ARMIS + ESEYE

Pioneering Visibility and Security for Cellular IoT Devices

Cellular IoT adoption is growing at an increasing rate and the number of connected devices is expected to triple by 2025. As more cellular IoT devices come online, organizations around the world need to gain better cross-device visibility and control needed to ensure uptime and business continuity. Losing connectivity, or worse, losing the ability to access your critical devices due to a cyberattack, can be costly, brand -damaging, and bad for your organization's bottom line.

Identify and Secure Every Asset in Any Environment

Armis and Eseye deliver unified asset visibility, security, and continuous connectivity for any cellular device on any network. The Armis platform discovers and monitors every asset, continuously assesses vulnerabilities, risks, and policy violations, and automatically responds to anomalies that could put devices and your business at risk. It's non-invasive and uses no active scanning, so it won't disrupt critical business assets and processes.

Eseye's unique cloud-based Connectivity Management Platform allows cellular IoT devices to intelligently switch to any one of over 700 GSMA-compliant carriers to maximize device uptime and delivers near 100% global coverage. In addition to supporting cellular connectivity for 1X/2G/4G/LTE/5G, Eseye also supports private LTE and 5G networks capable of supporting over a million devices per square kilometer due to its inherent capabilities of handling greater device density than WLAN technologies.

Together, the unified Armis and Eseye solution protects and connects any device out of the box, and scales dynamically to support device requirements for each network.

Comprehensive Asset Visibility and Inventory Management

The Armis platform discovers and classifies every device in any environment, including corporate IT, IoT, operational technology (OT), and medical devices. Integration with Eseye extends the platform's coverage to devices connecting through Eseye's global cellular IoT platform. For example, this includes telematics and sensors used for transportation,

medical devices that are often moved throughout and among different medical centers, and remote devices like those used in the banking industry (ATMs), industrial and energy industries (industrial automation sensors) and vending industries (various vending machines).

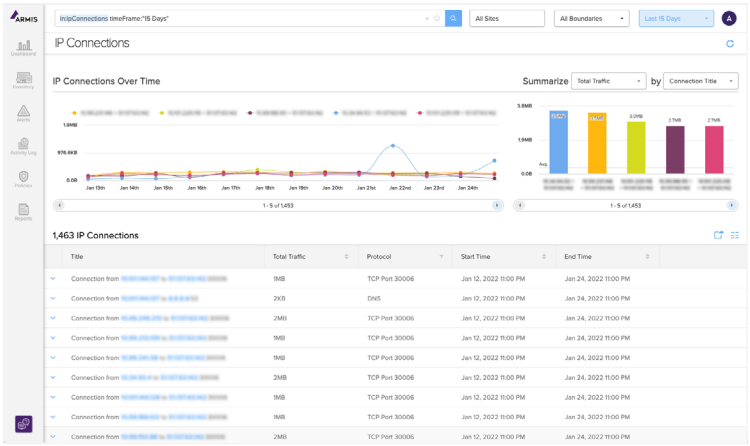
Risk Management

The Armis platform calculates a risk score for each device based on factors like vulnerabilities, known attack patterns, and the behaviors observed on each device. This risk score helps you understand your exposed attack surface and meet compliance with regulatory frameworks that require identification and prioritization of vulnerabilities.

The Armis platform continuously monitors the behavior of every device on your network, in your airspace, and on Eseye-connected cellular networks to detect behavioral anomalies and threats in real time, allowing you to effectively respond to and mitigate damage.

Reporting and Metrics

Reporting in the Armis platform can provide a full, detailed inventory of all assets in your environment, an assessment of assets that are risky or exhibit suspicious behavior including any assets out of compliance with your organization's policies. This will reveal critical findings including banned devices, risky protocols, and devices with unencrypted credentials.
The Armis platform gives you an inventory of every device in your environment with details such as IP address, MAC address, OS, version, user information, what software is installed on the device, and what vulnerabilities they have. The platform can even provide information such as connections and activities each device has made when it was first seen on the network and when it was last seen. It also provides a risk assessment of each device so customers can prioritize actions to reduce their attack surface.



Automatic Detection & Response

If the Armis platform detects a threat, it alerts your security team and triggers automated action to stop an attack. It also integrates with your existing IT infrastructure and security enforcement points to restrict access or quarantine malicious devices. This automation gives you peace of mind that an attack on any device will be stopped effectively.

The Armis Device Knowledgebase

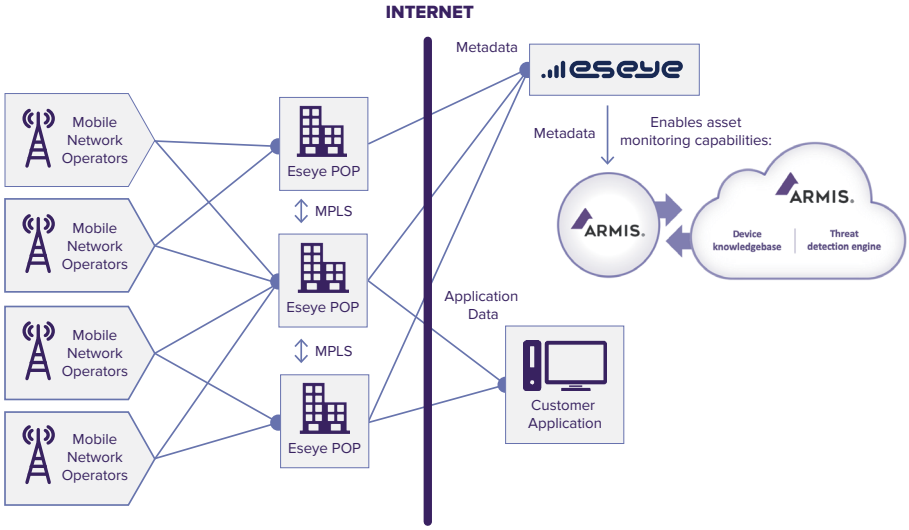
Core to the Armis platform the extensive Armis Device Knowledgebase—the world's largest body of knowledge about devices and their behavior—which eliminates the need for any learning period or baselining.

It uses the collective intelligence of over two billion devices, their characteristics, vulnerabilities, and behaviors to identify and classify any device, evaluate risks, and stop threats accurately, quickly, and automatically.

Our knowledgebase understands what a device is and what it should (and should not) be doing. It compares a device to all similar devices to correlate its characteristics and behavior against known-good profiles of devices to identify issues or threats.

Frictionless Deployment and Integrations

The Armis platform requires no agents or additional hardware to deploy, so it can be up and running in minutes, and API-based integration with Eseye is equally fast and simple. The platform also integrates with your other IT and security tools like network enforcement points, SIEM, ticketing systems, and asset databases so these tools can leverage the rich information the Armis platform provides.



How It Works

Without any additional hardware or software, the Armis platform integrates with Eseye in the cloud for device inventory, risk assessment, and threat detection and response.

- A device using the latest Eseye-provisioned eSIM technology connects to a mobile network local to the device.
- The mobile network operator (MNO) recognizes the Eseye eSIM and directs the device's traffic to the Eseye infrastructure.
- The Armis platform's integration with your Eseye instance detects and identifies devices connecting to Eseye's global network.
- The Armis platform calculates a device risk score using known attributes for similar devices in the Armis Device Knowledgebase. If no similar device is found, the platform creates a new profile and uses machine learning to identify the device and its risks.
- The Armis platform monitors the device's behavior in the customer's Eseye instance for suspicious or malicious activity.

To learn more or see a demo, contact us today!

Armis - armis.com/contact-us

Eseye - eseye.com/get-in-touch

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 and unmanaged devices, including IT, IoT devices, medical devices (IoMT), operational technology (OT) , industrial control systems (ICS) and now - cellular IOT. 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

About Eseye

Eseye empowers businesses to embrace IoT without limits. We help them to visualize the impossible and bring those solutions to life through innovative IoT cellular connectivity solutions that enable our customers to drive up business value, deploy differentiated experiences, and disrupt their markets. Our pioneering technology allows businesses to overcome the complexity of IoT deployment and develop, deploy, and manage IoT projects without the fear of getting it wrong. We guide them every step of the way. Supported by a powerful partner ecosystem, we seamlessly connect devices across 190 countries, agnostic to over 700 available global networks.

eseye.com