CYBERSECURITY

For Electric Utility Operational Environments

The security needs of electric utilities 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 the entire utility environment.

INTRODUCTION

The electric grid is considered to be among the most critical infrastructure in the world. However, each year, energy and electric utilities are exposed to more sophisticated and more frequent cyber attacks, and constant probing by hostile nation states has been reported.[1] Disruption to the grid can have far-reaching consequences, and cyber security is of paramount importance.

Critical Operational Technology, or OT, assets have traditionally been protected from cyber attacks by maintaining an effective air gap in the communications network. Most controls over the actual grid were manually applied, not automated. And disaster planning focused on storms and catastrophic physical events rather than cyber events.

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. The automated capability of these systems is increasing exponentially. All of these changes increase the risk that control systems can be compromised by sophisticated threat actors using cyber attack techniques borrowed from the world of IT. In short—what threatens IT now threatens OT.

This white paper explores the cybersecurity challenges that utilities face in a rapidly changing landscape.

MOVING BEYOND THE AIR GAP

Historically, utilities have relied upon the presence of an air gap to secure the OT environment. Physical separation of the OT network was maintained by traditional locks and fences, and logical separation was maintained by various types of network controls. Both types of air gaps allowed OT environments to implement completely different strategies for security, thus avoiding the challenge of applying traditional IT security controls to OT environments.

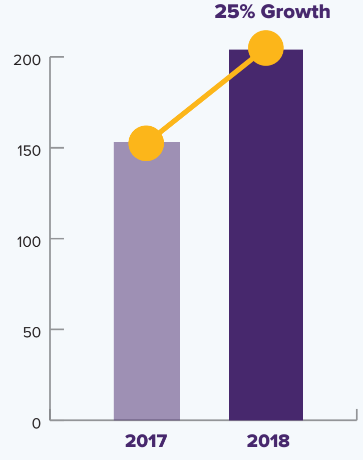
However, business practices are changing. An increasing number of automation devices are being connected to the grid. The locks and fences are still there, but the logical network separation is dissolving. Devices are talking with each other across network boundaries using TCP/IP.

UTILITY CYBER RISKS ARE INCREASING

Not only are OT devices increasingly accessible by cyber attackers (due to the increased connectivity), they are also increasingly vulnerable to attacks. Newer devices are likely to be running a common operating system such as Linux or VxWorks, but you cannot utilize traditional security methods like installing an agent on them. They are by definition "un-agentable."

Year over year, we see the number of vulnerability announcements coming from OT device manufacturers increasing. In 2018, we saw 204 public vulnerability advisories—an increase of 25% over 2017.[2] Vulnerabilities exist in many different types of in-field devices—voltage regulators, smart switches, capacitors, RTUs, etc.—as well as human-machine interface (HMI) systems and SCADA software. Over half of the ICS-related vulnerabilities reported in 2018 were rated "high" in terms of severity level.

OT Device Newly Announced Vulnerabilities



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

THE DISCOVERY OF URGENT/11

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

- ✓ VxWorks® by Wind River
- ✓ OSE by ENEA
- ✓ Integrity by Green Hills
- ✓ ThreadX by Microsoft
- ✓ Nucleus RTOS by Mentor
- ✓ ITRON by TRON Forum
- ✓ 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 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 the URGENT/11 vulnerabilities is available from Armis at armis.com/urgent11

CRITICAL UTILITY INFRASTRUCTURE IS UNDER ATTACK

Stuxnet, which attacked SCADA control systems at Iranian nuclear facilities, and BlackEnergy/CrashOverride, a nation-state attack which crippled the Ukranian power grid, are often cited as examples of attacks on the utility industry.[4] However, according to E-ISAC, there are many more attack methods being used against utilities. Traditional IT attack methods such as credential theft, denial of service and remote access trojans are proving to be just as effective on ICS networks as they are on IT networks. Attacks start on the IT network, and from there, the attackers move to more critical OT assets, using IT assets as a form of jump server.

The Triton malware that attacked a critical oil and gas facility in Saudi Arabia was used to disable the safety instrumented system (SIS) which is made by Schneider Electric.[5] We are now seeing the group that developed Triton malware targeting electric utilities in both the U.S. and Asia Pacific regions.

Dragonfly, aka Energetic Bear, is another threat actor that has been targeting utilities. They start by planting malicious content on commonly visited industry websites.[6] The malicious content includes social engineering tactics that aim to obtain user credentials. Once user credentials have been gained, the threat actor performs reconnaissance within the utility's IT network, looking for information that helps them build a network map. Then they launch a sophisticated attack on the OT network.

In another case, a cloud services provider serving the utility industry suffered a ransomware attack, shutting down billing operations for many utilities. While this didn't affect the grid, it caused inaccurate customer billing and highlighted the significant impact supply chain disruptions can have on the industry.

In September 2019, the North American Electric Reliability Corp. released a report that detailed a cyber attack that disrupted several electric utilities in the western United States.[7] And in the same month, Trend Micro's research team reported that Russian cyber underground forum members were looking into hacking smart electricity meters.[8]

THE "UTILITY OF THE FUTURE" CREATES ADDITIONAL CHALLENGES

In response to demands for cleaner energy, utilities are rapidly transforming into a more decentralized and digital model of electricity generation and delivery. Both trends often involve behind-the-meter technologies which extend the utlitity's network deeper into the customer premises. There is a growing expectation that the utility's smart meter network will talk directly to a customer's smart home devices. This exchange of information between smart meter and consumer devices is often handled through wireless protocols such as Zigbee or Bluetooth. Unfortunately, this introduces vulnerabilities such as BlueBorne through which utility meters can be attacked. New vulnerabilities in wireless protocols are being discovered every year.

Similarly, distributed energy production often requires complex interactions between generator and utility. Real-time communication between devices is crucial for safe and efficient operations. The result is that the utility's OT network is directly extended to these distributed energy installations which increases the attack surface that the utility needs to monitor. As well, information from the distributed energy resource often follows multiple logical paths, both for billing and operational purposes. This adds additional attack surface to the OT network.

In the examples above, it is clear that decentralization and digitization—the two technologies that are shaping the utility of the future—add significant challenges for security.

MANAGING REGULATORY COMPLIANCE AND SECURITY

In North America, NERC-CIP standards were instituted in 2007 with the goal of improving reliability and security for utility OT environments. NERC-CIP details a set of controls that utilities involved in power generation and transmission must adhere to for Bulk Electric Assets (BES). The NERC CIP requirements consist of 11 standards covering the security of electronic perimeters and the protection of critical cyber assets, as well as personnel and training, security management and disaster recovery planning.

While NERC-CIP is still important, the threats against OT devices and systems have grown larger than the standards have envisioned. Many utilities now believe that other security frameworks that were specifically designed for modern OT devices should also be utilized. Two such frameworks are published by NIST. One is the NIST Cybersecurity Framework (CSF) which lists 22 different categories of security outcomes.[9] The other is NISTIR 8228 which is titled “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks”.[10]

NISTIR 8228 is especially relevant for OT networks within utility environments. NISTIR 8228 lists four critically important areas for OT device security controls:

- **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 MEETING SECURITY GUIDELINES

While NERC-CIP regulations and NISTIR 8228 security goals are easy to read, implementing those regulations within a modern OT utility environment is difficult. 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.** Many OT devices do not tolerate network scans or probes, which can crash or disrupt the device. Consequently, obtaining an inventory of hardware, software, and vulnerabilities is far more challenging than in an IT environment.
- **Conventional network security products designed for OT environments have limited scope.** "SCADA-aware" firewalls and network IPS devices are often installed at the perimeter of the OT network, where traffic egresses to the enterprise network or to the Internet. From that location, they can't effectively monitor what is happening within the OT network. Other types of security tools that attempt to monitor remote OT sites from a central location quickly run into bandwidth limitations that render them useless.
- **Old devices are everywhere.** The asset lifecycle of devices in a utility environment is far greater than typical IT devices. These old devices use legacy protocols and haven't been built with today's cyber security standards in mind. Patching is difficult or impossible due to age and uptime requirements.
- **Wireless connectivity evades security controls.** Manufacturers of OT devices are increasingly building wireless connectivity into their devices. These protocols, which include Bluetooth, Near Field Communication, Zigbee, etc. are invisible to traditional OT and IT security controls.
- **Complexity is increasing.** Utilities are using more automation, technology and connectivity than ever before. It is difficult to keep pace with increased device count and technical complexity of operations. The lines between IT and OT are increasingly blurred.
- **Network access control (NAC)** only decides what devices should and shouldn't be on the network. It is not designed to monitor the behavior of devices, so it can't tell you if an OT device starts to behave maliciously.

A BLUEPRINT FOR SUCCESS

The regulatory requirements and security outcomes needed for today's modern utilities are well understood, but they can't be achieved using specialized tools that were designed for yesteryear, when the air gap still existed.

What is needed is a security platform that meets the needs of modern connected environments—both IT and OT environments at the same time. Both OT and IT personnel must be aware of what is happening in their networks. For maximum success, such a security platform would have the following characteristics:

Security needs to span both OT and IT environments.

- **Comprehensive device coverage.** The scope should include all connected devices in the enterprise—from the substation 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 security controls.** The security system should meet all of the important cybersecurity goals specified by NISTIR 8228 (see above).
- **Comprehensive communication coverage.** The security platform 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.
- **Agentless.** The security platform should be able to function without any reliance on agents because most OT devices as well as enterprise IoT devices (printers, IP cameras, HVAC systems, etc.) cannot accommodate agents.
- **Passive.** The security platform should be able to function using only passive technologies. This is because network scans and probes can disrupt or crash OT devices.
- **Cross-domain.** With increased awareness of cyber security in OT environments, there is an increased need for OT and IT teams to work closely together. The traditional air gap often meant that IT had very little exposure to what was happening in the OT network. Today's advanced threats require the knowledge and capability that sits within both teams. Asset visibility and management is crucial for both teams. Thus, the security platform should have role-based functionality to meet the needs that are appropriate to whomever is logged into the management console.
- **Comprehensive controls.** Just for the sake of simplicity, the security platform should meet as many of the security and regulatory requirements as possible.

You can't secure OT without securing IT along with it.

PROTECT OPERATIONAL TECHNOLOGY (OT) WITH ARMIS

Armis is an agentless device security platform that is purpose-built to protect both OT and enterprise IT environments from the risks of cyberattack. The Armis platform meets all of the requirements listed above. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical infrastructure, information and systems by identifying suspicious or malicious devices and quarantining them.

Below is a description of how Armis helps utilities meet both regulatory and cybersecurity goals.

NERC-CIP compliance

Standard	Requirement	Armis Value
CIP-002	**R1:** BES Cyber System Identification Requires the identification and documentation of high impact, medium impact and low impact BES Cyber Systems	Armis provides relevant data to assist in the development of the annual compliance report. Through passive listening techniques, Armis discovers and identifies all connected devices on your network and in your local airspace. Armis' passive listening approach has several benefits compared to agent-based or network scanning approaches: ● It is more comprehensive. ● It is more real-time. ● It does not require configuration or maintenance. ● It can not disrupt endpoint devices. The information that Armis generates includes device type, manufacturer, model, MAC address, IP address, location, operating system, host name, applications, connections, and risk score.

Standard	Requirement	Armis Value
CIP-005	**R1:** Electronic Security Perimeter All External Routable Connectivity must be through an identified Electronic Access Point (EAP). BES Cyber Systems must be segmented on the basis of differing trust levels Must have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Armis continuously monitors all connections in your environment—wired, Wi-Fi, Bluetooth, BLE, Zigbee—and will alert you if we see connections that either violate your security policy or are consistent with a data leak. For example: ● Connections across different Electronic Security Perimeter trust levels ● Connections to unauthorized networks ● Connections to known malicious domains ● Anomalous quantities of data being transmitted ● Anomalous times of data transmission Armis identifies rogue devices in the vicinity of your Wi-Fi network; these represent risks for your cyber systems. Armis automatically identifies vulnerabilities in your Electronic Access Points, for example: software vulnerabilities, configuration errors. Armis' threat detection engine requires no tuning or learning period. It compares current state and behavior of devices in your environment to previous state and behavior in your environment as well as other similar ICS and utility environments. The threat detection engine is complemented by premium threat intelligence and by a device knowledgebase that contains over 110 million devices.
CIP-007	**R1:** Enable only logical network accessible ports that are needed	Armis provides centralized, automated security monitoring and analysis that can immediately detect and alert on communication that utilizes unauthorized network ports and services.
	R2: Security Patch Management Know, track, and mitigate the known software vulnerabilities associated with BES Cyber Assets, Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). Implement a patch management process for both critical and non-critical cyber assets.	Armis uses passive monitoring technologies to discover vulnerabilities in all wired and wireless devices. Armis is one of the only vulnerability detection systems that can do this without performing network scanning or device probing, both of which are dangerous activities that can disrupt sensitive OT devices. The scope of Armis' solution includes all assets—both critical and non-critical cyber assets including BES Cyber Assets, Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). Once a decision has been made to roll out a patch to a certain type of device, Armis can monitor the progress of this process via a dashboard that shows the number and locations of devices that do not yet have the patch.

Standard	Requirement	Armis Value
	R3: Malicious Code Prevention Deploy method(s) to deter, detect, or prevent malicious code.	Malicious code almost always manifests via abnormal device behavior. Armis monitors device behavior continuously and is able to detect advanced and unknown threats such as zero-day attacks. When Armis detects abnormal device behavior, it alerts your security team in real-time and, depending on your policies, can initiate an automated response. Armis also communicates this event detection to your existing management systems such as your SIEM.
	R4: Security Event Monitoring Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: **4.1.1.** Detected successful login attempts; **4.1.2.** Detected failed access attempts and failed login attempts; **4.1.3.** Detected malicious code.	Armis monitors and logs successful and failed login attempts 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. Beyond just login monitoring, Armis continuously monitors the behavior of every device in your environment. The presence of malicious code almost always manifests via abnormal device behavior. Armis compares every device's real-time activity to the established and "known-good" activity baseline for the specific device which is stored in our Device Knowledgebase. When abnormal behavior is detected, Armis updates the risk score, generates a security alert, and can communicate the event to your other security monitoring systems, such as your SIEM. All events are stored for at least 90 days and are available to you for analysis and investigation.
	R5.7: Where technically feasible, either: Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Armis can alert you if too many failed remote authentication attempts occur within a certain period of time. Armis will indicate both the source and target of the unsuccessful attempts, so that response can be quickly initiated.
CIP-008	**R1:** One or more processes to identify, classify, and respond to Cyber Security Incidents	Armis provides threat detection and real-time alerting to help you immediately identify, analyze and initiate response to a cyber security incident. The detailed information that we include in alerts helps you understand the source, target, nature and potential impact of a threat.

Standard	Requirement	Armis Value
CIP-010	**R1:** Configuration Change Management Develop a baseline configuration, individually or by group, which includes operating system, application software, and communication ports.	Armis' Device Knowledgebase contains over 10 million distinct device baselines gleaned from multiple sources including Armis research, device manufacturers, and Armis' enterprise customer environments. The baselines include over 8,000 different device characteristics including: ● Operating system ● Application software ● Communication ports ● Communication patterns ● And many more
	R2: Configuration Monitoring Monitor at least once every 35 calendar days for changes to the baseline configuration. Document and investigate detected unauthorized changes.	The Armis platform can detect in real-time certain types of misconfigurations, for example wireless transmissions that are unencrypted, wrong software installed, missing patch, and many more. Once a misconfiguration has been detected, Armis' policy engine can perform many different kinds of automated actions, including sending alerts to your other security systems.
	R3: Vulnerability Assessments Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	The Armis platform constantly monitors all devices in your environment, identifies vulnerabilities, and generates a risk score based on thirteen different device attributes. Armis does this without any need for an agent on the endpoint. This capability encompasses not just your OT environment but also your IT environment. It includes common un-agentable devices that are on enterprise networks such as IP video cameras, badge readers, wireless access points, printers, building automation systems, and many more. All of these devices can be an entry point for attacks. You can't secure OT unless you secure IT along with it.

The Armis platform detects threats in real-time, generates alerts, and can take action to block the kill chain.

NISTIR 8228 CYBER SECURITY FRAMEWORK

In addition to helping you comply with NERC-CIP regulations, the Armis agentless security platform is effective on all four of the risk mitigation areas listed in Goal 1 of NISTIR 8228 "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks". These four areas overlap the NERC-CIP regulations, but they are broader in scope. In particular, they recognize the importance of securing all IoT devices in your environment—both BES Critical Assets and other devices in your environment and your airspace that may be used as part of a cyber attack kill chain.

The following is a description of the major security functions and manner of operation of Armis' security platform.

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 takes only minutes to a few hours, depending on the environment.

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 wireless) 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 additional hardware sensors. This includes devices in your OT environment such as SCADA, RTUs, switches and sensors as well as devices in your enterprise 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. The Armis Device Knowledgebase contains over 10 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 serived 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

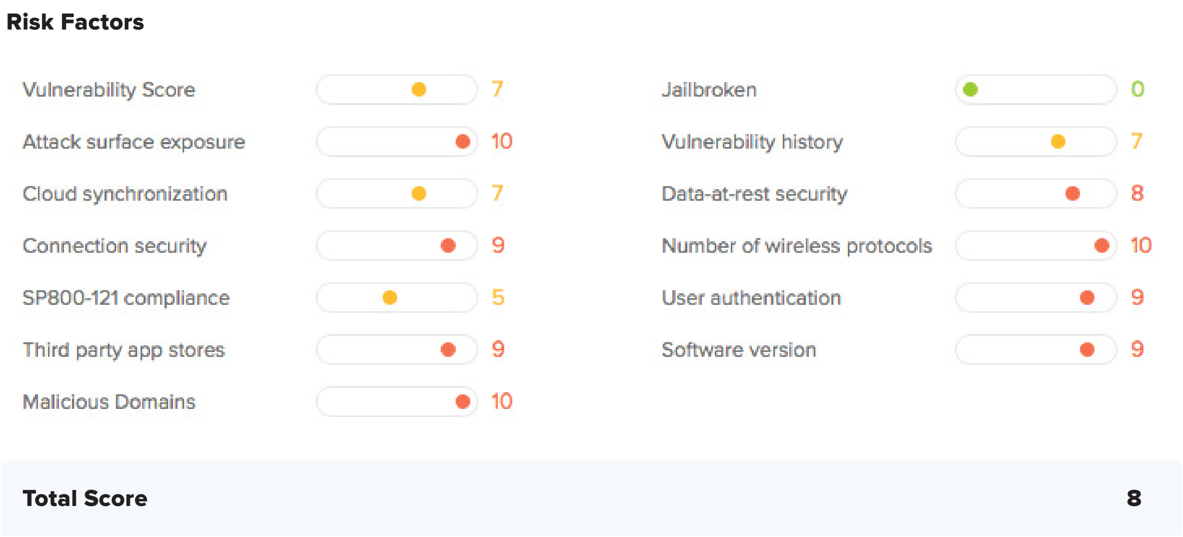
- Switch name and location
- Switch CPU utlization
- Switch configuration
- Internet domains accessed

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

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 NISTIR 8228 which requires 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

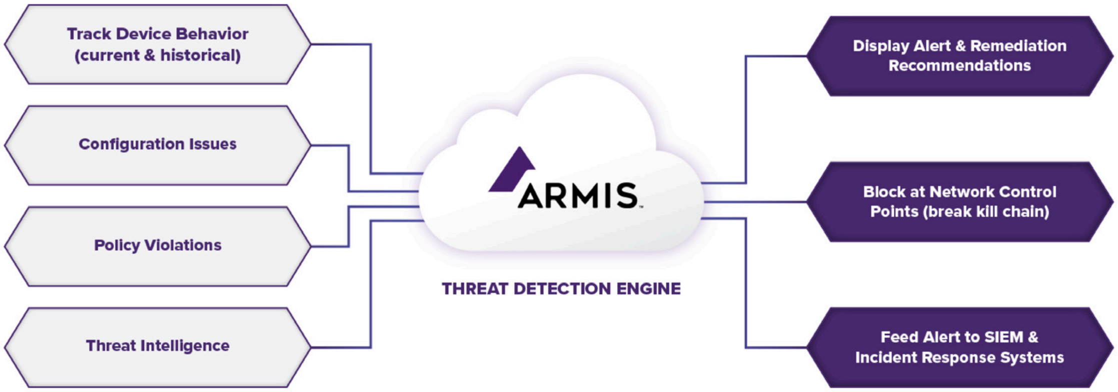
Armis shows you all connections between devices, including connections to unmanaged devices, rogue networks and unauthorized wireless communication channels that you might not be aware of. This can help both with the planning and validation of your network segmentation strategy.

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 all devices on your network and in your airspace. When a device operates outside of its known-good profile, Armis issues an alert or can trigger 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.


Track Device Behavior (current & historical)
Configuration Issues
Policy Violations
Threat Intelligence
ARMIS
THREAT DETECTION ENGINE
Display Alert & Remediation Recommendations
Block at Network Control Points (break kill chain)
Feed Alert to SIEM & Incident Response Systems

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.

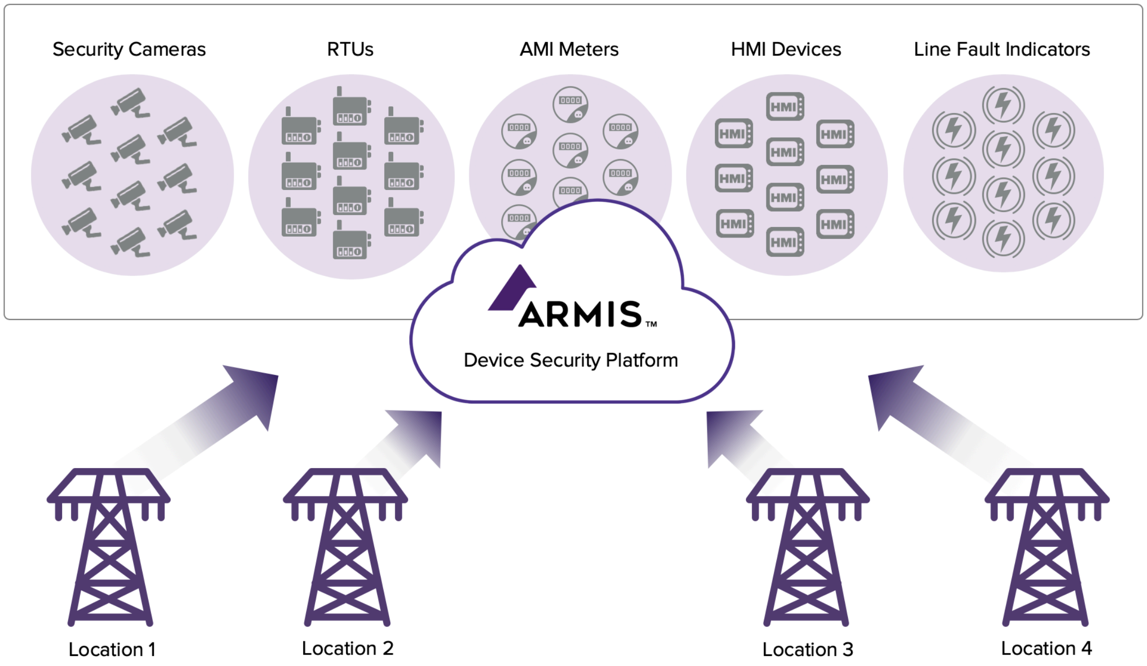
6 | CROWD-SOURCED DEVICE KNOWLEDGEBASE

In order to detect threats with a high degree of accuracy, Armis leverages a massive crowd-sourced device knowledgebase. Information in the knowledgebase comes from historical observations from all of our customers' environments plus claims from device manufacturers. The device knowledgebase continuously updates itself based on approximately 1 petabyte of data that our software gleans every day from our customer environments. Actual data transfer rate depends on the scope of the deployment, but the amounts sent are very low, enabling Armis to meet the needs of geographically distributed facilities with low bandwidth connectivity..

Armis only sends metadata to the cloud, meaning we never capture or transmit any data payloads. Transmission of metadata is provided through a secure architecture.

Armis' device knowledgebase allows Armis to detect compromised devices immediately upon deployment. There is no learning period or tuning period. Any pre-existing error conditions or threats will be detected.

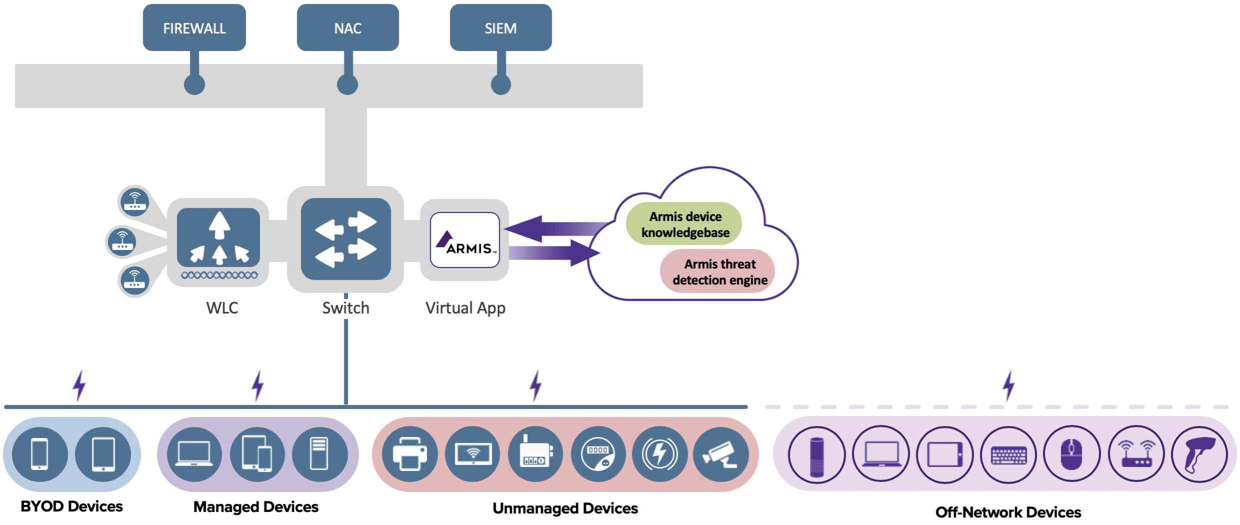
Crowd-sourced device knowledgebase



7 | EASY DEPLOYMENT

The benefits of the Armis platform are many, but deployment is fast, and the impact on your resources is low. The Armis platform does not require agents or additional hardware. Instead, it works with your existing network infrastructure to collect the data it needs to discover, identify, and analyze all devices in your environment. The Armis platform collects data using a virtual appliance that sits out-of-band and passively monitors traffic. (See diagram below.) Since the virtual appliance is not in-line, it has no impact on network performance or OT devices. It does not require any changes to your existing network, and it does not introduce any latency.

Simple installation with no agents or hardware required



CONCLUSION

Because of the changes occurring in the utility industry, a new kind of security system is needed—one that functions in both OT and IT environments. Armis is a unified enterprise security platform that has been specially built to function in both IT and OT 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. The security controls that Armis provies span all of the Goal 1 requirements listed in NISTIR 8228 and many of the requirements stipulated in NERC CIP.

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

FOOTNOTES

[1] Wired, Russian Hackers Haven’t Stopped Probing the US Power Grid, November 28, 2018

[2] Armis research from a variety of web sources.

[3] ICS-CERT Advisories.

[4] ICS Alert (IR-ALERT-H-16-056-01) – Cyber-Attack Against Ukrainian Critical Infrastructure, ICS-CERT, February 25, 2016.

[5] Triton is the world’s most murderous malware, and it’s spreading, MIT Technology Review, March 2019.

[6] Alert (TA18-074A) – Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. ICS-CERT, March 15, 2018.

[7] Report reveals play-by-play of first U.S. grid cyberattack, E&E News, Sept. 6, 2019.

[8] Uncovering IoT Threats in the Cybercrime Underground, Trend Micro, Sept. 10, 2019.

[9] Cybersecurity Framework, NIST.

[10] NISTIR 8228 – Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, NIST, June 2019.

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.

ARMIS™

☎ 1.888.452.4011 armis.com