Solution Brief:

Advances in IoT Cyber Protection

CSPi and Seceon provide a joint solution to address the unique security challenges found in medical and commercial IoT devices,

CSPi CYBERSECURITY PRODUCTS

seceon

Introduction

As the interest and adoption in IoT continues to rise organizations are on the look-out for an easy and effective way to secure these devices. This solution brief provides an overview of a joint solution by CSPi and Seceon optimized for commercial IoT security with automated detection, containment and the disruption of any intrusion prior to data exfiltration or other damage. These capabilities will prove especially of value in the industrial, facility and medical markets where legacy technologies or EDR applications are not deployable.

The Rise of Commercial IoT

IoT is one of today's fastest-growing technologies. Gartner forecasts over 20 billion devices will be deployed by 2020, with the highest deployment growth in the commercial sector. However, it's no secret that these devices are also the most difficult to secure, accounting for the greatest cyber risk with their widespread appearance within an organization's network.

Commercial IoT		
Medical IoT	**Industrial Controls**	**Building Automation**
Wearables	Sensors and Controls	Environmental
Critical Systems	Automation	Safety

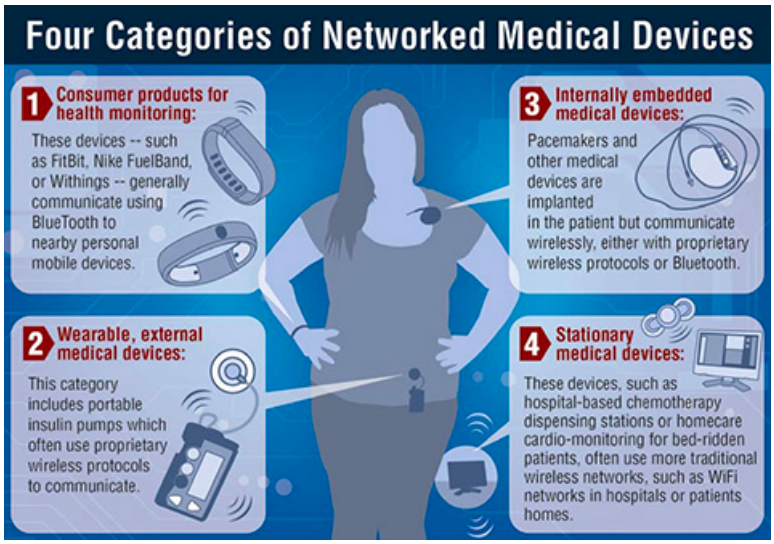
Commercial IoT is Difficult to Secure

Most standard endpoints under IT control are deployed with Endpoint Detection and Response (EDR) applications. EDRs protect these devices from cyber infection and help detect many issues that cannot be stopped.

Unlike other endpoints, IoT devices cannot typically support add-on security applications. These tend to be closed devices, often with limited processing power and memory—the result of being optimized for cost performance and battery life. Yet there's a conflict here since the most effective EDR applications are anything but processor-, power-, and memory-efficient.

Commercial IoT products range from building automation and control systems, to industrial controls, scanners, sensors, security systems, biometric systems, and medical IoT (IoMT) devices. Such devices can be deployed by business groups without the knowledge of IT or security teams, typically for legitimate business purposes. Most organizations are now also

being inundated with "Bring Your Own IoT," which includes increasing amounts of desktop devices, wearable devices, and additional examples of IoT.



Medical IoT Challenges

The internet of medical things (IoMT), or Healthcare IoT, brings its own challenges—these devices can be critical to a patient's health and their data critical to sustaining proper body functions. The most concerning are the patient wearables or in-body devices like pace makers, drug pumps, etc. that "walk" into an environment and must dealt with accordingly; in most cases this means they will be allowed on the network.

On the other extreme are devices that have been around for 15 years or longer—the PACs, X-Ray, and CAT scan equipment. Many of these devices are running operating systems that were developed in the last millennium. These systems simply can't host a modern EDR solution and are no longer getting patch updates. As old as they are, they need the same protection as the most cutting-edge wearables.

The challenge with this vast variety of IoMT devices is multifold. First, how to identify them, and then how to decide what other applications, systems, and devices they can communicate with. Finally, and most importantly, how to ensure they do no harm to the rest of the organization.

To solve this problem, CSPi developed the ARIA™ Software Defined Security (SDS) solution that allows IoMT devices to be detected and monitored by looking through the network data as it flows out from such devices. ARIA SDS successfully classifies data on the fly without impacting its delivery. This allows monitoring for various IoMT devices in network aggregation points that are usually one step back in the wireline network. Finally, a feature set known as Threat Reaper™ is used to stop detected threat conversations without disabling legitimate communications from the device.

CSPi's ARIA SDS solution provides four significant benefits:

1. Enables clientless threat containment of specific conversations for IoMT devices as detected/confirmed by security systems, such as the Seceon aiSIEM.
2. Generates NetFlow record metadata for every packet seen. This can be fed to threat detection systems such as Seceon's aiSIEM to find network-born threats.

This is critical to securing IoMT devices, since most of these devices don't generate any logs to feed a SIEM.

3. Captures and sends requested packet conversations with suspected threats for further investigation, automatically or upon request.
4. Applies and enforces micro-segmentation. Working with tools like the aiSIEM to ensure that ARIA prevents rogue IoT devices from trying to communicate with devices or applications they should not.

Seceon's aiSIEM is one of the best available SIEM solutions at both detecting and stopping threats, all in one platform. It takes the data fed by a variety of devices and applications, as well as NetFlow data and runs it all through the industry's most comprehensive threat models to detect threats of all kinds. The aiSIEM's ability to correlate logs and network data sourced from the ARIA SDS solution make it very effective at finding difficult to detect network-born threats, including those originating from IoMT devices.

Seceon's aiSIEM is unique in its ability to take automatic action to stop threats once it detects them. This is where the joint solution from CSPi and Seceon is so effective. Seceon can talk back via APIs to the resident in-line ARIA SDS devices to stop the specific threat conversations. This stops the threat while allowing critical applications and devices to continue to operate.

Since all other remediation techniques either take out the endpoint device entirely, block all communication from it, or shut down the critical applications the devices communicate with this makes the Seceon/CSPi solution all the more powerful because the typical security approaches can't perform any of these actions for the following reasons:

- It's not an option to take out the IoMT device since it has no EDR.
- Blocking all communication is possible. However, allowing the good communication while blocking the bad is critical if the endpoint in question must keep working. This is the case with pacemakers, insulin pumps, CAT scan machines, and the like.
- Stopping all communication from such devices could be life threatening. In addition, you may not know every device on your network and also don't want to worry about the underlying OS version being vulnerable to attack.

Another benefit of leveraging ARIA is that it allows medical facilities to forgo the normal worries about fitting a client EDR on their various devices and instead protect them in-line with fewer CSPi ARIA instances.

Securing Commercial IoT Devices

The combined CSPi-Seceon solution is not just for the IoMT devices; it also detects threats and protects the critical applications that the devices talk with and feed data to. In general, most SecOps teams are very uncomfortable running EDRs alongside critical business applications within a virtual machine (VM). Factors such as the stability of the EDR client and the competition for limited CPU resources can make the critical application unstable, crash, or become non-responsive when under load.

Deploying the CSPi ARIA instances in the network under the Seceon aiSIEM control helps SecOps teams to detect the threats from the NetFlow metadata. Once a threat is detected, the combined solution can shut down the specific threat conversation. This will stop the threat while the application is still able to run and perform its valued functions within the organization.

Finally, prevention is critical to keeping IoT devices talking to their proper controllers. The challenge is that nearly every microsegmentation solution on the market relies on an EDR solution to function. Again, that approach does not work on IoT. Fortunately, CSPi's ARIA can perform microsegmentation policy enforcement one step back in the network in order to properly enforce communication polices. Seceon's aiSIEM also plays a critical role as it can visualize the communication and can communicate via API to ARIA to set the enforcement policies. Visualization helps SecOps teams figure out what devices are communicating, and with which applications. Such information makes it easier to develop proper communication policies.

End-to-End Approach with MSSP

Seceon's aiSIEM has become a favorite solution of MSSPs with the advent of the aiMSSP solution—a multi-tenant variant of the aiSIEM. The combination of the aiSIEM/aiMSSP and the ARIA SDS give both enterprises and MSSPs a powerful new MDR solution capable of surgically stopping more threats within the network. Extending this unique combination into the IoT market gives the industry new tools to solve one of its most challenging security problems.

Summary

Seceon and CSPi provide a simple to deploy solution that secures your IoT environment by:

- Automatically detecting and stopping threats.
- Transparently deploys in the network, requiring no EDRs.
- Never disrupting your applications.
- Only stopping threat conversations, not your critical communications.
- Preventing the spread of threats from unsecured IoT into the rest of your environment.

About CSPi

CSPi Cybersecurity Products take a radically different approach to automated enterprise-wide data and application security by focusing on the data at its source, accelerating incident response and leveraging all internal network traffic for enhanced insights to detect and stop network born threats. Learn more at www.cspi.com/security

About Seceon

Seceon is focused on "Cybersecurity Done RIGHT". We empower organizations, of any size, to visualize, proactively detect known and unknown threats, automatically eliminate and or contain threats and achieve regulatory compliance through continuous monitoring, assessment, policy enforcement and reporting. Learn more at www.seceon.com