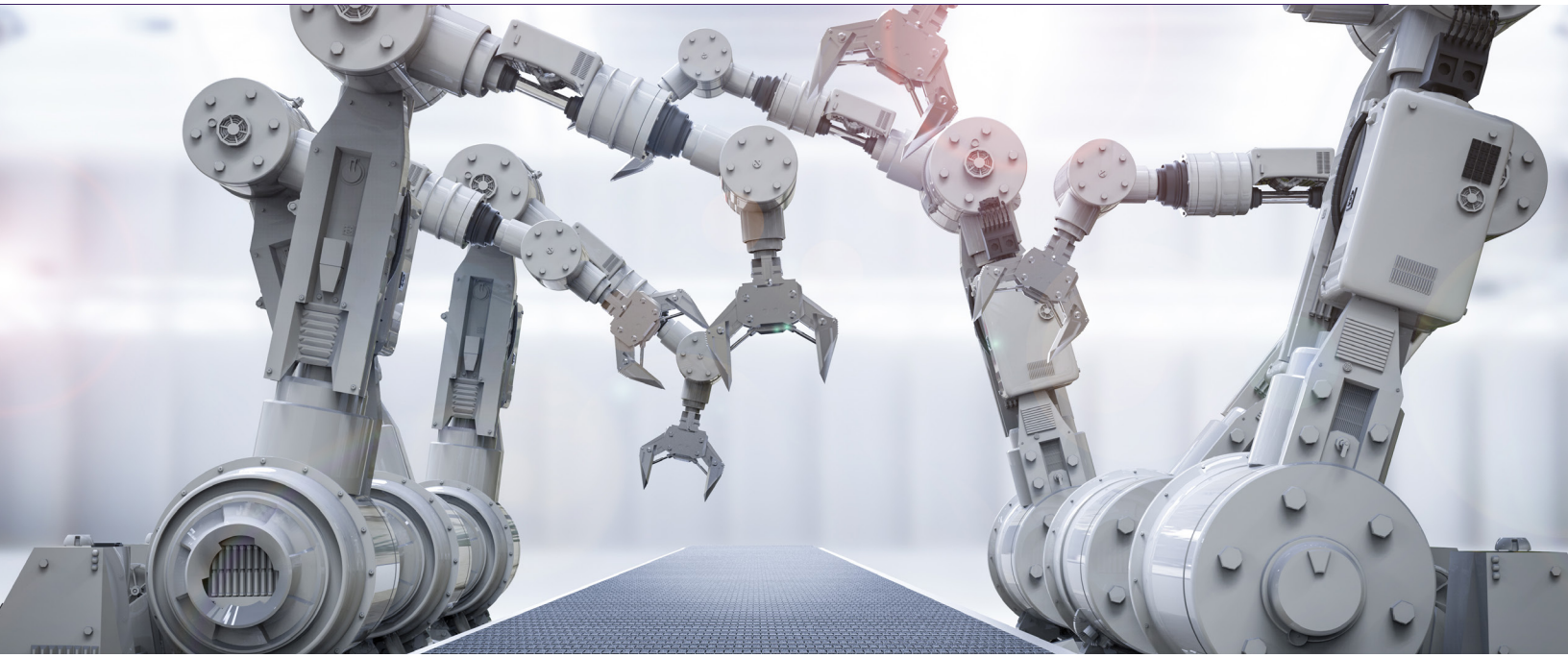
SECURING IT AND OT

in Industrial and Manufacturing Environments

The security needs of Industrial Control Systems (ICS) and Operational Technology (OT) environments are changing as these environments are rapidly being connected to enterprise networks and exposed to hackers and Internet-borne malware. What is needed is a new generation security solution that secures connected devices spread across both industrial and IT environments.



INTRODUCTION

For many years, industrial control systems—often called “Operational Technology” or OT—have been relatively safe from cyber attacks. The control and telemetry systems used in industrial plants 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 difficult to attack because they were relatively obscure and unknown to most attackers.

All of this is changing. Control system architectures are being connected to traditional enterprise IT networks (Ethernet, Wi-Fi, etc.), and device manufacturers are building OT devices and control systems on top of common operating systems such as Windows, Linux, Android, and VxWorks. These changes increase the risk that control systems can be compromised by the same kind of attacks used to compromise devices on corporate IT networks. According to a commissioned study conducted by Forrester Consulting on behalf of Armis, 66% of manufacturers have experienced a security incident related to IoT devices over the past two years.[1]

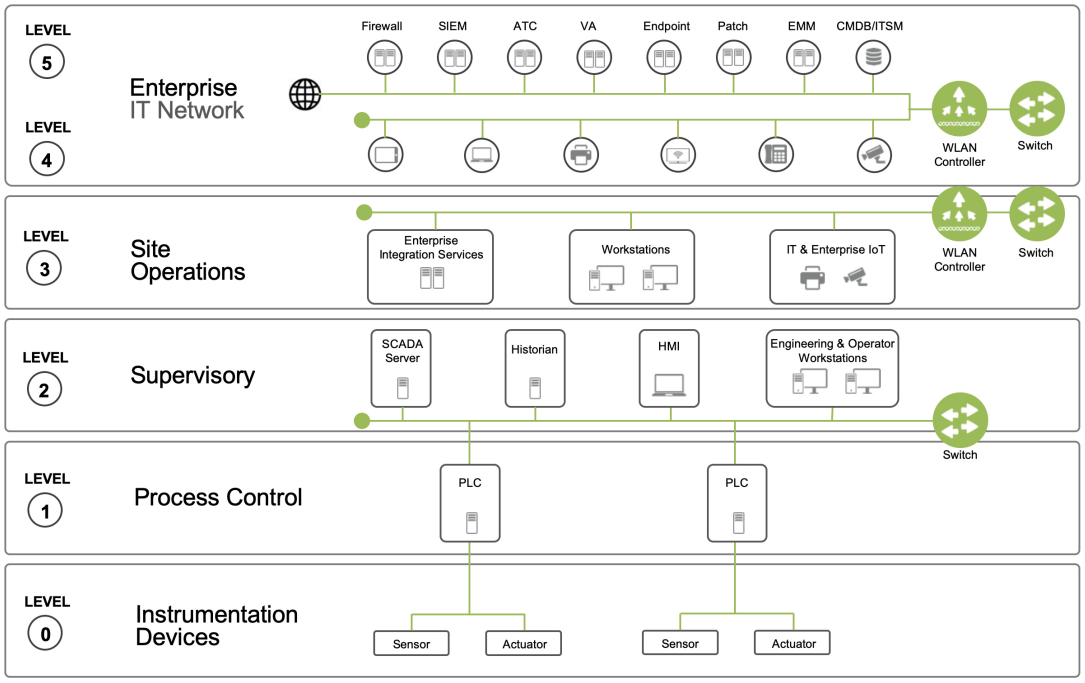
This white paper explores the cyber security challenges in manufacturing and industrial environments and propose ways to address them.

THE AIR GAP IS DISSOLVING

Although many legacy control systems still maintain an effective air gap, the trend in manufacturing and industrial plants is to connect OT devices directly to the enterprise network. As a result, the Purdue Enterprise Reference Architecture, which for years indicated a standard hierarchy of applications, controls, data flows and enforcement boundaries, is being flattened and the lines between levels are dissolving.

To determine the extent of these changes, the SANS Institute conducted a survey in 2018.[2] The results indicated that devices at all levels of the Purdue model are now routinely being connected to enterprise networks using a variety of communication technologies—wired, Wi-Fi and cellular. On average, SANS reported 37% of devices in the Manufacturing Zone (Purdue levels 0, 1, 2 and 3) were connected to enterprise networks, and 32% of IIoT devices were connected directly to the Internet.

The Purdue Enterprise Reference Architecture



These architectural changes are happening across many different kinds of control systems, including:

- Programmable logic controllers (PLCs)
- Supervisory control and data acquisition (SCADA)
- Distributed control systems (DCS)
- Manufacturing execution systems (MES)
- Telematics
- Robotics

OT DEVICES ARE UN-AGENTABLE

OT devices in industrial and manufacturing environments often have no built-in security, nor can you install a security agent on them. They are “un-agentable”. They were designed this way by manufacturers who were operating on the (now invalid) assumption that these devices would not be installed on a network that conveys any type of threat. However, the convergence of IT and OT networks means this is no longer the case. The devices are now exposed to many types of threats coming from the Internet and/or the larger enterprise network.

The fact that OT devices cannot accommodate security agents robs security managers of visibility to what the device is, what risks it harbors, and whether it is behaving outside the norm.

RISKS TO OT SYSTEMS ARE INCREASING

Not only are OT devices increasingly accessible by cyber attackers (due to the dissolution of the air gap), they are also increasingly vulnerable to attacks. Year over year, the number of vulnerabilities in OT devices as well as breaches to operational infrastructure continues to increase.

In July of 2020, NSA and CISA warned that cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against critical infrastructure (CI) by exploiting internet-accessible operational technology (OT) assets[3]. The agencies recommended that organizations take immediate actions to reduce exposure across operational technologies and control systems.

OT Device Vulnerabilities & Breaches

- July 2019: URGENT/11 affects billions of industrial and medical devices
- June 2020: Ripple20 TCP/IP vulnerabilities affect more industrial devices
- July 2020: NSA and CISA warn of the OT/ICS “Perfect Storm”
- January 2021: Westrock core OT systems attacked
- February 2021: Oldsmar Water Treatment facility control systems breached
- April 2021: NAME:WRECK vulnerabilities discovered affecting OT devices
- April 2021: MSFT discloses Bad:Alloc vulnerabilities affecting OT devices
- May 2021: Colonial Pipeline infrastructure shutdown

ICS-CERT's advisory page shows that a large number of vendors have disclosed vulnerabilities.[4] Here is a representative list:

Vendors with Disclosed Vulnerabilities

ABB	General Electric	Moxa	SCADA Engine
Advantech	Geutebruck	Omron	SICK
Adcon Telemetry	Hetronic	OSI soft	Schneider Electric
Computrols	Honeywell	Panasonic Control	Siemens
Delta Electronics	Horner	Philips	Thales
Emerson	Janitza	Phoenix Contact	Tridium
eWON	Johnson Controls	Quest	Unitronics
Flexera	Kunbus	Red Lion Controls	WAGO
Fuji Electric	Microsoft	Rockwell Automation	Weidmueller
GarrettCom	Mitsubishi Electric	Sauter	Yokogawa

Not only are OT devices increasingly vulnerable to attack, but they typically are not able to accommodate a security agent that could possibly monitor and protect the device from attack. This design choice allows the device manufacturer to maximize economy and power efficiency, which in the past (and arguably still) have been seen as more important than security.

URGENT/11

URGENT/11 is a set of eleven zero-day vulnerabilities that were discovered by Armis. URGENT/11 impacts the following Real Time Operating Systems (RTOS):

- ✓ VxWorks® by Wind River
- ✓ ITRON by TRON Forum
- ✓ Integrity by Green Hills
- ✓ Nucleus RTOS by Mentor
- ✓ OSE by ENEA
- ✓ ThreadX by Microsoft
- ✓ ZebOS by IP Infusion

DEVICE TYPES

Real Time Operating Systems are used by SCADA systems, industrial controllers, PLCs, firewalls, routers, satellite modems, VoIP phones, printers, and many other devices. Soon after URGENT/11 was announced, equipment manufacturers including ABB, Belden, BR Automation, Rockwell, Schneider Electric and Siemens announced that their equipment was based on VxWorks and was impacted by URGENT/11.

RISKS

- Attackers can remotely exploit and take over mission-critical industrial and healthcare devices, bypassing traditional perimeter and NAT security.
- Once a single device has been compromised, other devices can be compromised quickly and easily, similar to the “wormable” vulnerability EternalBlue.

The complete report detailing URGENT/11 vulnerabilities is available at armis.com/urgent11.

MODIPWN

MODIPWN is a new vulnerability (CVE-2021-22779) in Schneider Electric Modicon PLCs that bypasses security mechanisms added to these PLCs to prevent abue of undocumented Modibus commands.

PLC MODELS

- Modicon M340 and M580 PLCs

RISKS

- Attackers can take over Modicon M340, M580, and other models from the Modicon series of PLCs.

WannaCry and NotPetya malware had major impacts on manufacturing companies like Merck, causing hundreds of millions of dollars in quarterly losses due to production downtime, in addition to loss of customer satisfaction due to missed shipments.[5] Five Renault-Nissan factories halted or reduced production, causing significant losses.[6] After suffering a WannaCry attack across its worldwide network, Maersk lost communication with its OT network, shutting down entire ports.[7] The digital systems at the smelting plants of Norsk Hydro, one of the world's largest aluminum producers, were shut down after the firm was attacked by LockerGoga.[8] Norsk Hydro reportedly lost $40 million because of the incident, and aluminum prices were driven to a three-month high. Details were not confirmed, but it is known that PLC, ICS engineer laptops, and SCADA systems commonly run Windows operating systems and may have been affected by LockerGoga.

Attackers used a social engineering attack on a German steel mill to gain access to the IT network, enabling a targeted attack on the OT network which shut the plant down. According to a SANS report, "the combined impact may have resulted in a Loss of Control (LoC) for plant operators and possible malicious control leading to physical destruction".

The Triton malware damaged a critical infrastructure facility in the Middle East when it attacked the plant's industrial control system (ICS). The attack targeted a safety instrumented system (SIS) made by Schneider Electric, which responded appropriately by shutting down operations.[9]

Impacts that Armis has seen include:

- Changes to process automation which impacted product quality
- Stoppage of production lines
- Human machine interface (HMI) devices that were infected with WannaCry
- Vulnerable industrial control devices that were exposed to the Internet
- Third-party devices that opened reverse tunnels which breached network segmentation

Recently, hackers created a new worm called PLC-Blaster that lives solely in a PLC and scans the IP network to identify and spread to additional vulnerable PLCs.[10] To our knowledge, this malware has not yet had a major impact on industrial control systems, but the fact that it exists indicates the intentions and capability that cyberattackers have with respect to industrial control systems.

These attacks also demonstrate the increasingly connected nature of OT. A joint study by Deloitte and the Manufacturers Alliance for Productivity and Innovation showed that only 50% of manufacturing environments currently maintain isolation between their OT networks and their IT networks. 76% are using Wi-Fi to enable communication between connected systems. A telling 39% of respondents to the Deloitte survey said they experienced a breach of their OT network in the previous 12 months.[11]

GROWING AWARENESS OF INDUSTRIAL DEVICE RISK

The good news is that although risk has increased, so has awareness of the challenge. A SANS survey from June of 2017 titled “Securing Industrial Control Systems-2017” provides insight into how organizations are addressing the OT security problem.

Source: “Cyber risk in advanced manufacturing“, Deloitte and the Manufacturers Alliance for Productivity and Innovation.[12]

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.”[13]

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.

A market research study commissioned by Armis and conducted by Forrester Consulting found that 78% of manufacturing organizations believe that unmanaged and IoT devices are more vulnerable to cyber attack than corporate-managed computers.[14]

CYBERSECURITY GOALS FOR OT ENVIRONMENTS

Any cybersecurity program designed to mitigate risks in an OT environment should have the same outcomes as a cybersecurity program designed for IT devices. These outcomes are listed in security frameworks such as the NIST Cybersecurity Framework (CSF) or the Center for Internet Security Critical Security Controls (CSC). The CSF lists 22 categories of outcomes, and the CSC lists 20 categories of outcomes. The two frameworks are roughly similar.

A report by NIST titled "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" (NISTIR 8228) is especially relevant because it is focused entirely on OT device security. This report highlights four critically important areas for OT device risk mitigation:[16]

- **Asset Management –** Maintain a current, accurate inventory of all OT devices and their relevant characteristics throughout the devices' lifecycles in order to use that information for cybersecurity and privacy risk management purposes.
- **Vulnerability Management –** Identify and eliminate known vulnerabilities in OT device software and firmware in order to reduce the likelihood and ease of exploitation and compromise.
- **Access Management –** Prevent unauthorized and improper physical and logical access to, usage of, and administration of OT devices by people, processes, and other computing devices.
- **Device Security Incident Detection –** Monitor and analyze OT device activity for signs of incidents involving device security.

THE TECHNICAL CHALLENGES OF OT SECURITY

Despite authoritative guidance on cybersecurity goals and outcomes from NIST and other organizations, security managers working for manufacturing and industrial firms have difficulty finding security tools that can provide these outcomes. There are several reasons for this.

- **Agents don't work.** You cannot install an agent on most OT devices. This renders invalid an entire class of security tools that are often used to help identify, protect and monitor devices on enterprise networks.
- **Network scanners can't be used.** Unlike traditional IT devices, many OT devices do not tolerate network scans or probes, which can crash or disrupt OT devices. Consequently, obtaining an inventory of hardware, software, and vulnerabilities is far more challenging than in an IT environment.
- **Conventional network security products are insufficient.** The traditional placement of network IPS systems is at the perimeter and in the core of the network. This makes protecting OT systems at the edge of the network difficult or impossible. Furthermore, network equipment can be compromised[15] by a determined hacker, so relying exclusively on network controls (e.g. firewalls and network segmentation) is just as unwise in an OT environment as it is in an IT environment.
- **Patching is extremely difficult.** Unlike traditional computers (e.g. Windows) which can be patched quickly and automatically by centralized patch management systems, OT devices are very difficult to patch. The typical manufacturing facility includes equipment from dozens of different vendors, and most of the equipment can not be patched by any type of centralized patch management tool. Furthermore, OT devices typically need to be taken offline to patch them, but it is rare that the business will tolerate this kind of operational downtime. As a result, patching is seldom done, and as a result, OT devices tend to accrete vulnerabilities over time, enlarging the risk.
- **Wireless connectivity evades security controls.** Manufacturers of OT security products are increasingly building wireless connectivity into their devices. These protocols, which include Bluetooth, Near Field Communication, Zigbee, etc. are invisible to traditional security controls which monitor traffic on the wired Ethernet, and sometimes also on the Wi-Fi network, but never peer-to-peer wireless protocols such as these.
- **Complexity is increasing.** Innovation and progress are driving more and more automation, technology and connectivity on the manufacturing plant floor. It is difficult to keep pace with increased device count and technical complexity of operations. The lines between IT and OT are increasingly blurred.
- **Connectivity is a risk.** With added complexity and connectivity comes more risk. It is difficult today to know what, who, where and when access is granted, maintained and used. The air gap has not aged well, and security managers have a very limited ability to audit and enforce the policies that maintain isolation of OT environments. Jump boxes, legacy VPN, legacy equipment, vendor access and rogue access are all examples of daily challenges to maintaining the security of OT environments.

A BLUEPRINT FOR SUCCESS

In summary, the security outcomes needed for OT environments are well understood but can't be achieved using traditional security tools. Neither specialized OT security tools nor traditional IT security tools were designed for today's hybrid OT/IT environment.

What security managers need is a different approach to security—one that is designed for the unmanaged devices across OT environments. Such a security system would have the following characteristics:

- **Agentless**. The security system should be able to function without any reliance on agents because most OT devices and enterprise IoT devices (printers, IP cameras, HVAC systems, etc.) cannot accommodate agents.
- **Passive.** The security system should be able to function using only passive technologies. This is because a security system that relies on network scans or probes can disrupt or crash OT devices.
- **Comprehensive security controls.** The security system should meet most of the important cybersecurity goals specified by security frameworks such as NIST CSF or CIS CSC and especially the four goals highlighted by NISTIR 8228 (see above). In the IT world, this typically requires the use of several different security tools. For the OT environment, it would be desirable to obtain comprehensive coverage of the required security controls using as few tools as possible.
- **Comprehensive device coverage.** The scope should include all unmanaged or industrial IoT devices in the enterprise—from the manufacturing floor to the executive suite—because in an interconnected environment, you can't secure OT unless you secure IT along with it. The security platform should work for all types and brands of industrial control systems along with other kinds of devices common to the enterprise such as HVAC systems, IP security cameras, fire alarm systems, switches, firewalls, wireless access points, printers, and more.
- **Comprehensive communication coverage.** The security system should be able to directly monitor all communication pathways that could be used by a cyber attack. In most environments, this would include Ethernet, Wi-Fi, Bluetooth, BLE, and possibly other wireless protocols such as Zigbee. Wireless coverage is important because attackers can exploit vulnerabilities such as BlueBorne, KRACK and Broadpwn to compromise OT devices over the air, without any user interaction.

PROTECT OPERATIONAL TECHNOLOGY (OT) WITH ARMIS

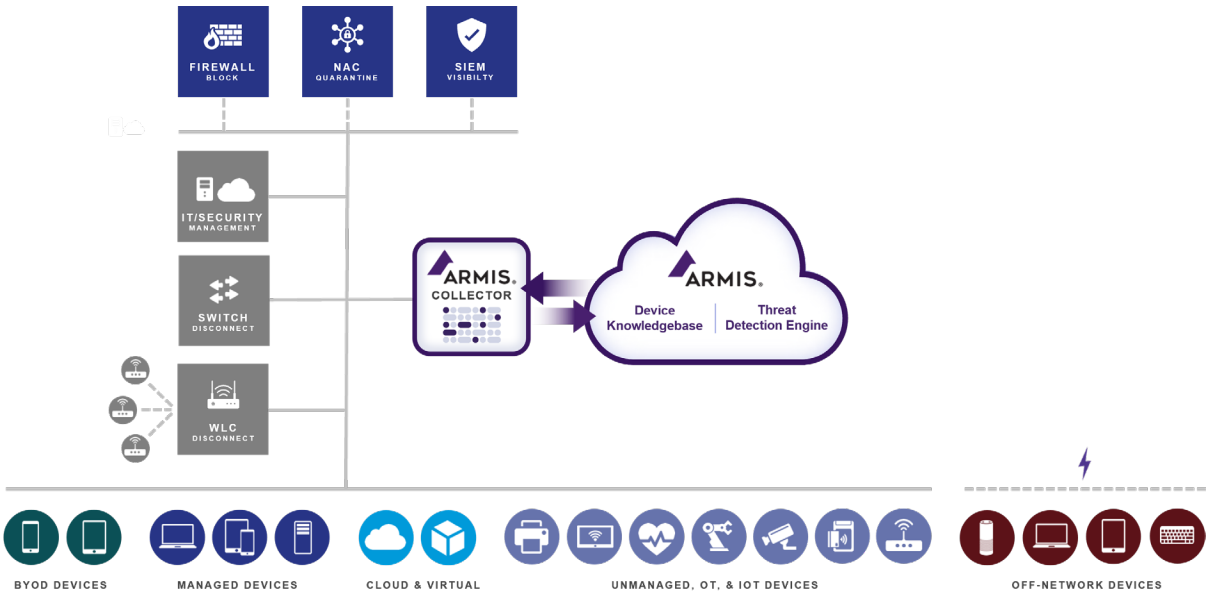
The list of objectives above may seem daunting, but it is actually achievable using existing technologies. Armis is a security platform that is purpose-built to protect manufacturing and industrial environments from the risks of cyberattack. The Armis platform meets all of the requirements listed above. Below is a description of how Armis meets each of the cybersecurity goals.

1 | 100% AGENTLESS AND PASSIVE

Armis utilizes 100% passive monitoring technologies. There is nothing to install on a device nor any sort of invasive access (scanning or remote login) that can disrupt endpoints. As a result, Armis is frictionless and fast to deploy.

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



OT Protocols Supported by Armis

Automation & Production

Siemens S7/S7-Plus
CIP
PCCC/CSPv4
CCC
Lantronix
GE PAC8000
GE-SRTP
Mitsubishi Melsec/
Melsoft SSL
Sattbus
OPC DA/AE/UA
Profibus
Profinet-DCP
Modbus
Modbus Altivar
Modbus Concept/Momentum
Modbus RTU
Modbus Schneider

Building Management Systems

Siemens P2
Bacnet

Distributed Control Systems

Honeywell Experion
FTE (Honeywell)
Emerson Ovation DCS protocols
Emerson DeltaV DCS protocols
Yokogawa ProSafe H1
GE Mark6e (SDI)

Electric & Distribution

ABB 800xA DCS protocols
MMS
ICCP TASE.2
IEC104/101
DNP3
GOOSE
Schweitzer
Bently Nevada

Medical

ASTM
DICOM
HL7
HL7 aECG BKV
SCP-ECG Medical
Smiths Medical
Welch Allyn Medical
X12

Oil & Gas

VNC Emerson ROC
ABB TotalFlow

Safety

Triconex
Yokogawa VNet/IP

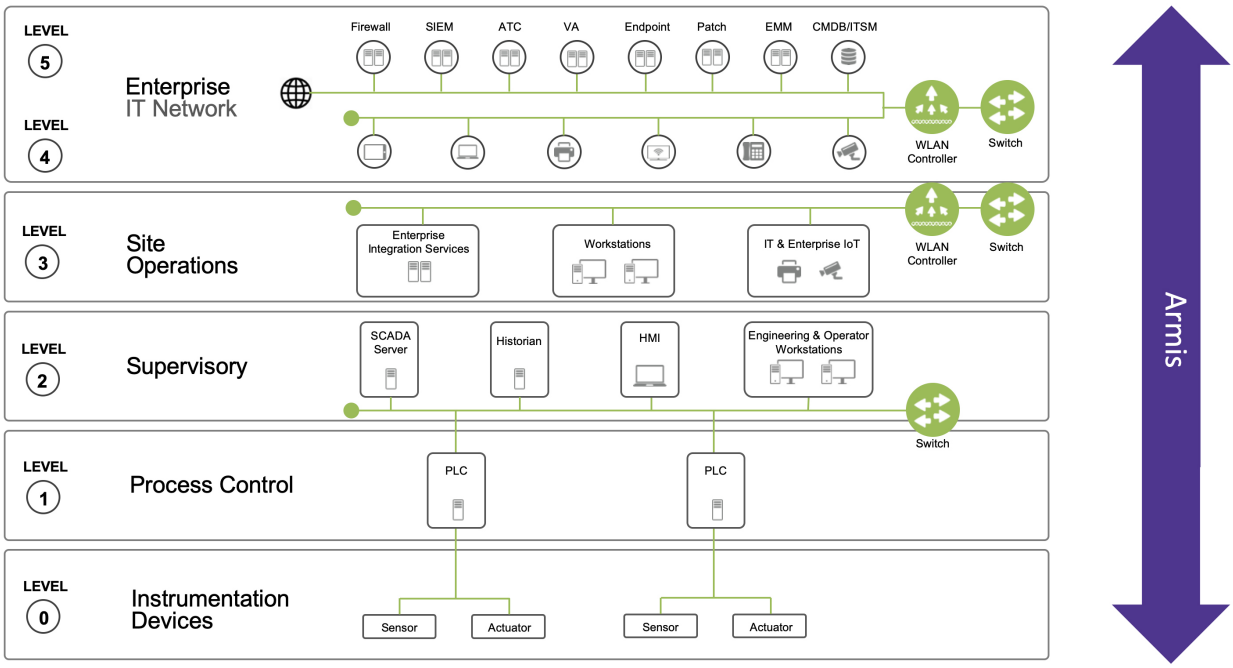
Vendors Supported by Armis

ABB
EMERSON
Honeywell
MITSUBISHI
Rockwell Automation
Schneider Electric
YOKOGAWA

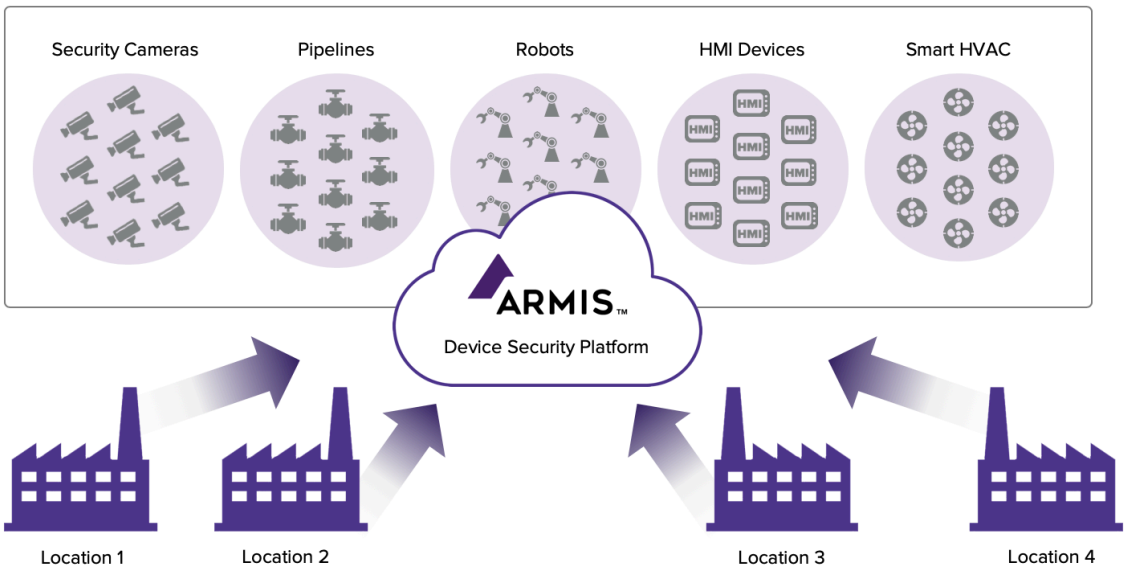
2 | ASSET MANAGEMENT

Armis discovers and classifies every managed, unmanaged, and IoT device in your environment. The comprehensive scope includes devices on your network (both wired and Wi-Fi) as well as off-network devices that are communicating via Wi-Fi, Bluetooth, and other peer-to-peer IoT protocols—a capability no other security product offers without requiring the deployment of new hardware sensors. This includes devices in your OT environment such as SCADA, PLCs, and DCS as well as devices in your IT environment such as servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC controls, and much more. The Armis platform's ability to classify devices with a high degree of accuracy is a result of our extensive Device Knowledgebase. As of June 2021, the Armis Device Knowledgebase tracked

Armis Provides Visibility Across All Levels



more than one billion devices with 12 million distinct device profiles. Each profile includes unique device information such as how often each device communicates with other devices, over what protocols, how much data is typically transmitted, whether the device is usually stationary, what software runs on each device, etc.



The Armis platform generates a wide range of information about each device, which is important for an asset inventory. Below is a partial list of device characteristics we identify:

Device Information

- Device type
- Manufacturer
- IP address
- MAC address
- Computer name
- User name

Endpoint Behavior

- Stationary vs. moving
- Communication timing
- Communication volumes
- Cloud services accessed
- Tunnels utilized
- Encryption usage

Connection Information

- Connection type (wired, WiFi, Bluetooth, etc.)
- Connection point (corp, guest, rogue, etc.)
- Traffic volume and timing
- Internet domains accessed

Software Information

- OS type and version
- Applications

Wi-Fi Information

- AP name
- AP CPU utilization
- AP bandwidth utilization
- AP OS version

Switch Information

- Switch name and location
- Switch CPU utilization
- Switch configuration
- Internet domains accessed

Armis can feed all of the asset information that it generates into your existing asset management database system. This helps you maintain a trusted single-source-of-truth repository for better decision-making.

3 | VULNERABILITY MANAGEMENT

Being aware that a device exists isn't enough. You need to know whether or not it is risky. Armis tells you, in simple terms.

As part of its discovery process, the Armis platform generates a risk score for each device, based on multiple risk factors and the extensive knowledge that is stored in our Device Knowledgebase. This risk score helps your security team take proactive steps to reduce your attack surface. It also helps you comply with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

Unlike other vendors, Armis provides risk scores for all devices automatically. There is nothing that you need to enter into the system—no policies or whitelists that you need to know in advance. Also, Armis uses 100% passive monitoring technologies that cannot disrupt your sensitive OT devices.

Risk Factors

Vulnerability Score	7	Jailbroken	0
Attack surface exposure	10	Vulnerability history	7
Cloud synchronization	7	Data-at-rest security	8
Connection security	9	Number of wireless protocols	10
SP800-121 compliance	5	User authentication	9
Third party app stores	9	Software version	9
Malicious Domains	10		

Total Score	**8**

4 | ACCESS MANAGEMENT

Armis shows you all connections between devices, including connections to unmanaged devices, rogue networks and unauthorized communication channels that you might not be aware of. This can help both with the planning and validation of your network segmentation strategy.

Armis monitors and logs every successful and failed login attempt for every device in your environment. These events are stored for at least 90 days and are available to you for analysis and investigation. Armis detects and alerts on brute-force login attacks.

5 | DEVICE SECURITY INCIDENT DETECTION

Armis passively monitors the state and behavior of all devices on your network and in your airspace. When a device operates outside of its known-good profile, Armis issues an alert or triggers automated actions. The alert can be caused by a misconfiguration, a policy violation, or abnormal behavior such as inappropriate connection requests or unusual software running on a device.

- **Behavior –** Compares real-time device activity to established, "known-good" baselines that are stored in the Armis Device Knowledgebase. These are based on the historical behavior of the device; behavior of similar devices in your environment; and the behavior of similar devices in other environments.
- **Configuration –** Compares the configuration of each device to other devices within your environment, looking for anomalies.
- **Policies –** Lets you create policies for each device or type of device, and identifies violations.
- **Threat Intelligence –** Utilizes premium threat intelligence to inform the Threat Detection Engine of real world attack activity and patterns. The Threat Intelligence Engine then correlates observed activity in your network with this threat intelligence, as well as taking into account the presence of vulnerabilities and other risk factors, in order to detect actual attacks with higher confidence.

Because of the crowd-sourced nature of the Armis Device Knowledgebase, Armis can detect compromised devices immediately upon deployment. There is no learning period, no tuning period. And unlike behavior anomaly tools that simply look at deviations from historical traffic flows, Armis generates practically zero false positives.

Armis continuously records information about the state and connections made by each device on your network so that when a security event occurs, your security team can scroll back in time to see the scope of the breach—what communications occurred, over what protocols, how much data was transmitted, recent OS or application updates, abnormal traffic patterns, or even devices changing locations.

6 | DEVICE KNOWLEDGEBASE

The Armis Device Knowledgebase is a critically important component of the Armis platform, and it is what allows Armis to identify devices, assess their risk, and detect threats with a high degree of accuracy.

The Armis Device Knowledgebase is a giant, crowd-sourced, cloud-based repository of information about devices. It is the largest such knowledgebase in the world. It contains attribute information for more than one billion devices broken out into over 12 million distinct device profiles. Each profile includes unique device information such as how often each device communicates with other devices, over what protocols, how much data is typically transmitted, whether the device is usually stationary, what software runs on each device, etc. This information is based on historical observations from all of Armis' customer environments plus information provided directly from device manufacturers. The Device Knowledgebase continuously updates itself based on approximately 1 petabyte of data that Armis' virtual appliance gleans every day from customer environments.

The Armis Device Knowledgebase allows Armis to completely and passively classify devices with a higher degree of accuracy than traditional IT discovery products. Traditional discovery products utilize less information—typically just the MAC address and DHCP negotiation—to identify each device. Because of the highly granular nature of Armis' Device Knowledgebase, Armis can even detect how each device is being used—for example, when a tablet computer is being used to control a video system in a conference room vs. being used as a personal computing device or a point-of-sale device.

To classify each device, Armis' cloud-based device classification engine finds a best-fit between the device attributes that Armis observes in your environment and the device attributes that are stored in the Device Knowledgebase.

The information in the Armis Device Knowledgebase also enables Armis to detect compromised devices with a high degree of accuracy. Armis compares real-time device activity to "known-good" baselines in the Device Knowledgebase. When a device operates outside of its baseline, Armis issues an alert or triggers automated actions. Alerts can be triggered by a misconfiguration, a policy violation, or abnormal behavior like inappropriate connection requests or unexpected software running on a device.

CONCLUSION

There are a variety of unique challenges associated with protecting OT devices from cyberattack, but it can be done if you have the right kind of tools. Armis is an example of a new type of unified enterprise security platform that has been specially built to function in both OT and IT environments. Armis provides a broad range of security controls for all devices in your enterprise—both OT and IT devices—because you can't secure OT without securing IT along with it.

FOOTNOTES

1 "State of Enterprise IoT Security: A Spotlight on Manufacturing," Sept. 2019, Forrester Consulting

2 "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS, June 2018,

3 "National Cyber System Awareness Alert," July, 2020, CISA

4 ICS-CERT Advisories

5 https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

6 https://www.straitstimes.com/world/europe/renault-hit-by-global-cyber-attack-companys-management-says

7 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018.

8 https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880

9 https://threatpost.com/triton-ics-malware-second-victim/143658/

10 https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

11 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-cyber-risk-in-advanced-manufacturing-executive-summary.pdf

12 Ibid.

13 "Securing Industrial Control Systems-2017," SANS, July 2017.

14 "State of Enterprise IoT Security: A Spotlight on Manufacturing," Sept. 2019, Forrester Consulting

15 See US CERT alert TA18-106A among others. Also see Armis' demonstration at the RSA security conference.

16 "NISTIR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," National Institute of Standards and Technology, June 2019.

ABOUT ARMIS

Armis the leading unified asset visibility & security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

ARMIS™

1.888.452.4011 armis.com