INTEGRATION BRIEF

Armis and Elisity

Delivering Frictionless, Centrally Managed Zero Trust Access

The IoT/OT/IoMT Cybersecurity Challenge

The exponential growth of connected devices, including IoT, OT, IoMT and other network components, has significantly enhanced operational efficiency across industries. However, this surge in connectivity has also expanded the attack surface, making networks more vulnerable to external threats. Traditional security measures often struggle to keep pace with the dynamic nature of modern network environments, leaving critical assets exposed. Organizations face the dual challenge of managing diverse and numerous devices while ensuring robust security to protect sensitive data and maintain regulatory compliance. This challenge is compounded by the increasing sophistication of cyber threats, which require advanced and adaptive security solutions that can provide comprehensive visibility and control over all networked assets.

The Power of Bidirectional Integration

The Elisity-Armis integration has evolved to create a powerful security feedback loop through bidirectional data exchange. While Armis provides comprehensive device intelligence to Elisity's IdentityGraph™ (including risk scores, device types, and firmware versions), Elisity now returns critical enforcement status data back to Armis. This closed-loop system enables security teams to verify microsegmentation coverage directly in the Armis interface, while enriched flow metadata enhances Armis' behavioral analysis.

For organizations with thousands of devices that can't support traditional endpoint protection, this integration delivers dynamic policy automation that automatically quarantines devices when risk scores exceed thresholds—all without requiring agents. Organizations can deploy microsegmentation in hours rather than months, strengthening zero trust implementation without disrupting critical operations..

Key Features & Beneifts

Visibility

Comprehensive Asset Discovery: ARMIS uncovers previously unknown devices and application traffic, enhancing Elisity's asset inventory and providing real-time visibility.

Control

Granular Policy Enforcement: Manage traffic with identity and context-based least privilege access policies, independent of network infrastructure.

Dynamic Access Management: Utilize enriched asset attributes to create and enforce adaptive, context-aware security policies.

Simplicity

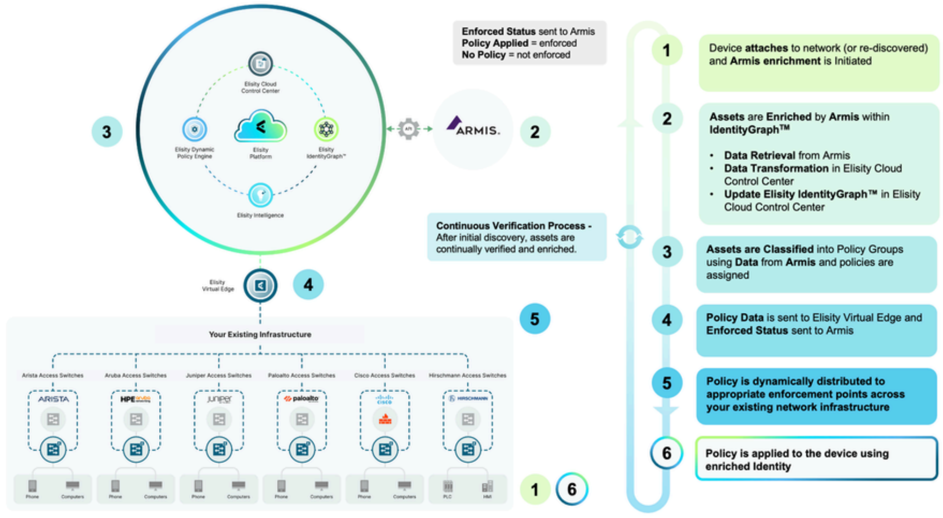
Rapid Deployment: Quickly deploy the integrated solution over existing infrastructure, delivering immediate value without extensive reconfiguration.

Simplified Segmentation: Automate and simplify segmentation projects using detailed asset data, reducing operational complexity and costs.

Enhanced Security Posture

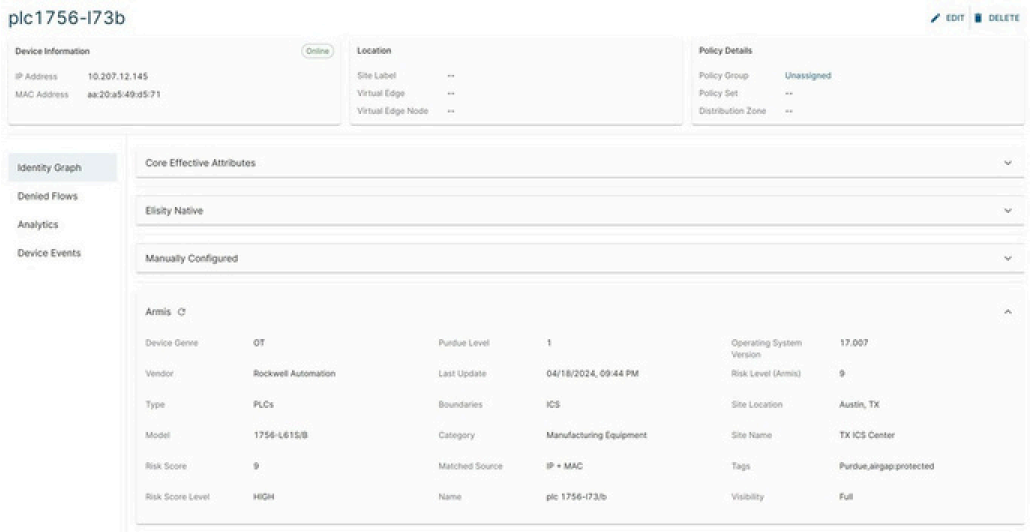
Proactive Risk Management: Prioritize and address high-risk assets using ARMIS's risk scores and attributes for robust threat protection.

How it Works


Enforced Status sent to Armis
Policy Applied = enforced
No Policy = not enforced
Elisity Cloud Control Center
Elisity Dynamic Policy Engine
Elisity Platform
Elisity IdentityGraph™
Elisity Intelligence
API
ARMIS.
3
2
Continuous Verification Process - After initial discovery, assets are continually verified and enriched.
Elisity Virtual Edge
4
5
Your Existing Infrastructure
Arista Access Switches
Aruba Access Switches
Juniper Access Switches
Paloalto Access Switches
Cisco Access Switches
Hirschmann Access Switches
Phone
Computers
PLC
HMI
1
6

1. Device **attaches** to network (or re-discovered) and **Armis enrichment** is Initiated
2. **Assets** are **Enriched** by **Armis** within **IdentityGraph™**
   - **Data Retrieval** from Armis
   - **Data Transformation** in Elisity Cloud Control Center
   - **Update Elisity IdentityGraph™** in Elisity Cloud Control Center
3. **Assets are Classified** into Policy Groups using **Data** from **Armis** and policies are assigned
4. **Policy Data** is sent to Elisity Virtual Edge and **Enforced Status** sent to Armis
5. **Policy is dynamically distributed to appropriate enforcement points across your existing network infrastructure**
6. **Policy is applied to the device using enriched Identity**

Simple API level integration – Connect Elisity and Armis together in minutes by entering API credentials in Cloud Control Center



plc1756-I73b

Device Information — Online

IP Address	10.207.12.145
MAC Address	aa:20:a5:49:d5:71

Location

Site Label	--
Virtual Edge	--
Virtual Edge Node	--

Policy Details

Policy Group	Unassigned
Policy Set	--
Distribution Zone	--

Core Effective Attributes

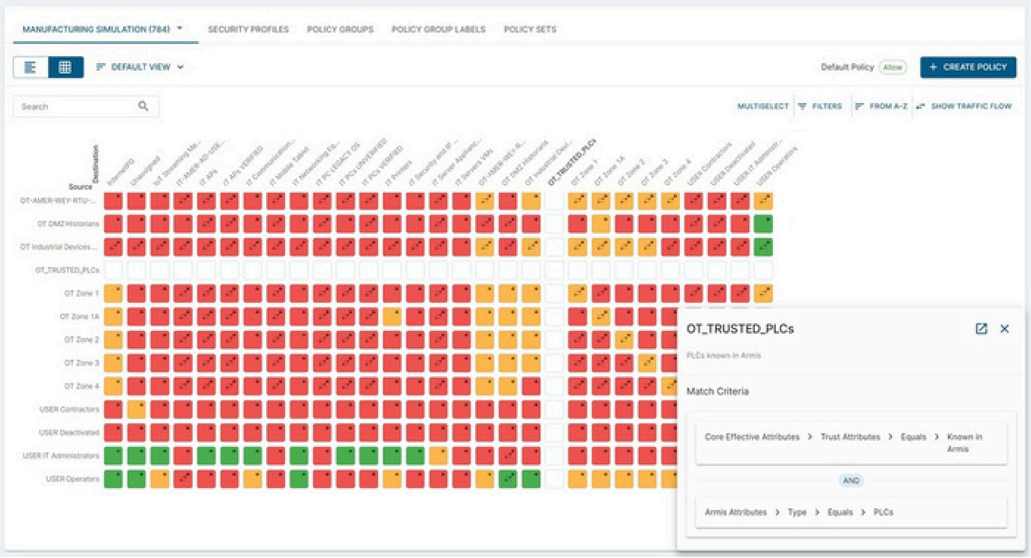
Elisity Native

Manually Configured

Armis

Device Genre	OT	Purdue Level	1	Operating System Version	17.007
Vendor	Rockwell Automation	Last Update	04/18/2024, 09:44 PM	Risk Level (Armis)	9
Type	PLCs	Boundaries	ICS	Site Location	Austin, TX
Model	1756-L615/B	Category	Manufacturing Equipment	Site Name	TX ICS Center
Risk Score	9	Matched Source	IP + MAC	Tags	Purdue,airgap:protected
Risk Score Level	HIGH	Name	plc 1756-I73/b	Visibility	Full

Elisity device attributes are immediately enriched with data from Armis



OT_TRUSTED_PLCs

PLCs known in Armis

Match Criteria

Core Effective Attributes > Trust Attributes > Equals > Known in Armis

AND

Armis Attributes > Type > Equals > PLCs

Elisity enables you to leverage the device attributes to create effective Least Privilege Access policies in a rapid manner and meet industry standards such as IEC 62443

Armis and Elisity

Armis

ARMIS is designed to help both IT and OT teams overcome challenges associated with digital transformation and a converged IT/OT network environment. It enables detection and response to the earliest indicators of threats while extending existing enterprise security and risk infrastructure to industrial networks. This solution ensures that the controls used in IT environments to minimize risks are similarly applied in OT environments, enhancing overall network security.

The Elisity Platform

Elisity offers a versatile identity-based microsegmentation platform designed for seamless integration with existing access layer switching infrastructure, requiring no additional hardware or network downtime. The platform delivers a wide range of benefits, including non-disruptive deployment, quick time-to-value, comprehensive microsegmentation, adaptability, scalability, and visibility, making it suitable for organizations at any scale.

By leveraging Elisity IdentityGraph™, the platform provides context for effective security policy management, enabling granular, least privilege access policies through identity-based microsegmentation. This approach secures not only IT assets but also Operational Technology (OT) devices, ensuring compliance with industry-specific regulations. With cloud-delivered agility and speed, Elisity can be deployed within an hour, without the need for hardware or network upgrades, making it a highly efficient and robust solution for organizations seeking to enhance their network security and compliance.

About Elisity

Elisity is a leap forward in network segmentation architecture and is leading the enterprise effort to achieve Zero Trust maturity, proactively prevent security risks, and reduce network complexity. Designed to be implemented in days, without downtime, upon implementation, the platform rapidly discovers every device on an enterprise network and correlates comprehensive device insights into the Elisity IdentityGraph™. This empowers teams with the context needed to automate classification and apply dynamic security policies to any device wherever and whenever it appears on the network. These granular, identity-based microsegmentation security policies are managed in the cloud and enforced using your existing network switching infrastructure in real-time, even on ephemeral IT/IoT/OT devices. Founded in 2019, Elisity has a global employee footprint and a growing number of customers in the Fortune 500

About Armis

ARMIS, a leading asset intelligence cybersecurity company, safeguards the entire attack surface and manages an organization's cyber risk exposure in real time. In today's rapidly evolving, perimeter-less world, ARMIS ensures continuous visibility, protection, and management of all critical assets. The company secures Fortune 100, 200, and 500 companies, as well as national governments and local entities, helping to keep critical infrastructure, economies, and societies safe and secure around the clock. ARMIS is a privately held company headquartered in California.