SEPIO

ENERGY SECTOR

PROBLEMS AND SOLUTIONS

A Sepio white paper

INTRODUCTION

The energy sector is entering a digital revolution as a means to improve efficiency and operational capabilities. However, in doing so, the industry increases its exposure to the threats associated with such a transformation – namely cyber-attacks. Due to the nature of its operations, the energy sector is one of the most important components of a nation's critical infrastructure.

Almost every other industry relies on energy providers to deliver their services. Hence, disruptions to the energy sector would cause spillover effects to numerous other industries and organizations, some of which could have fatal consequences. In other words, the energy sector is extremely critical, and the event of a cyber-attack would cause significant damage.

> **“Due to the nature of its operations, the energy sector is one of the most important components of a nation's critical infrastructure.”**

THREAT ACTORS

State Actors

Due to its criticality, the energy sector presents itself as an attractive target for hostile state actors, or state-sponsored groups. Nation-state actors targeting an energy sector are primarily seeking to sabotage their adversary – whether it be to cause economic or security damage. As such, state-sponsored cybercriminals often engage in cyberattacks that conduct espionage activities. In some cases, state actors may carry out more aggressive cyberattacks that cause physical damage to the equipment and systems used by energy providers. Moreover, nation-state actors possess the necessary capabilities to carry out such attacks, hence increasing the risk.

Terrorists

Similar to state actors, terrorists perceive the energy sector as an ideal target due to a country's dependency on it. Targeting an organization within the energy sector can have very detrimental consequences, including physical damage, which terrorists seek to achieve. Unlike state actors, however, terrorist groups typically lack the necessary skills to execute a successful attack on the energy sector.

Cybercriminals

Many times, perpetrators of cyberattacks are merely criminals seeking financial gains. The energy sector can provide monetary rewards in several ways. An immediate financial payout can come from a successful ransomware attack. Alternatively, cybercriminals may deploy attacks that result in data theft, whereby the information obtained can be sold on the dark web.

Hacktivists

Activist groups, such as Anonymous, are turning to cyber tactics to make a statement. Many activist groups oppose activities carried out by the energy sector and wish to protest against them. Cyber-attacks can be deployed as a statement of opposition against energy sector projects or general agendas.

ATTACK METHODS

Advanced Persistent Threat

Advanced persistent threat (APT) attacks are those which, as the name suggests, persist for a prolonged period of time – sometimes months, if not years. As such, APTs are ideal for conducting espionage activities and are often deployed by state actors. Additionally, APTs require sophisticated skills and capabilities, which state, or state-sponsored, groups typically possess.

The Stuxnet attack, supposedly perpetrated by the US and Israel, is a famous example of one of the most sophisticated APTs ever carried out, lasting several years before being discovered.

Distributed Denial of Service

The energy sector is extremely vulnerable to distributed denial of service (DDoS) attacks due to the harm that can come from disrupted operations. DDoS attacks generate a botnet that overwhelms a targeted system with high volumes of traffic, eventually causing it to become unavailable.

As mentioned, being an essential component of a nation's critical infrastructure, the energy sector cannot afford to have its operations halted or disrupted in any way. Hence, DDoS attacks are extremely threatening to this industry.

Ransomware

Ransomware attacks can be very successful in the energy sector due to the industry's criticality. Unavailability of files and/or systems is often not an option for energy providers, thus increasing the likelihood of the victim willing to pay the ransom.

Virus

A virus targeted at an energy provider can have substantial consequences due to the industry's organizational structure (which will be reviewed further on). The interconnectedness of the various systems within an energy provider means that a virus can quickly spread throughout the targeted organization.

Even more threatening are worms, which can self-replicate and propagate independently as soon as they have breached the system.

HARDWARE SECURITY CONCERNS

Attackers are increasingly turning towards hardware tools and techniques to carry out the aforementioned attacks. Hardware security is still widely misunderstood, and there is a general lack of awareness regarding hardware security risks.

As such, Rogue Devices can go undetected and increase the chances of a successful attack.

Spoofed Peripherals are recognized as legitimate HIDs and therefore not deemed harmful, thus not raising any security alarms. Moreover, these devices are visually unsuspecting to the human eye, further increasing their appeal to attackers. On the network interface, Network Implants sit on the Physical Layer which is not covered by existing security software solutions which, again, means no security alerts are triggered.

In addition to being covert, these devices are malicious by nature and intend to cause harm to the victim.

Numerous devices on the market can carry out many different attacks, thereby appealing to a range of threat actors. The energy sector is extremely vulnerable to hardware-based attacks for reasons expanded upon below.

VULNERABILITIES

Cyber-physical Interdependencies

The modern-electrical grid is dependent on cyber-physical systems, which means that the physical equipment and systems are digitally-controlled. Within the energy sector, the systems are highly complex and are essentially systems made up of systems – all of which are vulnerable. As such, there is a large attack surface, with a vast amount of entry points, that attackers seek to exploit. Such interdependency with cyberspace gives perpetrators greater access to systems and networks.

Organizational Complexity

The organizational complexity of energy providers increases the risks associated with cyber-physical interdependencies. The sector relies on several business units resulting in a complex structure that is difficult to provide comprehensive protection for, making an attacker's job easier. According to a report by the North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy (DOE),

"The North American bulk electric system is comprised of more than 200,000 miles of high voltage transmission lines, thousands of generation plants, and millions of digital controls. More than 1,800 entities own and operate portions of the system, with thousands more involved in the operation of distribution networks across North America. These entities range in size from large investor-owned utilities...to small cooperatives. The systems and facilities comprising the larger system have differing configurations, design schemes, and operational concerns".

Energy providers typically have a large workforce due to their organizational complexity. And, in the cybersecurity world, employees pose the greatest security risk. Hence, the more employees, the greater the risk. Similarly, the more vendors in the supply chain, the greater the vulnerability to cyberattacks as perpetrators often access their target by infiltrating its supply chain. Energy providers require copious amounts of vendors, all of which have different security postures, and you are only as strong as your weakest link. Moreover, many vendors will perform critical roles, and these entities must have the highest levels of security measures in place.

Moreover, the energy sector has integrated information technology (IT) and operational technology (OT), magnifying the cybersecurity risks. Networks connect the various components of OT and IT environments, and hardware attacks often target these networks as an entry point. Therefore, the integration between IT and OT means that an attack on the former can impact the latter and, subsequently, cause operational disruption.

Finally, due to organizational complexities, the energy sector undertakes a decentralized approach to cybersecurity. Although this can bring some benefits, such an approach means that there are inconsistencies throughout the organization vis-à-vis cybersecurity. Moreover, when responding to a cyber incident, a decentralized cybersecurity approach presents the risk of an incomplete mitigation process due to differences in response.

Expansive Footprint

The complexity of energy providers partly stems from the sector's expansive footprint. Due to the nature of the industry's operations, organizations in this field must operate nationally, if not internationally, including a wide physical geographic distribution. As such, energy companies will possess a considerable number of IT assets – all of which are vulnerable to hardware-based attacks.

Moreover, it becomes increasingly challenging to protect against such attacks as the more IT assets, the less visibility. And how can one provide protection for something that they do not even know is there?

Additionally, energy providers require large physical sites, such as solar and wind farms. Solar farms, for example, can have a capacity of anywhere between 1MW to 2,000MW, with a 1MW solar farm requiring around 5 acres of land. The larger the land size, the more challenging it is to provide full physical protection. Since hardware-based attacks require the perpetrator gaining physical access, a lack of comprehensive physical security only makes the task easier. During security research, researchers successfully infiltrated an entire wind-turbine farm's network within minutes, in part due to physical vulnerabilities.

Should the attack have been carried out by malicious actors, it would have caused anywhere from $10,000 to $30,000 worth of revenue losses per hour, or even destroy the turbines entirely.

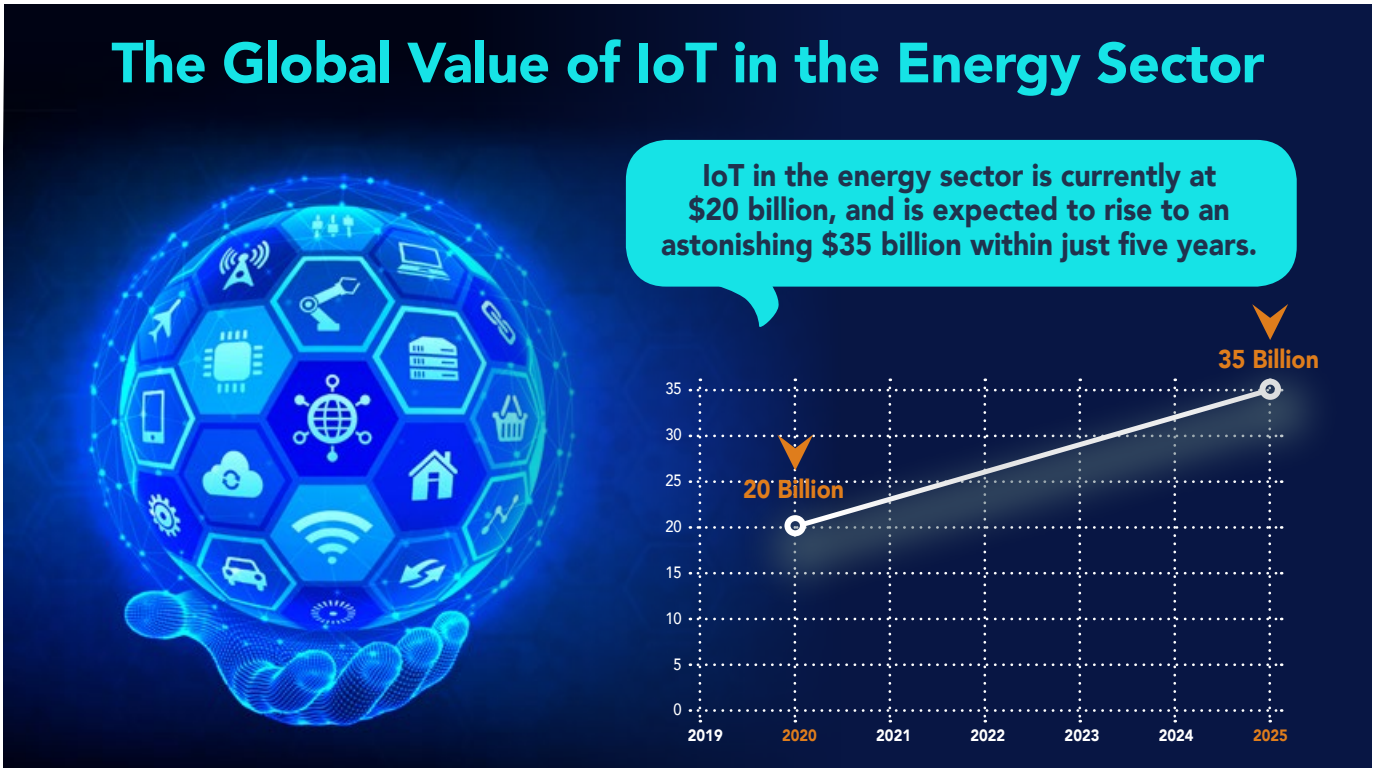
The energy sector has used technology to its advantage to reduce the challenges that come with such an expansive footprint, including the deployment of remotely accessible devices and equipment to enhance productivity. In doing so, however, the sector has increased its cybersecurity risks.

Accessible Devices

The global value of the Internet of Things (IoT) technology within the energy sector is currently at $20 billion, expecting to rise to an astonishing $35 billion within just five years. However, the usage of IoT devices increases the attack surface as the more devices in use, the more entry points there are. This is especially concerning since many IoT devices within the energy sector are used to operate equipment, meaning that an attack on one of those devices could potentially provide the perpetrator with control over the machinery.

Additionally, the energy sector deploys consumer-facing devices, such as smart meters and electric vehicle chargers, which are typically found in less secure environments. These devices can be, and have been, used as an entry point.

Furthermore, with IoT devices requiring a network connection, successful network manipulation can provide a bad actor with access to the IoT devices connected to that network.



Legacy Systems

Although deploying modern technology, the energy sector still heavily relies on legacy systems which were not built with cybersecurity in mind, such as programmable logic controllers (PLCs). OT within the energy sector largely depends on these PLCs, including SCADA systems, which control and monitor plant equipment. Hence, an energy provider's apparatus is highly vulnerable to manipulation due to the reliance on legacy systems. Should PLCs be manipulated, as they were in the Stuxnet attack, the equipment could be severely, if not permanently, damaged.

CONSEQUENCES

Physical Damage

As mentioned, an attack on an energy provider can provide the perpetrator with control over the OT, potentially causing the equipment to malfunction, fail, or be permanently damaged. As a result, there will likely be power disruptions or even complete blackouts. In 2016, Ukraine's power grid was attacked by malware, causing parts of Kiev to be subject to complete darkness.

Moreover, heavy reliance on the energy sector means that there will be inevitable spillover effects onto other industries following an attack, some of which can be lethal. Hospitals, for example, require energy for their operations and, should an attack cause significant disruptions, there is a strong possibility of fatalities.

Financial

Operational disruption can have high associated costs – both direct and indirect. Because of the expansive nature of energy providers' operations, an attack that shuts down a network can result in millions, or even billions, of dollars' worth of losses. The machinery used within the energy sector is expensive, meaning that an attack that results in physical damage to the equipment has high associated costs due to the need to replace the defective machines. The financial implications following an attack can last for an extended period due to the abundance of indirect costs, including clean-up time, regulatory fines, reputational damage, and more.

Political

Attacks carried out by nation-states, or state-sponsored actors, will likely increase tensions between the perpetrator and the victim. Although not specifically targeting the energy sector, the recent SolarWinds attack is an example of how a state-initiated attack on an adversary's critical infrastructure resulted in increased hostilities. With the attack attributed to Russia, President Biden is reportedly preparing sanctions to punish Moscow for its actions.

Furthermore, an attack on the energy sector can undermine the nation's trust in its government. A successful hit on the energy sector suggests that the government is incapable of securing its critical infrastructure, which can raise doubts regarding the state of national security.

Societal

An attack on the energy sector can have substantial effects on daily life and productivity. Blackouts and other power disruptions can completely halt day to day actions, including the ability to work, travel and, in some cases, communicate.

Additionally, there can be psychological impacts on society in the form of fear and distress. The perception that the government is unable to provide strong national security measures can be very disconcerting for society, and result in unwanted mental health effects.

HAC-1 Solution

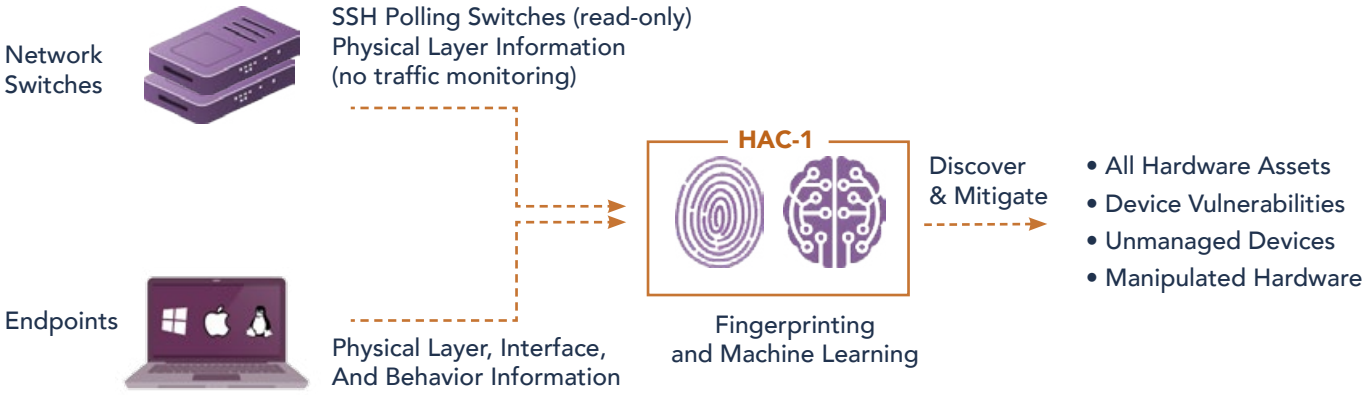
Many times, IT and security teams in the energy sector struggle in providing complete and accurate protection of their hardware assets - especially in today's extremely challenging IT/OT/IoT environment. This is because, often, there is a lack of device visibility which leads to weakened policy enforcement of hardware access. This vulnerability may result in security incidents such as ransomware attacks, data leakage, etc. In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of device characteristics and the interface used for connection.

Moreover, malicious actors have adapted to the dynamic cybersecurity defenses deployed to block cyber-attacks by taking advantage of the "blind spots" – mainly through USB HID-emulating devices or Physical Layer network implants. These Rogue Devices are covert by nature and go undetected by existing security software solutions, thereby leaving the organization extremely vulnerable.

Sepio has developed the Hardware Access Control (HAC-1) solution to provide a panacea to the gap in device visibility. As the leader in Rogue Device Mitigation, Sepio's solution identifies, detects and handles all peripherals; no device goes unmanaged. HAC-1 uses Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices and compares them against known fingerprints. In doing so, HAC-1 is able to provide organizations with ultimate device visibility and detect vulnerable devices and switches within the infrastructure.

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. When a device breaches the pre-set policy, HAC-1 automatically instigates a mitigation process which instantly blocks unapproved or Rogue hardware.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

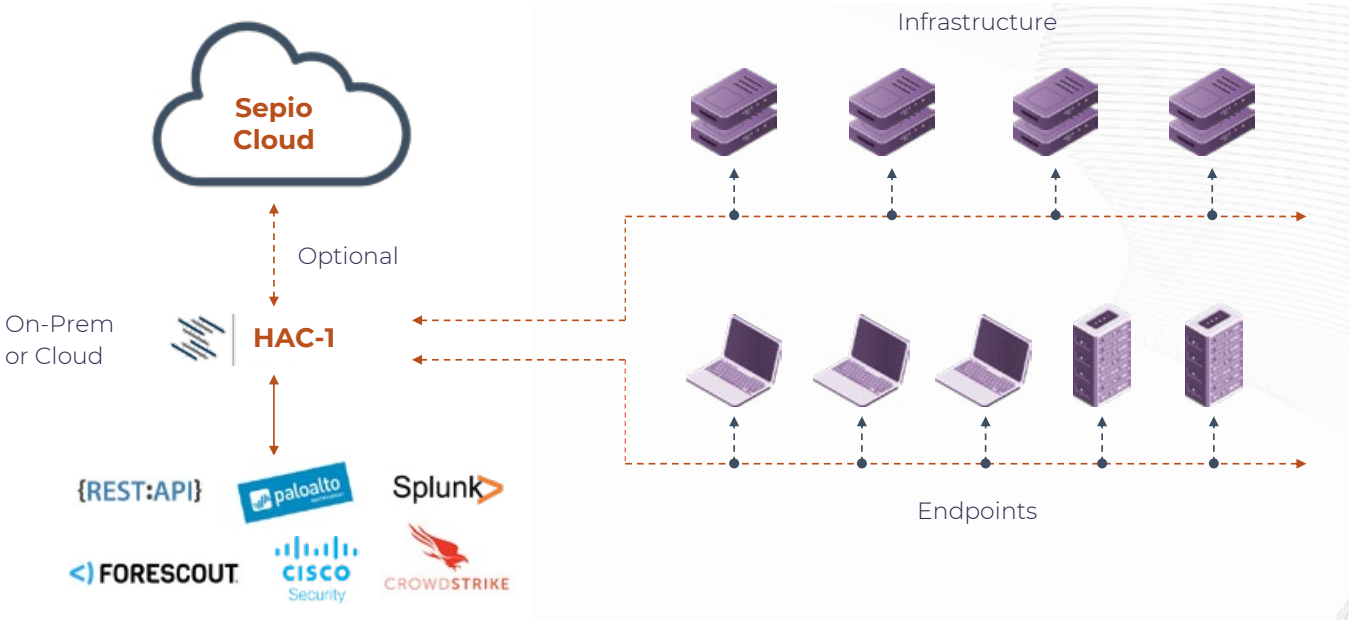
Main Benefits:

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.

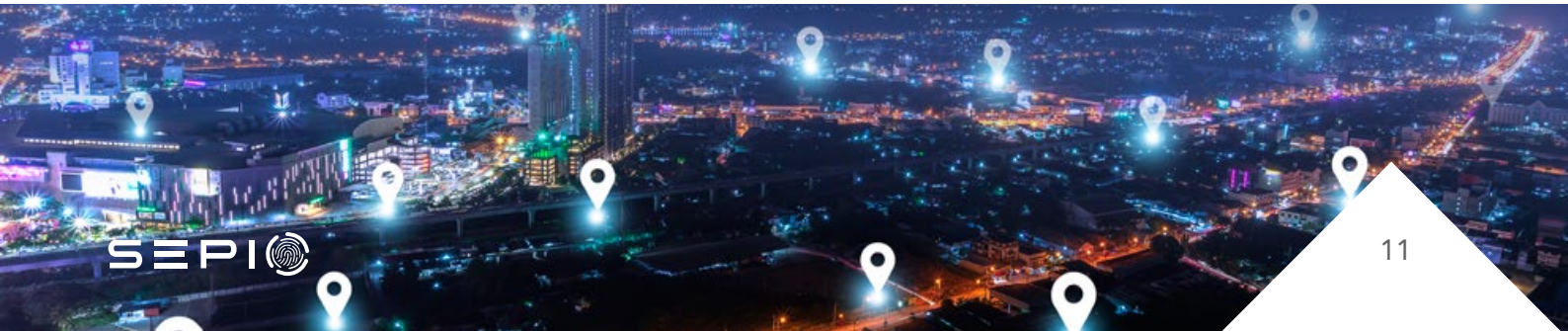
Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

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