Elisity and SentinelOne

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 SentinelOne
- Control access to on-prem resources based on trust and compliance from SentinelOne
- Simplify segmentation by automating policy using identity, without network redesign or manual configuration

The Challenge of Managing Access in Hybrid Environments

Modern enterprises rely on platforms like SentinelOne to deliver autonomous protection, detection, and response at the endpoint—forming a critical layer of defense in any Zero Trust architecture. Yet as organizations expand across hybrid networks, they need a way to extend that same level of control and intelligence to the access edge. Elisity integrates with SentinelOne to translate endpoint risk and compliance insights into dynamic network policies, ensuring that trusted devices maintain appropriate access while minimizing opportunities for lateral movement. Together, they bridge the gap between endpoint protection and network segmentation to deliver continuous, adaptive Zero Trust enforcement.

Intergation Overview

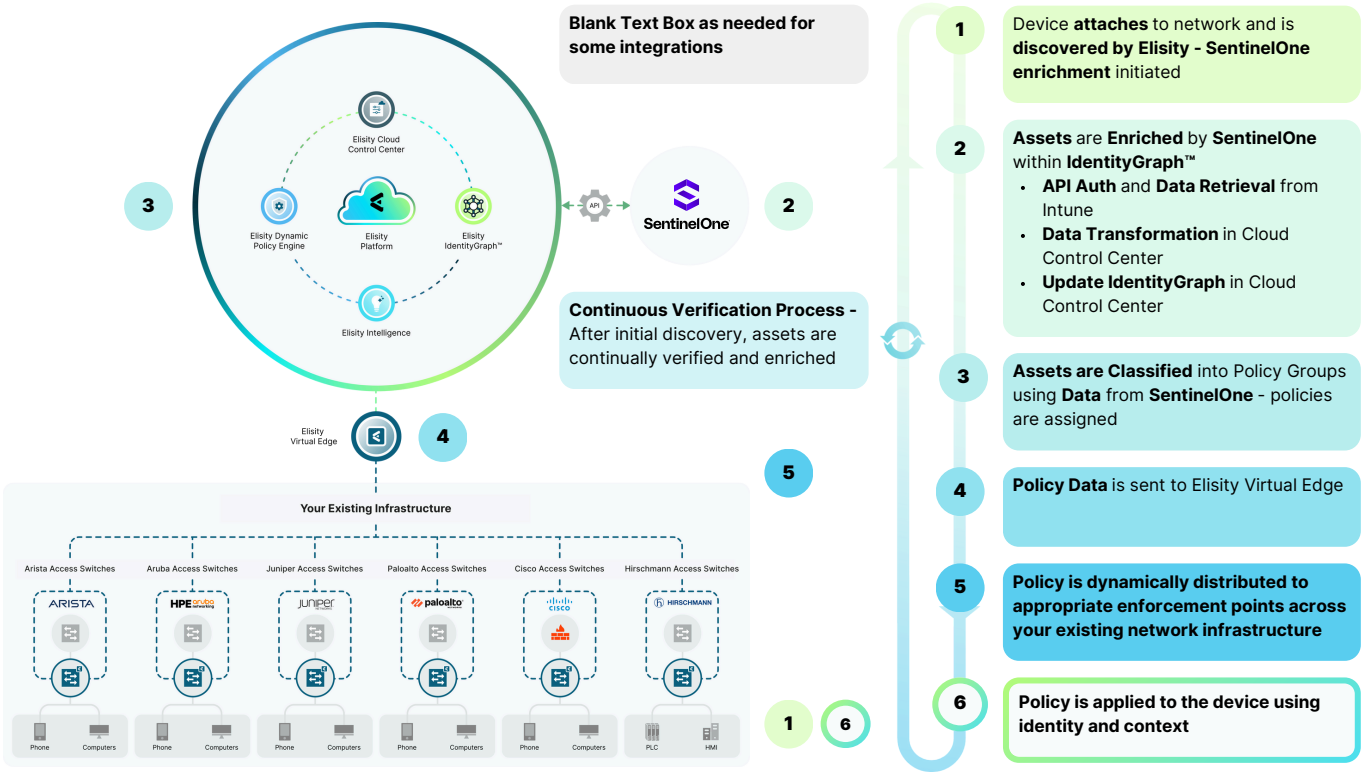
Elisity's Integration with SentinelOne

Elisity integrates with SentinelOne through a native API connector to ingest rich endpoint data into IdentityGraph™. Attributes such as operating system, hostname, IP and MAC addresses, agent version, and domain context are used to classify endpoints into Policy Groups.

Context-Aware Access Control

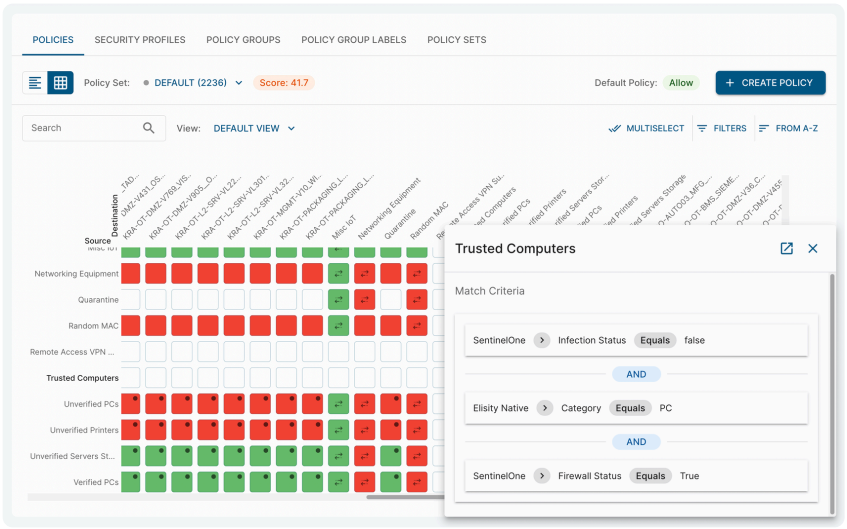
This identity enrichment enables precise, context-aware microsegmentation policies. Security teams can build dynamic trust policies based on SentinelOne-managed device visibility, ensuring that access is only granted to verified, managed, and trusted assets. By combining SentinelOne's deep endpoint telemetry 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 SentinelOne through a simple API integration. Devices are discovered by Elisity and enriched with identity and operational metadata from SentinelOne. This data is ingested into IdentityGraph™, where it's used for classification and enforcement decisions. Enriched devices are dynamically assigned policies, and policies are distributed to only relevant onboarded infrastructure. Assets are continually verified and policy is updated if new data is discovered from SentinelOne, useful in any kind of active breach or quarantine scenario.

Elisity Platform



Devices enriched with SentinelOne attributes are classified into Policy Groups using match criteria from IdentityGraph and Trust Attributes like "Known in SentinelOne". 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 behavioral threat intelligence from SentinelOne to automate containment, accelerate response, and reduce risk across your network. Elisity integrates SentinelOne telemetry into IdentityGraph, allowing dynamic classification of infected or high-risk assets into Policy Groups. These groups can then drive automatic policy updates and incident response workflows at the network edge, without manual intervention.

- Dynamically assign assets to Policy Groups based on SentinelOne threat indicators
- Automate enforcement actions across sites using Policy Sets and Site Labels
- Minimize lateral movement and isolate infected devices in real time
- Reduce mean time to respond (MTTR) through integrated policy and endpoint telemetry

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.

SentinelOne

The SentinelOne Singularity™ Platform is an AI-powered Extended Detection and Response (XDR) solution designed to provide autonomous cybersecurity across endpoints, cloud workloads, identities, and network-connected devices.

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.

SentinelOne is the world's most advanced cybersecurity platform.

The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and networkconnected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

Gartner COOL VENDOR 2025