ELISITY
COGNITIVE TRUST

Use Case:
ECT for Multi-Cloud

Multi-Cloud Strategy

The New Normal

www.elisity.com

Multi-Cloud Strategy: the New Normal

As enterprises accelerate their transition to the cloud, the majority of companies favor an approach that leverages multiple cloud vendors. According to Gartner, ”Most organizations adopt a multi-cloud strategy out of desire to avoid vendor lock-in or to take advantage of best-of-breed solutions.” As a result, companies choose to work with multiple cloud providers such as AWS, Azure, Google to host their private applications. However, multi-cloud environments present a new challenge: managing and securing access to applications across multiple cloud providers, when access management is fragmented across these same environments.

Multi-Cloud Security Challenges

While the benefits of adopting a multi-cloud strategy are clear, such deployments can create numerous operational and security challenges for enterprises, including:

Fragmented access —Identity and access management are critical parts of cloud security, but they are difficult to achieve in a multi-cloud environment. With so many users accessing disparate cloud resources at once, it can be hard to know who can see which files and applications.

Poor governance —Improper governance of access management can result in end users having access to data they shouldn't — leaving an entire organization open to attack. If hackers gain access to user accounts, they can potentially view, edit, and download sensitive files.

Poor hybrid cloud networking solutions —To extend their data centers to cloud environments, enterprises leverage gateways with IPsec connections. However, this strategy increases the attack surface and creates a poor performance for users, as traffic is backhauled to the data center. Enterprises need more efficient and secure solutions.

Difficulty securing connectivity across clouds —To accelerate cloud adoption and perform large-scale workload migrations, organizations need seamless and secure connectivity across clouds — without networking challenges getting in the way.

Complexity —Cloud IAMs are the technology of choice for managing access with individual clouds. However, these tools operate as islands, creating access fragmentation across a multi-cloud environment. At the same time, access management is static, with "set and forget" security policies that don't adapt to user behavior. Lastly, enterprises are left without unified auditing and traceability of access across their digital footprint.

To address these challenges, enterprises have turned to several market solutions. However, existing solutions only offer a piecemeal resolution to the problem, or else provide sub-optimal results. For example, solutions that create site-to-site VPNs often result in IPSec tunnel "explosions"; elsewhere, solutions that encrypt and decrypt traffic at multiple points can introduce service delays; other solutions offer no coverage for east-west data protection. These access challenges have led to increased attacks, overhead, and cost in cloud deployments.

Elisity Cognitive Trust for multi-cloud environments offers unified and fine-grained control for applications and resources

Elisity Cognitive Trust for Multi-Cloud Access

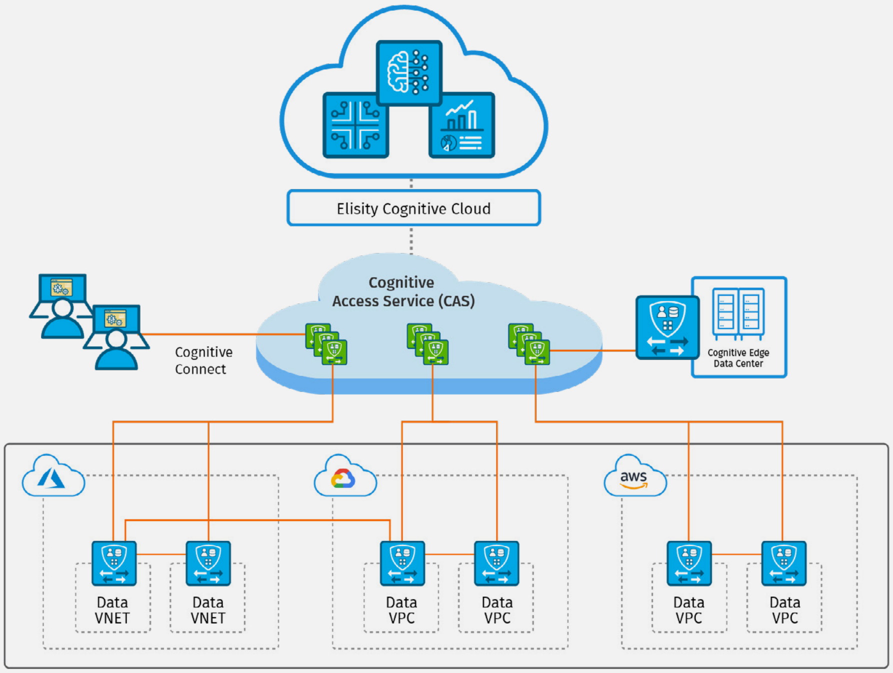
Elisity Cognitive Trust (ECT) is the industry's first combined Zero Trust networking and Software-Defined Perimeter solution. Designed from the ground up to solve the multi-cloud access problem, ECT offers an end-end implementation overcoming the challenges of Multi-Cloud and other offering weaknesses. It offers a new paradigm that transforms access for cloud deployments to a Zero Trust model and proactively protects access to organizations' critical applications, data, and resources across their multi-cloud deployments. With ECT, any user can connect directly and securely to any cloud application, from anywhere.

Next Generation Access Management

Elisity Cognitive Trust (ECT) is a cloud-delivered solution that provides identity-based access control with software-defined segmentation and policy enforcement, based on user identity and group membership. Trust is never taken for granted and it is continuously monitored, which allows enterprises to create fine-grained segmentation — reducing risk and improving security.

ECT solution components include the Cognitive Cloud, Cognitive Edge, and the Cognitive Access Service (CAS). The Cognitive Cloud is a centralized place for managing control, policy and the AI engine. The Cognitive Edges build an encrypted overlay data plane, the e-Mesh, on top of the existing underlay as transport without altering its network or security configuration. The CAS, a next-generation VPN alternative, enables Zero Trust remote access to cloud, data center, or other corporate assets from any location worldwide. Any asset — device, app, or application — is only connected to the e-Mesh with a policy. Access is never taken for granted and is continuously monitored by the Cognitive Cloud AI engine for risk, health, and behavior, with automatic policy recommendations.

Elisity Multi-Cloud Deployment



Key Highlights

Unified access —ECT provides enterprises with unified access control and ubiquitous policy for cloud-based applications and services, from a single, cloud-delivered portal. Access policies are based on the identity of users, applications, devices, or native cloud constructs, regardless of cloud. Organizations can now connect and secure access to their applications in the cloud, multi-cloud, or data center environments.

Rigorous and transparent governance —ECT ensures that only the right people have access to the resources they need. Moreover, at the click of a button, administrators can get automated access authorization logs across every application in their multi-cloud environment.

Optimal hybrid cloud networking —Organizations can save on costs from site-to-site VPN deployments and directly connect their branch and campus to multi-cloud applications. This approach saves on overhead, avoids low latency and poor performance to users, and ensures security through end-to-end encrypted data.

Secure connectivity across clouds —Using encrypted data traffic from edge to edge, organizations can instantly connect clouds to and across public clouds, intelligently insert on-demand network services, and ensure security, visibility, and a seamless user experience.

Simplicity —ECT not only eliminates the complex, inconsistent, and costly networking overhead in cloud environments today, but also simplifies access across all enterprise digital resources.

Additional Capabilities

ECT integrates with your existing cloud deployments to discover all your organization’s digital assets — users, applications, instances and data — and provides extensive visibility into traffic flows to these cloud applications. Additional capabilities include:

- **Cloud visibility, monitoring, and reporting:** Full visibility into users, applications, cloud native instances, and traffic; all access is centrally logged
- **Application-based segmentation:** Access is granted to specific applications only after users are authenticated
- **East-West traffic protection:** Full protection for application-to-application traffic
- **Improved user experience:** Connect users directly to cloud applications, without routing them through internal networks. Connect from branch, data center, campus, and other domains
- **End-to-end encryption:** End-to-end encryption, as opposed to encrypt-decrypt at multiple locations
- **Right sized access:** “Just in time” access and “just enough” policy avoids management overhead in configuring and maintaining rules
- **Continuous monitoring:** Access is never taken for granted, access is always monitored, and policies are revised based on user behavior.
- **Integration**: Cloud-native integration with AWS, GCP, Azure

Key Benefits

Elisity Cognitive Trust for Multi-Cloud gives enterprises the ability to manage access policies across their cloud environments from a single, centralized platform. Other benefits include:

- **Access auditability:** Full access auditing across all cloud deployments and cloud-based applications, from a cloud-delivered portal
- **Simplified access:** Seamless and fast access to applications, with reduced management overhead and TCO with a single solution
- **Increased security, visibility, and control:** Every user and device is authenticated and authorized before connecting, and traffic flows are monitored from end to end, providing unprecedented visibility and control
- **Cloud readiness:** As more and more applications move to the cloud, organizations can position themselves for managing access across all devices and users in a highly granular, context-aware way
- **Cognitive Engine:** AI-generated policy recommendations mean enterprises can adapt policy to changing user behaviors and resolve access vulnerabilities in their cloud deployments
- **Governance:** Automated access authorization log across all applications in multi-cloud, and the information is available in a click of a button

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.