Use Case:
Remote Access with Elisity Cognitive Access Service (CAS)

Enabling anytime, anywhere secure Remote Workforce

A Next-Generation VPN Alternative, with Elisity Cognitive Access Service (CAS)

www.elisity.com

Enabling anytime, anywhere secure Remote Workforce with Elisity Cognitive Access Service

Enterprises have used VPN technology for remote access for years. Yet, VPN solutions leave significant security gaps. Elisity Cognitive Access Service (CAS) eliminates the need for VPN with a solution that combines Zero Trust access and Software-Defined Perimeter, powered by AI.

Enterprises have increasingly embraced remote work in recent years. Yet, none were prepared for the pandemic that would force a majority of companies to adopt full-time work from home (WFH) policies overnight.

As organizations embrace WFH as the new normal, they continue to use legacy remote access solutions — namely VPN — that leave them exposed to attack. While VPN technology is ubiquitous, it is inherently insecure, and comes with numerous limitations, including:

- Risk of lateral movement. Remote access users are typically placed directly onto the internal network, which means that compromised end user machines can potentially access the entire corporate network
- Limited visibility and reporting on VPN traffic flows, especially for SaaS and Cloud traffic
- Minimal segmentation with VPN filters, with little precision and zero automation of network policies
- Unencrypted communications, once the VPN is terminated
- VPNs lack the security layers required for enterprise, which makes them an easy target for attackers

Remote access VPN breach examples

- ✗ Attacks against VPN and RDP are up 330% since the COVID-19 pandemic began[1]
- ✗ A VPN provider recently had a compromised service go undetected for months
- ✗ Recently, a terminated employee used VPN to access protected corporate systems used for consumer demand forecasts

Enterprises cannot compromise on remote access security, when remote work has become a baseline business requirement. Instead, organizations need a permanent and highly secure remote access solution that enables the connectivity, visibility, and high-availability requirements that digital transformation demands.

[1] Atlas VPN. https://atlasvpn.com/blog/rdp-attacks-surged-by-330-in-the-us-amid-pandemic

Retire your legacy VPN with Elisity Cognitive Access Service (CAS)

Elisity Cognitive Access Service (CAS) was designed from the ground up to address these challenges in remote access. Using both Software-Defined Perimeter and Zero Trust Network Access, CAS creates rapid, secure, "right-sized" connections for remote users to both on-premises and cloud based applications and resources — enabling organizations to achieve both adaptive access protection and attack prevention. With highly granular, application-level access controls, CAS ensures that no user can connect to any application or resource unless they are explicitly permitted — but can connect immediately, with outstanding quality of service, when they are permitted. CAS works with both web applications and common enterprise applications. Elisity CAS is a holistic solution, and enables organizations to retire their VPN point solutions.

Key Benefits

- Secure application access and network resources; reduce the attack surface with Zero Trust access for all users
- Minimize risk of lateral movement with least privilege access
- Replace slow, awkward VPN connections with a global backbone that allows remote users to connect to the nearest region for better performance and quality of service from anywhere in the world
- Get identity based access — every user device has a unique identity that is authenticated, authorized and verified for every packet in real time, not only on initial access, with always on security
- Manage all policies from a centralized place in Elisity Cognitive Cloud
- Seamless and centralized auditing and reporting of application access
- With Elisity's data protection and access protection capabilities, customers can eliminate the need for VPN in their environments

Solution Components

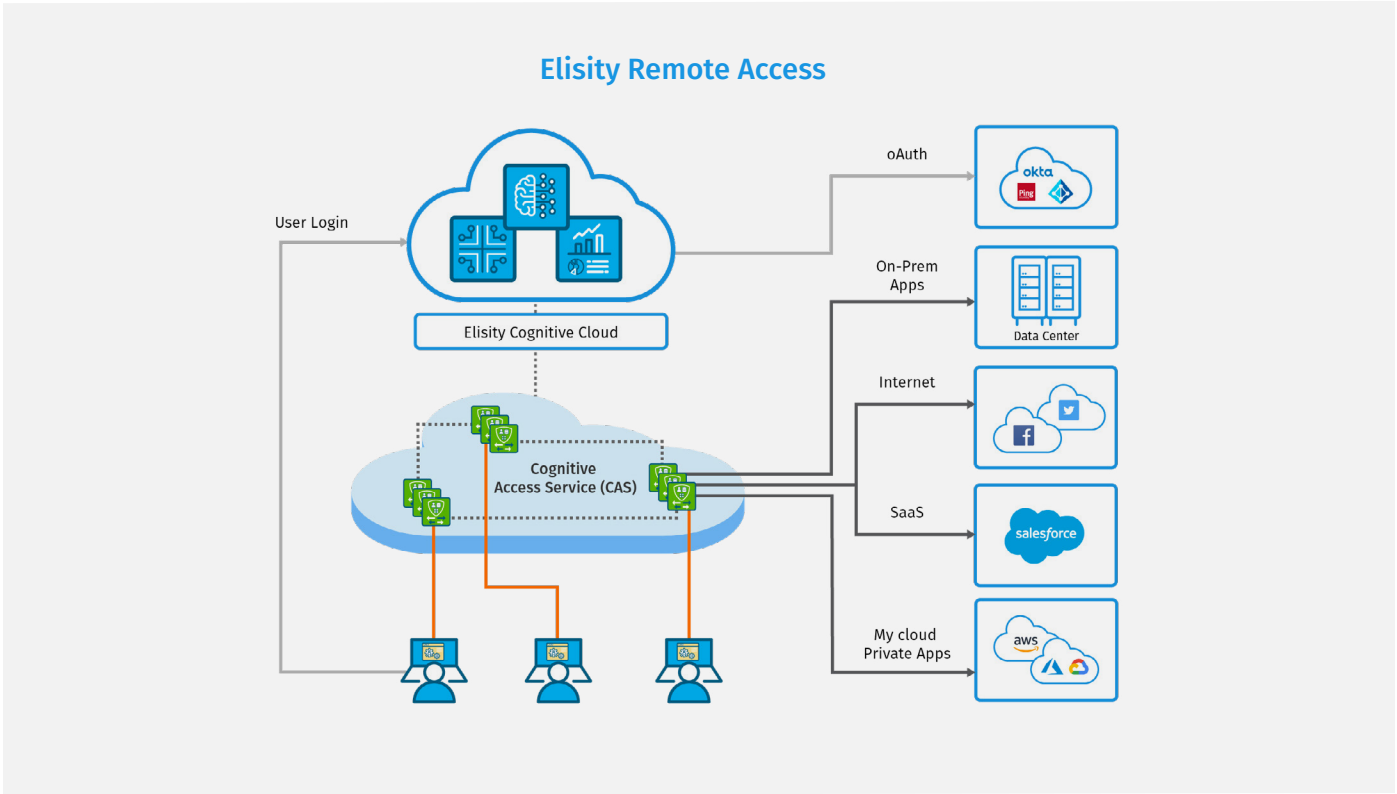
The Elisity Cognitive Access Service solution achieves Zero Trust and Software-Defined Perimeter by providing policies that grant access to specific applications or cloud resources, and not the underlying network. The solution has three major components: Cognitive Access Service, Cognitive Connect, and Elisity Cognitive Cloud.

Cognitive Access Service (CAS)

Elisity 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

Advantage: 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 initiates secure connections directly between the remote user's device and enterprise resources, through the cloud-delivered Cognitive Access Service (CAS).

- Initiates secure connections to the nearest Elisity Cognitive Access Service (CAS)
- Integrates with MFA and SSO authentication with leading Identity providers (Azure AD, Okta, Ping)
- Provides end-to-end encryption of remote traffic
- Provides precise segmentation for applications and cloud resources
- Supports replacing both clientless and client-based VPN
- Works on all popular platforms including Windows, MACOS, Android, and iOS

Advantage: Cognitive Connect provides "right-sized," Zero Trust access for any remote user, from anywhere, without the use of a VPN.

Elisity Cognitive Cloud

The Elisity Cognitive Cloud is a centralized, cloud-delivered platform. The platform contains:

- A policy plane for comprehensive remote security policy management
- A control plane for managing routing context
- An AI layer that continuously monitors risk for all remote assets — users, devices, applications, and data — and automatically provides policy recommendations

Advantage: The Cognitive Cloud Platform pushes access policies "just in time" for remote access users, privileging security over connectivity. The platform enables identity-based access and continuous risk monitoring, from an access perspective.

About Elisity

Elisity is solving the challenge of securing access to enterprise assets and enterprise data in the complex modern world of blurring enterprise boundaries and mobile workforces. Elisity provides unified policy and identity-based access solutions, powered by AI. The Elisity team is made up of experienced entrepreneurs with deep technical backgrounds in enterprise networking and security with the world's largest and most security-conscious organizations.

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.