ELISITY
COGNITIVE TRUST

White Paper

Making Identity the New Perimeter with Elisity Cognitive Trust

Secure your enterprise data and assets in a world transformed by cloud, mobility, and connected devices

www.elisity.com

Making Identity the New Perimeter with Elisity Cognitive Trust

In this paper, we will cover:

- An overview of current access protection solutions and their technical limitations
- An overview of ECT, its components, architecture, and how it delivers ubiquitous access policy and Zero Trust security across the organization

Traditional enterprise boundaries are shifting, as the industry is transformed by cloud, mobility, remote access, and the proliferation and diversity of connected devices. With an increasingly mobile and remote workforce — and as enterprises come under constant attack by increasingly sophisticated bad actors — there is a need to proactively secure access to enterprise data and assets across every digital domain.

Yet even as the attack surface expands, enterprises are still using outdated and disparate software and hardware to secure access to their data and assets in the campus, branch, data center, for remote workers, and more — retrofitting complex solutions with tools that weren't built for today. Moreover, enterprises have been left with fragmented islands of identity across their digital domains, with "set and forget" approaches to policy. These approaches only complicate enterprise security and access, while exposing organizations to increased risk of lateral movement, insider attacks, and DDoS, and unintentionally revealing cloud applications to the public internet.

Enterprises need an architectural security transformation — resolving legacy silos and enabling connectivity anywhere, while proactively protecting access to enterprise assets and data. Elisity Cognitive Trust (ECT), the industry's first combined Zero Trust and Software-Defined Perimeter solution, provides a single, comprehensive way to solve each of these challenges simultaneously. With the ability to apply identity-based access policy ubiquitously and nano-segment their environments, organizations can make identity the new perimeter, adopt a "never trust, always verify" security model, and enable secure access to any data or application, from any device, by any user, anywhere.

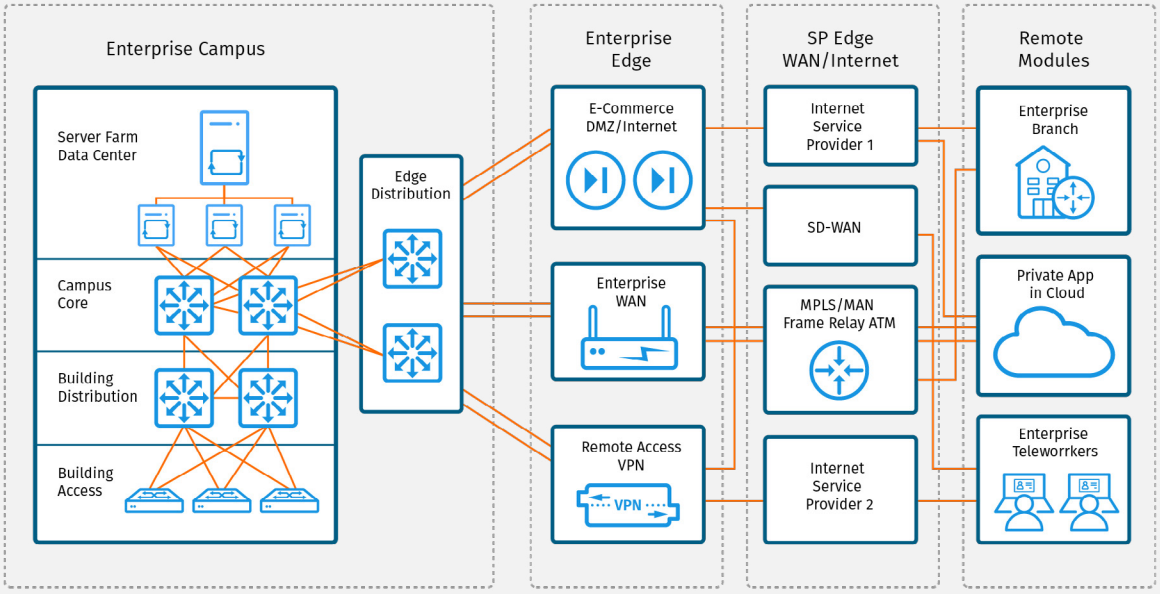
ECT represents a new paradigm in enterprise security — enabling organizations to fundamentally transform their approach to assess while improving their security posture. ECT allows organizations to:

- Software-define their perimeter, securely
- Zero Trust their networks, safely
- Transition to multi-cloud, securely
- Work from home, securely
- Operationalize access visibility, to any user, device or asset, quickly

The limits of traditional security architectures

Despite organizations embracing digital transformation, many enterprises still deploy a traditional networking architecture to connect their campus sites, branch sites, data center, and remote employees. Moreover, with the rise of cloud and multi-cloud, many companies are using legacy strategies like using IPsec protocols to extend their data center to cloud sites.

While these strategies were perfectly suited for an older era, they have a number of limitations in the hyper-connected, mobile, remote, cloud-enabled world of today:



Legacy networks are inherently insecure

Traditional networks typically provide excessive trust for users and devices, which leaves enterprises continually at risk from malicious actors moving laterally within their environment. The reason is that network authentication is a binary function: users and machines are either authenticated against 802.1x/RADIUS protocols — meaning they are "trusted" — and placed on the corporate network, or they are not. Unfortunately, many enterprise networks are relatively flat or use simple segmentation — resulting in excessive trust and the risk of lateral movement. This means that if an attacker or malicious actor gets placed on the network, they can move with relative ease to other applications, data, and assets.

Moreover, such deployments also expose every enterprise network and data center in the organization to every campus or internal user — increasing the risk that breaches have serious

consequences. The reason is that campus or internal users are typically on device or user networks, whether wired or wireless, but they are also able to connect to data center networks, as these networks are traditionally "trusted." This potentially provides attackers with access to internal applications routed over the LAN, and Internet-based or SaaS applications routed through the internal data center security stack.

In general, traditional networks suffer from one major assumption: that just because you "own" and control the network, you should automatically trust all users and devices on it. Another issue, moreover, is that because network communications are in unencrypted clear text, enterprises risk exposing legacy apps and devices.

Traditional security solutions are complex and costly

Enterprises are aware of the risk to their networks, of course. To mitigate some of this risk, they employ a number of strategies to improve their security posture — including VLANS, ACLS, firewalls, VRFs, and VPNs. Not only are enterprises left with fragmented, mismatched solutions, but each of these strategies has its security limitations. In other words, even though enterprises make significant capital, operational, and overhead expenses to secure their networks, these solutions fall short.

For instance, many organizations segment their campus networks with end-to-end VLANs, which help to limit excessive trust by breaking up accessible portions of the network into smaller units. However, this solution creates instability in the network, caused by Spanning Tree Protocol convergence problems. A second problem is that companies use different VLANs between pre-authentication and post-authentication — before and after users and devices are "trusted" and are placed on the network. Unfortunately, this solution fails for IoT devices, which are pervasive in today's enterprises, because there is no way to automatically refresh their IP addresses when the VLAN changes, creating connectivity problems.

Other organizations use more traditional strategies for segmentation, such as ACLs, firewalls, and VRFs. These strategies suffer from three primary challenges. First, it is a significant technical challenge to insert firewalls where they are most needed, such as in security gaps in the distribution layer, where coverage from VLANs terminates. In other words, the network is still unsecured. Second, it can significantly increase CAPEX and OPEX to insert firewalls into areas that are not their traditional perimeter roles, such as the cloud or the edge. Simply put, centralized firewall technology is not designed for, and does not work well in, distributed environments. Finally, the amount of overhead required to manage these solutions creates significant operational challenges. For example, one major financial institution informed us that it dedicates 24 global resources just to manage firewall ACL rules.

Remote work is not secure with VPN solutions

The bottom line is that VPN technology has a limited shelf life in the remote work pandemic era. Many companies use VPNs because it allows remote users to pass through firewalls and connect to internal systems with some degree of security. The problem with this approach is that it leaves enterprises highly vulnerable to lateral movement from malicious actors. Once remote users are authenticated and are placed on the network with VPN, they are considered "internal" — which means they can move laterally to any internal system or services. Any compromised user — contractor, partner, employee — has unlimited access to critical enterprise resources and applications.

Of course, some organizations have built workarounds to the VPN security problem. These solutions, too, have security failures. Most commonly, enterprises will place the front end of internal services in a safe, segmented part of the network with direct internet connectivity — referred to as a demilitarized zone (DMZ). This way, remote users can access the service without a VPN. Unfortunately, this strategy also creates excessive trust and can be abused by attackers. Consider this: if the service is exposed in the DMZ, anyone on the internet — including attackers — can inspect it, even if it is protected by a web application firewall (WAF). Ultimately, VPNs are a temporary fix for enterprises with remote workers, not a long-term security solution.

Enterprises have fragmented islands of identity

The advent of digital trends like mobile, social, cloud, and IoT have created unprecedented opportunities for enterprises, but have also left them with significant challenges — namely, fragmented islands of identity for users and devices across every digital domain. Enterprises typically manage these identities with different identity and access management (IAM) policy tools.

However, these tools often differ for each digital domain, resulting in users having numerous "identities" across the organization. Moreover, such identities are traditionally based on IP addresses, which creates security vulnerabilities, as IP addresses are often visible and easily faked. All of this results in unnecessary complexity in managing identity and access management, while weakening the security posture of the organization. Enterprises need to shift to a model where identities of assets include users (and group memberships), devices, applications, and data — with strong authentication and authorization measures that ensure access is warranted for that identity.

Access policies are “set and forget”

The state of enterprise security is a state of change. However, the policies that govern access to enterprise data and assets are static, more often than not. This leaves organizations vulnerable to attack and accidental exposure of data and assets, as user behavior can shift rapidly. For instance, a user with access to sensitive data might move to a different area of the organization or leave the organization altogether — but the access policy might remain the same. If one of this user’s devices becomes compromised, so too does the data to which they have access.

Yet, access policies are often fragmented across the organization, and cybersecurity professionals often have little visibility into where policy may be mismatched or mismanaged. Instead, organizations need to shift to a state of security where access is continuously and comprehensively monitored, reassessed, and adapted in real-time to the changing demands of the enterprise — ensuring trust is never granted unless it is earned.

Multi-cloud interconnect solutions increase the attack surface

Organizations are also embracing cloud and multi-cloud strategies, and many companies want to extend their data centers to the cloud. The most common solution is to deploy IPsec tunnels — secure network connections — between cloud environments and legacy data centers. The advantage of this approach is that organizations can use IP addresses from the data center in the cloud instance. The drawback of this solution is that it increases the attack surface of the organization. To put it broadly, cloud access controls require meaningfully different solutions and configurations than with existing campus and branch environments; by using legacy IPsec access controls in the cloud, many organizations have been breached by attackers.

Similarly, organizations are interconnecting their multi-cloud and multi-VPC environments. Yet, typical solutions — VPN gateways for each VPC, peering between VPCs, or the use of transit gateways — are not ideal. For instance, VPN gateways have the problem that users must switch between multiple VPN certificates when crossing multiple cloud environments, and the organization has to provision users for each VPN gateway separately. This is a complicated and not cost-effective solution. Meanwhile, VPC peering is not scalable, as it is difficult to manage segmentation in cloud environments — for instance, between Development and Production groups. As the number of VPCs grows to segment multi-cloud deployments, costs quickly rise. Finally, transit gateway solutions, while popular with some companies, require adopting a wholly new cloud architecture, which may not be possible for many enterprises. None of these methods provide enterprises with the on-demand secure connectivity they need between clouds, nor the fine-grained access control they require to ensure security, as users connect from one VPC or cloud to another.

Rethinking the enterprise security model: Zero Trust networking and Software-Defined Perimeter

In summary, the traditional networking security model no longer suits the needs of enterprises in a world where the cloud is the data center, every device is a work device, and applications are delivered from, and to, anywhere. Moreover, current solutions are too limited, complicated, and expensive to be effective at protecting enterprise data and assets while enabling digital transformation and remote work. Such solutions create excessive trust in the network and expand the attack surface — weaknesses that will inevitably be exploited by malicious actors. As a result, the industry needs a transformational rethinking of the enterprise security model.

Identity as the new perimeter: a new paradigm for end-to-end enterprise security

Elisity has developed a new security paradigm to address these challenges. Elisity Cognitive Trust. Elisity Cognitive Trust (ECT) is the first cybersecurity approach to combine both Zero Trust networking and Software-Defined perimeter. ECT provides organizations with a comprehensive, cloud-delivered way to secure access across every digital domain — campus, cloud and multi-cloud, data center, remote access, branch, SaaS apps, IoT devices, and more. Purpose-built for the demands of the digital enterprise, ECT lets organizations manage identity-based policy ubiquitously and secure all of their users, data, applications, and assets from a central, cloud-delivered portal.

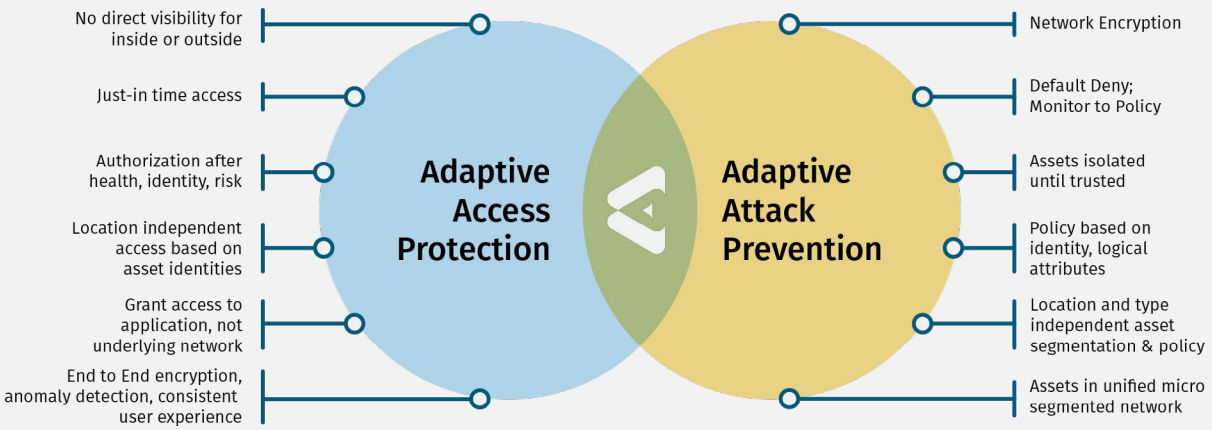
ECT combines both Zero Trust Network Access (ZTNA) approaches with Software-Defined Perimeter technology, resulting in a solution that enables both adaptive access protection and adaptive attack prevention. With ECT, no assets are directly visible to users or devices, either inside or outside the network, and no user or device can connect to any enterprise asset without a policy. The policy itself is based on the identity of users, devices, and applications, plus critical contexts like risk, behavior, location, the sensitivity of data involved, and more.

How ECT unifies identity and policy

ECT fundamentally changes traditional identity and access management from a model based on IP address to one rooted in the identity of users, devices, application, and data. By identity, this means:

- Users and their group membership, as defined in Active Directory and other stores;
- Devices, both managed and unmanaged, verified by unique fingerprints to determine if they are in the domain and compliant with policy;
- Applications, both three-tiered and distributed, based on their criticality to the business;
- Data, based on its sensitivity, with policies that verify access by risk, location, time of day, and other context

Integrated SDP and ZTN



With ECT, enterprises can manage both identity and policy in a unified way, because access is based on identity. In fact, every organizational asset is connected with a policy, and no user or device can connect to any asset without first authenticating and authorizing their identity with policy. In addition, policies are application aware — with features like L7 protocol and flow filtering — and ubiquitous across the organization.

Policies are managed centrally, in the cloud, and are dynamically created and pushed to the edge for "just in time" access. ECT supports "7-11" connectivity, with seven different asset communication models across eleven site-level connections:

Asset Communications

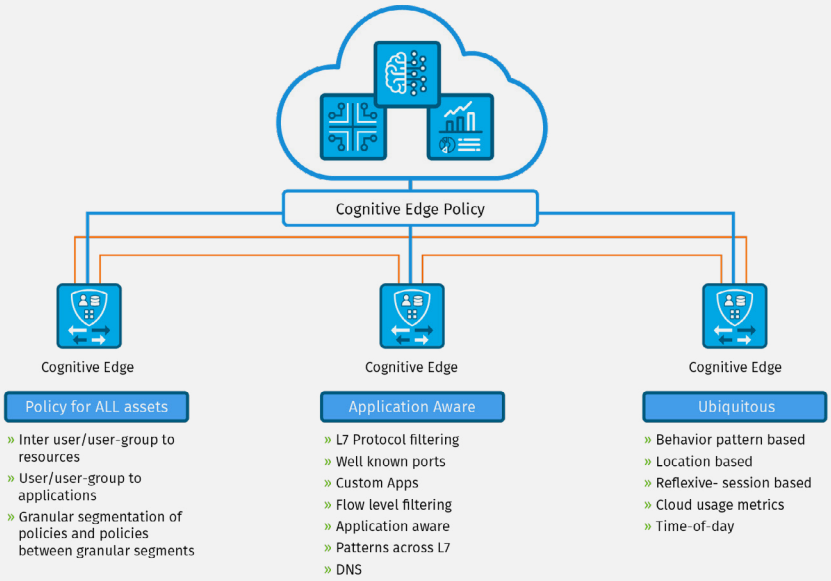
- User to User
- User to Device
- User to on-Premises App
- User to Cloud App
- Device to Device
- Device to Apps
- App to App

Site-level connections

- Campus-Campus
- Campus-DC
- Campus-Cloud
- Campus-SaaS
- Branch-Branch
- Branch-DC
- Branch-Cloud
- Branch-SaaS
- DC-Cloud
- Cloud-Cloud (across Clouds)
- Cloud Region-Cloud Region (within Cloud)

In this way, enterprises can resolve their fragmented islands of identity and policy with ECT, coming away with a simpler, more comprehensive, and more secure way to protect access.

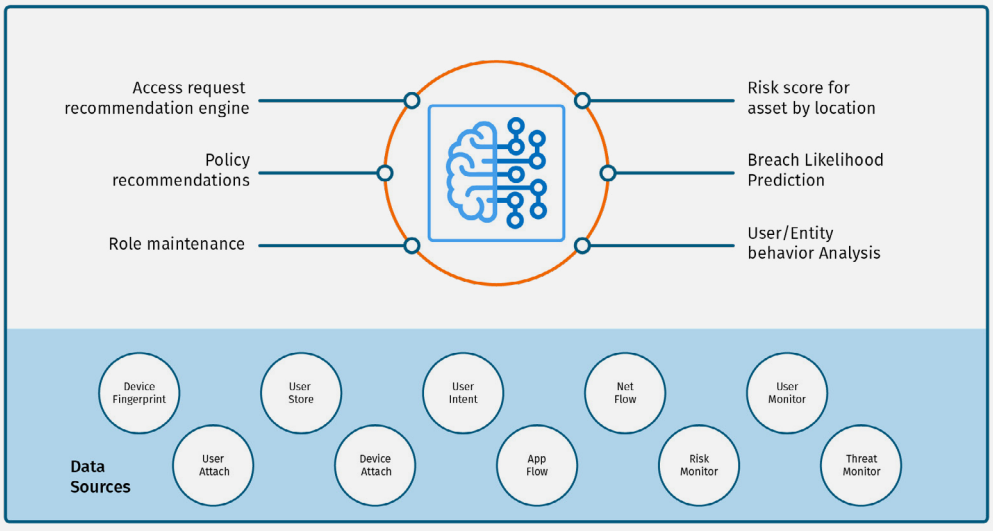
Logical Semantics Drive Policy Configuration



Continuous monitoring and risk-based policy with Cognitive Cloud

At the same time, policy with ECT is never static or "set and forget." ECT is powered by an AI engine, Cognitive Cloud, that continuously monitors access for all users, devices, and traffic flows and makes automatic policy recommendations based on user behavior and risk. In addition, Cognitive Cloud provides risk scores for every asset, by location, combined with predictions for the likelihood of breaches. By continuously analyzing the behavior of users and entities, Cognitive Cloud enables organizations to perform continuous role maintenance and update policy adaptively, as user behavior changes and the enterprise evolves.

Cognitive Cloud Continuous Verification



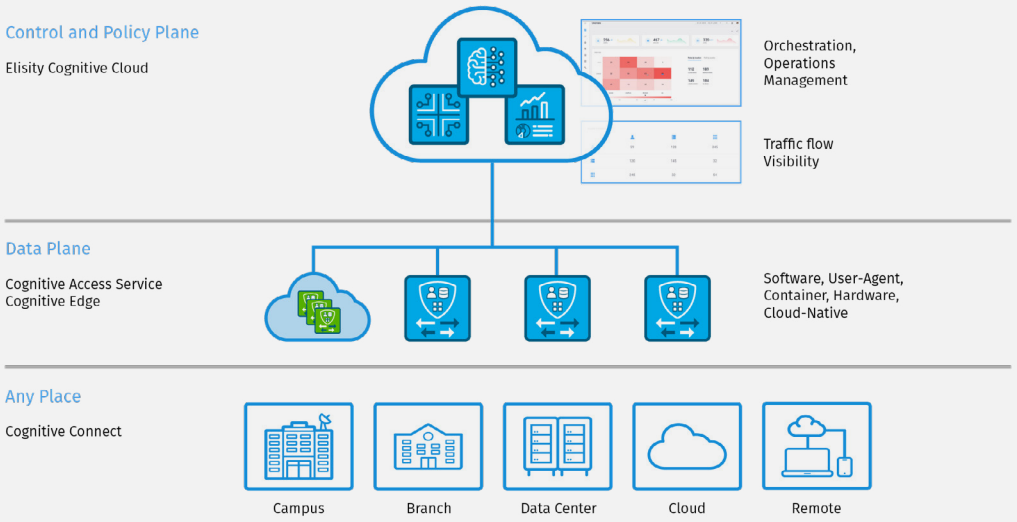
Solution Components

How ECT Works

ECT transforms enterprise network access from a traditional binary model — trusted or untrusted — to a "never trust, always verify" networking model, where access is based on identity, along with contextual data like location, time of day, risk scores, the sensitivity of data or application, and more.

ECT achieves this with four major solution components: Cognitive Cloud, Cognitive Edge, Cognitive Access Service, and Cognitive Connect.

ETC Architecture



Cognitive Cloud

The core of ECT is a centralized, cloud-delivered platform. The platform contains:

1. A policy plane for comprehensive policy management
2. A control plane for managing routing context
3. An AI layer that continuously monitors risk for all assets — users, devices, applications, and data — across every PIN

ECT overlays on existing infrastructure and connectors to automatically discover all enterprise assets. This enables enterprises to manage and enforce identity-based policy for any resource, at any location in the network. Moreover, ECT supports seven asset communication models (e.g. User to Device, Device to App), across all PINs.

Cognitive Edge

The Cognitive Edge is the data plane deployed at the edge, enabling distributed policy, close to the point of data creation. The Cognitive Edge:

- Implements and enforces access policy pushed from the Cognitive Cloud
- Provides inspection of the traffic stream for excessive risk, relative to the sensitivity of data
- Can enable edge-to-edge encryption of network communications
- Is deployed at the edge with hardware, software, container, or as a user agent (with Cognitive Connect)

The Cognitive Edge enables secure access, by ensuring that assets are only connected with a policy. The Cognitive Edge also removes all enterprise assets from direct visibility, while obviating the need for VLANs, ACLs, VRFs, or Zones.

Cognitive Access Service (CAS)

Elisity Cognitive Access Service (CAS) is a next-generation VPN replacement that combines Zero Trust access and Software-Defined Perimeter. CAS is an Elisity-managed, cloud-delivered remote access service with a global backbone that allows remote users to connect to the nearest region from anywhere in the world, for better performance and quality of service.

In addition, CAS:

- Implements and enforces identity-based policy pushed from the Cognitive Cloud
- Provides policies without decrypt-encrypt cycle
- Can provide network functions such as QoS, path selection, and routing
- Integrates with security capabilities such as DLP, FWaaS, threat prevention, and more
- Securely connects users to applications in Cloud, data center, Public Cloud, or SaaS
- Integrates with SIEMs to provide comprehensive logging and user behavior metrics

The cloud-delivered Cognitive Access Service delivers the required services and policy enforcements on demand, independent of location of the entity requesting the service, and the access to the capability.

Cognitive Connect

Elisity Cognitive Connect is a software agent that creates “right-sized,” Zero Trust access for any remote user, without the use of a VPN. Cognitive Connect initiates secure connections directly from a remote user’s device to an enterprise resource, through the Elisity-managed Cognitive Access Service (CAS). The Cognitive Connect software agent:

- Initiates secure connection to the nearest Elisity CAS
- Integrates with MFA and SSO authentication with leading Identity providers (Azure AD, Okta, Ping) to provide authentication
- Provides end-to-end encryption of remote traffic
- Precise segmentation of application or a cloud resource
- Supports replacing both clientless and client-based VPN
- Works on all popular platforms including Windows, MACOS, Android and iOS

Together, Cognitive Connect and Elisity CAS enable enterprises to deliver Zero Trust networking and Software-Defined Perimeter for any remote user, in any location, without the use of a VPN.

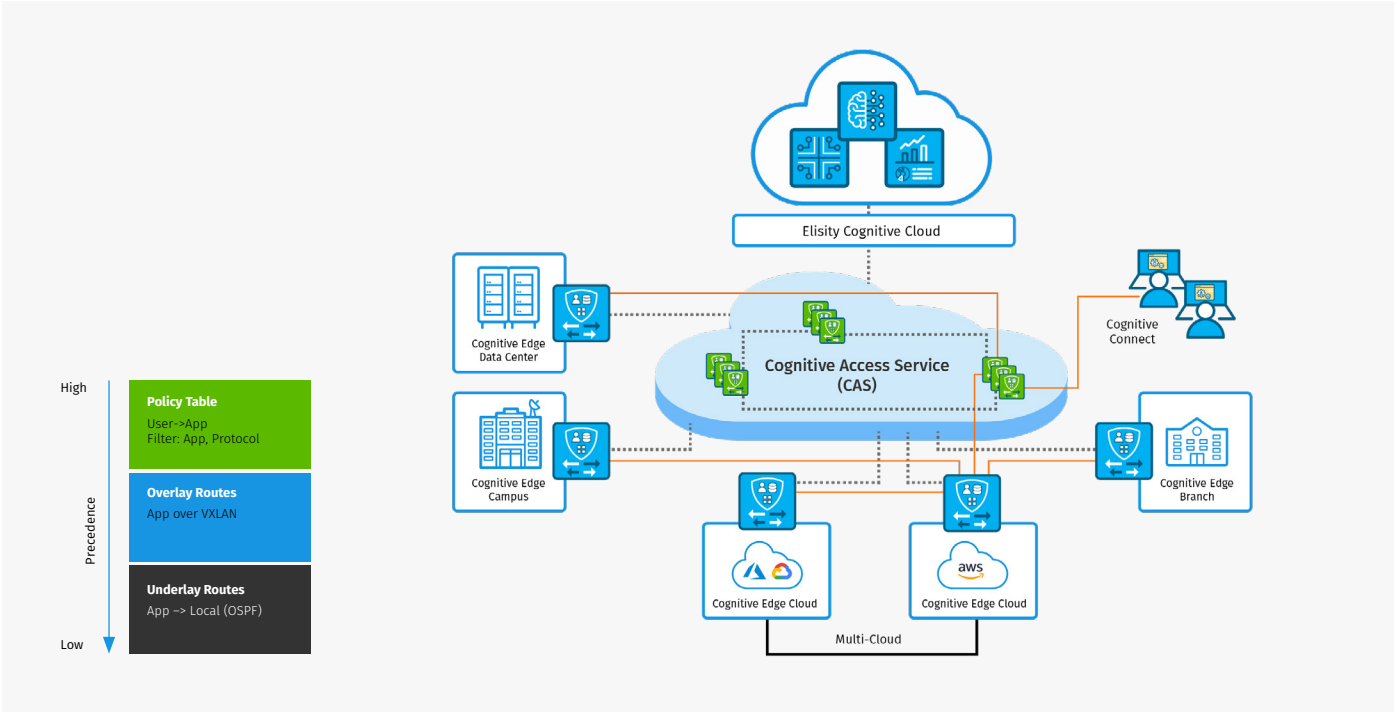
Enabling identity based, Zero Trust access

Elisity Cognitive Trust works by discovering all organizational assets (users, applications, and devices), regardless of their digital footprint, and connecting them to an encrypted “e-mesh” fabric — a software-defined, application-centric virtual network — built on top of existing IP/MPLS transport networks and infrastructure. The e-mesh overlay approach enables rapid application access and instant application connectivity, without having to change the underlying enterprise network topology and security. For instance, distribution and core settings, firewalls, VPN headend, and WAN devices all remain intact.

ECT achieves identity-based access and Zero Trust networking across the digital footprint by simplifying the enterprise networking architecture. ECT changes the traditional, hierarchical enterprise network into a flat, secure, virtual network that spans multiple digital domains. Moreover, ECT enables edge-to-edge encryption across the enterprise. With ECT, organizations that have assets spread over numerous domains — including cloud, hybrid cloud, remote access, edge, branch, and more — can be confident about Zero Trust pervasive security, while embracing agility, remote access, and other digital transformation efforts.

Unlike with legacy networking models, Elisity Cognitive Trust decouples application access from underlying network access. The network is inherently assumed to be untrustworthy. Users need not be “placed on the network” before accessing applications or resources, either on-premise or in the cloud. This approach removes the need for organizations to manage ACLs, VLAN-based segmentation, along with VRFs, VPNs, and FW policies. ECT also eliminates the need for inter-domain policy translations and removes unnecessary flows from reaching the WAN. From a single, centralized platform, ECT enables detailed visualization and dynamic provisioning and connectivity for all enterprise assets and workflows, across every digital domain.

The following diagram shows a simplified representation of the ECT solution:



Key Capabilities

- Gives you real-time information regarding who is accessing resources and from where;
- Allows you to nano-segment your environment based on traffic flow and machine identity;
- Allows you to manage a unified, cognitive, trust-based access policy across your digital footprint;
- Allows you to securely connect your campus, remote access and branch networks directly to the cloud;
- Supports the requirements of remote access in a secure way that meets the needs of the customer; and,
- Allows you to migrate workloads across clouds or within a VPC in a cloud, securely.
- With Elisity's data protection and access protection capabilities, customers can eliminate the need for VPN in their environments

Powering an architectural security transformation

Elisity Cognitive Trust represents a true paradigm shift in enterprise security, enabling organizations to embrace digital transformation and workforce mobility, while securing access with identity-based policy for all users, devices, applications, and data, from one centralized, AI-based platform. These are several of the key advantages of the Elisity Cognitive Trust approach:

There is no "trusted" or "internal" network

Users and devices can only access internal applications and Internet-based or SaaS applications after they are authenticated and authorized with identity-based policy. There is no trusted network, and to use a cliché, a hacker can never get "in." All-access is continuously monitored by the Cognitive Cloud AI engine, which also analyzes the behavior risk of users, devices, and apps. Many organizations assume that, just because they "own" and control the network, they can trust all users and devices on it. ECT resolves this problem and removes the excessive trust and risk of lateral movement that traditional networks create.

Remote users do not require a VPN

Remote users can access internal applications and resources via ECT, after being authenticated with multi-factor authentication. Still, they could never move laterally to any other resource inside the data center, as the request would simply be blocked by the Cognitive Edge. Indeed, with ECT, the default network position becomes "deny." Besides, every denied access attempt and traffic flow is logged by ECT — allowing security teams to proactively monitor and address suspicious user behavior. For instance, security teams could easily integrate the logs with a SIEM, such as Splunk, and create automatic alerts if any user generates X number of blocked policies in X number of minutes. In such cases, the network is always protected — the user is blocked with policy — but security teams can reach out to see if the user's device is compromised or if the user has malicious intent.

All user networks are treated as guest WIFI

Regardless of whether a user is at campus HQ, at a branch office, in a manufacturing plant, or traveling, they are never placed on the network, where they can route to application servers and data centers. At the same time, seven other communication models, including device-to-app, server-to-server, and branch to-cloud are supported. This removes the need for private network connectivity entirely — increasing security while reducing both CAPEX and OPEX costs.

Enterprises no longer need costly segmentation methods

In large campus environments, ECT enables enterprises to move away from existing segmentation methods, including ACLs, Firewalls, VRFs, etc. This helps organizations to save on both CAPEX and OPEX expenditures. Still, organizations can continue to maintain robust user-to-user, user-to-app, or user-to device-segmentation with identity-based policies managed centrally in the cloud. Enterprises can also route their traffic through the security stack — either on-premise or in cloud deployments — to ensure the best security and user experience.

Campus users (wired and wireless) can use existing authentication methods to connect to the campus edge

ECT eliminates the need to stretch VLANs across the enterprise. The reason is that, with ECT, no campus or cloud-based assets are exposed to campus users — network, data center, port, protocol, app, etc. — unless they are authenticated and authorized via policy. This means that enterprises can leverage their existing networks while removing operationally intensive and expensive elements like VLANs. Meanwhile, by nano-segmenting their environments with ECT, organizations can also ensure that access is highly granular and need-based.

Private networking is no longer necessary

Private networking, such as MPLS or even site-to-site VPNs, is no longer needed between data centers and Cloud IaaS environments, where server-to-server communication is required. For instance, if an organization moves its website to AWS, but the backend SQL database remains in a physical datacenter, they can still support private and secure connectivity between these elements, without the expense of private networking. This saves significantly on both CAPEX and OPEX expenditures.

Cloud and multi-cloud interconnect are enabled and secure

Finally, organizations can interconnect multiple clouds or VPC environments securely — without relying on unsecure or operationally intensive solutions like IPsec tunnels or transit gateways. With ECT, enterprises can be confident about hosting or moving workloads among private and public clouds, securely. Moreover, ECT guarantees on-demand, secure connectivity, with fine-grained access and policy mobility, to ensure that users can connect from one VPC to another, or from one cloud to another.

Key Benefits

Access without compromise

- Any user from any device can access enterprise applications from anywhere, without compromising security
- Compatible with any infrastructure: cloud and multi-cloud, remote access, campus, branch, data center and more
- With Elisity's data protection and access protection capabilities, customers can eliminate the need for VPN in their environments

Full visibility

- User, device, and application visibility and analytics across all infrastructure
- Integration with Microsoft AD, AWS, Claroty, ServiceNow, BMC, and other Identity and Discovery machines

Protection

- Identity-based access and nano-segmentation anywhere
- Encryption from edge-to-edge
- Ubiquitous policy across all infrastructure

Automated policies

- Behavioral-based policies based on AI deployed anywhere
- Integration with SIEM

The benefits of transforming your enterprise security to a Zero Trust networking, Software-Defined Perimeter model are manifold. Enterprises can shield every asset in their environments from visibility on the public internet and ensure that no users can connect to any resource without a policy — dramatically increasing their security posture. At the same time, ECT brings significant improvements in terms of user experience, agility, adaptability, and ease of policy management. Indeed, ECT enables digital business transformation scenarios that are ill-suited for legacy access approaches.

As a result of digital transformation, most enterprises will have more applications, services, and data outside their enterprises than inside. Traditional enterprise boundaries are already shifting dramatically. Elisity Cognitive Trust places the security controls where the users and applications are — in the cloud — and enables enterprises to thrive in a world without boundaries, by making identity the new perimeter.

Elisity Headquarters

1900 McCarthy Blvd, Suite 107
Milpitas, CA 95035

To see how Elisity Cognitive Trust can power digital transformation in your enterprise, schedule a demo today or request your complimentary Trust Report.

Visit elisity.com.