SOLUTION BRIEF

Using Armis with Cisco Identity Services Engine (ISE)

Seamlessly Create, Manage & Enforce Security Policies Across Connected Assets

The Problem

McKinsey predicts that by 2030 more than 50 billion devices will be connected IoT devices consisting of over 180 zettabytes of data. (DataBridge Market Research)

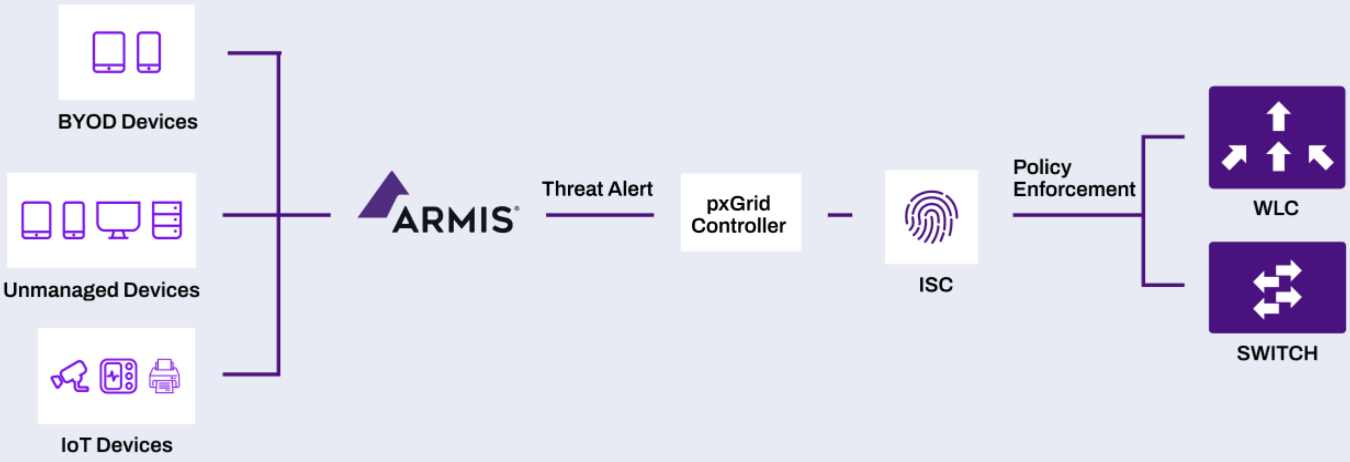
- **Unmanaged assets** are growing in number and are becoming ubiquitous in corporate environments – Connected printers and scanners, VoIP phones, IoT-enabled access points, smart ID badge readers or biometric scanners, Smart inventory and warehouse sensors RFID readers and much more.
- Visibility, security, and control over the explosion of both managed & unmanaged assets are a major challenge. Most existing security tools were built to monitor traditional computing devices on conventional networks. However, they are blind to the growing wave of connected assets, leaving critical blind spots across enterprise environments.

The Joint Solution

Armis Centrix™ is designed to solve these problems. Armis discovers all devices on your network, managed and unmanaged.

Armis delivers the deep, real-time visibility organizations need to manage today's complex and diverse asset landscape. It builds a comprehensive, continuously updated inventory of every connected asset by identifying manufacturer, model, OS, installed applications, physical and logical location, historical communications, and assigning a unique, context-aware risk score. This empowers security teams to proactively reduce the attack surface and make informed decisions based on actual asset behavior and risk.

Armis Centrix™ continuously monitors each asset, using advanced behavioral analytics powered by the Armis Asset Intelligence Engine and Armis Labs. By comparing real-time activity against a massive cloud-based knowledgebase, Armis can instantly identify anomalies and policy violations even on devices that cannot support traditional endpoint agents.When integrated with Cisco Identity Services Engine (ISE), Armis enables automated, closed-loop threat detection and response across both managed and unmanaged devices. Upon detecting a threat, Armis alerts Cisco ISE, which can dynamically enforce policy-based actions such as quarantining suspicious devices or segmenting them from critical systems thus neutralizing threats before they spread. In addition, Armis derived device context can be ingested into Cisco ISE to drive Adaptive Network Control policies, enabling fine-grained, risk-based access decisions that align with Zero Trust principles and reduce operational risk at scale.



1 Armis discovers, contextualizes and classifies all assets.

2 Armis monitors asset behavior to detect threats.

3 When threat is detected, Armis sends alert to Cisco ISE via pxGrid.

4 ISE quarantines malicious devices to neutralize threat.

How Automated Quarantine Works

Step 1: Armis leverages a powerful multi-detection engine. It discovers, contextualizes and classifies every managed,unmanaged, IT, OT, IoMT, IoT, cloud and virtual device in your environment. The inventory that Armis generates includes important information such as device manufacturer, model, serial number, location, username, operating system, installed applications, risks, vulnerabilities, and connections made over time.

Step 2: Armis continuously monitors asset behavior for indicators of attack by comparing real-time device activity to “known-good” baselines in the Armis Asset Intelligence Engine.

Step 3: When Armis detects abnormal behavior, it alerts Cisco ISE via pxGrid.

Step 4: Cisco ISE quarantines malicious devices to neutralize the threat.

Better Asset Management with Armis + Cisco ISE

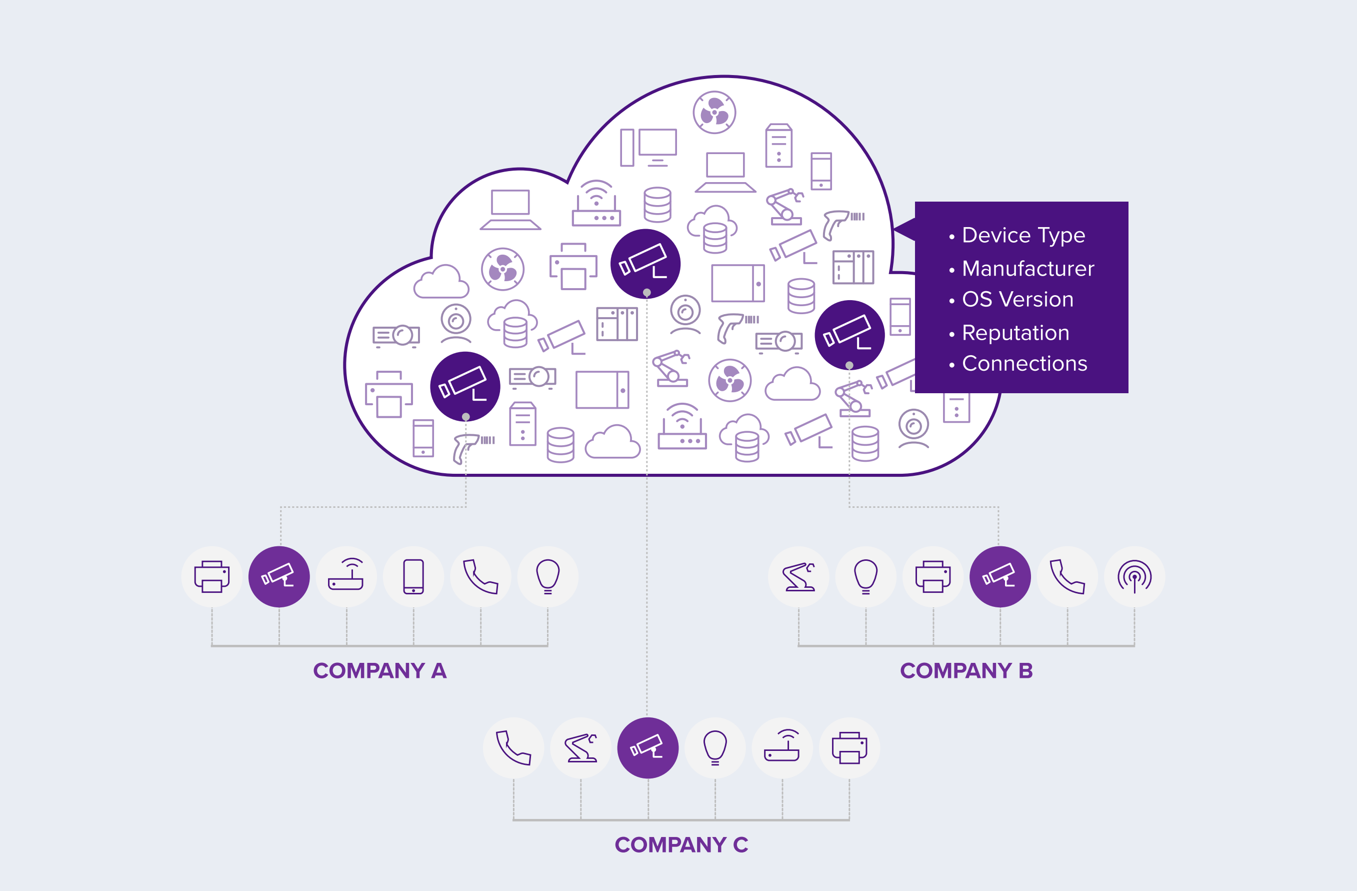
In addition to Policy Enforcement and Adaptive Network Controls, Armis and Cisco ISE can also share asset information mutually improving overall Cybersecurity Asset Management. If this option is selected, this bi-directional integration will pull device information from Cisco ISE into Armis and send additional information related to assets from Armis to Cisco ISE, enriching the context of all assets so IT and Security teams can make informed decisions quickly to reduce their attack surface and improve their security posture. Users also have the option to make the integration uni-directional, only pull asset information from ISE into Armis and not send Armis asset information to Cisco ISE.

Capability	Armis	Cisco	Joint solution Benefit
See MAC and IP address	YES	YES	Basic visibility
See Device Type, manufacturer, etc	YES	YES	Basic visibility
See software and apps running on unmanaged devices	YES	NO	More complete visibility to software
See device-to-device connections	YES	NO	More complete visibility to risk
See device vulnerabilities and risc scores (managed and unmanaged)	YES	NO	More complete visibility to risk
Detect live threats and attacks	YES	NO	Detect attack
Store historical data of all device behavior over time for forensics	YES	NO	Improved ability to respond to attack
Authenticate known corporate devices to the network	NO	YES	Reduce risk by allowing only trusted devices onto your network
Assign IP devices to specific network zones via ACLs, VLANs, etc.	YES	YES	Reduce risk by segmenting your IP network into different trust zones
Assess policy compliance (antivirus status, patch management status, configuration) of managed endpoints	YES	YES	More complete visibility to security risk
Block from corporate network - wired of wireless	YES	YES	Automated response to risk or attack

The Armis AI-Driven Asset Intelligence Engine

The Armis Asset Intelligence Engine is our AI-powered knowledge base, monitoring billions of assets world-wide in order to identify cyber risk patterns and behaviors. It feeds the Armis Centrix™ platform with unique, actionable cyber intelligence to detect, prioritize and remediate real-time threats across the entire attack surface.

When a device operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine a device. Alerts can be triggered by a misconfiguration, a policy violation, or abnormal behavior like inappropriate connection requests or unexpected software running on a device.



Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your enterprise, transforming your infrastructure, and empowering your teams for a global and inclusive future.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo