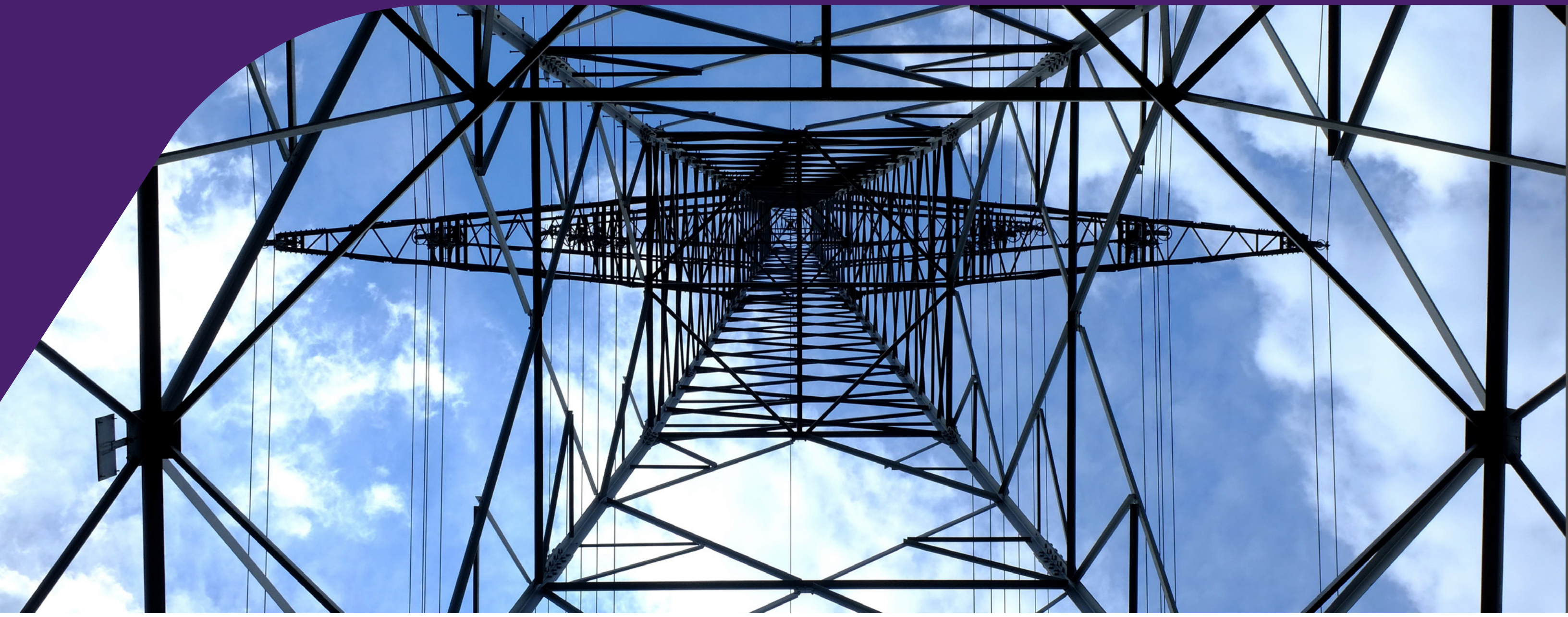
ARMIS® SOLUTION BRIEF



CYBERSECURITY FOR ELECTRIC UTILITY OPERATIONAL ENVIRONMENTS

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.

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.

The Armis Difference

Comprehensive
Delivers and classifies all devices in your environment, on or off your network.

Agentless
Delivers and classifies all devices in your environment, on or off your network.

Passive
Delivers and classifies all devices in your environment, on or off your network.

Frictionless
Delivers and classifies all devices in your environment, on or off your network.

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 industrial control systems on top of common operating systems such as Windows, Linux, Android and VxWorks. The automated capability of these systems is increasing exponentially. Today's utility network world includes smart metering Head-End Systems hosted in the cloud, billing platforms connected to metering infrastructures, smart meters supporting DNP3 protocols that now act as a sensor on the distribution network. 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.

The Armis approach to cybersecurity for electric utilities provides the following:

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 systems. As a result, Armis is frictionless and fast to deploy.

2 | Asset Management

Armis discovers and classifies every managed, unmanaged, OT 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 protocols—a capability no other security product offers without requiring additional hardware sensors. This includes devices in your OT environment such as SCADA, PLCs, 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.

3 | Vulnerability Management

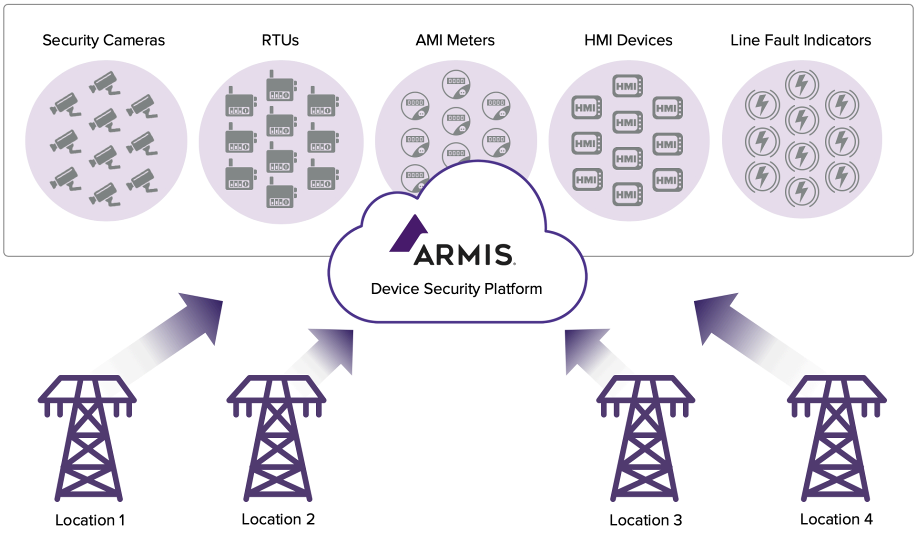
As part of its discovery process, the Armis platform generates a risk score for each device, based on multiple risk factors and the extensive knowledge that is stored in our Device Knowledgebase. This risk score helps your security team take proactive steps to reduce your attack surface. It also helps you comply with NISTIR 8228 which requires you to identify and prioritize all vulnerabilities.

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.

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 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.



6 | Collective Intelligence - The Armis Device Knowledgebase

In order to detect threats with a high degree of accuracy, Armis leverages a device knowledgebase that contains collective intelligence from tracking and analyzing over one billion devices on a daily basis. 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 intel that our software gleans every day from our customer environments.

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 or physical appliance that sits out-of-band and passively monitors traffic. Since the ARMIS 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.

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.

The Armis Difference

Comprehensive

Discovers and classifies all devices in your environment, on or off your network.

Agentless

Nothing to install on devices, no configuration, no device disruption.

Passive

No impact on your organization's network. No device scanning.

Frictionless

Installs in minutes using the infrastructure you already have.

About Armis

Armis is the leading unified asset visibility and 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.com
1.888.452.4011

202100902-1