INDUSTRIAL AND MANUFACTURING IoT

Security for Industrial and Manufacturing Environments

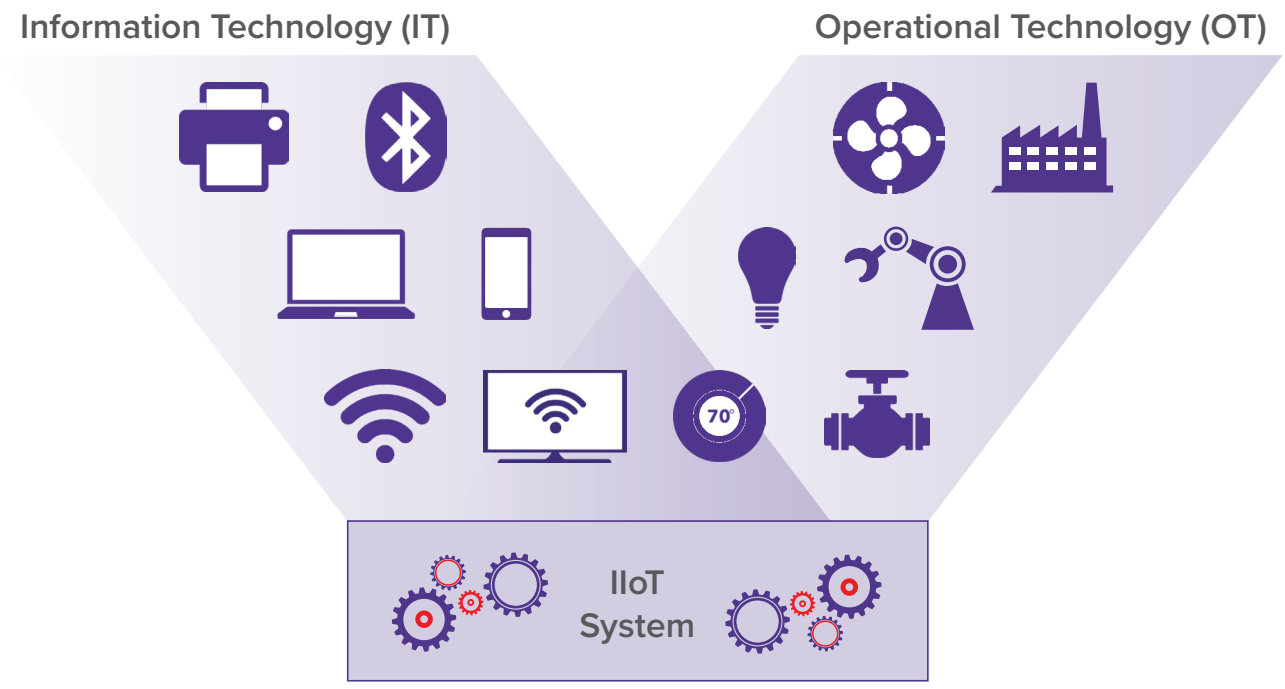
The convergence of IT and operational technology (OT) is giving rise to Industry 4.0 initiatives and the Industrial Internet of Things (IIoT). It also gives rise to an expanded attack landscape that needs to be protected.

The convergence of IT and operational technology (OT) is giving rise to Industry 4.0 initiatives and the Industrial Internet of Things (IIoT). This white paper will explore security issues associated with IIoT devices and propose some ways to address the problem.

For many years, industrial and manufacturing technology – often called “Operational Technology” or OT – has been relatively safe from cyber attack. The control and telemetry systems used in industrial and manufacturing environments were typically placed on isolated or “air gapped” communication networks, and the systems themselves were based on highly specialized operating systems which were relatively immune to attack.

All of this is changing. Device manufacturers are increasingly building OT devices that run on common operating systems such as Windows, Linux, and Android. In addition, device manufacturers are teaching those devices how to communicate using standard IP protocols. And finally, enterprises are increasingly connecting their OT devices and management systems directly to their IP networks – thus removing the air gap – because it is useful for traditional IT systems to be able to acquire information directly from the OT devices for planning, analysis and forensic activities. This is driving a vast range of efficiency initiatives under the umbrella term “Industry 4.0”.

The convergence of OT with IT has created a new class of devices commonly known as the Industrial Internet of Things – IIoT. These devices are exposed to many of the same security risks that traditional computers are exposed to.



THE SCOPE OF THE IIOT SECURITY PROBLEM

IIoT is being used in all of the traditional places where OT has been used. This includes:

- Programmable logic controllers (PLCs)
- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)
- Distributed control systems (DCS)
- Manufacturing execution systems (MES)
- Telematics
- Robotics
- Fleet management systems
- Building automation systems

The convergence of IT with OT gives cyber attackers a greater opportunity to affect the physical world and possibly impact the safety and lives of people. Water treatment, air quality, traffic control and other public safety systems that are accessible via the internet expose society to significant potential risk. Traditional malware attacks on IT can be a nuisance, but attacks on OT can have a real impact on the physical world.

A cyber attack that contaminates the water supply, or takes out the electric grid, or causes a deadly catastrophe at a manufacturing facility may seem like something that only happens in a cyber thriller novel. With each passing year, however, the line between operational technology systems and standard IT networks gets blurred, which means those events are increasingly a very real possibility. It is also a very real possibility that hackers can make minor changes and small shifts in how these devices function--either intentionally or inadvertently--that may have a massive impact on performance and output.

Certain industries seem to be at greater risk than others. For example:

Manufacturing

Most—if not all—manufacturing facilities use PLCs and SCADA systems to automate and manage the production process. In many cases, IIoT devices are used to monitor and control various aspects of the manufacturing process.

Energy

IIoT plays a crucial role in the energy sector. Water treatment, natural gas delivery, and production of electricity—whether from coal, water, nuclear, or other sources—all depend heavily on industrial control systems (ICS) which are being upgraded to run on IP-based operating systems.

Distribution

Inventory and tracking systems often leverage IIoT. Warehouses and distribution logistics use IIoT systems to accurately track items and help to automate the process of getting things from point A to point B efficiently.

Transportation

Fleets of vehicles—whether it's a fleet of buses for school or public transportation, a fleet of taxi cabs, or a fleet of delivery vehicles—often rely on IIoT. Similar to the way it's applied in Distribution, the transportation sector can use IIoT to efficiently manage fleets and make sure everything gets where it's supposed to go.

Infrastructure

Traffic control and railway systems use IIoT to manage the flow of cars and trains. IIoT is crucial for effective transportation and distribution within the public infrastructure, and play a critical role in protecting the safety of people as well.

THE STATE OF OT SECURITY – THE NEW ATTACK LANDSCAPE

The good news is that while risks have increased, so has awareness of the challenges. A SANS survey from June of 2017 provides tremendous insight into the current state of OT security and how organizations are addressing the problem.

The SANS report states: "Recognition that even dedicated, special-purpose ICS components, such as intelligent embedded devices and programmable devices that are used for command and control, can carry vulnerabilities exploitable by malefactors is increasing among ICS security practitioners and the broader security community, as is concern about ransomware, which has started to invade the corners of almost any digital system."

Here are a few of the key findings from that survey:

- Almost 7 in 10 of those surveyed believe that the threat to ICS is high or severe / critical.
- 44 percent of respondents consider the top threat vector to their ICS to be adding devices to the network that are unable to protect themselves.
- About a quarter of the survey participants consider embedded controllers to be at greatest risk and 32 percent believe the impact of that risk is the greatest in the event of a compromise.

In the "The State of Cybersecurity in the Oil & Gas Industry: United States" by Ponemon, 68% of respondents say their operations have had at least one security compromise in the past year, resulting in the loss of confidential information or OT disruption. 61% of respondents say their organization's industrial control systems protection and security is not adequate.

OIL & GAS COMPANY SECURITY ISSUES

68%

have had at least one security compromise in the past year, resulting in the loss of confidential information or OT disruption

61%

say their organization's industrial control systems protection and security is not adequate

The State of Cybersecurity in the Oil &Gas Industry: United States, Ponemon Institute LLC, February 2017

REAL WORLD EXAMPLES OF IIoT ATTACKS

Don't be fooled into thinking these attacks aren't truly possible. It's already happening.

- **December 2015:** The Ukraine suffered a series of outages of the electric grid that caused approximately 225,000 customers to lose power for a number of hours. Investigation of the event revealed that it was the result of a cyber attack—allegedly a state-sponsored attack from Russia. Foreign attackers were able to gain access from the Internet to the power utility's corporate IP network, which was connected to the Industrial Control System network. Thus they were able to enter the ICS network and remotely control the SCADA distribution system for the Ukrainian electric grid, disconnecting various substations.

- **March 2016:** Hackers were able to infiltrate and compromise the control systems of a water treatment facility. The actual utility and city affected have been changed in published news reports to conceal the true identity and location, but the rumor is that a Syrian hacktivist group was able to use a phishing attack and SQL injection (SQLi) to obtain access to the AS/400-based operational control system through a front-end web server. The hackers were then able to control the PLCs that regulated valves and managed the flow of chemicals used to treat the water—threatening the health and safety of the citizens served by that water treatment plant. A similar incident occured in 2011 with the Water and Sewer Department for the city of South Houston when hackers were able to infiltrate the network.

- **March 2017:** The WannaCry ransomware attack spread quickly across the internet, infecting machines and encrypting data until the ransom demand was paid. The National Health System (NHS) in the United Kingdom was hit, and healthcare was effectively shut down for a period of time. Hospital employees were locked out of systems and did not have access to critical patient data. Had internet-connected OT control systems been compromised and encrypted, a ransomware attack like WannaCry could have devastating impact.

In addition, malware designed specifically for IIoT is starting to appear for the first time. Security researchers recently demonstrated PLC-Blaster, a worm that lives solely in a PLC and scans the IP network to identify and spread to additional vulnerable PLCs.

Thankfully, we haven't yet experienced a massive IIoT-related catastrophe, but it seems like it's only a matter of time. As attackers adapt and learn more about navigating and managing OT systems, utilities, manufacturing facilities, traffic control, and other crucial networks may be compromised.

THE NEW TECHNICAL CHALLENGES OF IIoT SECURITY

There are several technical challenges that make it difficult to protect IIoT devices and to identify when they have been attacked.

1 Lack of Visibility

Unlike traditional IT devices, IIoT devices are typically not able to run an agent that can provide visibility to the devices. Tools exist that can scan an IP network in order to develop an inventory of assets and known vulnerabilities, but using these scanners to discover IIoT devices is not wise because the scanning disrupts many common IIoT devices and can cause those systems to crash.

2 Persistent Software Vulnerabilities

As previously stated, IIoT devices typically run reduced versions of standard operating systems like Windows, Linux and Android. However, IIoT devices typically cannot be patched by the IT department. Thus, the set of known vulnerabilities in these devices tends to increase over time.

3 Rampant Connectivity

Traditionally, the air gap has been a mainstay of OT network design. The belief was that only a physical gap between networks (both OT-to-OT and OT-to-other) could guarantee an appropriate level of protection for high-risk systems. The air gap is gradually eroding as more IT systems require information from OT systems to perform planning, analysis and forensic activities and as manufacturers include multiple forms of wireless and out-of-band connectivity that bypass the air gap, for example Bluetooth®, Near Field Communication (NFC), etc.

PROTECT IIoT WITH ARMIS

Armis is purpose-built to protect industrial environments from the risks associated with IIoT devices. Armis' agentless IoT security platform provides three essential capabilities:

1 Discover

Armis allows you to see all devices in your environment, both on and off your network. The reason why it is important to see devices that are off your network is because some IIoT devices are not constrained by traditional network boundaries. Attackers can use exploits such as BlueBorne, KRACK and Broadpwn to compromise IIoT devices over the air, without any user interaction.

Through a simple out-of-band connection to your network, Armis passively monitors traffic and is able to profile and classify IIoT devices, connections, applications and operating systems. Armis shows you the devices and the connections that exist, including connections to unmanaged devices or rogue networks that you might not be aware of. This is a unique Armis capability.

Armis maintains a Device Knowledgebase of over 8 million device profile characteristics which allows us to accurately classify almost all of the devices in your environment - managed and unmanaged endpoints, as well as non-traditional devices that are commonly found in industrial environments.

All the information that Armis discovers is displayed in an easy-to-use dashboard.

2 Analyze

Armis' cloud-based risk analysis engine compares device behaviors that we observe in your environment to our Device Knowledge Base which contains a baseline of normal behavior for each type of device. The Device Knowledge Base contains over 8 million individual device profile characteristics including such things as how often each device typically communicates to another device, over what protocol, how much data is transmitted, etc. The baseline includes historical observations in your environment, observations in other customer environments, and claims from device manufacturers. This allows us to detect threats from "patient zero" devices much faster, and with fewer false positives, than traditional security products that simply look for deviations from historical patterns or signature-based pattern matches.

Armis displays alerts corresponding to the risks and threats that we perceive on and around your network. Each alert includes drill-down capability so you can see the basis for each alert. Armis scores each device on the basis of thirteen different characteristics and behaviors.

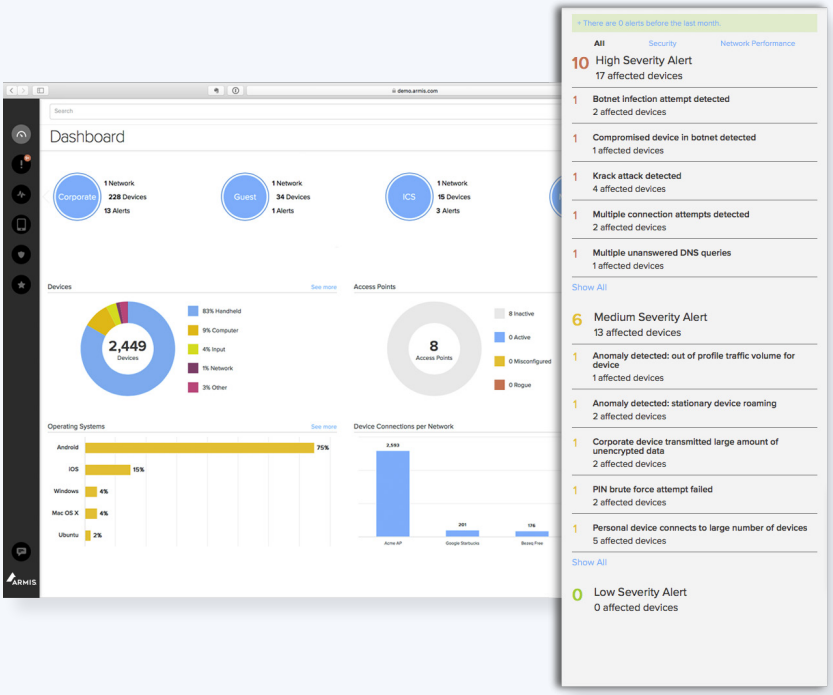
Armis can send alerts to your SIEM, if you have one. Typically, Armis is the primary source of information for IoT devices and the sole source of information for devices that communicate through Bluetooth, BLE, WiMax, Zigbee, and other IoT protocols.

Armis maintains a complete history of devices in your environment including their connections and behaviors. This is useful for forensics following an observed attack.

3 Protect

Once the Armis Risk Analysis Engine determines that there is a significant risk on your network, or once a security policy that you have defined has been violated, Armis allows you to automatically or manually block the device and/or restrict communication. Since Armis operates out-of-band, these actions are taken by your existing network infrastructure such as your switches, wireless LAN controller, firewalls, or whatever network access control system you might have in place. Armis is able to integrate with these systems and send triggers when needed.

Armis is even able to control connections with things that are outside the boundary of your traditional network. For example, Armis is able to stop a corporate device connecting to a rogue 802.11 network, to a Pineapple device, or to a Bluetooth device. This is another unique Armis capability.



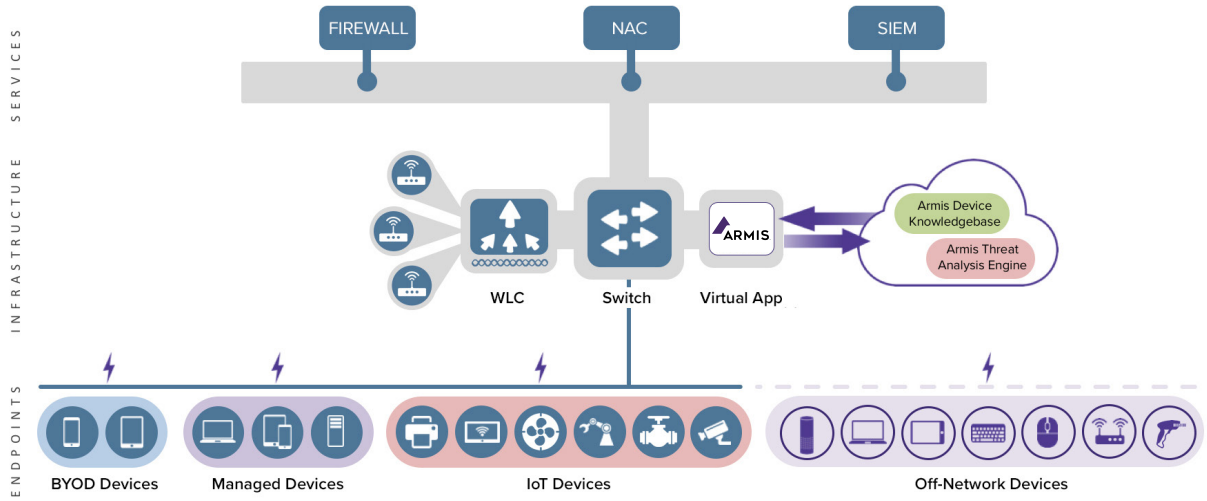
Armis Risk Analysis Engine discovers a wide range of hidden threats on your network.

Armis discovers risky devices and malicious behavior on your network.

FRICTIONLESS DEPLOYMENT

Most IIoT devices can not accommodate a security agent. For this reason, Armis has been designed to work without an agent. This also makes Armis easy to deploy. There is nothing to install on a device nor any sort of invasive access (scanning or remote login) to endpoints.

Armis runs on your network as a virtual appliance, passively collecting information. It requires a simple user account on your existing wireless LAN controller and, optionally, connections to your wired network via a SPAN port and to your existing firewalls. Complete installation typically take only minutes to a few hours, depending on the environment.



Simple installation with no agents or hardware required

CONCLUSION

Operational technology is not new, but the convergence of OT with IT has produced a new type of device called IIoT which exposes industrial and manufacturing enterprises to much greater risk than ever before. The growing usage of IIoT throughout many industries and market sectors, combined with the increased attacks on these unprotected devices that could result in potentially catastrophic consequences, make IIoT security a paramount concern.

There are a variety of unique challenges associated with securing and protecting IIoT, but it can be done. Armis can provide the visibility necessary to inventory, assess, monitor, and protect all devices on your network—including IIoT devices and unmanaged devices.

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 armis.com