INTEGRATION BRIEF

Claroty xDome and Elisity

Delivering Frictionless, Centrally Managed Zero Trust Access

The Industrial Cybersecurity Challenge

The explosive growth of Operational Technology (OT) and Extended Internet of Things (XIoT) devices has revolutionized industrial operations—but also exposed them to unprecedented risk. Many of these devices lack foundational security controls and are difficult or impossible to monitor using traditional tools.

Each new unmanaged device increases an organization's exposure to cyber threats. As digital transformation accelerates, organizations must secure operational networks without sacrificing uptime, introducing agents, or overhauling existing infrastructure.

The Power of Bidirectional Integration

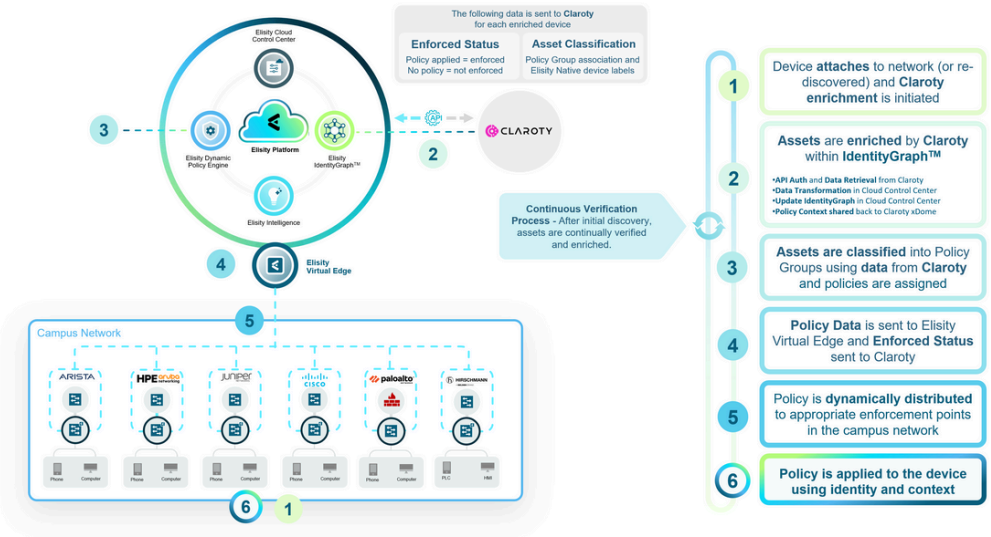
Elisity connects to Claroty xDome through a native API integration to establish a bidirectional flow of asset identity and policy context. Device attributes collected by xDome such as device type, model, manufacturer, serial number, OS, firmware version, Purdue level, and custom Claroty tags - are ingested into Elisity IdentityGraph™ and used as classification criteria for assigning devices into Policy Groups.

Elisity also shares policy context back to xDome for assets enriched by Claroty within IdentityGraph. For those devices, Elisity returns the current Policy Group classification, enforcement status, and any manually assigned device labels. This provides enforcement visibility directly in xDome, enabling teams to verify policy coverage and quickly identify unmanaged or unprotected assets.

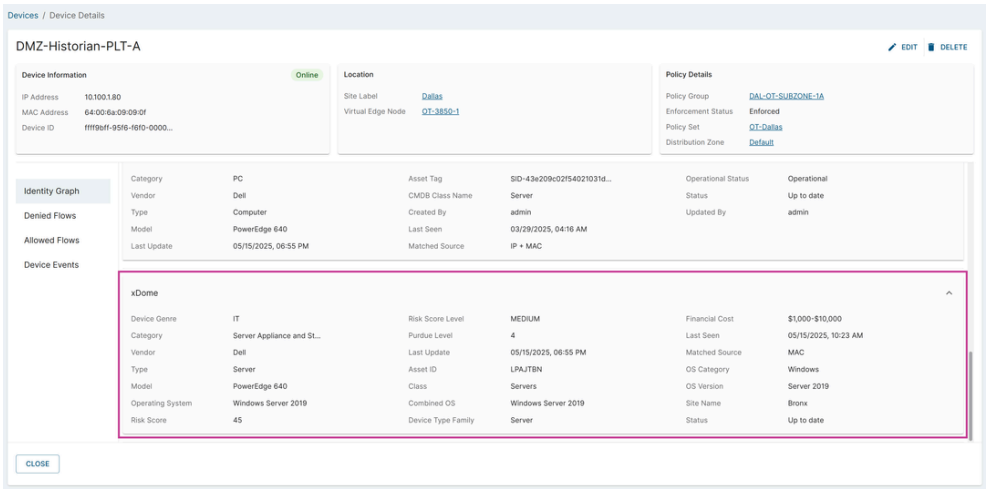
Key Features & Benefits

Discover	**Comprehensive Asset Discovery:** Elisity identifies all devices on the network and enriches them with data from Claroty, enabling behavior monitoring, continuous threat detection, and classification for policy enforcement.
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.
Bidirectional Integration	Elisity doesn't just ingest asset identity from Claroty - Elisity shares Policy Enforcement Status and Classification of Assets for enhanced visibility and alerting of gaps in policy.

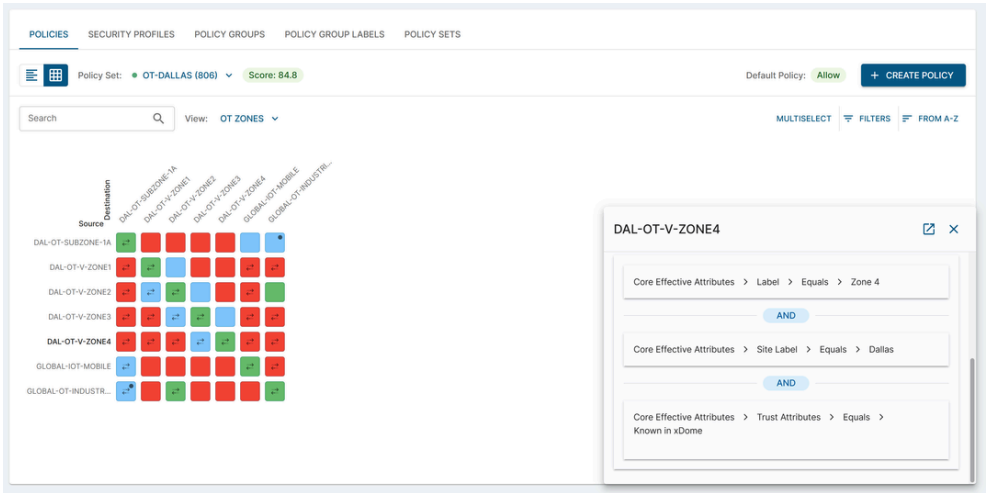
How it Works



Elisity connects to Claroty xDome through a simple API integration. Devices are discovered by Elisity and enriched with identity and operational metadata from Claroty. This data is ingested into IdentityGraph™, where it's used for classification and enforcement decisions. Enriched devices are dynamically assigned policies, and enforcement context is shared back to xDome.



IdentityGraph provides a unified view of Claroty-enriched assets, combining discovery, classification, and policy enforcement context, enabling fast and informed policy decisions.



Devices enriched with Claroty attributes are classified into Policy Groups using match criteria from IdentityGraph and Trust Attributes like "Known in xDome." These Policy Groups are used to build and enforce identity-based access policies, supporting segmentation aligned with IEC 62443 and similar frameworks.

Claroty xDome and Elisity

Claroty xDome

Claroty xDome was 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 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 a wide variety of both managed and unmanaged 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 Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally.

For more information, visit claroty.com or email contact@claroty.com.