Integration Brief

ELISITY

Remedio

Delivering Frictionless, Centrally Managed Zero Trust Access

The Industrial Cybersecurity Challenge

The challenge of unsecured endpoints represents one of the most significant vulnerabilities in an organization's network. As enterprises expand and adopt new technologies, the number of endpoints—ranging from traditional computers to IoT devices—continues to grow. This increases the attack surface and makes it a challenge to maintain comprehensive security across all devices.

The Integration

Elisity now seamlessly integrates with Remedio to enhance endpoint security and microsegmentation capabilities. By connecting with Remedio, Elisity's IdentityGraph is enriched with critical endpoint data, including configurations, compliance statuses, and vulnerability information. This allows organizations to create more effective and granular least privilege access policies, ensuring that only authorized devices and users can access sensitive resources.

Key Features & Benefits

Visibility: The integration provides comprehensive visibility into endpoint misconfigurations and compliance issues, helping identify and address security gaps.

Control: The integration enables enforcement of identity and context-based least privilege access policies, both for North-South and East-West traffic, across the network.

Simplicity: The integration deploys quickly and leverages existing infrastructure, simplifying the implementation of micro-segmentation — reducing operational complexity and costs.

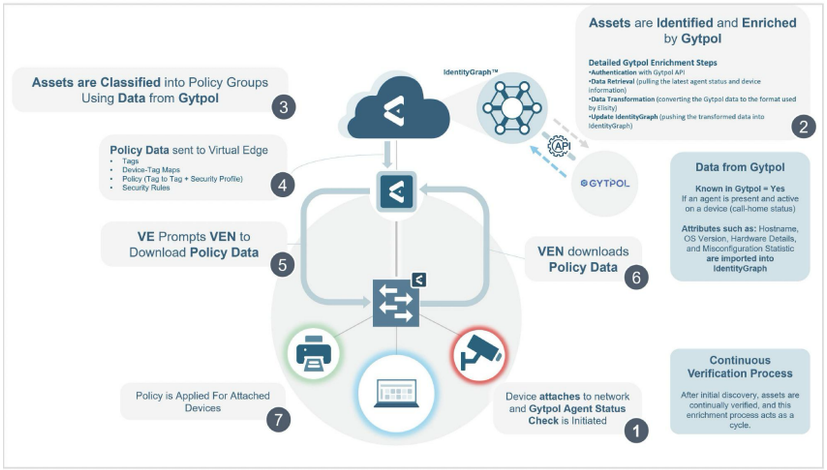
Integration Brief

ELISITY

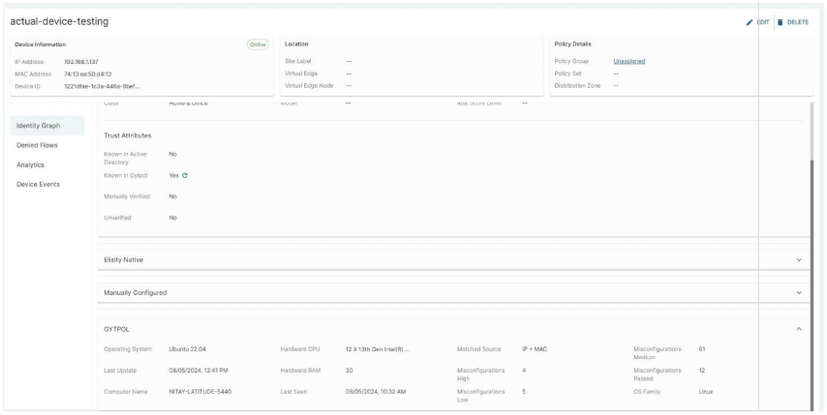
Remedio

Delivering Frictionless, Centrally Managed Zero Trust Access

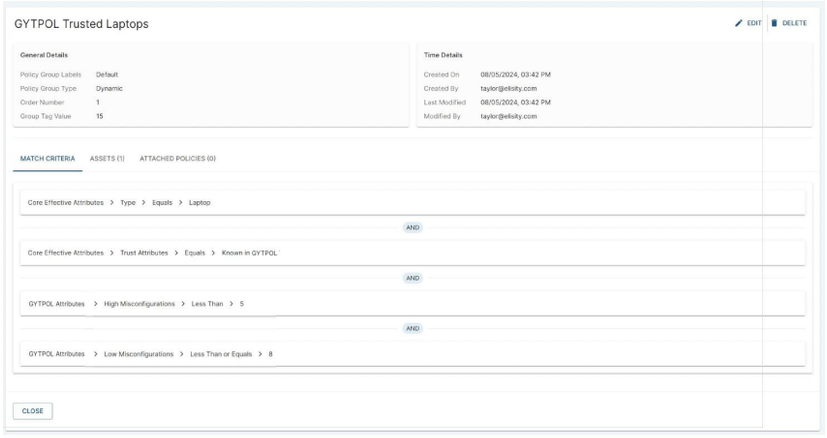
How it Works



Simple API Integration: Connect Elisity and Remedio through API credentials in the Cloud Control Center within minutes.



Enriched Endpoint Data: Elisity's IdentityGraph is immediately updated with endpoint data from Remedio.



Policy Enforcement: Utilize enriched data to rapidly establish and enforce least privilege access policies, meeting industry standards and enhancing overall security posture.

Integration Brief

ELISITY

Remedio

Delivering Frictionless, Centrally Managed Zero Trust Access

Elisity and Remedio

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 industryspecific 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.

Remedio Endpoint Security

Remedio specializes in endpoint security management, providing solutions that ensure endpoint compliance, mitigate vulnerabilities, and enforce security policies. The Remedio platform enables organizations to continuously monitor and manage endpoint configurations, ensuring that all devices adhere to corporate security standards.

Remedio helps identify misconfigurations and vulnerabilities that could be exploited by attackers. Remedio automatically analyzes potential impact before remediations take place to prevent disrupting of proper endpoint operation.

Integration Brief

ELISITY

Remedio

Delivering Frictionless, Centrally Managed Zero Trust Access

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 Remedio

Founded in 2019, Remedio is a first-of-its-kind solution provider focused on the configuration side of endpoint security. Predicated on principles of automation and prevention, Remedio continuously monitors your devices and systems, detecting unpatched vulnerabilities and insecure configurations. The platform enables proactive and non-disruptive remediation (or reversion) at the push of a button — ensuring safe and strict policy adherence while bolstering operational resilience and business continuity.

With Remedio, it's easy to bring any device or group in line with the standards of your choosing (e.g. CIS, NIST, etc.). Additionally, Remedio helps organizations create and enforce golden image configurations — assuring consistent and secure baselines across all devices.

Today Remedio secures more than than 3 million devices for over 300 companies, including several Fortune 500s.