Elisity® Cognitive Trust™

Software-Defined Zero Trust Access Security

- 33% of the Typical Deployent Time
- 25% of the Typical Cost

ELISITY

For the health of your network

What is Elisity Cognitive Trust?

Cognitive Trust is a cloud-native and cloud-delivered solution for identity-based segmentation and least privilege access of users, applications, and devices (managed and unmanaged), on-prem and in the cloud.

What does it do?

The solution delivers frictionless, centrally-managed, and software-defined zero trust access security to effectively and efficiently protect clinical devices and patient information from lateral movement of ransomware payloads, advanced persistent threats, and insider threats.

What are the benefits?

- **Visibility to reduce the attack surface.** Reduces risk by automatically discovering, classifying, and applying least privilege access policy to users, applications, and IoT, IoMT, and IT devices, including assets previously not managed in the network, thus isolating shadow IT and rogue devices from clinical resources.
- **Control and contain breaches.** Minimizes the impact of breaches by keeping malicious traffic from moving laterally in the network and by enabling continuous threat detection.
- **Flexibility and simplicity to reduce OpEx.** No new hardware is needed. No network reconfiguration is needed. The architecture can leverage existing switching infrastructure as policy enforcement points and integrates with platforms such as Active Directory, Azure AD, Okta, ServiceNow, **Medigate by Claroty**, and others, thus accelerating deployment time and reducing operational expenses.
- **Simplicity to adopt Zero Trust faster.** Security and networking defined by type of asset rather than IPs and ports, with simple policies that are identity-based.

Why is it different?

Simplicity and fast speed-to-value!

But zero trust us.
Trust what our customers are saying:

*"Within 24 hours of deploying Elisity Cognitive Trust on our Cisco Catalyst switches, **we discovered devices of which we had no prior visibility,** giving us insights into actions needed. With help from the Elisity team, we created simple and scalable policies to secure our assets, and we were able to enforce them in real-time. The potential of **gaining East-West security for managed and unmanaged users and clinical devices without additional hardware** in our campus network is **absolutely game-changing** for our organization."*

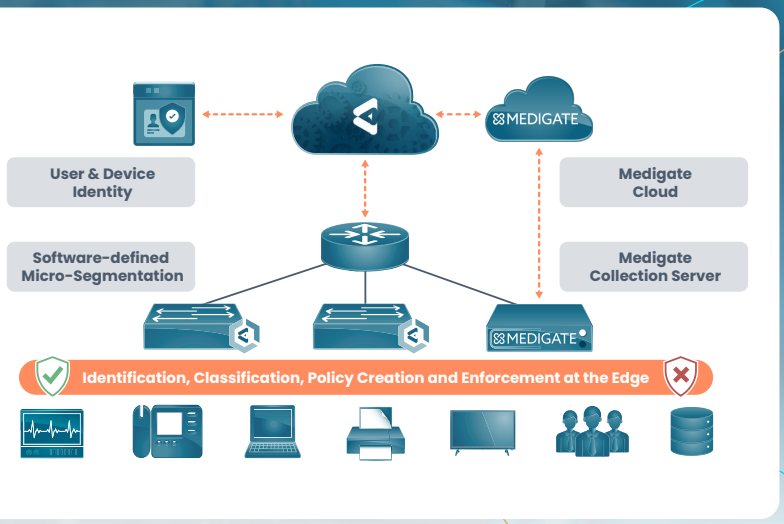
Alma Kucera
Business Information Security Officer

Bupa

How does Elisity Cognitive Trust work?

The solution architecture can leverage pre-existing investments in switches, by turning them into intelligent policy enforcement points with the use of containers, and makes use of hypervisors where edge computing is not available.

Cognitive Trust passively gleans, and continuously verifies, the identity of IoMT devices, users, and applications traversing the network, to enforce policies as close to the clinical assets as possible. It integrates with user, application, and device identity sources so organizations can very quickly gain visibility into network assets and traffic flows, assess risks, and begin building policies, enforced at the edge, to secure healthcare resources from malicious network traffic.



IoMT Discovery Using Medigate by Claroty

MEDIGATE

1. Medigate Collection Server sniffs, filters, and parses traffic to analyze medical device protocols.
2. The collector extracts device attributes to classify medical devices.
3. Filtered, non-protected health information identifiers sent for analysis to Medigate Analysis Server.
4. Medigate Analysis Server performs medical device analysis and identification.

ELISITY

5. Discovery and identification, continuously verified, of all types of users, applications, and devices.
6. Elisity Cloud Control Center queries Medigate Analysis Server via API to retrieve medical device classifications.
7. Medigate Cloud device classifications and policy recommendations enrich Cloud Control Center data.
8. Elisity Cognitive Trust policies for medical devices are applied and enforced at the edge close to the assets.

Request a Proof-of-Concept

- No Hardware
- No Network Disruption
- No Outage Window
- 2-3 Hours Remote (Discovery & Design Workshop, Setup & Initial Policies, Connect to Applications)
- 1-2 Days On Site (Integrations & Validation, Review & Further Policy Creation)

www.elisity.com
info@elisity.com
sales@elisity.com

elisity.com/request-poc

100 Century Center Ct
Suite 710
San Jose, CA 95112