ELISITY ORDR

INTEGRATION BRIEF

Elisity and ORDR

Delivering Centrally Managed Zero Trust Security

Device Intelligence | Risk Status

Key Features & Benefits

- Discover every device on the network and classify with enriched data with ORDR
- Control access to on-prem resources based on trust and compliance from ORDR
- Simplify segmentation by automating policy using identity, without network redesign or manual configuration

The Challenge of Managing Access in Hybrid Environments

Modern enterprise networks host a constantly evolving mix of IT, IoT, and OT devices, many of which operate without agents and offer limited native visibility or control.

While platforms like ORDR provide deep, real-time insight into device identity, behavior, and risk posture, many organizations still struggle to translate that intelligence into consistent access control at the network edge. Traditional segmentation methods lack the context needed to distinguish between trusted and unmanaged devices in real time. As environments grow more dynamic, security teams need a way to enforce access based on continuously updated device intelligence—not static network attributes—to reduce exposure and support Zero Trust initiatives.

Integration Overview

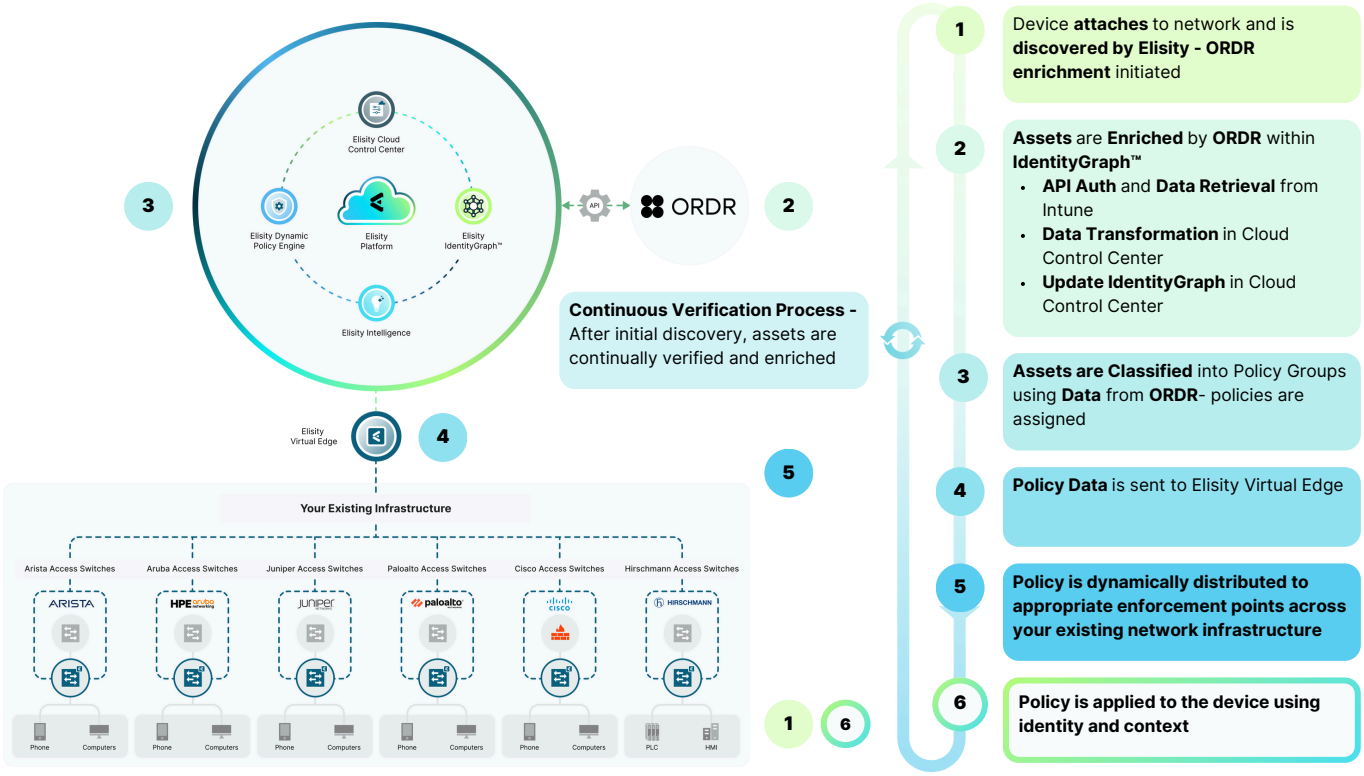
Elisity's Integration with ORDR

Elisity integrates with ORDR through a native API connector to ingest rich device telemetry into IdentityGraph™. Attributes such as MAC and IP addresses, device type, manufacturer, model, and behavioral fingerprinting are used to classify unmanaged and agentless assets into Policy Groups.

Context-Aware Access Control

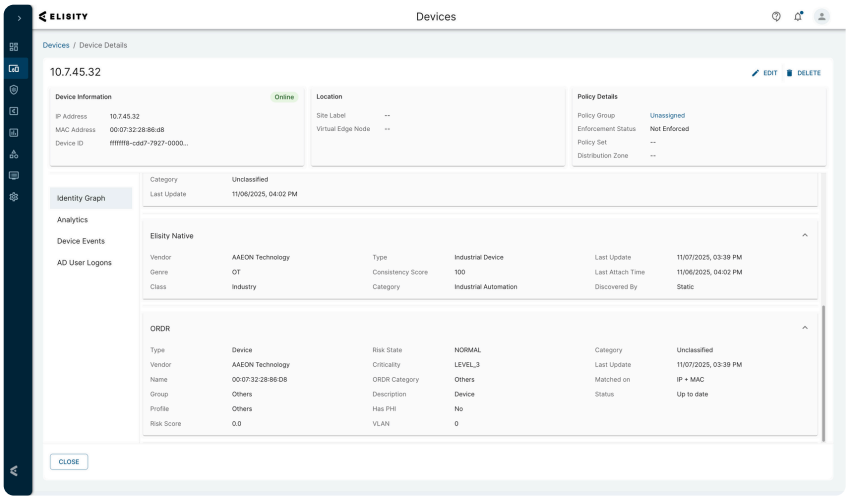
This identity enrichment enables precise, context-aware microsegmentation policies. Security teams can build dynamic trust policies based on ORDR-classified device insights, ensuring that access is only granted to verified, known, and trusted assets. By combining ORDR's real-time visibility with Elisity's identity-based policy engine, organizations can strengthen segmentation strategies and gain greater control over access behavior across distributed environments.

How It Works



Elisity connects to ORDR through a simple API integration. Devices are discovered by Elisity and enriched with identity and operational metadata from ORDR. This data is ingested into IdentityGraph™, where it informs policy group assignment and enforcement logic. Enriched assets are dynamically mapped to the appropriate policies, which are then distributed only to relevant onboarded infrastructure. As ORDR continues to monitor the environment, any change in device state or trust posture triggers an automatic policy reevaluation—enabling real-time containment and adaptive enforcement in breach or quarantine scenarios.

Elisity Platform



Devices enriched with ORDR attributes are classified into Policy Groups using match criteria from IdentityGraph and Trust Attributes like “Known in ORDR”. These Policy Groups are used to build and enforce identity-based access policies, supporting segmentation aligned with compliance frameworks and preventing lateral movement.

Better Together

Enrich identity-based microsegmentation with real-time asset visibility and risk telemetry from ORDR to automate containment, accelerate response, and reduce risk across your network. Elisity integrates ORDR telemetry into IdentityGraph™, enabling dynamic classification of unmanaged, agentless, and IoT/OT devices. This allows organizations to apply context-driven policies, quarantine risky assets instantly, and trigger policy updates directly at the network edge.

- Dynamically assign assets to Policy Groups based on ORDR trust posture and classification
- Automate enforcement actions across sites using Policy Sets and Site Labels
- Minimize lateral movement and isolate compromised or unknown devices in real time
- Reduce mean time to response (MTTR) through integrated policy enforcement and device telemetry

The Elisity Platform

Elisity offers a versatile identity-based microsegmentation platform designed for seamless integration with existing access layer switching infrastructure—no additional hardware or network downtime required. The platform enables rapid deployment, comprehensive visibility, and precise policy enforcement. With scalability and adaptability at its core, Elisity empowers organizations of all sizes to implement Zero Trust without disruption.

ORDR

ORDR delivers deep, passive asset discovery and classification across IT, IoT, and OT environments. Its platform provides rich device context—including behavior, risk posture, and classification—without requiring endpoint agents. By continuously monitoring devices on the network and surfacing actionable telemetry, ORDR enables security teams to gain visibility, assess trust, and drive enforcement decisions with precision.

Try the Elisity Platform and Receive a Personalized Microsegmentation Plan

Book a Demo

- Access Support Portal
- Take Virtual Product Tour
- Schedule a Demo

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.

ORDR is the leader in connected device visibility and security

ORDR enables organizations to discover, classify, and assess every connected asset—regardless of type or vendor—using passive monitoring and advanced analytics. The platform surfaces rich context such as device type, location, behavior, and trust score to help teams manage risk and automate policy decisions. Trusted across industries, ORDR helps enterprises secure everything from critical infrastructure to clinical environments, with a scalable solution that fits into existing network operations.

www.elisity.com

Gartner COOL VENDOR 2025