INTEGRATION BRIEF

Nozomi Networks and Elisity

Delivering Frictionless, Centrally Managed Zero Trust Access

The Industrial Cybersecurity Challenge

In recent years, the rapid integration of connected devices, particularly in Operational Technology (OT) environments, has created an expanded attack surface for organizations. As the number of devices increases, so too does the complexity and risk associated with managing them. The industrial sector is particularly vulnerable, with many legacy devices and systems that lack built-in security features, making them easy targets for cyber threats.

To address these challenges, organizations require comprehensive solutions that not only provide visibility into their network assets but also enable robust security controls tailored to the unique requirements of industrial environments.

The Integration

Elisity seamlessly integrates with Nozomi Networks to enhance Elisity's IdentityGraph, Elisity's identity engine that provides a powerful device identity and attribute database. This integration enriches the device data in IndentityGraph with critical attributes from Nozomi, including device type, manufacturer, model, operating system, firmware version, and other key details essential for precise security policy management.

With this enriched data, Elisity enables the creation of granular or broad least privilege access policies that are dynamically enforced at the network edge. This approach ensures that organizations can quickly establish a zero trust security model, protecting critical assets from unauthorized access and malicious traffic.

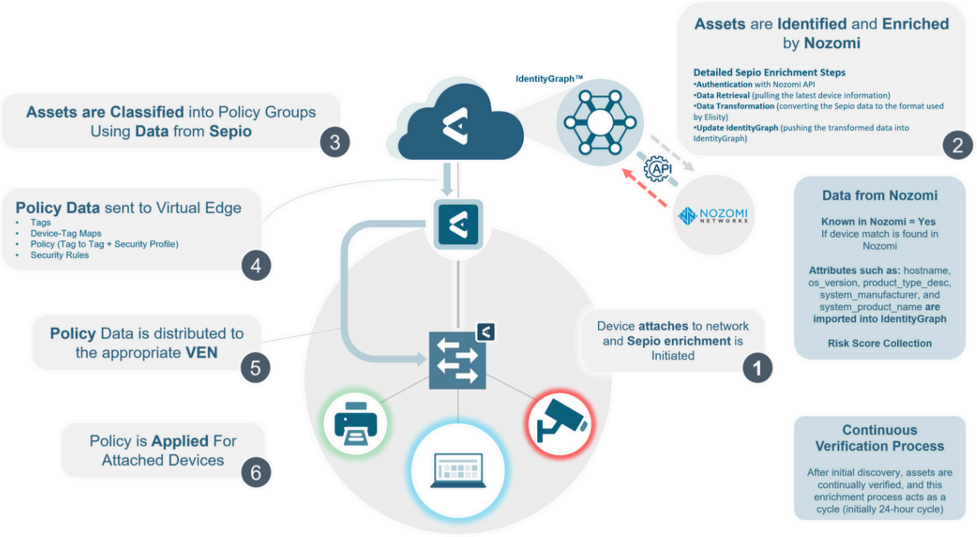
Key Features & Beneifts

- Comprehensive Visibility: By integrating with Nozomi, Elisity provides unmatched visibility into network assets and traffic flows, uncovering previously unknown devices and enabling continuous monitoring for potential threats. This visibility is crucial for identifying vulnerabilities and maintaining a secure network environment.

- Enhanced Control: Elisity's integration with Nozomi allows for the implementation of identity- based, least privilege access policies. These policies are decoupled from the underlying network infrastructure, enabling organizations to control both North- South and East-West traffic effectively, reducing the risk of lateral movement by threats within the network.

- Simplified Deployment: The integration is designed for quick deployment, leveraging existing infrastructure. This minimizes the complexity of segmentation projects and accelerates the time-to-value, reducing operational expenses while enhancing security.

How it Works



Assets are Identified and Enriched by Nozomi

Detailed Sepio Enrichment Steps
- •Authentication with Nozomi API
- •Data Retrieval (pulling the latest device information)
- •Data Transformation (converting the Sepio data to the format used by Elisity)
- •Update IdentityGraph (pushing the transformed data into IdentityGraph)

2

Data from Nozomi

Known in Nozomi = Yes
If device match is found in Nozomi

Attributes such as: hostname, os_version, product_type_desc, system_manufacturer, and system_product_name are imported into IdentityGraph

Risk Score Collection

Device attaches to network and Sepio enrichment is Initiated 1

Assets are Classified into Policy Groups Using Data from Sepio 3

Policy Data sent to Virtual Edge
- Tags
- Device-Tag Maps
- Policy (Tag to Tag + Security Profile)
- Security Rules

4

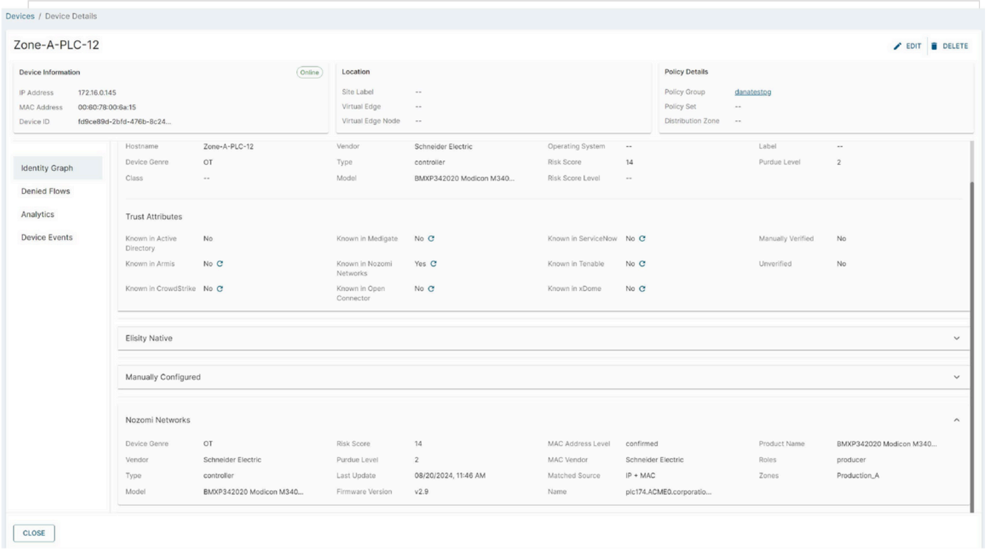
Policy Data is distributed to the appropriate VEN 5

Policy is Applied For Attached Devices 6

Continuous Verification Process

After initial discovery, assets are continually verified, and this enrichment process acts as a cycle (initially 24-hour cycle)

Simple API Integration: Connecting Elisity with Nozomi Networks is straightforward and can be accomplished within minutes by entering API credentials in the Elisity Cloud Control Center.



Devices / Device Details

Zone-A-PLC-12

Device Information Online

IP Address	172.16.0.145
MAC Address	00:60:78:00:6a:15
Device ID	fd9ce89d-2bfd-476b-8c24...

Location

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

Policy Details

Policy Group	danatestpg
Policy Set	--
Distribution Zone	--

Hostname	Zone-A-PLC-12	Vendor	Schneider Electric	Operating System	--	Label	--
Device Genre	OT	Type	controller	Risk Score	14	Purdue Level	2
Class	--	Model	BMXP342020 Modicon M340...	Risk Score Level	--		

Trust Attributes

Known in Active Directory	No	Known in Medigate	No	Known in ServiceNow	No	Manually Verified	No
Known in Armis	No	Known in Nozomi Networks	Yes	Known in Tenable	No	Unverified	No
Known in CrowdStrike	No	Known in Open Connector	No	Known in xDome	No		

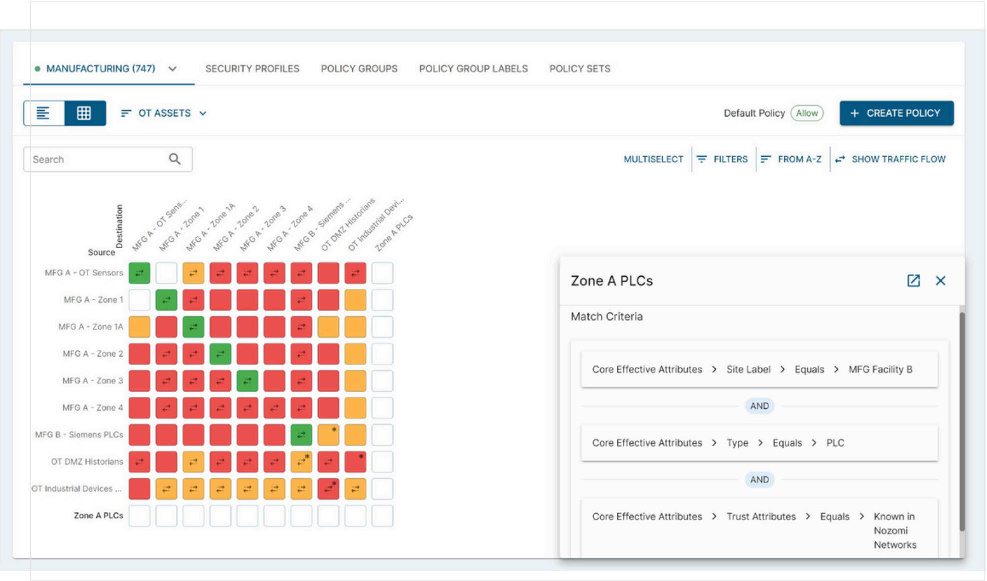
Elisity Native

Manually Configured

Nozomi Networks

Device Genre	OT	Risk Score	14	MAC Address Level	confirmed	Product Name	BMXP342020 Modicon M340...
Vendor	Schneider Electric	Purdue Level	2	MAC Vendor	Schneider Electric	Roles	producer
Type	controller	Last Update	08/20/2024, 11:46 AM	Matched Source	IP + MAC	Zones	Production_A
Model	BMXP342020 Modicon M340...	Firmware Version	v2.9	Name	plc174.ACME0.corporatio...		

Real-Time Data Enrichment: Once connected, Elisity's IdentityGraph is immediately enriched with data from Nozomi, providing a deeper understanding of each device on the network.



Source \ Destination	MFG A - OT Sens...	MFG A - Zone 1	MFG A - Zone 1A	MFG A - Zone 2	MFG A - Zone 3	MFG A - Zone 4	MFG B - Siemens ...	OT DMZ Historians	OT Industrial Devi...	Zone A PLCs
MFG A - OT Sensors	🟩⇄		🟧⇄	🟥⇄	🟥⇄	🟥⇄	🟥⇄	🟥	🟥⇄	
MFG A - Zone 1		🟩⇄	🟥⇄	🟥	🟥	🟥	🟥⇄	🟥	🟧	
MFG A - Zone 1A	🟧	🟥	🟩⇄	🟥	🟥	🟥	🟥⇄	🟧	🟧	
MFG A - Zone 2	🟥	🟥⇄	🟥⇄	🟩⇄	🟥	🟥	🟥⇄	🟥	🟧	
MFG A - Zone 3	🟥	🟥⇄	🟥⇄	🟥⇄	🟩⇄	🟥	🟥⇄	🟥	🟧	
MFG A - Zone 4	🟥	🟥⇄	🟥⇄	🟥⇄	🟥⇄	🟥⇄	🟥⇄	🟥	🟧	
MFG B - Siemens PLCs	🟥	🟥	🟥	🟥	🟥	🟥	🟩⇄	🟧*	🟧	
OT DMZ Historians	🟥⇄	🟥	🟧⇄	🟥⇄	🟥⇄	🟥⇄	🟧⇄*	🟥⇄	🟥*	
OT Industrial Devices ...	🟥	🟧⇄	🟧⇄	🟧⇄	🟧⇄	🟧⇄	🟧⇄	🟥⇄*	🟧⇄	
Zone A PLCs										

Zone A PLCs

Match Criteria

Core Effective Attributes > Site Label > Equals > MFG Facility B

AND

Core Effective Attributes > Type > Equals > PLC

AND

Core Effective Attributes > Trust Attributes > Equals > Known in Nozomi Networks

Policy Creation: Leveraging the enriched data, organizations can swiftly build and deploy least privilege access policies that comply with industry standards such as IEC 62443, ensuring both security and regulatory compliance.

Nazomi Networks and Elisity

Nozomi Networks

Nozomi Networks specializes in delivering real-time visibility, threat detection, and insights into OT and IoT environments, making it a critical partner in enhancing industrial cybersecurity. Its solutions help organizations protect critical infrastructure by offering in-depth analysis and robust security controls tailored to the specific needs of industrial networks.

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 of all sizes.

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 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 during 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 security policies are managed in the cloud and enforced across enterprise environments in real-time, even on ephemeral IT/IoT/OT devices, using your existing network switching infrastructure. Founded in 2019, Elisity has a global employee footprint and a growing number of customers in the Fortune 500.

About Nozomi Networks

Nozomi Networks is a leader in OT and IoT security, providing organizations with the tools they need to secure their critical infrastructure. The company's solutions deliver comprehensive visibility, risk management, and threat detection across industrial environments. Nozomi Networks' technology is deployed globally, protecting critical assets in industries ranging from energy and manufacturing to healthcare.

For more information, visit nozominetworks.com or contact the Nozomi Networks team for further inquiries.

NOZOMI NETWORKS | ELISITY