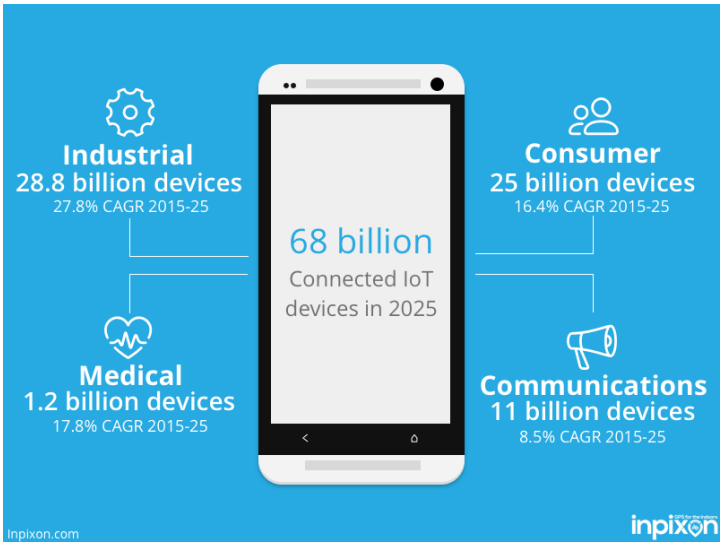
Physical Cybersecurity — Securing the Internet of Things

Internet of Insecure Things



This year there will be 20 billion Internet of Things (IoT) connected devices, with an economic impact of nearly $2 trillion. IoT is poised to supercharge the economy, enabling new business models and applications. But with these new opportunities come new threats.

No longer needing wires to connect, Wi-Fi, Bluetooth, LTE, or ZigBee allow IoT devices to connect through the airwaves. The world of IoT means increased connectivity, speed and efficiency for organizations of all kinds, but this brings the risk of infinite new attack vectors in this Internet of Insecure Things.

Security professionals are realizing that the new attack vectors can be used to gain access to valuable intellectual property, personably identifiable information (PII) and organizational assets. How can you develop comprehensive, 360-degree, wireless cyber situational awareness of how radio frequencies are being used in your environment?

Enter **Inpixon Indoor Positioning Analytics (IPA)**, a solution that allows security and operation teams to **detect**, **prevent**, and **continuously protect** the radio airwaves to mitigate risks posed by the Internet of Insecure Things.

IoT Threats	Inpixon IPA Response
Bluesnarfing, bypasses traditional network security, accessing information through mobile devices.	Inpixon IPA **detects** who is using Bluetooth devices and **monitors** if the pairing is with a known device or something that should be investigated.
Easily hidden **wireless audio and video recorders** are small, cheap and able to capture private conversations.	Inpixon IPA **detects** and locates all unfamiliar wireless devices **protecting** your environment from spying and espionage.
Rogue access points can impersonate legitimate Wi-Fi networks, allowing remote exfiltration of your data.	Inpixon IPA **detects** all access points, identifying when an unknown access point is activated, **preventing** access from those trying by-pass all your security measures.
Rogue cell towers can hijack cellphone connections, attackers can listen to calls and read texts.	Inpixon IPA **detects** all cellular signals which are then displayed on a floorplan of your premises, allowing monitoring of devices and **protect** information from outside access.
Wireless mice and **keyboards**, have vulnerabilities, allowing key stroke logging, exposing usernames and passwords.	Inpixon IPA **detects** any wireless device communication **protecting** you from any unapproved wireless peripherals, **monitoring** how they can affect your company.
Unapproved cellular devices break company "No Cell Phone Zone" policy in their sensitive areas, allowing data loss	Inpixon IPA **detects** and identifies all cellular devices , distinguishing between authorized and unauthorized devices, **continuously protecting** your premises.
Building control systems connects to the internet for ease of access and remote control without security policies in place.	Inpixon IPA **detects** any wireless signals and monitors interconnections between devices, so you can find and **continuously protect** against vulnerabilities in the IoT ecosystem.

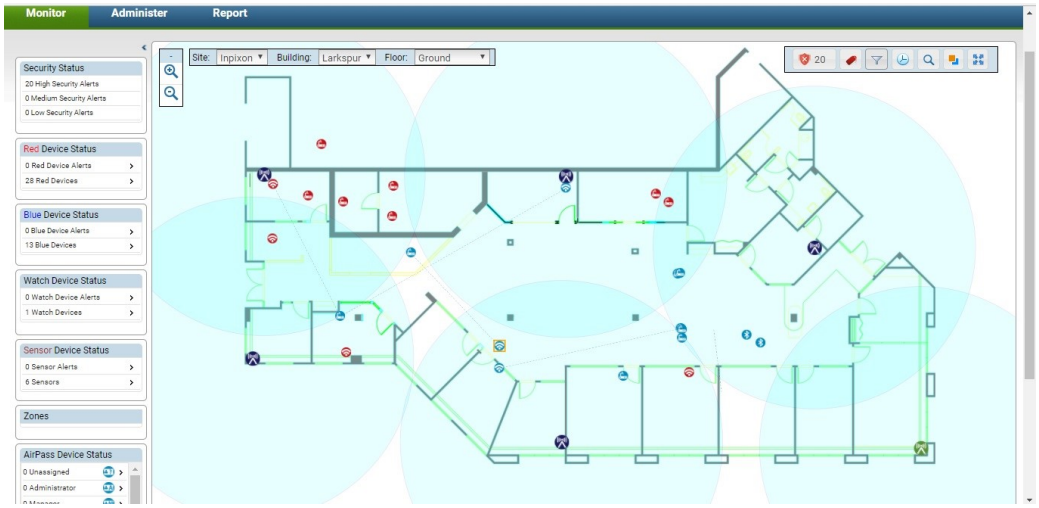
"We earn our customers' trust by continuously investing in technologies that improve our security posture. We're thrilled to select Inpixon's cutting-edge technology and analytics solution to enable our business to operate more optimally and securely." — Benson Choo, SVP & Manager, Information Systems & Technology

Hawaii's largest locally-owned depository financial services loan company, Finance Factors, has chosen Inpixon's Indoor Positioning Analytics (IPA) to maintain the security and privacy of their customer data and better secure its wireless environment.

IoT Evolution Magazine has named Inpixon IPA a 2017 IoT Security Excellence Award Winner. "It excites us to see the latest innovative products and solutions in the IoT Security industry, as we look forward to seeing their future successes!" - said Rich Tehrani, CEO, TMC

Security for the Internet of Insecure Things

Inpixon IPA scans the entire radio spectrum, identifying transmitting devices, creating a security dome over your sensitive operational spaces. Once collected, the data is analyzed and displayed on a floorplan of your premises, so that you can understand what devices are transmitting data, and from where within the security dome you have established. Inpixon IPA allows you to establish secure and unsecure zones on your premises and continuously monitors these zones to protect against and alert on a breach. In addition to securing spaces, Inpixon IPA can tag devices as known and trusted (default blue), so you can monitor when an untrusted device (default red) enters or when an asset (blue) is removed from a secure zone.



Inpixon Indoor Positioning Analytics pinpoint the location of any IoT device in your premises

Key Benefits

Detect

- Establish baseline of all devices on premises
- Find all devices emitting an RF signal
- Identify and tag authorized devices
- Remove potential threats before they can cause an issue

Protect

- Establish rules for new devices entering a space: public, private, secure zones
- Investigate unknown devices and determine threat level
- Use MDM where appropriate for employee mobile devices
- Extend uses of IPA, i.e. use IPA with an MDM for location based authentication
- Allow trusted devices in secured zones and locate the unknown ones real-time
- Alert for any breaches into secured zones

Continuous Prevention

- Track assets and devices throughout your premises to uphold policies
- Know where all critical devices are and when a device leaves
- Secure your customer data and intellectual property
- Enable staff to resolve issues in real time and forensically

Visit us today! www.inpixon.com/IPA