SEPIO

CRITICAL INFRASTRUCTURE

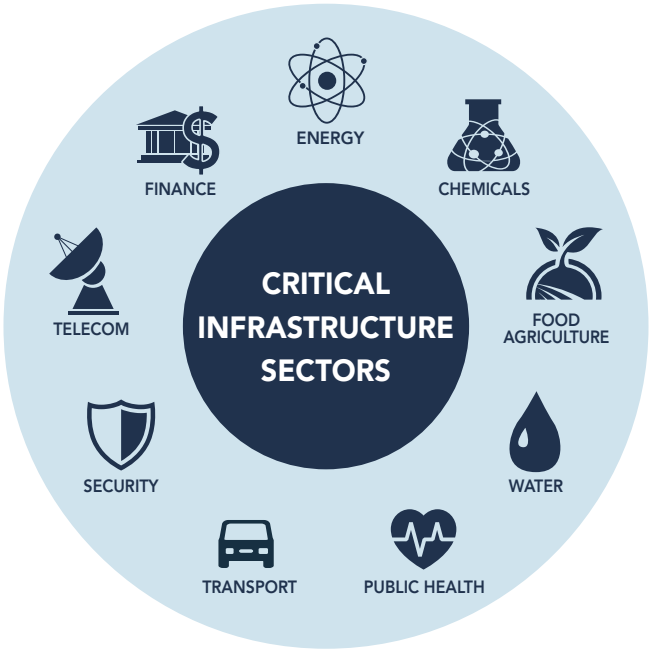
PROBLEMS AND SOLUTIONS

A Sepio white paper

INTRODUCTION

Critical infrastructure is recognised 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.



THREATS

PHYSICAL THREATS

These threats were more common a generation or two ago, in terms of man-made physical threats. Bombs and other forms of physical, intentional, destruction of critical infrastructure was something that was more frequently seen before the increased reliance on technology. Natural threats, however, are still prominent, with the weather and diseases being an extremely high risk. Hurricanes and tsunamis can wipe out critical infrastructure at the blink of an eye and widespread health pandemics, such as COVID-19, can cause such mass hysteria that it impacts critical infrastructure.

VIRTUAL THREATS

All industries are becoming more reliant on technology and any device connected to a network is at risk of being hacked. As such, cyberwarfare is very real and is growing in prominence. Critical infrastructure, due to its vital role in society, makes the perfect target for governments looking to cause mass destruction, with the Stuxnet attack on Iran's nuclear facility as an example. With facilities varying so widely, approaches must be very specific meaning governments, and state-sponsored actors, are the most likely perpetrators due to their almost unlimited capabilities. Nonetheless, cyberattacks can be carried out by non-state, or non-state-sponsored actors.

Malware attacks can be extremely effective, with the 2016 power cut in Kiev being attributed to a malware attack perpetrated by Russia. Similarly, ransomware attacks can be highly successful due to the critical nature of facilities. Moreover, some critical infrastructure is exposed to highly sensitive information, not only on employees and consumers, but also on the government and government personnel. As such, data breaches will be a popular attack by those wishing to gain access to this information. Again, for state, and state sponsored actors, this will be an appealing way to sabotage adversaries.

WHY IS CRITICAL INFRASTRUCTURE VULNERABLE?

OLD SYSTEMS

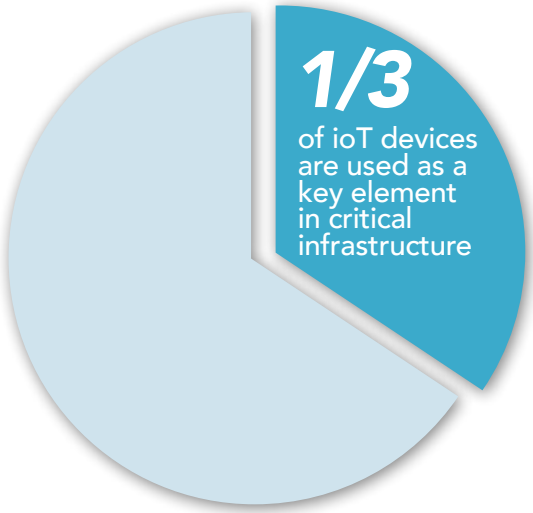
Programmable logic controllers (PLCs) are important components in every sector of critical infrastructure and many are poorly secured due to them being old and, therefore, not built with online security features in mind. The risk of a cyberattack on PLCs was demonstrated in 2017 by a PhD student at Georgia Institute of Technology who developed ransomware that attacked water supply by compromising PLCs, of which 1,500 were found online; and highly vulnerable to a cyberattack. The student was able to control the PLCs so that an abundance of chlorine was filtered into the water, making it undrinkable. Similarly, banks' legacy systems are also out of date, hence not having cybersecurity functions built within thereby making them an easy target.

LACK OF ATTENTION TO CYBERSECURITY

Clearly, there are cyber risks to critical infrastructure, but reports about cyberattacks on critical infrastructure rarely reach the public, thereby reducing concern for cybersecurity. Sectors within critical infrastructure mistakenly do not put cybersecurity as a top priority and rather focus on using new technologies to improve efficiency and customer experience. Malicious actors, however, are looking for the vulnerabilities in these new technologies that they can exploit.

INTERNET OF THINGS (IOT)

As owners of critical infrastructure are utilising new technologies, it is not surprising that around a third of the 25 billion IoT devices in the world are being used to monitor and control infrastructure. Operational technologies – the industrial control systems managing the equipment – are now connected to the internet. Although this improves efficiency and customer satisfaction, it also increases the number of entry points for an attack to be carried out, since they are connected to the network.



IMPORTANCE OF CRITICAL INFRASTRUCTURE

The simple fact that critical infrastructure is just that – critical – means a ransomware attack, whereby files and/or systems are blocked until a ransom is paid, will have high chances of being successful as nations need the equipment to be operational. The reliance on critical infrastructure by the nation might make owners of facilities more compliant with demands.

SIZE OF COMPANIES

Since companies that provide critical infrastructure are providing for an entire nation, the size of them will generally be very large. As such, there are more employees; the biggest risk to any organisation. 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.

ROGUE DEVICES

Although the solutions above provide substantial protection against the security risks involved with BYOD, they do not provide protection for undetectable hardware attacks. Personal devices are extremely susceptible to these attacks as it is easier for a perpetrator to target them than the devices secured within an organization.

Hardware attacks can be carried out on the network by using network implants at the Physical Layer (Layer 1), spoofed network elements or by using vulnerabilities of devices connected to the Enterprise's network.

Another popular attack interface is the USB , where attack tools fully impersonate (VID/PID/ ClassID) as a legitimate human interface devices (HIDs), thereby not raising any alarms. Sepio has developed a solution to detect, alert and block rogue devices operating over network and USB interfaces; this is the only software security solution for this type of attack.

By discovering rogue devices through hardware fingerprinting and behavior analytics, SepioPrime, which orchestrates Sepio's solution, provides alerts for security threats, enforces policies and delivers risk insights and best practices recommendations.

By supplying organizations with ultimate visibility of the enterprise's IT assets, a stronger cybersecurity posture is achieved. The software is augmented by real-time cloudbased intelligence that provides early warning of the latest malicious hardware and threat pattern.

Sepio's SaaS-based security suite can be deployed on any physical or virtual environment in any combination of on-premises, private and public cloud. With its "read-only" network access privileges, SepioPrime cannot change or alter anything within the organization.

Its existing integration with various SIEM/NAC solutions, eases the deployment and onboarding process.

CONSEQUENCES OF A CYBERATTACK ON CRITICAL INFRASTRUCTURE

If critical infrastructure was to shut down, even momentarily, there would be a significant impact on society and indirect ripple effects in numerous aspects of individuals' lives. Importantly, some critical infrastructure (e.g. transport, water and agriculture) relies on others (e.g. power and energy). An attack on one might very possibly cause significant damage to another.

Consequences include, but are most definitely not limited to, impacts on:

- Health – healthcare facilities may not be able to perform surgery or provide medication to patients whereby consequences can be fatal. Additionally, an attack on water and food manufacturers can result in a lack of access to these two important needs. Furthermore, power failures, such as those to traffic lights, can cause major traffic problems and, as a result, serious accidents.

- Productivity – implications of a shutdown of critical infrastructure might include having to work remotely which, for some organizations, is very ineffective thereby causing a loss of productivity. Power cuts will also add to a loss of productivity as all organizations require electricity to function.

- Psychology – the impacts of a cyberattack on critical infrastructure can cause a great deal of psychological distress, mainly fear, amongst the population which results in irrational actions, causing further damage within society.

- Communication – an attack on a telecommunication company will make it extremely challenging for there to be communication between individuals and between the government and the public. This is especially ironic when the government attempts to comminute with the nation to unite them in mitigating the effects of the attack.

HAC-1 Solution

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.

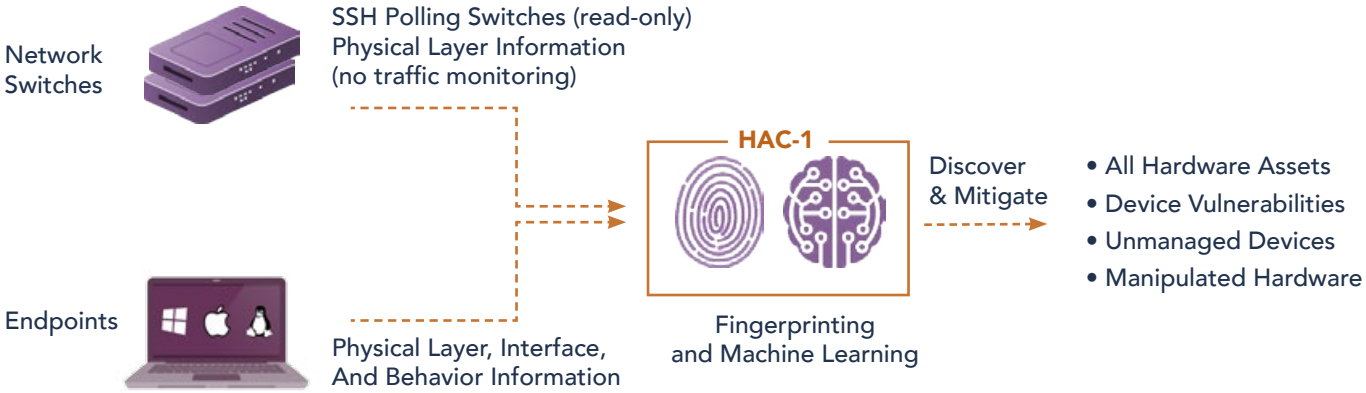
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, 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.

Sepio is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

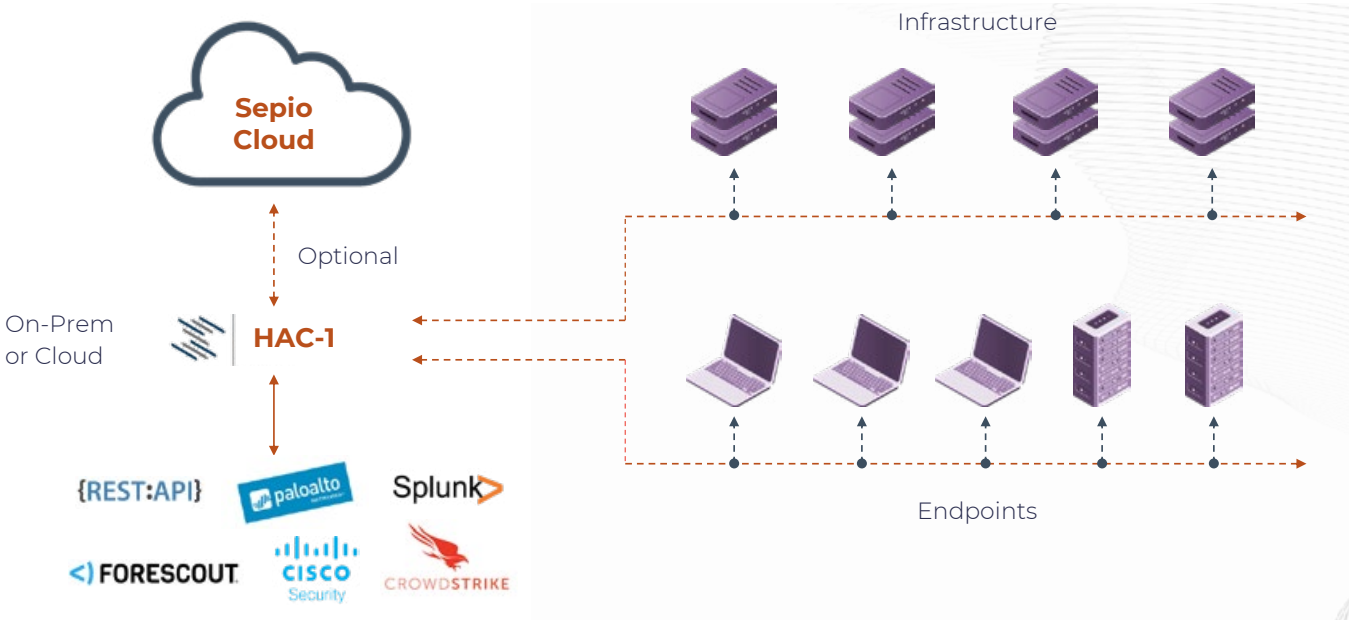
Main Benefits:

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.

System Architecture



LEARN MORE

SEPIO