
ELISITY
COGNITIVE TRUST

Elisity Summary

Vision

- Dominant enterprise provider of edge-to-edge secure connectivity on Elisity Cognitive Trust platform
- Cognitive Trust policy engine and control plane, delivered XaaS. Ecosystem of Elisity provided dataplane services / endpoints, extend to rich 3rd party ecosystem

Market

- Role-based access and control, implemented in network layer. Initial OT/ICS connecting to cloud edge and Lean Trust Use-cases in Pharma/Chemical Mfg, IoMT Diagnostic Systems, FiServ
- Zero-trust networking TAM ~$38.6BN in 2024 growing at 19% CAGR, Elisity focused use-cases/verticals represent $9BN serviceable available market in next 36 months

Team

- Industry leaders with enterprise networking and security background from Cisco, Insieme, Viptela, Extreme Networks, Meraki, and Aviatrix.
- GTM team from Viptela, acquired by Cisco for $610M in 2017, now $500M/yr business

Why now?

- Software-Defined perimeter required for ALL assets, not just user->SaaS
- Explosion of OT/IOT devices requiring access from distributed edge to cloud

The Team

James Winebrenner
Chief Executive Officer

Burjiz Pithawala
Chief Product Officer

Sundher Narayan
Chief Architect

Khalid Raza
Seed Investor & Strategic Advisor

Srinivas Sardar
VP Engineering

Matthew Krieg
VP Sales

Brent Colwell
VP, Systems Engineering

Pete Doolittle
VP, Growth

Over 50 patents in security and networking across product team, 20 Elisity-specific patents in progress.

Disruptive technologies have triggered a fundamental shift in how you secure an enterprise.

moat-based trust

cognitive trust

Cognitive trust enables secure connectivity at the **asset** level, based on *contextual knowledge—over time.*

users apps data devices

What we know

Identity | Environment | Permissions | Behavior

A novel approach to securely connecting every enterprise asset with cognitive trust.

Visibility and Inventory

Micro Segmentation

Least-Privilege Access

Monitoring and Enforcement

Elisity Cognitive Trust

Management,
Orchestration,
Flow Visibility,
Cognitive Risk

Elisity Cloud Identity Connectors

PingID · okta · bmc Discovery · now · ARMIS · CLAROTY

Asset-level Control and Policy Plane

Software, User-Agent, Container, Hardware, Cloud-Native

Data Plane

Elisity Cloud Edge	Elisity Cloud Edge	Elisity Access Service	Elisity Edge	Elisity Connect
AWS Outposts, vmware, Azure Stack	aws			
Private	Public	Site Connect	Edge Connect	User Connect

Any Place
Any Asset

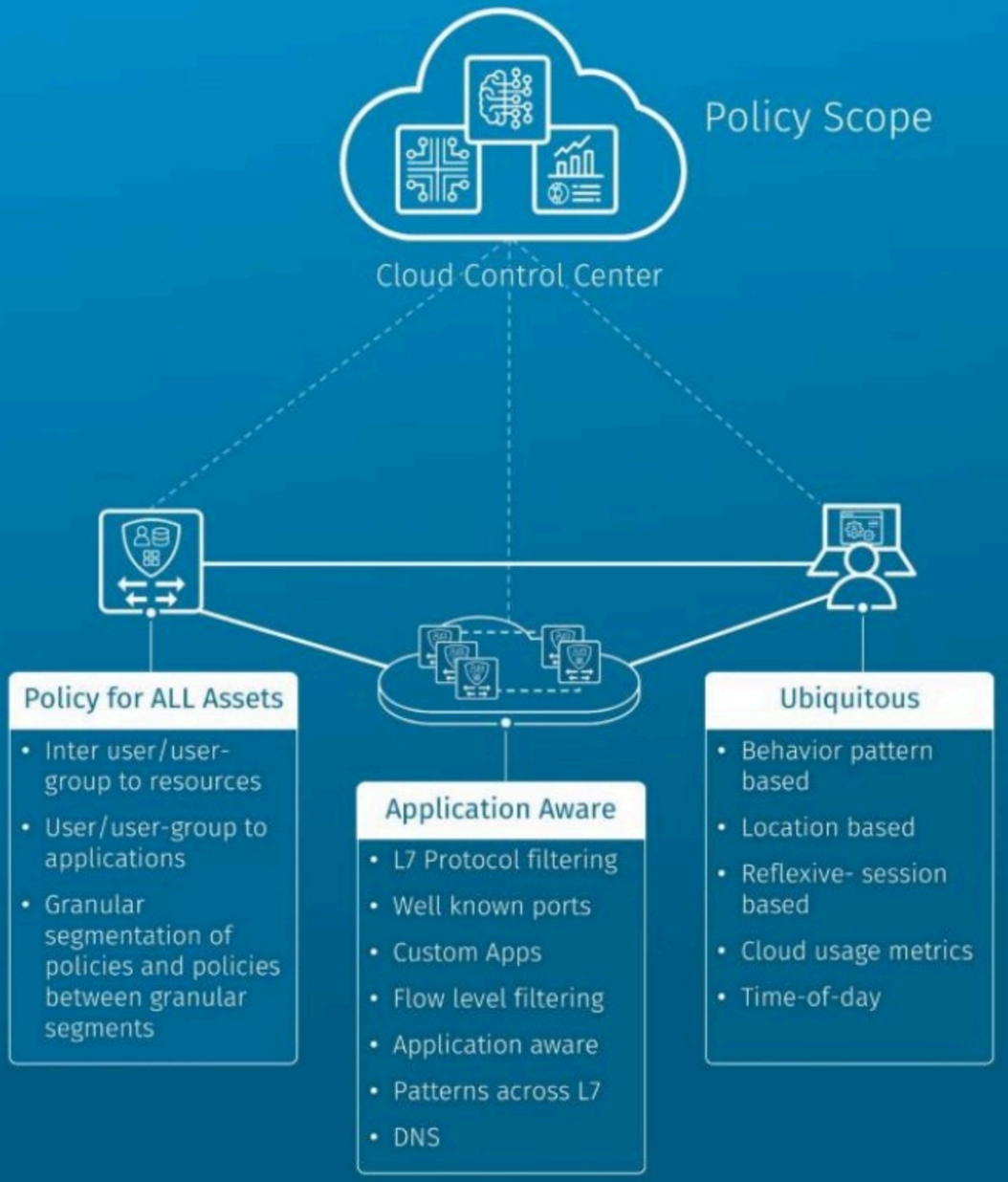
Campus · Branch · Data Center · Cloud · Remote

What sets Elisity Architecture apart?

- Purpose built multi-tenant cloud-based control and policy plane
- Integrated adaptive access control, adaptive asset protection, data & threat protection
- Flexible data plane deployment via the Elisity Edge, Access Service, and Connect
- Industry's first SDP + Zero Trust Solution
- Continuous verification of identity AND behavior

Elisity Basics: Policy and Connectivity

- Cloud Control Center is the Elisity control, policy and management plane.
- Data plane/Policy distribution & enforcement is distributed between site access, edge access and user access.
- Consistent software across campus, cloud, DC, branch sites, remote user,
- Security policy controls who has access to what resources.
- **Policy takes precedence over routing.**
- Security policy is pushed to the edge and site in real time and limits access via user, device, or application policy.
- Elisity Edges integrates with the local network via standard routing protocols (OSPF, BGP, etc.).



We've architected Elisity to be better on Day 100 than Day 1.

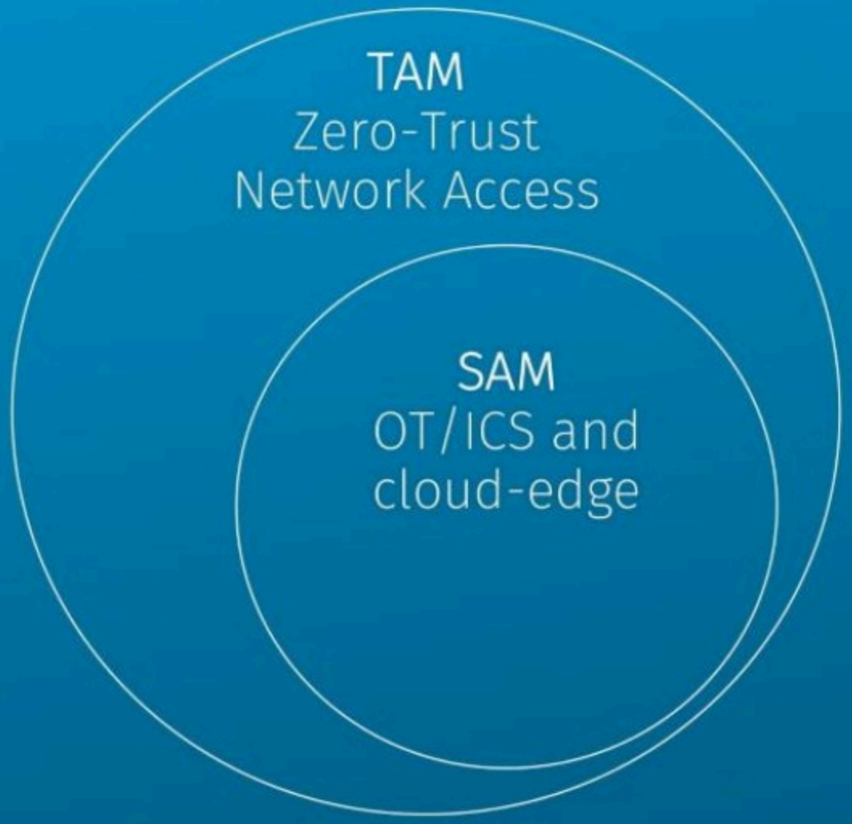
When new users, devices, apps or data show up, Elisity intelligently maps to appropriate policies.

Provide ongoing visibility into interactions between different assets and asset classes.

Continuously re-prioritize risks and vulnerabilities to mitigate.

Recommend finer contextual parameters to improve and tighten policies over time.

Market Opportunity



Total Addressable Market

$38.6 Billion

Zero Trust Networking TAM forecast to grow from 16 Billion to 38.6 Billion by 2024.[1]

Serviceable Addressable Market

$9.6 Billion

North America and Vertical focus addressable market for Elisity for the next 24-36 months.[2]

1. Markets and Markets: Zero-Trust Security Market by Solution Type - Global Forecast to 2024
2. RBC Capital Markets: Imagine 2025 - Faster to the Future; Thinking through the evolving Security Software landscape

A top-5 global pharma is deploying Elisity Cognitive Trust.

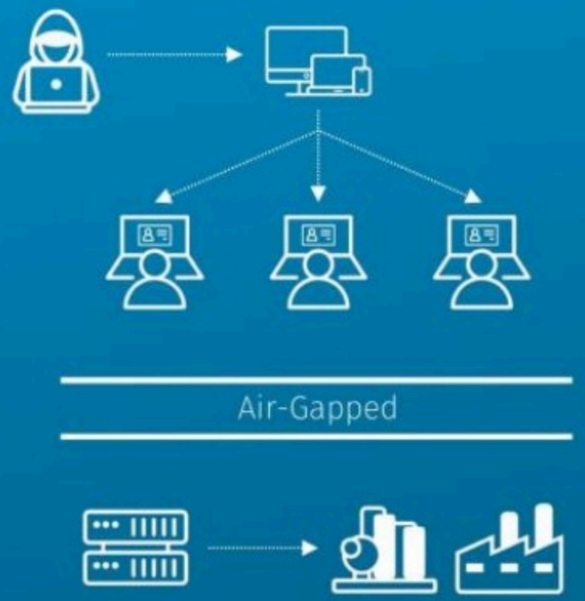
Scenario

73 manufacturing facilities worldwide
500,000 OT devices
3-year deployment plan

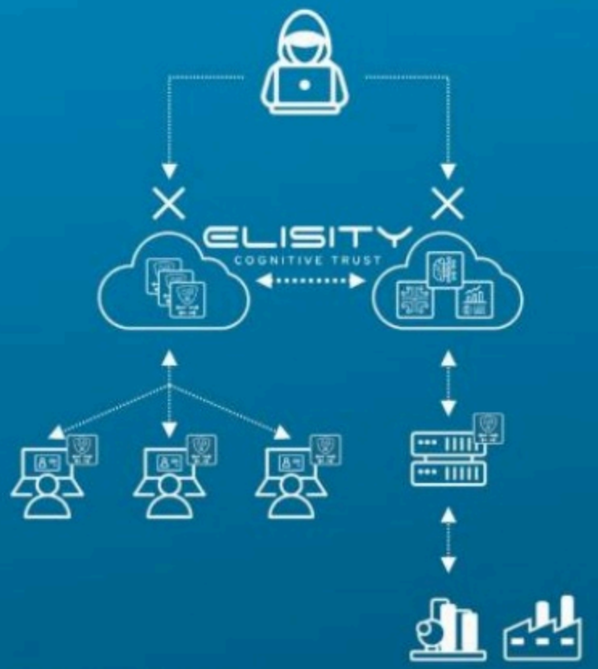
Problem

Digitization has driven the need to collect and analyze data from 500,000 OT devices and industrial control systems. These systems had no reason to connect to the corporate network and needed to be air-gapped. Connecting these highly vulnerable devices to the corporate network exponentially expands the attack surface.

Yesterday



Tomorrow



Legacy Solution

- $200M layer 2 infrastructure refresh and next-gen firewall upgrade
- 4-years attempting to deploy
- Couldn't get out of POC
- Corporate IT team couldn't keep up with the rule changes required by OT/ ICS Systems

Elisity Solution

- Elisity Cognitive Trust provides security at the asset level
- Context and device identity enables micro-segmentation and policy at scale
- No need for constant rule changes

A national financial services firm is deploying Elisity Cognitive Trust at scale.

Scenario

62K employees, 18K IoT devices, 10K ATMs
New acquisition catalyst for the project
3-year deployment plan

Problem

With 53K branch and back-office users, perimeter security based on place in the network is no longer sufficient. Admin needs the ability to restrict user and device access based on context, and limit broad application access allowed from anywhere in the network. Zscaler implementation does NOT address branch least-privilege.

Legacy Solution

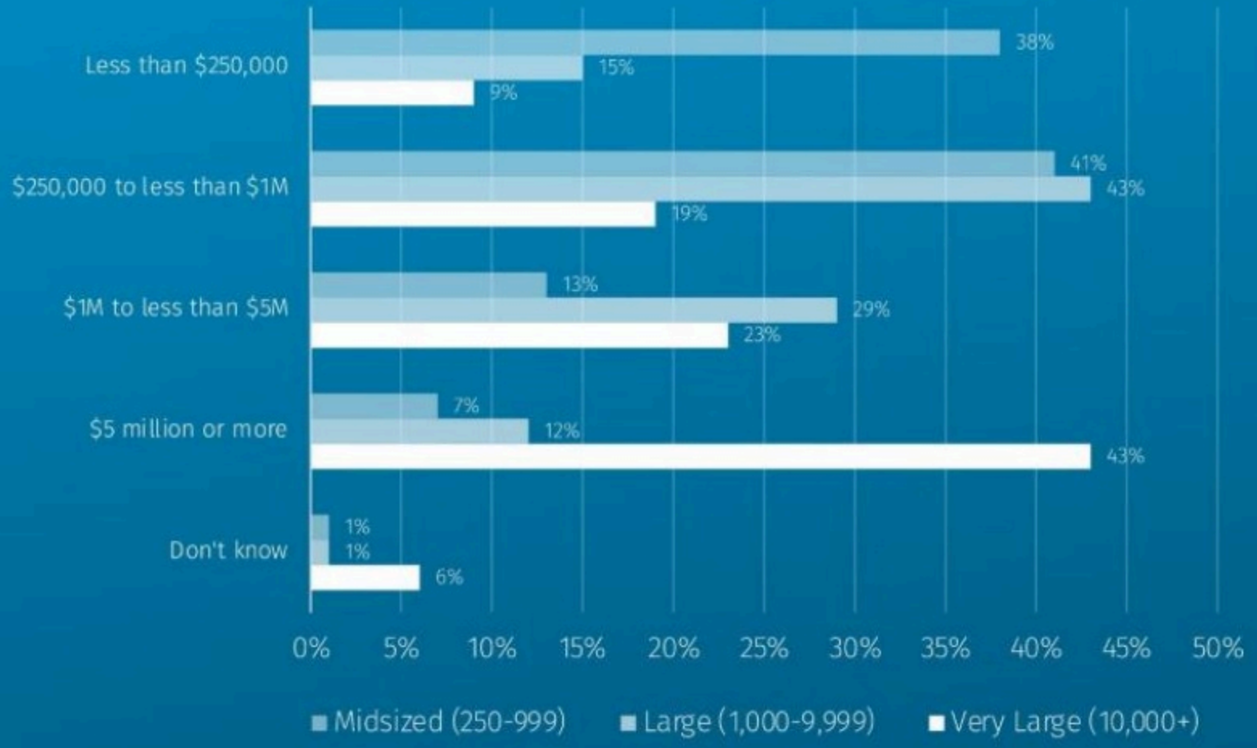
- Move to "big iron" for least trust access and network admission control
- Lack policy engine to implement access based on context
- Inadequate visibility to implement policy
- 6-Month PoC

Elisity Solution

- Security defined at the asset level with context-based policy
- Cognitive Cloud allows for policy to be defined and modified at scale
- Lightweight deployment methodology allows for brownfield implementation

84% of large companies have a budget $250k+ to implement Zero Trust networking.

Annual budget allocation for Zero Trust networking[1]



Multi-Disciplinary Buying / Budget Personas:

- InfoSec
- IT/Network Operations
- OT/ICS Security

Strategic Initiatives for early adopter focus:

- OT/ICS Segmentation and IT/Cloud Integration
- Smart Factory Transformation
- ZTNA for CloudEdge

1 EMA Enterprise Zero Trust Networking Strategies: Secure Remote Access and Network Segmentation

General Licensing Model

Free Tier

Users

- Maximum of 10 policies, 20 users, and 3 applications. Applications and Users can be located in up to 3 AWS regions in US + Canada. Onboarding 20+ users will result in all users being charged at base rate
- Limited Support

$7/User/Month

Users

- All Functionality
- 24x7 Support

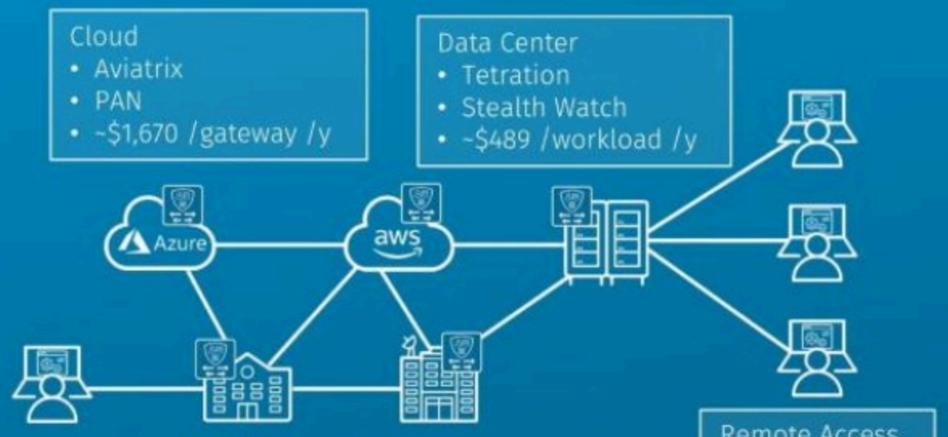
$5/Device/Month

Devices

- All Functionality
- 24x7 Support

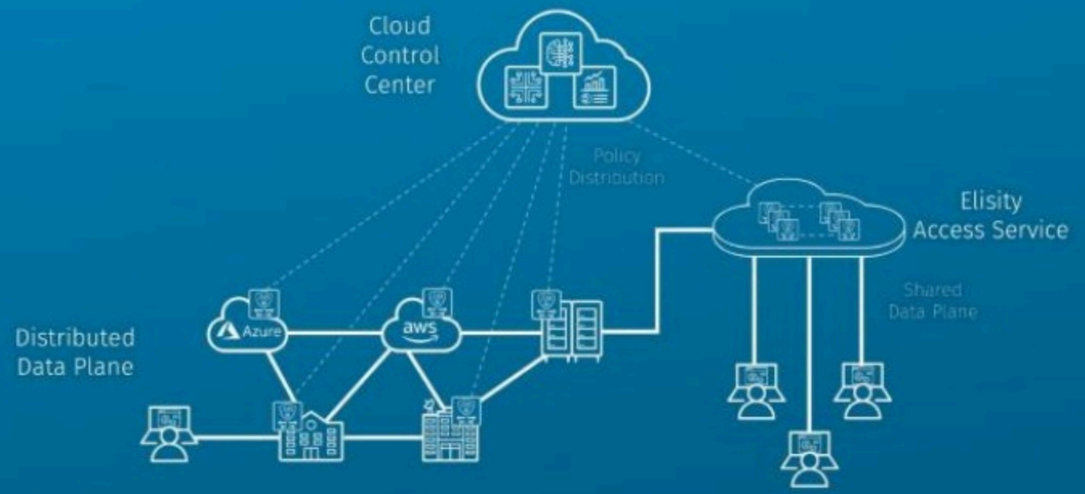
From a patchwork of solutions to a single platform

Before



- 62K users
- 18K IoT Devices
- 4k branches
- 9K ATMs

After



Elisity subscription or per user per year