

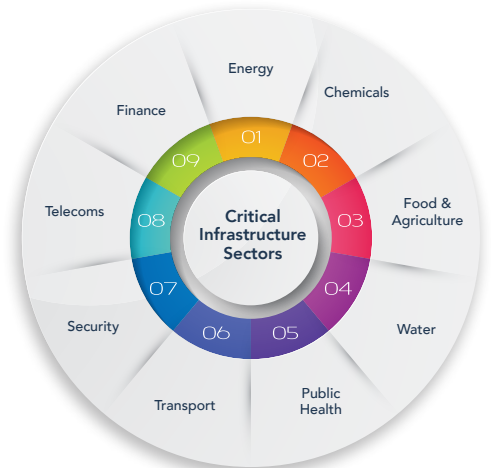
Hardware Access Control

Visibility, Control and Mitigation of all Hardware Assets

Critical Infrastructure

Critical infrastructure is recognized by governments as the body of systems, networks and assets (be that physical or virtual) that is so essential that their continued operation is required to ensure the security of a given nation, its economy and the public's health and/or safety. Essentially, these are assets that are crucial for the functioning of society.

The destruction of these assets would have a debilitating effect on security in all aspects and the consequences are so perilous that mitigating any threat is imperative.



Risks

There are various risks involved for critical infrastructure. Physical risks, although still pertinent, are not as frequently carried out with intention. Physical destruction, today, is mainly unintentional and can be a result of dramatic weather conditions or diseases. Virtual threats, however, are much more perilous as the world increasingly becomes more reliant on technology.

Critical infrastructure is the perfect target for governments that want to cause mass damage to their adversary and, as such, these types of attacks are often attributed to state, or state-sponsored, actors. Types of virtual attacks include malware attacks, such as ransomware attacks, and data breaches. The consequences of a cyberattack on critical infrastructure, even momentarily, would be substantial and there would be a ripple effect into numerous aspects of society. Importantly, some critical infrastructure (e.g. transport, water, and agriculture) relies on others (e.g. power and energy), increasing the impact of an attack.

Vulnerabilities

Critical infrastructure is highly vulnerable due to old systems. Programmable logic controllers (PLCs) are important components in every sector of critical infrastructure, and many are poorly secured due to them being old and, therefore, not built with online security features in mind. Similarly, the legacy systems used by power facilities were not built with cybersecurity in mind and, as such, do not have sufficient protection. There is also a lack of attention given to cybersecurity within industries of critical infrastructure. New technologies are used to improve efficiency and customer experience, yet there is little interest given to the fact that bad actors are constantly looking for vulnerabilities to exploit. The internet of things (IoT) is being more commonly implemented by owners of critical infrastructure, with around a third of the 25 billion IoT devices in the world being used to monitor and control infrastructure. However, this increases the number of entry points for an attack to be carried out, since they are connected to the network. Furthermore, the importance of critical infrastructure makes attacks more likely to be successful, specifically ransomware attacks.

The reliance on critical infrastructure by the nation might make owners of facilities more compliant with demands. Finally, the size of the companies that provide critical infrastructure will most likely be very large since they are providing for a whole nation. Such, there are more employees, the biggest risk to any organization. The lack of knowledge and awareness regarding cyberattacks means employees might not take appropriate action to prevent them where they can. There are a large number of employees that can, wittingly or unwittingly, cause a cyberattack and this large number makes it more challenging to identify the perpetrator.

HAC-1

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment. This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.






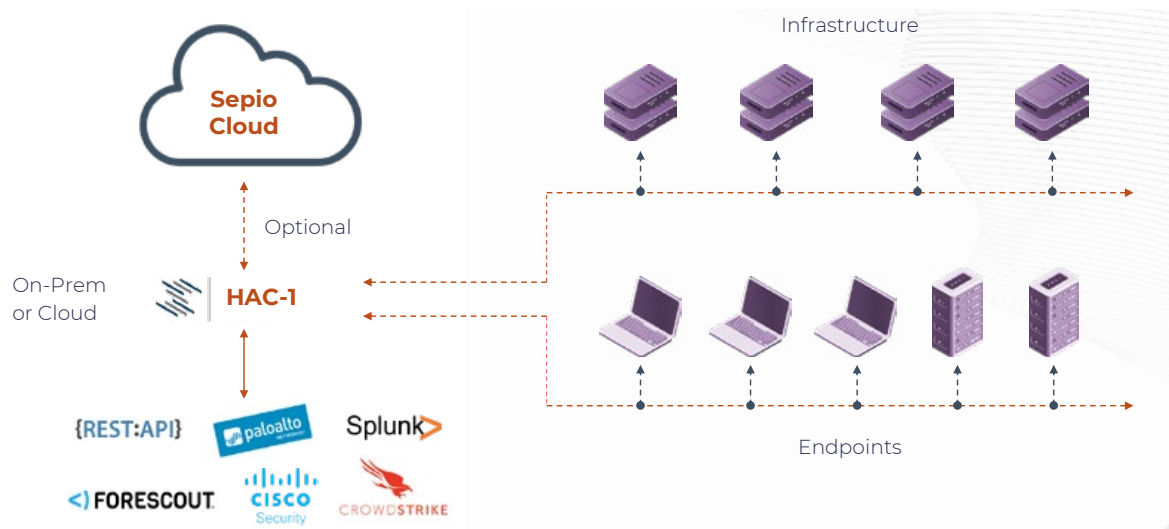
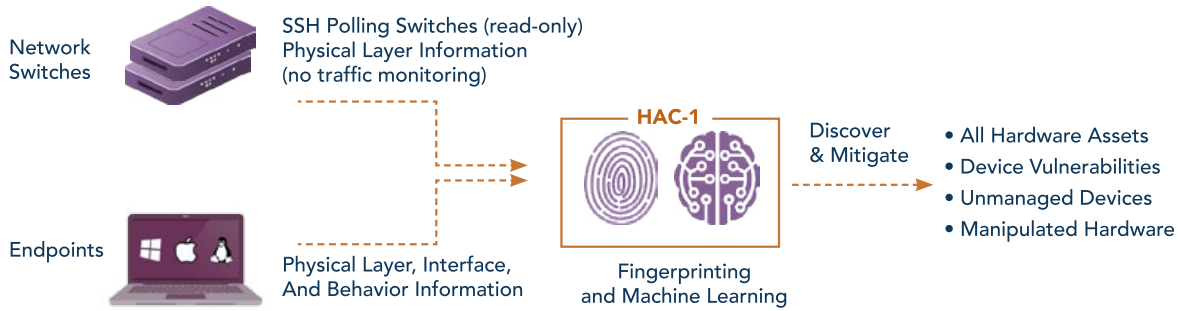


Rogue Devices

Rogue devices are peripherals which have been manipulated to act with malicious intent. They have the ability to carry out various types of malware attacks, including ransomware attacks, and data breaches. The aforementioned vulnerabilities of critical infrastructure can all be exploited by rogue devices, making them a useful attack tool for perpetrators, but a dangerous enemy for the victim. Most importantly, these devices not only look genuine to the human eye but also go undetected by security software solutions which simply identify them as legitimate human interface devices (HIDs), such as a mouse or a keyboard, and therefore will not raise any EPS/EDR alerts. Network implants and Spoofed devices attacks occur on the Physical Layer (Layer 1), which the existing security software, mainly NAC and IDS does not cover.

Main Benefits of HAC-1

- 
Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.
- 
Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.
- 
Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.



www.srccybersolutions.com

+91 120 2320960

sales@srccybersolutions.com



ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source, reflecting actual business, location, and rules. Sepio radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect. Visit: www.sepiocyber.com.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF++) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

