
- Zero Trust (ZT) reduces this risk by eliminating the component of trust.
- Every user, device and application/ workload is deemed untrusted, every time it attempts network connection.

Verify Explicitly

- Access to resources is determined by a dynamic policy.
- The policy relies on many data sources including identity and access management, continuous diagnostic and mitigation systems, and data access policies.
- Authentication and authorization should always be based on all data points to comprehensively evaluate the device and user's identity.
- The evaluation should be continuous for the entire length of the session.

Assume Breach

- Defending resources is based on the assumption that there has already been a breach.
- Devices and users are denies network access by default.
- Access is granted or blocked based on the Zero Trust Architecture (ZTA).
- The ZTA evaluates a requesting device's identity by heavily scrutinizing its characteristics.
- Mirco-segmentation splits the network into smaller parts, each requiring separate access which is granted or blocked based on the device's identity.
- The Principle of Least Privilege is integral to the ZT model.



Give us 24hrs.

We will provide you with complete visibility and control for hardware devices and augment hardware risk mitigation through Zero Trust Hardware Access.

Challenges

Visibility

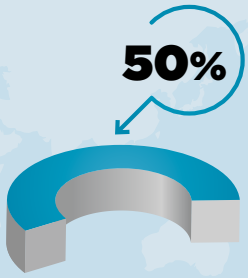
An effective ZTA relies on strong device identity and management capabilities to accurately evaluate access requests. However, attackers can bypass ZT security protocols by spoofing a legitimate, trusted device. Spoofing Devices sit on the Physical Layer and run passively with no inbound traffic, operating under the radar of existing security solutions, including NAC, resulting in a lack of complete asset visibility. The lack of visibility limits the ZTA's efficacy as it enables attackers to not only gain unauthorized network access but also move laterally throughout the network, circumventing micro-segmentation. IoT cybersecurity is at risk since IoT devices are also vulnerable to Physical Layer manipulation. As IoT devices require network access, they are valuable attack vectors for malicious actors, thus increasing the attack surface and, subsequently, the risk to the enterprise.

Access policies

Access policies are another source of information that the ZTA relies on when making access decisions. Such policies, however, are based on asset and network traffic data. The gap in visibility means that access policies are created without complete information, limiting their validity and reliability.

More importantly, the policies will not be enforceable on assets that are not visible. So, while the validity of access policies can be questioned, they do not actually protect the enterprise from hardware-based attacks since the attack tools go undetected.

Organizations have moderate means to discover, identify & respond to unknown, unmanaged, or insecure devices accessing network and cloud resources.



Cybersecurity Insiders' 2020 Endpoint & IoT Zero Trust Security Report

Zero Trust Hardware Access with HAC-1

To mitigate such challenges, and have a more effective ZTA, the ZT model needs to focus on the first line of defense – the hardware level; specifically, the Physical Layer. In doing so, the critical questions of "who, what, when, where, and how", which determine access decisions, can be answered. Accurately.

Sepio Systems' Hardware Access Control solutions (HAC-1) 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, HAC-1 verifies the device's true identity – not simply what it claims to be – and instantly detects vulnerable devices within the infrastructure. In doing so, the ZTA can make accurate access decisions and uphold the efficacy of micro-segmentation.

With complete device visibility, HAC-1 facilitates comprehensive Hardware Access Control through its policy enforcement mechanism that allows the system administrator to define a strict, or more granular, set of rules for the system to enforce, based on device characteristics. Hardware Access Control policies support the Principle of Least Privilege, which is integral to ZT, by restricting access to resources based on the device's role and identity.

The device visibility and policy enforcement capabilities, combined, enable the third component of HAC-1; Rogue Device Mitigation. The deep visibility ensures that the pre-set policy is comprehensively enforced on all assets, instantly detecting when a device breaches it. When breached, HAC-1 automatically instigates a mitigation process which instantly blocks unapproved or Rogue hardware.

As a result, HAC-1 provides the actional support necessary for ZT by preventing malicious devices from bypassing traditional ZT security measures.

Components of Zero Trust	Zero Trust enhanced by HAC-1
Comprehensive security monitoring for validation of users and their devices' security posture.	Ultimate device visibility that reveals a device's true identity by validating its Physical Layer information. Instantly detects the presence of vulnerable or Rogue devices.
Granular, dynamic, and risk-based access control through policy enforcement.	Policy enforcement mechanism defined by a strict, or more granular, set of rules that enables Hardware Access Control based on the device's characteristics.
System security automation that protects data and resources.	Rogue Device Mitigation that automatically blocks devices which breach the pre-set policy, protecting data and resources from unauthorized access.

About Sepio

Sepio delivers a hardware access control (HAC) platform that reduces the risk of unapproved and rogue devices by providing complete visibility, control, and mitigation of all hardware assets. Sepio's hardware fingerprinting, augmented by machine learning, discovers all managed, unmanaged and hidden devices that are invisible to all other security tools. Sepio's solution enhances zero trust, insider threat, BYOD, IT, OT and IoT security programs.

LEARN MORE