INTEGRATION BRIEF

Armis and Elisity

Delivering Frictionless, Centrally Managed Zero Trust Access

The Industrial Cybersecurity Challenge

The exponential growth of connected devices, including IoT, OT, 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 Integration

Elisity seamlessly integrates with ARMIS to enhance IdentityGraph, Elisity's comprehensive device identity and attribute database. This integration leverages ARMIS's extensive asset intelligence to provide detailed device attributes such as risk score, risk score level, boundaries, device type, manufacturer, model, operating system, firmware version, and network segment. These enriched attributes serve as critical criteria for Elisity's classification and policy enforcement, enabling precise, context-aware security policies across the network.

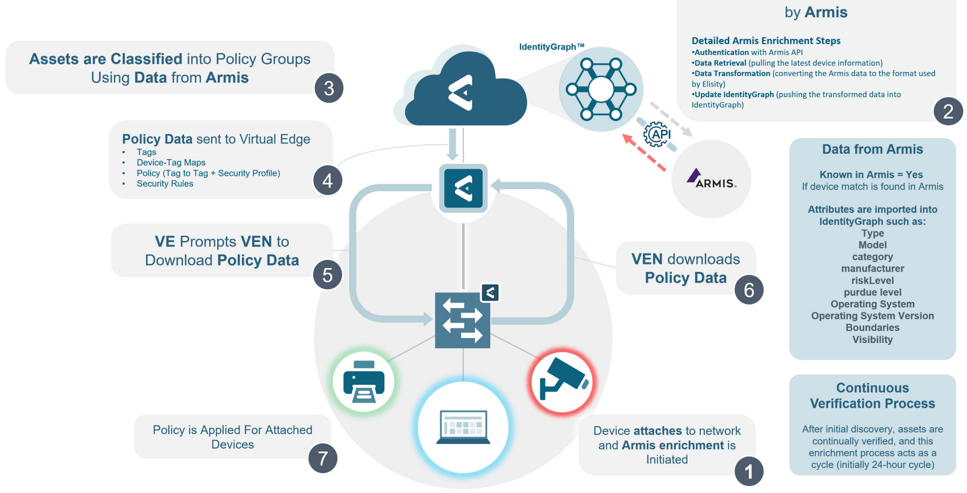
By combining ARMIS's in-depth asset visibility with Elisity's dynamic policy management, organizations gain immediate insight into their network environments. This visibility allows for the quick assessment of risks and the implementation of least privilege access policies. The integration ensures that security measures are dynamically enforced at the network edge, protecting critical enterprise assets from both internal and external threats.

Key Features & Benefits

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.

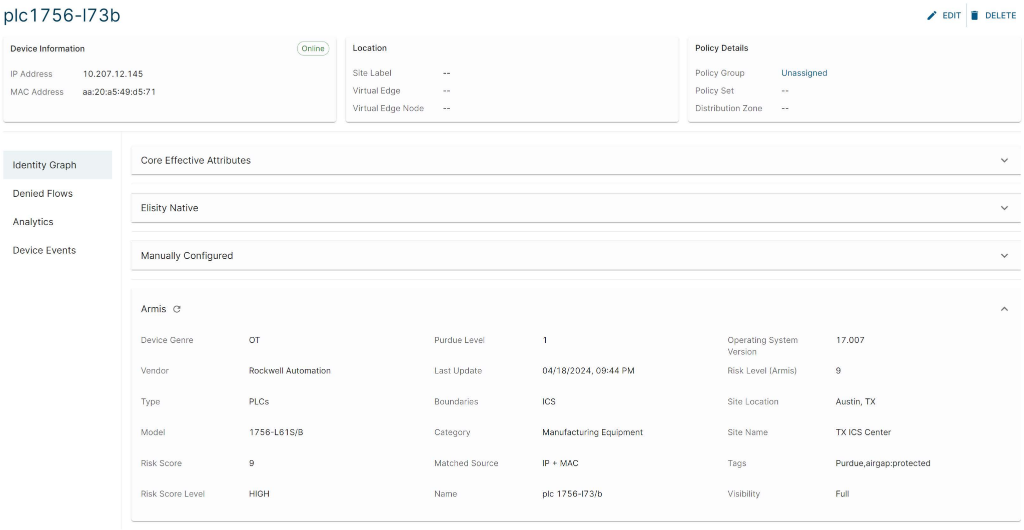
How it Works

Armis Enrichment



Assets are Classified into Policy Groups Using Data from Armis
3
Policy Data sent to Virtual Edge
• Tags
• Device-Tag Maps
• Policy (Tag to Tag + Security Profile)
• Security Rules
4
VE Prompts VEN to Download Policy Data
5
Policy is Applied For Attached Devices
7
IdentityGraph™
API
ARMIS.
Assets are Identified and Enriched by Armis
Detailed Armis Enrichment Steps
•Authentication with Armis API
•Data Retrieval (pulling the latest device information)
•Data Transformation (converting the Armis data to the format used by Elisity)
•Update IdentityGraph (pushing the transformed data into IdentityGraph)
2
Data from Armis
Known in Armis = Yes
If device match is found in Armis
Attributes are imported into IdentityGraph such as:
Type
Model
category
manufacturer
riskLevel
purdue level
Operating System
Operating System Version
Boundaries
Visibility
VEN downloads Policy Data
6
Continuous Verification Process
After initial discovery, assets are continually verified, and this enrichment process acts as a cycle (initially 24-hour cycle)
Device attaches to network and Armis enrichment is Initiated
1

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



plc1756-l73b

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 --

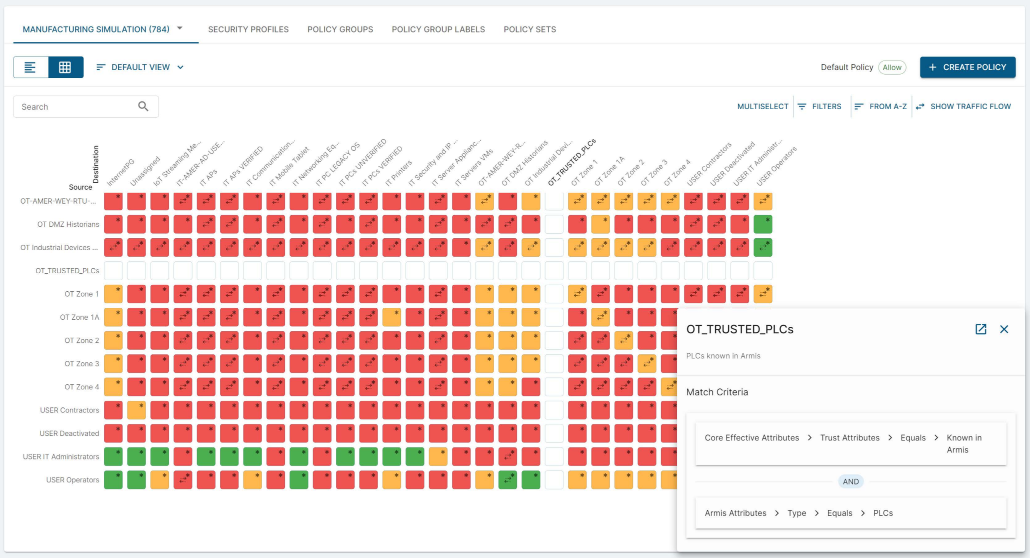
Policy Details

Policy Group Unassigned
Policy Set --
Distribution Zone --

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-L61S/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-l73/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 IdentityGraph, Elisity 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 cloud-native security solution that provides frictionless, centrally managed least privilege access to protect corporate data and critical assets from malicious lateral movement across the network. Their identity-based microsegmentation technology allows organizations to quickly gain visibility into network assets and traffic flows, enabling the creation of policies to protect the most critical enterprise assets. Elisity is simple to deploy and manage, offering non-disruptive deployment, rapid time to value, and adaptability to organizations of all sizes. Backed by Two Bear Capital, AllegisCyber Capital, and Atlantic Bridge, Elisity requires no additional hardware or network downtime, making it an ideal solution for enhancing existing access layer switching infrastructure.

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.