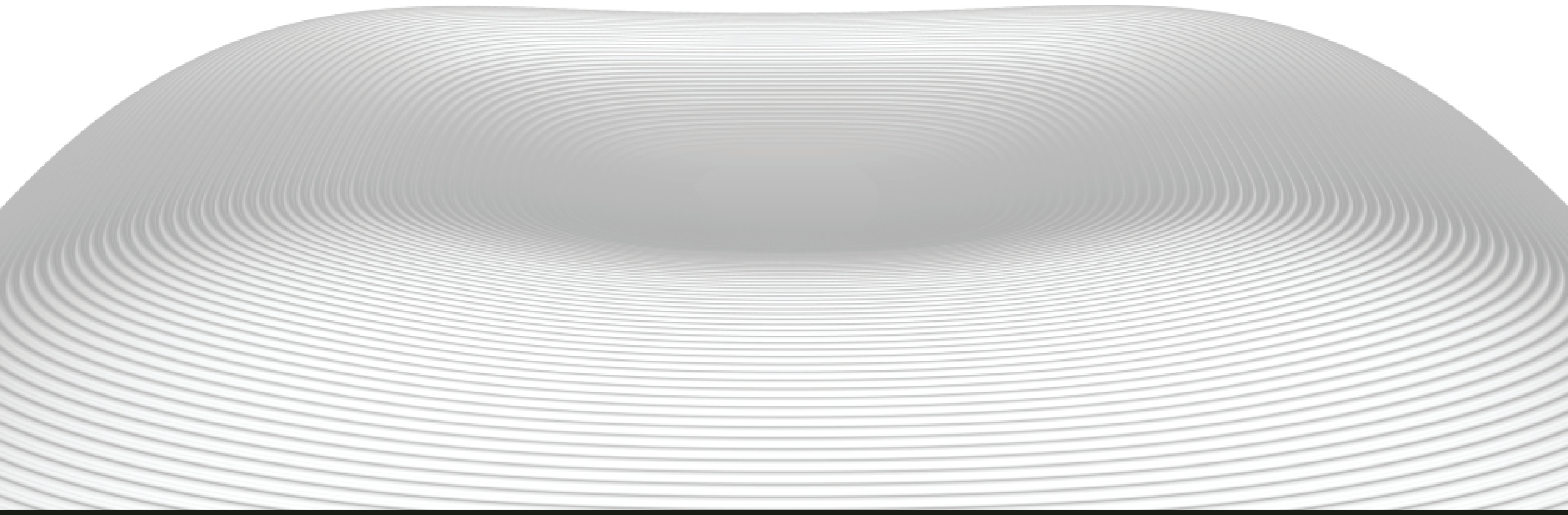
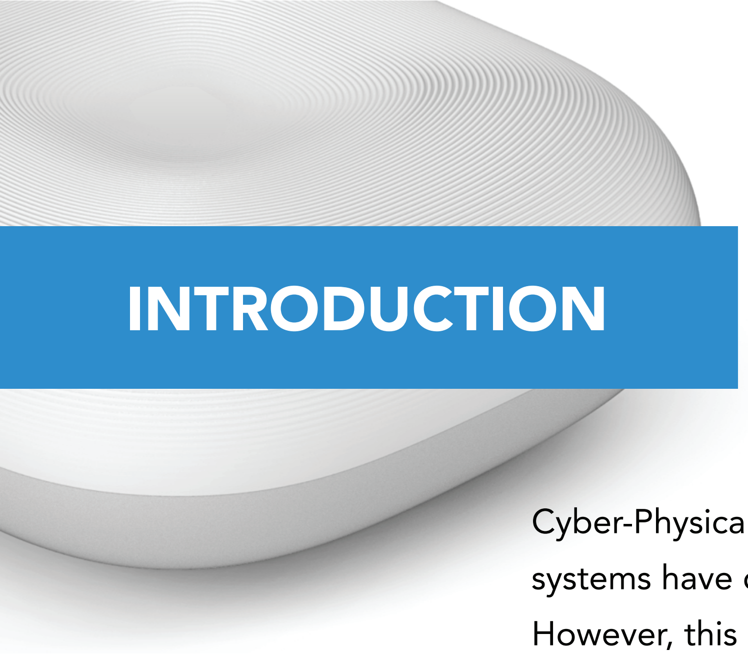
LOCH

Wireless IoT & OT Security for Cyber-Physical Systems and Operational Technology Networks

TABLE OF CONTENTS





INTRODUCTION

> Wireless is the New Frontier of IoT
>
> Garry Drummond, CEO LOCH Technologies, Inc.™

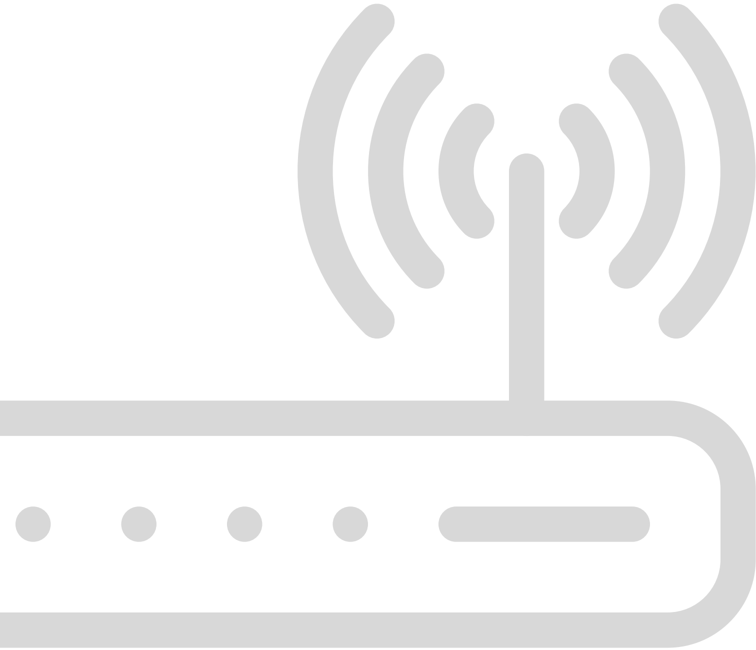
Cyber-Physical systems (CPS) and the convergence of IT and OT systems have challenged traditional security approaches; However, this new change has security and risk management leaders looking for a new vision and strategies to be able to detect, assess and prevent risk from this emerging new threat landscape.

75%

By 2023, 75% of organizations will restructure risk and security governance to address new cyber-physical systems and converged IT, OT, Internet of Things (IoT), and physical security needs. This is a significant increase from less than 15% today.

According to Gartner, By 2023, 75% of organizations will restructure risk and security governance to address new cyber-physical systems (CPS) and converged IT, OT, IoT, and physical security needs, which is an increase from fewer than 15% today.

Cyber-Physical Security has emerged as a relatively new term intended to address the convergence gap between Cyber Security of traditional networks and the emerging Physical Systems Security. This group of Physical Systems includes everything from an organization's Building Automation, such as IoT-enabled lighting, HVAC, and power. It also consists of the Industrial Internet of Things (IIoT) and OT (Operational Technology) consisting of wireless sensors and systems used across Smart Factory, Industrial Control Systems (ICS), Critical Infrastructure, and more.



80%

80% of new IoT and OT deployments are wirelessly enabled, not wired; therefore, wireless is becoming the first network and new attack surface.

Traditionally, these Physical Systems have either existed on a closed or separate network which is not connected to the Internet or the enterprise network. But with the explosion of IoT-enabled devices (including IIoT and OT), the risk landscape has vastly expanded, thereby putting these systems at risk of disruption and breaches just like we see on the enterprise network. To further complicate things, 80% of new IoT and OT deployments are wirelessly enabled, not wired; therefore, wireless is becoming the first network and new attack surface.

This new network connectivity creates a massive lack of visibility as Information Security teams have been focused primarily on monitoring the enterprise networks and not operational systems. These OT networks have been separate from the enterprise network in the past, which means a new security framework is required to understand the risk impact from this convergence.

KEY CHALLENGES

The goal of CPS security is to understand the changes within the physical environment, investigate their effects, and settle on a best-practice approach to any unacceptable exposure-states. At the same time, you want to be able to push out command and control orders to revert to a healthy working state.

2X

By 2020, spending on OT security will double due to increasing attacks on critical industrial infrastructure and subsequent regulatory responses.

The convergence of IT and OT systems is proving to be a challenge for security organizations. For all the benefits that convergence brings, the sheer volume of billions of intelligent IoT, IIoT, and OT endpoints is proving to be a cybersecurity nightmare as there is now an ever-expanding attack surface, with each device becoming a possible entry point.

New vulnerabilities are exposed everyday, and businesses not only have to stay compliant with ever-changing regulatory standards but also keep aware of new threats targeting OT operating systems and applications running within the environment.

The fact that wireless seems to be the preferred method of connectivity also creates a new set of headaches for organizations. According to Gartner, by 2020, "spending on OT security will double due to increasing attacks on critical industrial infrastructure and subsequent regulatory responses."

These challenges cannot be mitigated using traditional security approaches alone. Businesses need to adopt OT security best practices that fit this new converged environment optimally.

Regulatory compliance pressure is mounting as governments issue new guidelines to enhance the security of critical infrastructures. This comes with the need to keep costs down, remain competitive, and to stay informed of the new risks created by the IT/OT convergence.

Security risk leaders who are planning on converging IT/OT environments should consider the following best practice guidelines:

> Improve the security strategy with the use of a hybrid approach combining "wired and wireless" IoT/OT threat correlation to protect OT environments. The relationship should be based on a data-centric model and not a network-centric model, i.e., protection of the IP (intellectual property).

> Security risk leaders should reference security frameworks guidelines like CIS and IEC 62443 to protect their ICS environment. The three main classes of ICS are: Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Supervisory Control and Data Acquisition (SCADA). Cybersecurity controls should adhere to new regulations.

DIFFERENCES IN IT AND OT CYBERSECURITY CHALLENGES

Security Topic	Information Technology (IT)	Operational Technology (OT)
Wireless Instrution Detection	Common technology used to detect, assess and prevent risk. New IoT is pushing broader RF monitoring/detection. Part of Defense in Depth Strategy.	Not common, as not part of a Defense in Depth Strategy.
Asset Classification and Vulnerability Assessment	Typically performed on an ongoing basis, results help drive new budgets.	Only performed when regularity compliance is required, accurate inventories uncommon for non-vital assets. Vulnerability Assessment not common as scans are typically intrusive.
Incident Response and Forensics	Used as part of a SEIM (Security event information management) required for ease of development and scalibility, regulatory compliance drives budget for this technology.	OT is more focused on sytem availability and uptime, forensics procedures can be immature. Typically requires good IT/ICS relationships in place in order to complete tasks.
Patch Management	Easily defined, can be pushed-out to whole enterprise via remote and automated.	New patch installs take a long time to validate and get approved. OEM has different push mythologies and may break ICS functionality.
Technology Support Lifetime	2-3 years life cycle, multiple vendors in supply chain.	10-20 year life cycle, usually same vendor/supplier, product end-of-life can creates new security concerns.
Change Management	Regular and scheduled.	Requires strategic scheduling, nontrivial to implement on production / live systems.
Secure Systems Development	Key part of development process.	Not an integral part of the development process, slower adoption rate as IT and ICS engineering have different goals / scope of work.
Security Compliance	Mandatory and regulatory oversight gets avaliable budget, depending on sectors.	Depending on industry sector, compliance adherence will drive new budget.
Antivirus	Easily deployed and updated. Users have control over install, can be endpoint or enterprise push.	ICS systems have limited memory, organizations typically protect legacy systems only, usually requires non-instrusive updates only with minimal files.

IOT AND OT CYBERSECURITY BATTLEGROUND

As more IT and OT devices become Internet-enabled, they can be used as a launch-pad to hack into a company's network to exfiltrate data and bring down critical systems, or become an infection vector to spread malware.

The IoT revolution has introduced a wide range of consumer, enterprise, and industrial IoT devices. These devices communicate in a variety of ways unfamiliar to most organizations. Organizations lack insight into the many new operating systems, protocols, and frequencies that IoT, IIoT, and OT utilize.

Over the years, we have expanded from 4 primary operating systems (Windows, MacOS, iOS, and Android) to dozens of new operating systems with little standardization. Furthermore, an explosion in new IoT protocols and frequencies has created enormous new challenges for organizations. This inflection point requires a unique view of the attack flows with new countermeasures. With 80% of these new connections now wirelessly enabled, the organization must now adopt security controls that understand the broader radio frequency attack surface.

Most organizations focus predominantly on securing WiFi connected to their primary networked systems. However, the fast growth of new IoT devices has ushered in a new wave of operating systems such as Nucleus, Tizen, QNX, Green Hills, VxWorks, Riot, and many others that organizations are not equipped to manage and secure. In addition to the unsecured operating systems, new IoT devices communicate via a growing set of unprotected protocols, including ZigBee, Z-Wave, LoRa, Bluetooth, Sigfox, LTE, as well as frequencies outside of 2.4 GHz and 5 GHz. OT systems rely on protocols such as Modbus, OPC, and DNP3 for communications, and they very often lack security, authentication, and integrity in their communication stack. Organizations are blind to these devices in their environments, creating a security blind-spot.

The combination of these new IoT operating systems, protocols, and frequencies has created an original Critical Path to Exposure™ for adversaries. As this attack surface increases, it quickly becomes apparent that endpoint security is not the solution to the problem.

Lack of visibility

50+ Billion Devices by 2025

Lack of assessment tools

Plethora of new OS's and new software packages

ARMmbed
Google Developers
Green Hills SOFTWARE
TIZEN
NUCLEUS

Attack surface is increasing

Exploding number of protocols and frequencies

ZigBee
6LoWPAN
P25
Wi Fi
LoRa
Lte
sigfox
Z WAVE

Wireless sensors connected by the Internet-of-Things (IoT) are central to the design of advanced cyber-physical systems (CPS). In complex, heterogeneous networks, communication must meet strict requirements on throughput, latency, and range, while adhering to tight security levels. The gap between the security features in the communication standards used in CPS and OT and their actual vulnerabilities should be documented with practical examples and recent exploits to understand the risks and threat impact. The mass adoption of IPV6 enabled devices (e.g., IoT /OT sensors) in CPS and the increasing wireless connectivity have blurred the boundary between CPS and the Internet-of-Things (IoT).

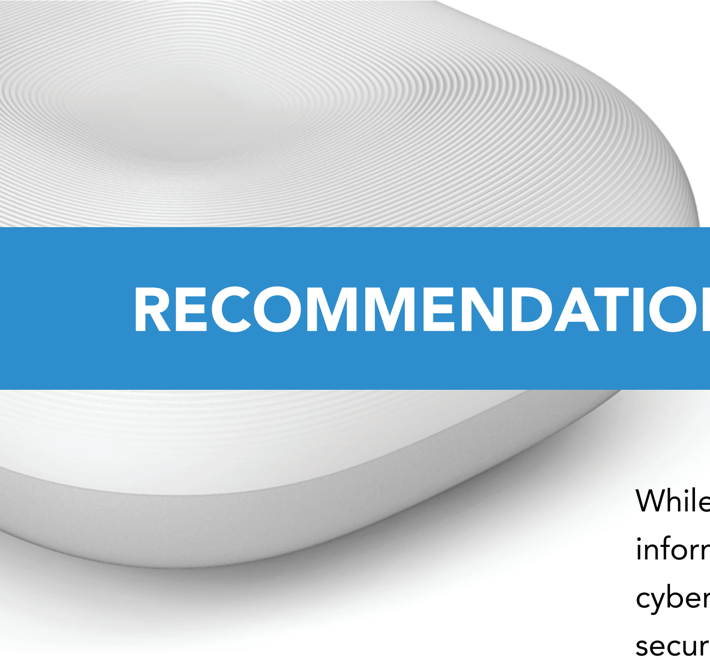
DESIGN SECURE CPS/OT SYSTEMS

Security policy – Security policies have to be implemented based on confidentiality, integrity, and availability. The focus should be given to specific application and requirements aspects.

Secure system – Network topology choice is also key and should be based on application requirements (proximity, bandwidth, and throughput). Options include Star Network, Tree Network, MESH Network and Cellular Network. Wired and wireless interoperability security controls should also be considered.

Secure inventory – Evaluation of components in the network is essential. Sensors, switches, and IoT devices all have assorted security flaws that should be recognized.

Security auditing – Continuous surveillance and monitoring should be set up to distinguish anomalies. According to the Verizon 2019 Data Breach Report studying over 56% of the company's clients, hackers were in the environment for a half year before being discovered.



RECOMMENDATIONS

While OT and IT security teams both need to secure their information systems, OT security experts tend to approach their cybersecurity frameworks differently in contrast to conventional IT security teams because they have different priorities.

For example, control engineers responsible for ICS systems tend to be reticent to upgrade their information systems even when it is sometimes necessary for security enhancement. This is because the focus is on maintaining uptime performance and overall systems effectiveness.

Crucial tenants in running a mission-critical ICS environment differ in many ways to an IT environment. In ICS the top priorities are:

> **Safety** is first, saving human lives takes precedence over a data breach. The fact that an organization could lose millions of dollars from a data breach is significant, but compared to a power outage affecting millions of users from loss of power or a compromise in a nuclear facility could be devastating.

> **Quality** in an industrial environment is everything; consistency is critical. Regardless of the finished product, any threat to quality output could be financially impactful.

> **Cyber** events that do not directly impact the operations are not a priority, focus on the ability to detect anomalies affecting quality is essential to the ICS process integrity.

> **Uptime** is critical within ICS environments. Cyber events can financially impact industrial organizations in several ways, from the theft of intellectual property to a denial of service (DoS) attack. Security firmware updates and patch management become a second thought.

A HYBRID MODEL APPROACH TO SECURITY

Protection of OT environments using a combination of traditional security controls and specialist controls offers a best practice approach. Air-gapping OT environments alone is insufficient protection from today's advanced threats because it can be next to impossible to isolate wirelessly connected OT networks and devices as they are exposed to various invisible risks.

Gartner cites LOCH as one of the vendors that security and risk management (SRM) leaders must consider for their OT asset discovery and monitoring.

For example, to secure OT networks, do not rely exclusively on traditional approaches such as stateful inspection firewalls, intrusion detection and/or intrusion prevention systems (IDS/IPS), or network access control (NAC) solutions only. Although they do provide some level of benefit, they are mostly reactive controls.   Depending on the unique security requirements of your OT environment, consider implementing additional measures like continuous OT asset discovery that is target-aware of the mission-critical data-centric intellectual property (IP) systems.

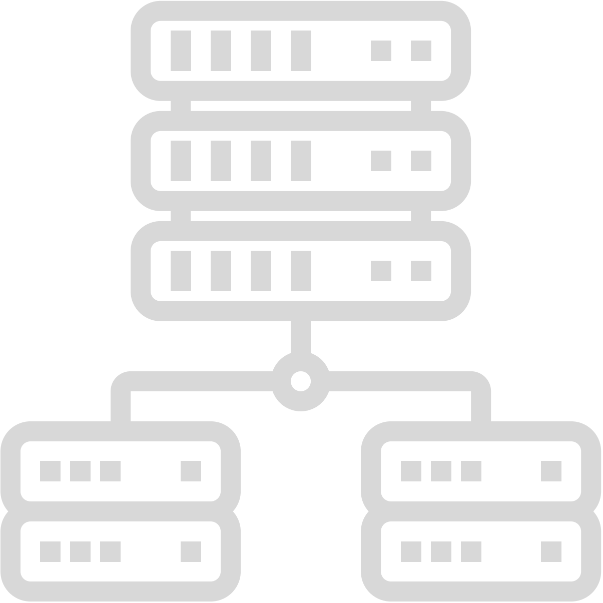
Implement Critical Path to Exposure monitoring that is dynamically in-tune with the ICS environment for both wireless and wired connections. This new data-centric approach, as compared to a traditional network-centric approach, is preferred.

According to Gartner, OT asset discovery and monitoring are among the most popular and effective OT specialist controls to secure OT environments. This approach supports the detection of anomalies, threats, and incidents. In the most recent OT Security Best Practices report, Gartner cites LOCH as one of the vendors that security and risk management (SRM) leaders must consider for their OT asset discovery and monitoring.

EXISTING CPS-OT SECURITY FRAMEWORK

LOCH is on the front lines of securing emerging attack technologies that are infiltrating the enterprise from both wired and wireless vectors. OT systems are now avaliable for a host of new operating systems, wireless protocols, and embedded processors affecting many IT/OT devices across smart grid meters, industrial equipment, point of sale devices, HVAC ventilation PLCs, and HMI, among other things.

The Purdue Model is reflective of best practice guidelines to help secure these systems, devices, and networks. This model can guide you through implementing a logical segmentation of your OT systems, as well as mapping the OT and IT networks and endpoints. This will enable you to better protect your facilities and identify the right controls to deploy.



This model, however, may not be sufficient for securing IIoT because these "things" communicate using new channels, protocols, and wireless standards. You cannot protect them using conventional security approaches, particularly those designed for wired technologies. It is now recommended that broader radio frequency detection be implemented to:

Assess the inventory of your enterprise IoT/OT devices

Prioritize device classification with protection measures, and use it to build appropriate controls

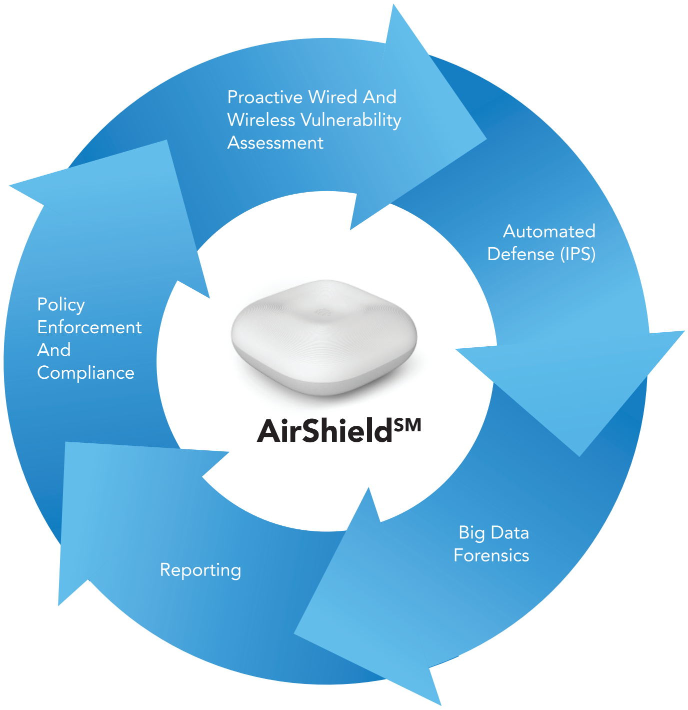
Raise awareness on the growing IoT/OT security risks

Anticipate future trends by implementing device visibility, continuous risk assessment, threat detection, and protection specific to IoT/OT devices.

When making decisions about refining your OT security, carry out an accurate asset inventory and vulnerability evaluation. Based on this inventory, implement a risk-based assessment that is data-centric, protecting the intellectual property on mission-critical systems. Create a plan of action guided by established frameworks such as Purdue, NIST, CIS, or IEC 62443, which address both IT and OT security as well as the physical and digital facets of your organization.

PREVENT, DETECT, ASSESS, RESPOND

Converged OT/IT infrastructures are exposed to various sophisticated threats that require more than just a preventive security approach. It is crucial that you can predict, detect, and respond to threats so you can proactively mitigate them. Below is an ecosystem of continuous improvement that will help implement a best practice approach.


Proactive Wired And Wireless Vulnerability Assessment
Automated Defense (IPS)
Big Data Forensics
Reporting
Policy Enforcement And Compliance
AirShield℠

PREVENT

Implement 1st line of defense — breach of policy

Baseline systems and security posture

Harden / patch systems

Isolate systems through segmentation

DETECT

Implement 2nd line of defense — identity and fix vulnerabilities

Assess risk — prioritize risk exposures

Implement intelligent driven orchestration

RESPOND

Critical Path to Exposure Reporting™

Remediate

Design policy change

Investigate incidents

ASSESS

Implement 3rd line of defense — target aware data-centric IDS/IPS

Inventory assests of critical systems and prioritize risk

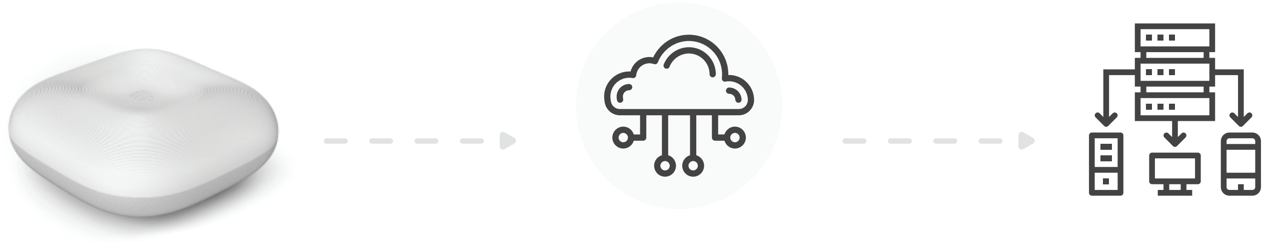
Contain incidents

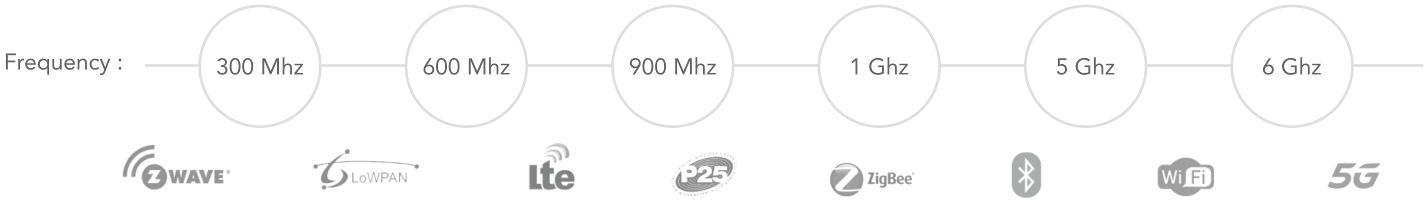
SOLUTION

With 80% of new IoT and OT deployment now being wirelessly enabled/connected, wireless is now the new network and new attack surface – the new frontier.

As IoT and OT endpoints provide an ever-expanding attack surface for hackers to compromise, companies need a continuous wireless monitoring solution that provides immediate visibility and cyber protection for both information technology (IT) and operational technology (OT) devices.

LOCH's AirShield^{SM} solution continuously monitors your air space, gathering information and behaviors about IoT and OT devices, checking connections and risk factors, classifying their purpose and more. It also offers complete control over the device activities at all times. Because each environment is unique, our customized software-defined-radios (SDR) is tailor-made for each environment which allows for the detection of specific RF communications and applications across the broader radio spectrum, alerting you to any deviation of policy or unacceptable exposure state – prior to loss or incident occurring.


Ethernet or Cellular Internet Connection
Cloud Deployment
Cloud - 125 million IoT Devices Profiled



BEYOND THE NETWORK

AirShield scans beyond the network to uncover risky IoT and OT devices and systems that pose a threat, compliance issue, or potential breach to company infrastructure, data, or safety across all Cyber-Physical Systems (CPS) environments.

BEYOND WIFI

AirShield looks at both the traditional WiFi 2.4Ghz and 5.8Ghz networks for rogues but also across Bluetooth, Bluetooth Low Energy, WISAN, 6LoWPAN, 802.11ad, UHF, RFID, NFC, ZigBee, Z-Wave, EnOcean, 2G/3G/4G/5G Cellular, and more, identiying wireless risks on other protocols and non-standard frequencies bringing visibility to the Internet of Things (IoT), Industrial Internet of Things(IIoT), Operational Technologies (OT) systems collectively known as cyber-physical things.

IOT FIDELITY

While traditional network monitoring products provide long lists of MAC addresses, AirShield wireless deep packet inspection is necessary to determine the fingerprint of an actual IoT device. For example, distinguishing between a surveillance camera vs. a spy camera significantly impacts the ranking of risk within an organization.

TARGET-AWARE IP PROTECTION

IOT-SHIELD compliments the AirShield platform by providing real-time visibility and threat analytics across both wired and wireless IT/OT/CPS environments. This unique approach will allow customers to implement their 1st, 2nd and 3rd lines of defense:

> **1st Line of Defense** — alert notification to any deviations of policy. An inventory assessment of your IoT/OT devices. A measurement of what “should be” against “what is”.

> **2nd Line of Defense** — identify and fix any unacceptable IoT/OT vulnerability conditions —prior to loss to loss or incident occurring. Prioritize devise classification and protection, and use it to build the appropriate controls.

> **3rd Line of Defense** — target-aware data-centric incident response solution that’s dynamically in tune with the ever changing network environment as well as building intelligent driven orchestration in mission critical environments.

The reason for this is that, according to Forrester, 68% of security technology decision makers state that using automation and orchestration tools to improve security operations is a high critical priority.

CONTACT INFORMATION

Garry Drummond

CEO and Founder, LOCH Technologies, Inc.™

Tel: 510-703-6149
Email: gdrummond@loch.io

Kurt Grutzmacher

Co-founder and Chief Scientist, CTO

Tel: 415-238-2571
Email: grutz@loch.io