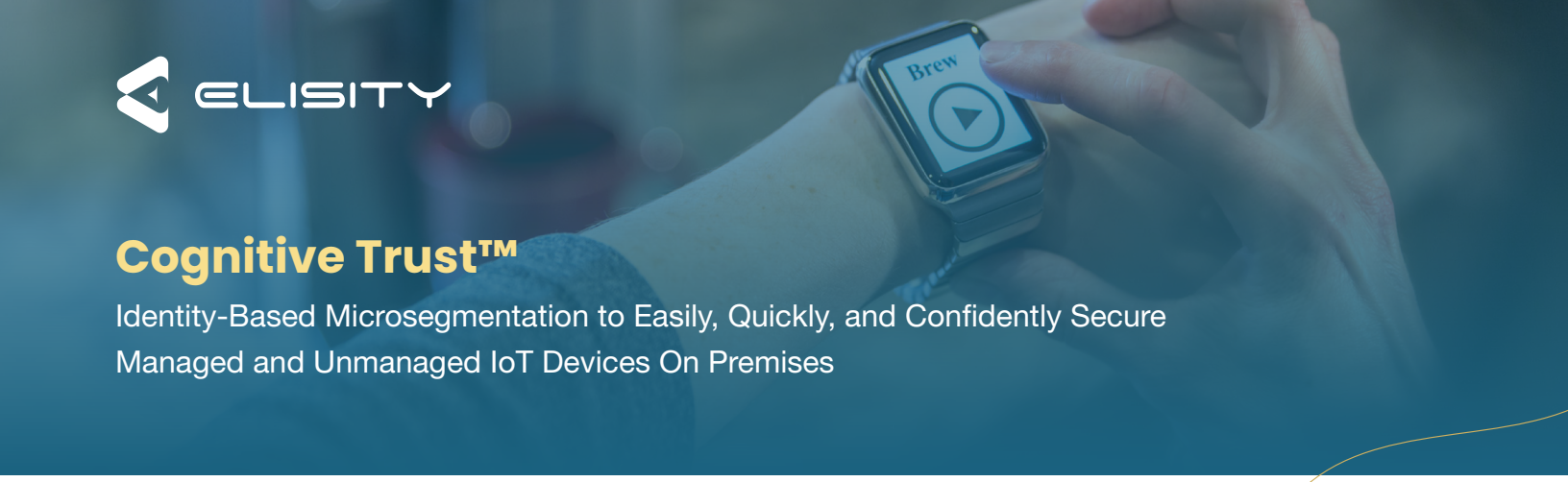


Cognitive Trust™

Identity-Based Microsegmentation to Easily, Quickly, and Confidently Secure Managed and Unmanaged IoT Devices On Premises

No Hardware. No Agents. No Disruption.

Elisity offers an identity-driven control plane for IoT visibility and secure networking without tying customers to a particular network or network security technology. Cognitive Trust, delivered as a cloud-based service, is quickly deployed to automatically identify, onboard, and secure IoT devices. It seemlessly integrates with leading IDP, CMDB, and SIEM used as Policy Information Points, and installs software on your existing switches to act as Policy Enforcement Points.

You Are in Control

It's not just device identity, but telemetry and behavioral intelligence that delivers the power of end-to-end protection for all of your IoT devices, regardless of their location in the network. Elisity Cognitive Trust is the Zero Trust Architecture and platform that unifies the policy control plane, securing connectivity of IoT devices, while enabling macro (site), micro (device), nano (flow), and transactional (session command control) segmentation to manage risk effectively and efficiently.

- Seamless integration with leading device identity and telemetry providers acting as Policy Information Points for data enrichment and more granular access policies
- Cloud-delivered platform that provides consistent policy across brownfield and greenfield edge
- Continually evolving risk policy enforcement for all types of IoT devices, from managed devices and rogue IoT at the office, to Industrial and Medical IoT devices
- Abstracts policy from underlying network constructs and enables enforcement as close to the asset as possible via Elisity Virtual Edge code installed on your in-line switches
- Unprecedented visibility to data flow between assets
- Macro, micro, nano, and transactional segmentation to deny network visibility to attackers should a breach occur, and to minimize the blast radius of malware payloads

ELISITY

VISIBILITY & INVENTORY

- Device visibility, integrating with leading device identity and telemetry providers (IDP, CMDB, SIEM)
- Automatically discover, identify, onboard, and apply policy for IoT devices coming online on your network
- In-depth analytics and reporting

IDENTITY-BASED SEGMENTATION

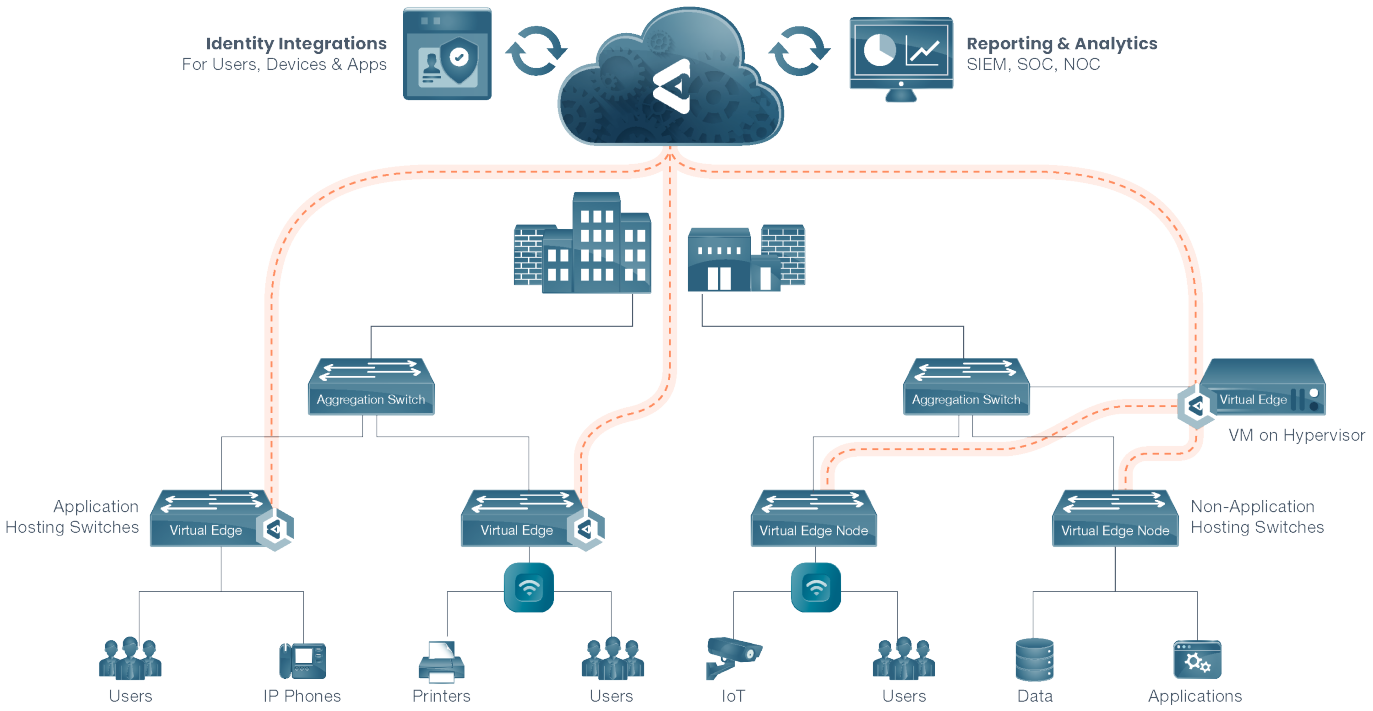
- Microsegmented access at the site, device group, individual device, flow, or transactional level
- Ubiquitous policy across all IT and OT infrastructure domains for identity and context-based access
- Prevent lateral movement across the infrastructure

LEAST-PRIVILEGE ACCESS

- Define policies based on what assets are, not where they are
- Implement consistent zero trust principles across the enterprise
- Control and protect all North-South and East-West device data traffic

MONITORING & ENFORCEMENT

- Continously monitors assets, data flow, and risk to make policy recommendations
- Ensure business continuity through auto-quarantine of individual compromised devices, applications, and/or users, and not the whole site
- Track all data flows



Elisity Cognitive Trust Sample Architecture

Request a Proof-of-Concept

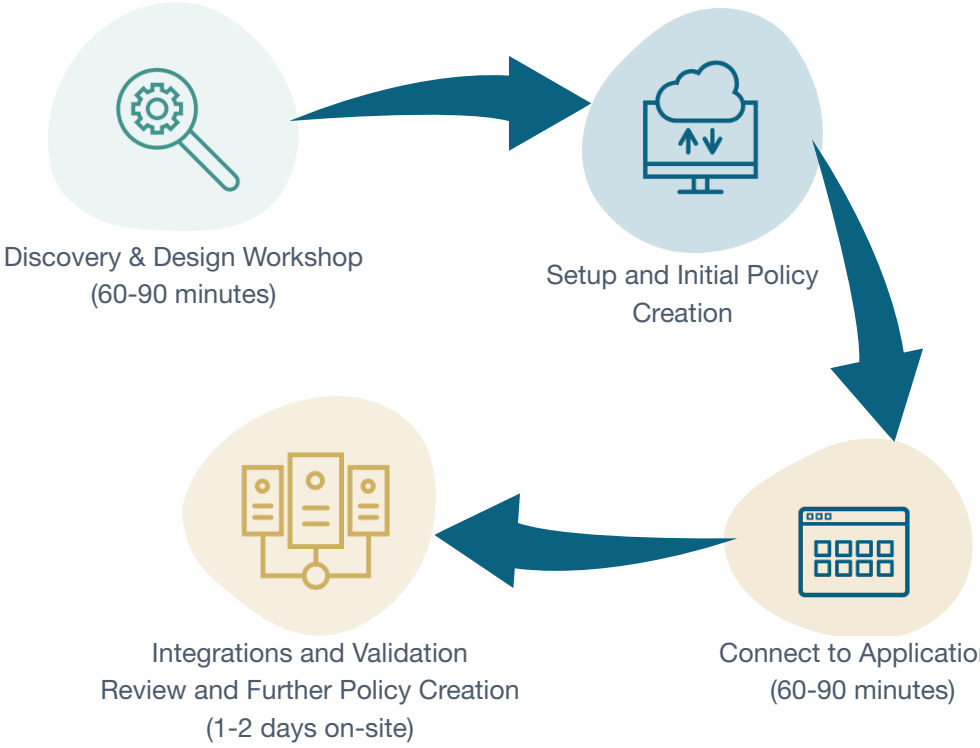
ZERO TRUST. ZERO FRICTION.

Start your zero trust journey with Elisity Cognitive Trust.

Request a non-disruptive proof-of-concept of the Cognitive Trust platform at **www.elisity.com/request-poc**

PoC Framework

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



ELISITY

Elisity Headquarters

100 Century Center Ct, #710
San Jose, CA 95112

To see how Cognitive Trust can secure your IoT on premises, schedule a demo today or request a proof-of-concept on site.

Visit elisity.com.

Follow us on Linkedin and Twitter.