SEPIO

Mitigating Wi-Fi Risks

Ensuring Wireless Infrastructure Trust

A Sepio white paper

INTRODUCTION

Today, Wi-Fi is everywhere; we find it in homes, offices, coffee shops, airports, hospitals, and even the street. Humans rely on an internet connection on a day-to-day basis, whether it be for personal or professional reasons.

The internet's role in society is only growing; the Cisco Annual Internet Report (2018–2023) predicts that two-thirds of the global population will have internet access by 2023, up from just over half in 2019. However, the threat of Wi-Fi attacks means that these figures only provide greater exposure for malicious cybercriminals.

> **Humans rely on an internet connection on a day-to-day basis, whether it be for personal or professional reasons.**

ROGUE ACCESS POINTS

A rogue access point (AP) can be classified as any AP that is not authorized to be operating on the network. Some rogue APs are benign in nature, only set up to provide greater coverage or access to blocked websites. While these APs do present a serious security risk to the user and network administrator, the most threatening rogue APs are those created by bad actors with malicious intent.

Known as an Evil Twin, the rogue AP impersonates a legitimate AP by spoofing its SSID to trick users into connecting to it. Evil Twins have allowed cybercriminals to adapt to the dynamic cybersecurity defenses deployed to block cyber-attacks by exploiting the "blind spots". Organizations lack the ability to identify unauthorized BSSIDs, so, when a rogue AP is present there is no indication of this. Users are therefore at risk of connecting to the Evil Twin, completely unaware of its malicious nature. The attacker can remotely carry out attacks once users have connected to the rogue AP and, essentially, steal data out of thin air.

> **Evil Twins have allowed cybercriminals to adapt to the dynamic cybersecurity defenses deployed to block cyber-attacks by exploiting the blind spots.**

SEE NO EVIL

Establishing connection

The rogue AP attempts to break up any connection between a user and a legitimate AP by sending deauthentication packets. For users not yet connected, this step is not necessary. From here, the rogue AP transmits signals stronger than those of the legitimate AP to ensure users connect to it. Because the rogue AP has the same SSID as the legitimate AP SSID, there is no indication to the user of malicious activity taking place. Persons connected to the Evil Twin are at risk of man-in-the-middle (MiTM) attacks, packet sniffing, data breaches, and more.

Attack

The rogue AP acts as the middleman between the user and the parties with which they communicate. Hence, the attacker can view all data transmissions emanating from the user and alter data packets. In doing so, the perpetrator can steal sensitive information such as financial data, credentials, or network activity. Advanced Evil Twin attacks provide attackers with access to additional systems where further damage can be done.

Stealing information in thin air

Evil Twin attacks are nothing new, and they can enable sophisticated reconnaissance. In 2018, the US Department of Justice (DoJ) charged Russian hackers with carrying out Evil Twin attacks on several organizations, including a number of anti-doping agencies. The attackers reportedly attempted to steal data and even hijack the network of some of their targets. All this took place while operating remotely in a nearby vehicle.

ENTRY POINTS FOR ACCESS POINTS

Internet of Things

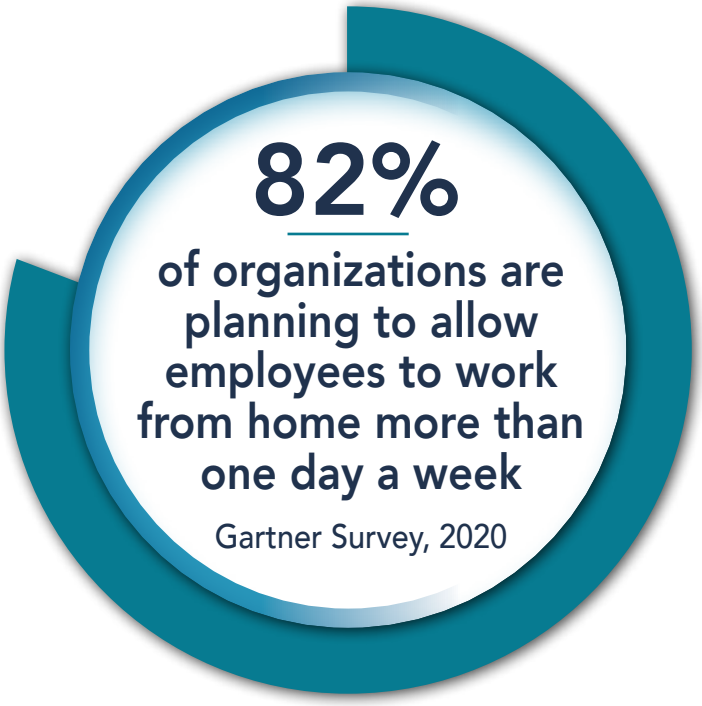
Today, there are around 35 billion IoT devices in the world. A 2020 study by Juniper Research predicts that this figure will reach 83 billion by 2024. With so many internet-connected devices – and only more to come – there are ample opportunities for a successful Evil Twin attack, 35 billion to be exact. Additionally, as IoT devices become an integral component of critical infrastructure's operations, the damage can transcend from the cyber domain into the physical one. The healthcare industry is an example of critical infrastructure that relies on IoT.

The Internet of Medical Things (IoMT) market is growing by almost 30% a year, and such devices provide patients with critical care. Should an IoMT device accidentally connect to a rogue AP, the consequences could be life-threatening.

Remote work

The COVID-19 pandemic forced a global shift to remote work. What was assumed to be temporary has now become a feature offered by many organizations. Gartner found that 82% of organizations plan to allow employees to work from home at least one day a week. While bringing numerous benefits to both employee and employer, remote work leaves users more exposed to attacks. As COVID restrictions begin to ease, remote work can essentially take place anywhere.

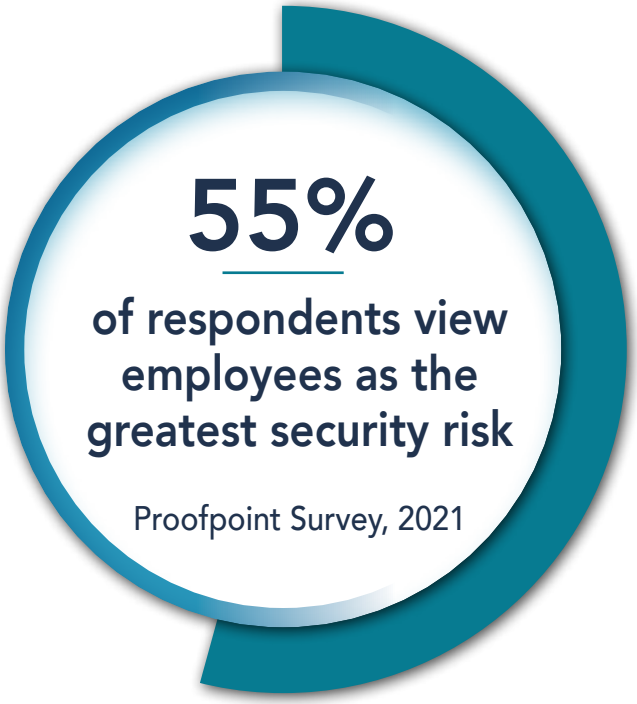
Coffee shops and libraries are popular locations for remote work, yet their public networks also make them popular with attackers. Naturally, public networks are less secure, even those with security features, making the perpetrator's job easier. Adding to the risk is that users want the strongest internet connection when working and, when seeing two "StarbucksFreeWiFi" networks, will connect to the AP with the strongest signal. This, of course, is the rogue AP. Additionally, home networks are vulnerable to Evil Twin attacks meaning employees cannot assume that their personal environment is risk-free.



Employee negligence

Employees are an organization's greatest security vulnerability due to their insider privileges coupled with carelessness. Research by Proofpoint found that human error is the biggest risk for more than half of organizations. Should an employee fall victim to an attack, their insider access can provide the perpetrator with access to sensitive information and confidential data. When it comes to Wi-Fi risks, organizations essentially rely on their employees to not connect to a rogue AP.

This, however, is a challenge due to the covert nature of Evil Twins and a lack of cybersecurity awareness. Users tend to connect to APs without a second thought and will unlikely question an AP's legitimacy if it appears to be genuine. This vulnerability extends beyond working hours as, nowadays, devices often store or have access to company information. Hence, there is a constant risk of connecting to a rogue AP; employee negligence, even during off-hours, can put the organization at risk.



THE DOS AND DON'TS

Do	Don't
Avoid public Wi-Fi if/when possible	Access sensitive personal or corporate data
Check warning notifications	Use personal financial information
Always use a VPN	Connect to unsecure public networks
Disable automatic connectivity on devices	
Businesses should establish strict rules for employees and ensure that they are easily available.	
Businesses should deploy Wi-Fi specific security solutions	
Businesses should preconfigure a list of authorized clients in the network	

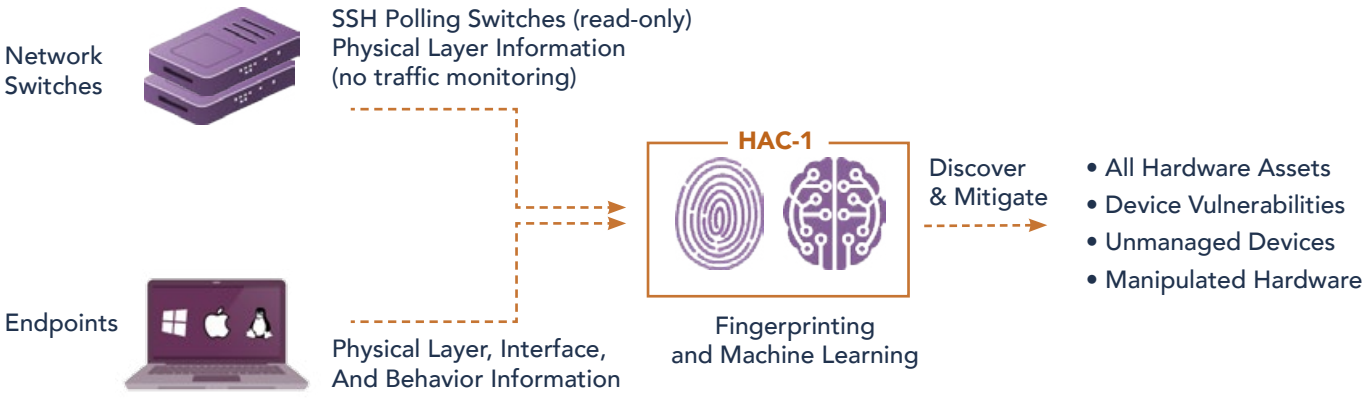
HAC-1 SOLUTION

Sepio's Hardware Access Control (HAC-1) solution provides a panacea to the gap in visibility by identifying the presence of rogue APs. When a rogue AP is detected, HAC-1 triggers a mitigation process through integrated security solutions. The extensive automation and integration capabilities with other products support a hands-free process and a Zero Trust Hardware Access approach.

In addition to its Wi-Fi capabilities, HAC-1 provides ultimate asset visibility. As the leader in Rogue Device Mitigation (RDM), Sepio's solution identifies, detects, and handles all IT/OT/IoT devices across the network and peripheral infrastructure; no device goes unmanaged. 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. Such capabilities enable a Zero Trust Hardware Access approach, and when a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process that instantly blocks unapproved or Rogue hardware

HAC-1 deployment requires no hardware and there is no need for traffic monitoring, meaning it will not impact the user's experience, or infringe on their privacy rights. Importantly, the deployment of HAC-1 is extremely fast and, within 24 hours, can provide your organization with complete asset visibility.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

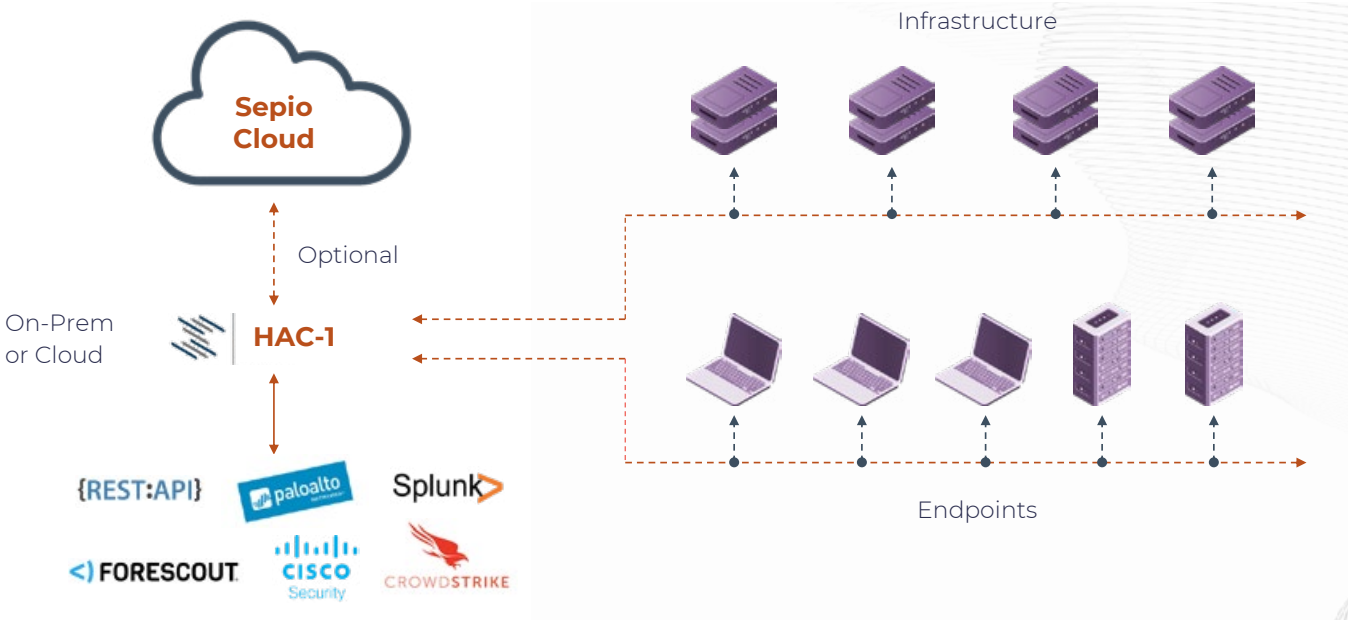
Main Benefits

Complete Visibility of AI 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