ELISITY

Elisity® Cognitive Trust™

Simple. Agile. Smart.

How to implement
identity-based microsegmentation
using your **Cisco Catalyst**
switching infrastructure

TECHNICAL WHITEPAPER

April 2022

Elisity Cognitive Trust unleashes the power of your Cisco Catalyst switches

From Implicit Trust to Zero Trust

in days instead of years

How long does it take for your network segmentation projects to start delivering any value? Months? Years? What if we told you that you could deploy identity-based microsegmentation at a large site in just two days? What if we told you that you no longer need to deploy and micromanage additional hardware, VLANs, ACLs, and VRFs anymore?

Indeed, you can achieve this fast speed-to-value with Elisity Cognitive Trust because **the solution leverages your existing Cisco Catalyst 3650, 3850, 9300, and 9400 switches.** In fact, the solution can be tailored to support other vendor switches as well.

When deploying on Catalyst 9000 series switches, no additional hardware is required. Also, no outage window is necessary when deploying the solution. No hardware, no network disruption, no friction.

In this technical whitepaper, we'll explain how it's done. But first, let's take a step back and go through what Elisity Cognitive Trust can do for your organization.

What is Elisity Cognitive Trust?

Traditional network segmentation projects that rely on NAC solutions and East-West firewalls take too long to deploy and to deliver any value, are complex to maintain once deployed, and hair-pin traffic through network chokepoints.

Cognitive Trust is Elisity's cloud-native and cloud-delivered solution for identity-based microsegmentation and least privilege access of users, applications, and devices (managed and unmanaged), on-prem, and in the cloud, that delivers value at speed with simplicity and cost-efficiency at its core.

But zero trust us.
Trust what our customers say.

*"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

What are the Benefits?

- **Full visibility to reduce the attack surface**
  Reduces risk by automatically discovering, classifying, and applying least privilege access policy to users, applications, and IT, IoT, IoMT, IIoT and OT devices, including assets previously not managed in the network, thus isolating shadow IT and rogue devices from critical resources.
- **Full control to 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, Fing, Okta, Ping, ServiceNow, Claroty, 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.

Common Use Cases

Carpeted Spaces
Secures access for managed and unmanaged (IoT) devices, full time employees, contractors, and guests, on campus and branches.

Healthcare Facilities
Protects clinical devices (IoMT) and patient information.

Manufacturing Plants
Secures industrial control systems (ICS) and operational technology (OT).

VISIBILITY

Uncovers previously unknown devices and application traffic across the infrastructure and enables behavior monitoring and policy building.

CONTROL

Controls North-South and East-West traffic easily with identity, context, and behavior-based adaptive policies decoupled from the underlying network construct.

AGILITY

Delivers value FAST, with a technology solution that deploys quickly over existing infrastructure, simplifying network security operations, and reducing cost and complexity over time.

Solution Architecture

The solution offers a cloud-based control plane that can be layered across existing wide-area network (WAN) and/or software-defined WAN (SD-WAN) infrastructure, or deployed atop a managed WAN/SD-WAN service. It supports both brownfield and greenfield environments, delivering fast time to value. Its components are:

Elisity Cloud Control Center

Centralized, cloud-delivered multi-tenant administration platform that abstracts and centralizes the security access policies.

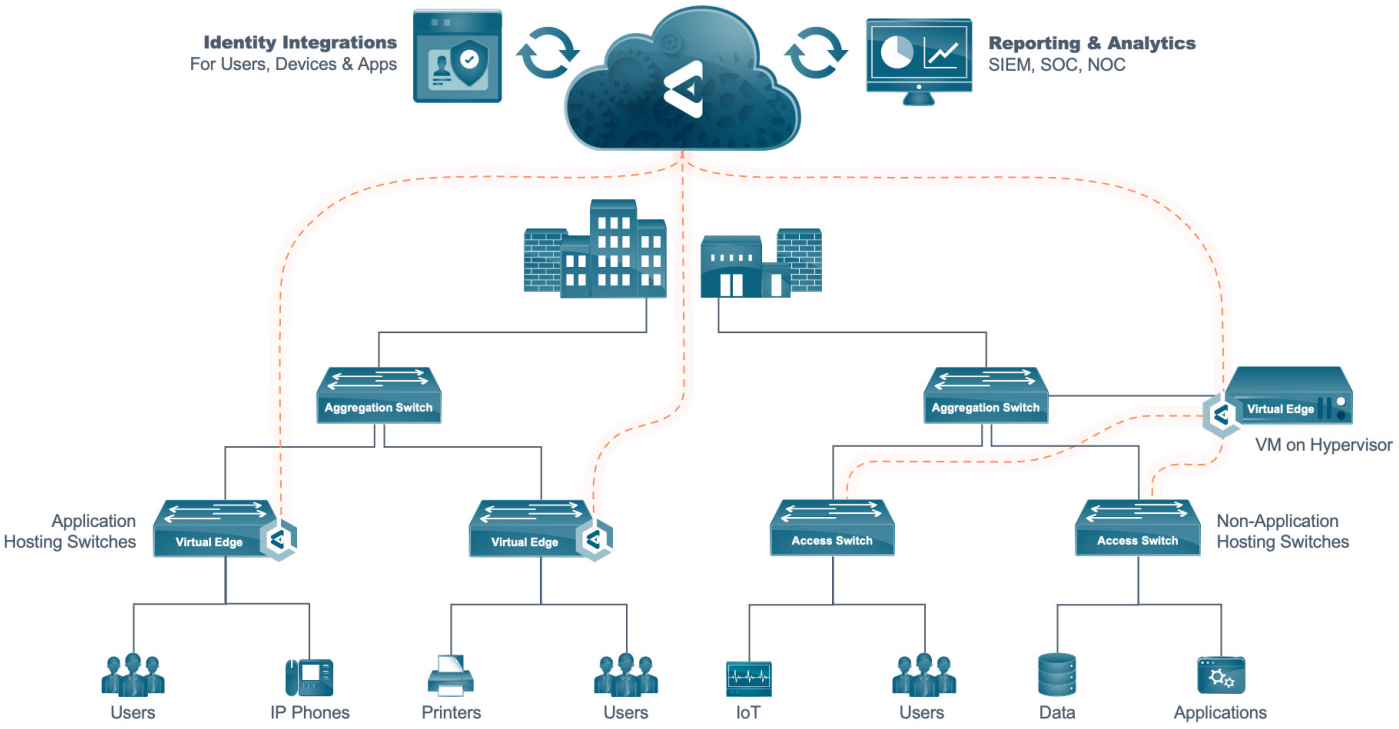
Elisity Cloud IaaS Integration

Provides granular security for users and devices accessing your cloud hosted applications.

Elisity Virtual Edge

Deployed as a container on Cisco Catalyst 9000 series switches, and as a VM on a hypervisor to support other platforms such as the Cisco Catalyst 3650 and 3850, Elisity Virtual Edge enables identity-based segmentation and policies on those switches, turning them into SDP gateways in addition to enabling transactional segmentation.

Non-Disruptive Implementation



Elisity Cognitive Trust Sample architecture

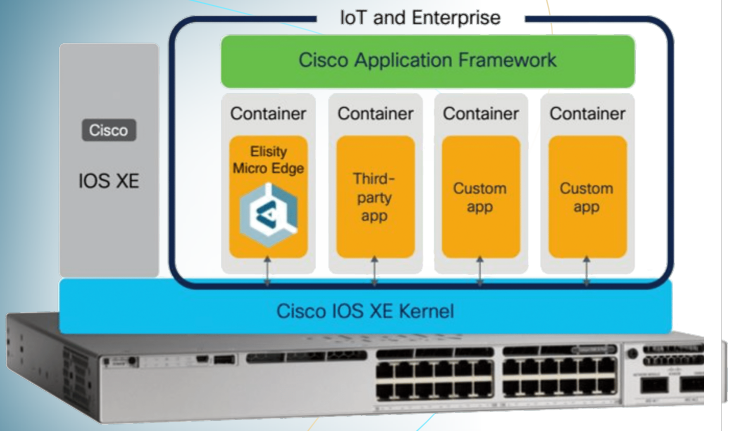
Cisco Catalyst 9000 Series Switches

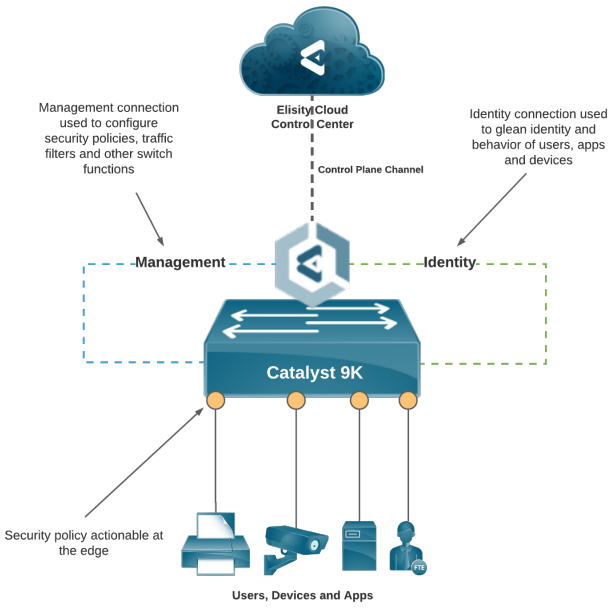
as Intelligent Policy Enforcement Points

The Elisity Micro Edge container hosted by a Catalyst 9000 series switch has two virtual interfaces; a management interface and an uplink interface.

- The Micro Edge management interface is used for communicating with the switch over the default out-of-band switch management VRF. This connection is leveraged to read the Catalyst configuration and configure security policies, traffic filters and other switch functions.
- The Micro Edge Identity (or Uplink) interface is used as the source interface to reach Cloud Control Center and as a connection for the Micro Edge to glean identity and behavior of users, apps and devices.

The following image is a high-level depiction of the Elisity Micro Edge architecture hosted on a Catalyst 9000 series switch:





For more details refer to:
www.elisity.com/knowledge/elisity-micro-edge

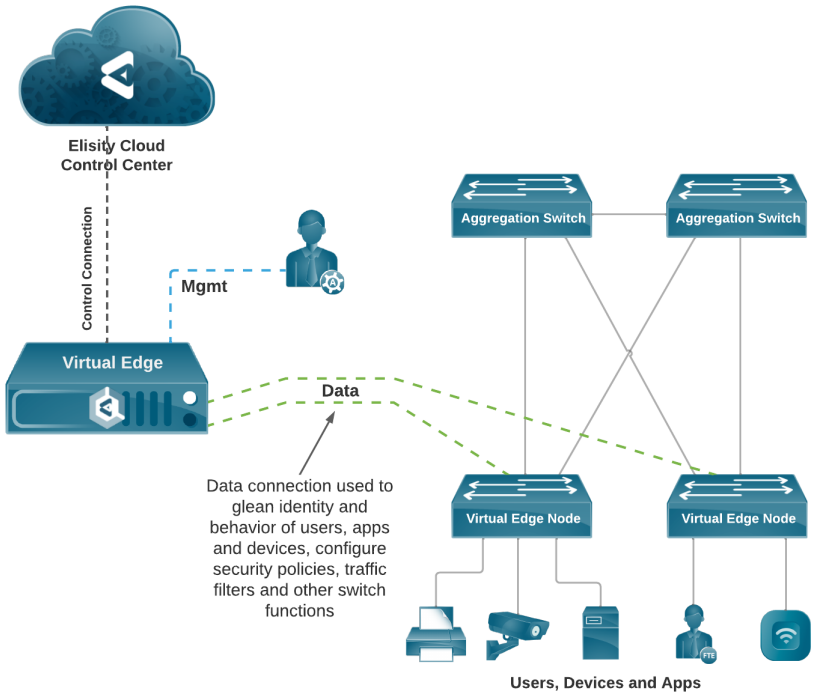
Cisco Catalyst 3650 and 3850 Switches

as Intelligent Policy Enforcement Points

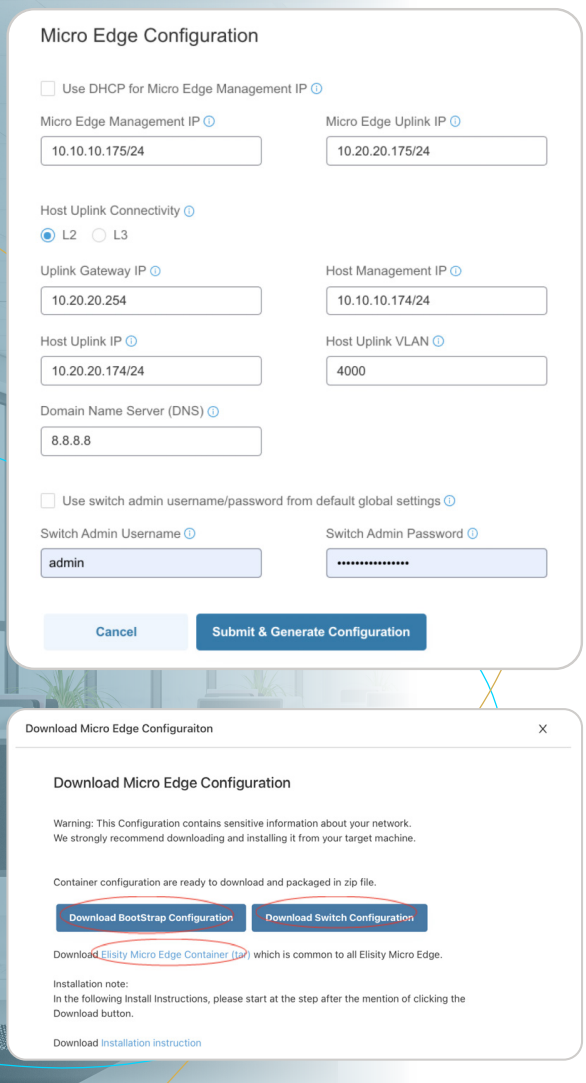
Elisity supports Cisco Catalyst 3650 and 3850 switches as network enforcement points in a similar manner. Since Catalyst 3650 and 3850 switches do not support application hosting, the Elisity software is deployed externally as a Virtual Edge on a hypervisor and connects to switches remotely.

The Virtual Edge establishes a secure connection to each access switch (Virtual Edge Node). This connection is leveraged to read the Catalyst configuration and configure security policies, traffic filters and other switch functions. It is also used as an Identity connection for the Virtual Edge to glean identity and behavior of users, apps and devices connected to the switch.

The following image is a high-level depiction of the Elisity Virtual Edge deployment supporting Catalyst 3650 and 3850 switches:

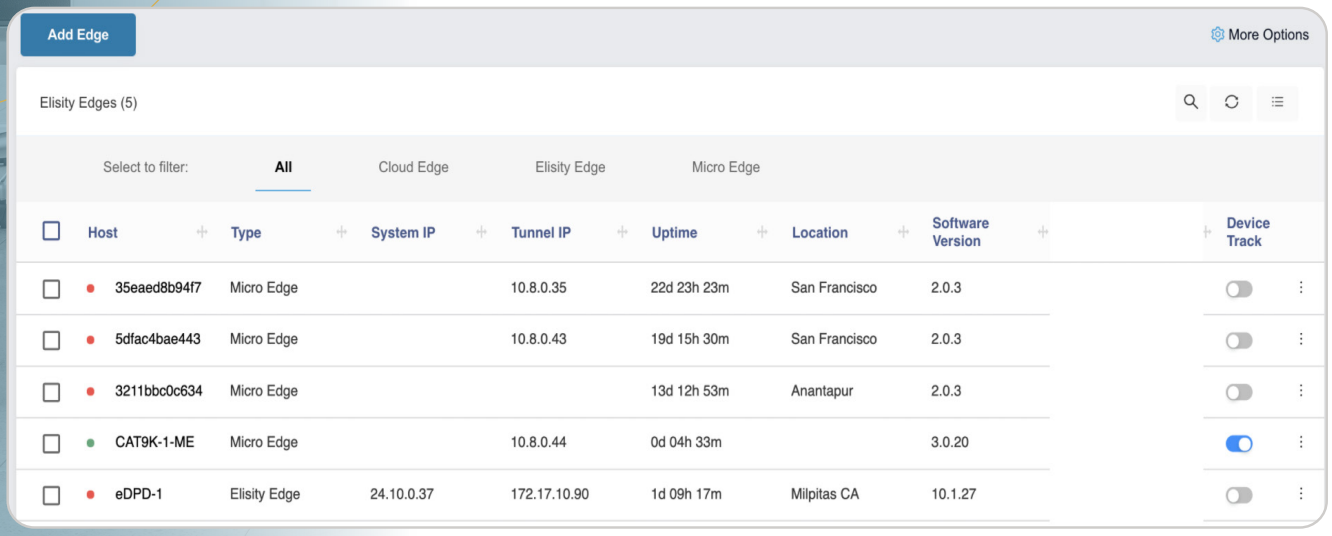


Elisity Micro Edge Deployment on your Catalyst 9000 with 4 simple steps



1. Provision the Micro Edge in Cloud Control Center by entering basic information about your network which generates the Micro Edge bootstrap file and the initial switch configuration.
2. Download the Micro Edge container installer from Cloud Control Center.
3. Copy the Micro Edge bootstrap file and the Micro Edge container installer to supported switch flash.
4. Copy and paste the configuration from the initial switch configuration file and run the Micro Edge container installer with a simple command.

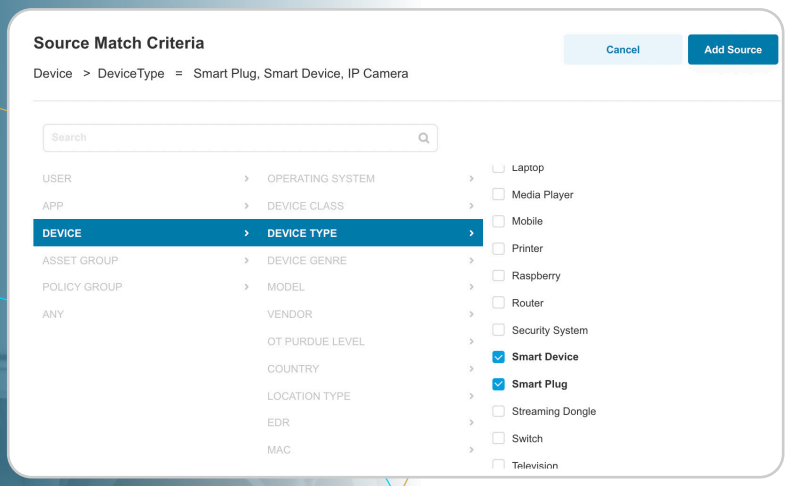
Elisity automation handles the rest of the Catalyst 9000 series switch onboarding process.

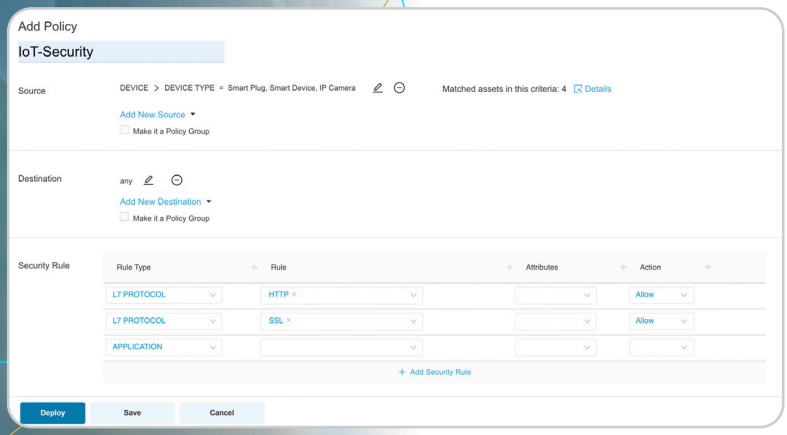


Building your Elisity software defined perimeter is even simpler

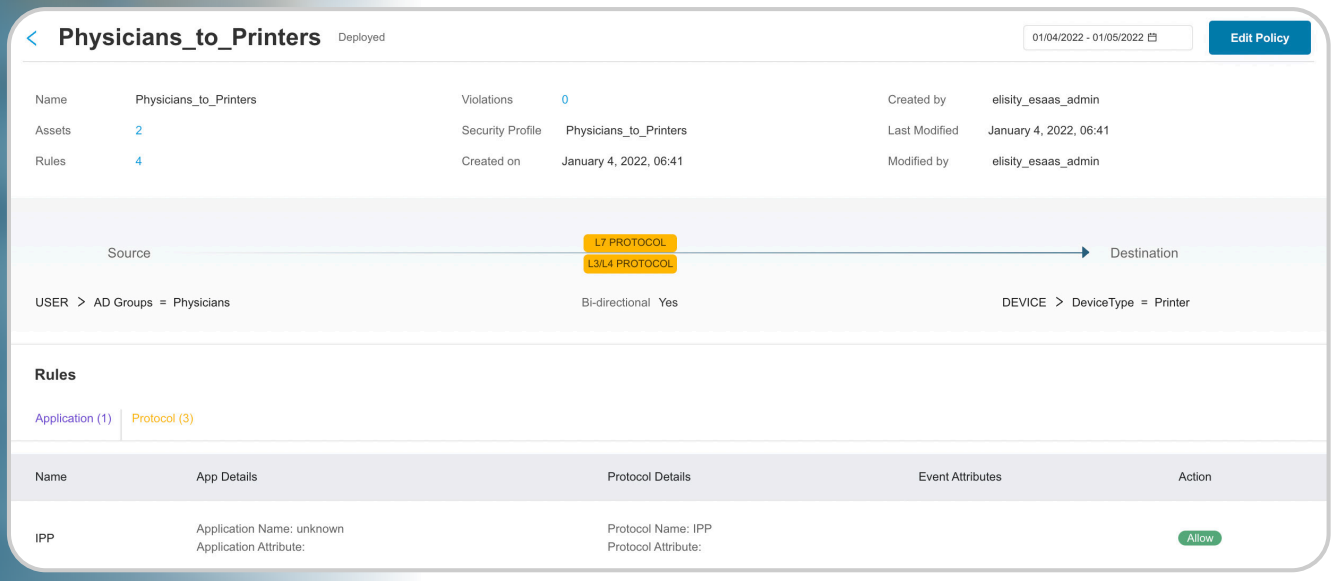
Building Elisity Cognitive Trust policy only takes a few simple steps.

1. Select your dynamically discovered app, user or device as a source
2. Select your dynamically discovered app, user or device as a destination
3. Create your L3-L7 based security rules
4. Click Deploy





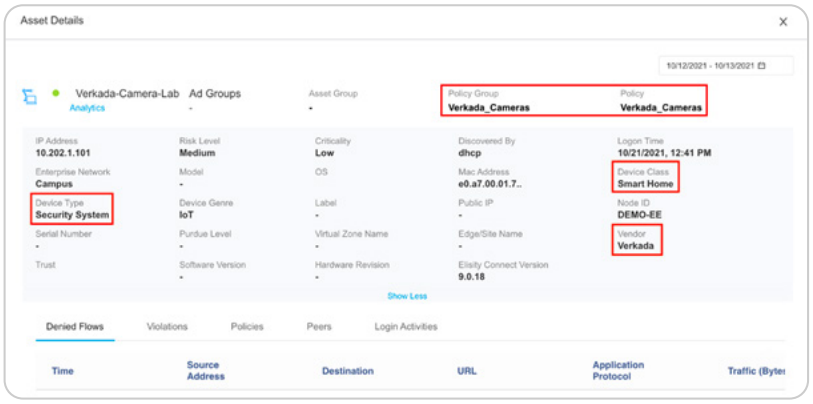
Cloud Control Center will immediately configure all the relevant Catalyst 9000 series, and Catalyst 3650/3850 switches as Elisity enforcement points with the desired policies.



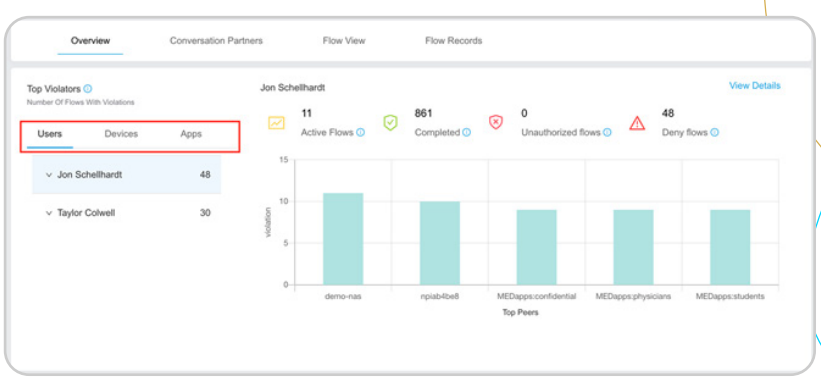
Elisity Dynamic Device Discovery and Network Visibility

Elisity Cognitive Trust deployed at the edge of the network enables robust device discovery and network visibility. Elisity Cloud Control Center has access to a continuously updating catalogue of thousands of devices.

If you connect an OT/IoT/IoMT device to the network, through several network layer mechanisms and catalogue mapping, Elisity can dynamically discover what the device is, the manufacturer of the device, the device type, and other metadata that can then be referenced during policy creation.



As traffic passes through an Elisity enabled switching infrastructure, security policy and network analytics are collected and presented to the administrator in several different easily digestible formats. Elisity is capable of collecting and alerting on new application, user, and device attachments, while also providing in depth network conversation mapping between these same entities.



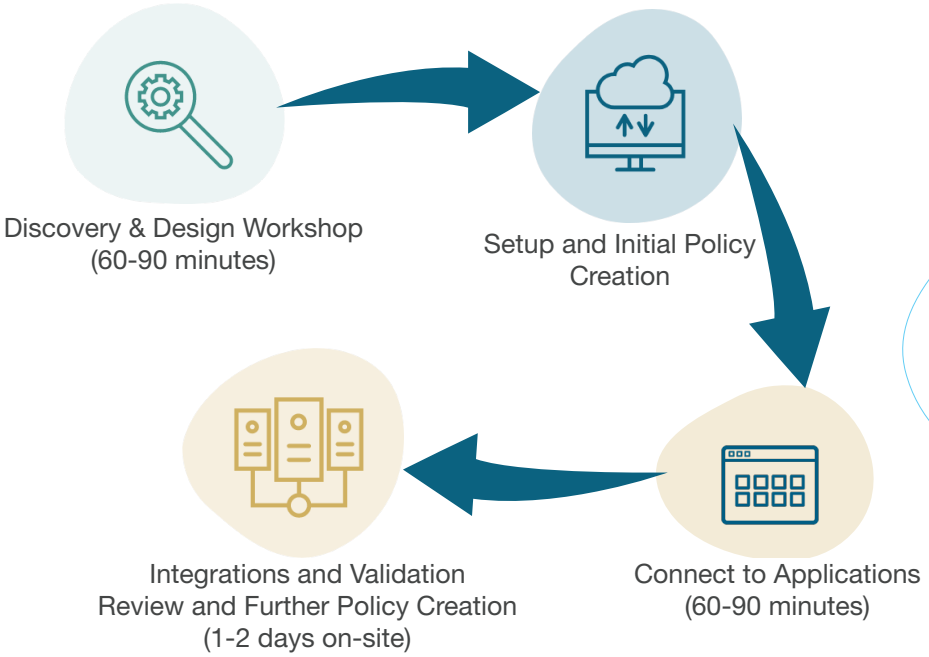
More information on visibility can be found on the knowledgebase: www.elisity.com/knowledge/visibility-and-troubleshooting

Frictionless Value Assessment

Request a Proof-of-Concept
with a non-disruptive deployment

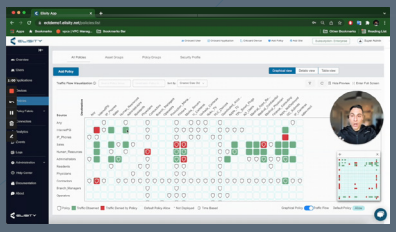
www.elisity.com/request-poc

- 3-4 hours remote
- 1-2 days on-site



Additional Resources

Policy Visualization Features



https://vimeo.com/675875855

Micro Edge Introduction

https://vimeo.com/664501285

About Elisity

Elisity delivers frictionless, centrally managed zero trust access security to effectively and efficiently protect corporate data and critical assets from malicious lateral movement across the network. Cognitive Trust is Elisity's 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. The solution enables organizations to quickly gain visibility into network assets and traffic flows, and begin building policies to protect the most critical enterprise assets. Elisity is backed by Two Bear Capital, AllegisCyber Capital, and Atlantic Bridge.
Follow on Twitter and LinkedIn or go to www.elisity.com.

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

100 Century Center Ct
Suite 710
San Jose, CA 95112