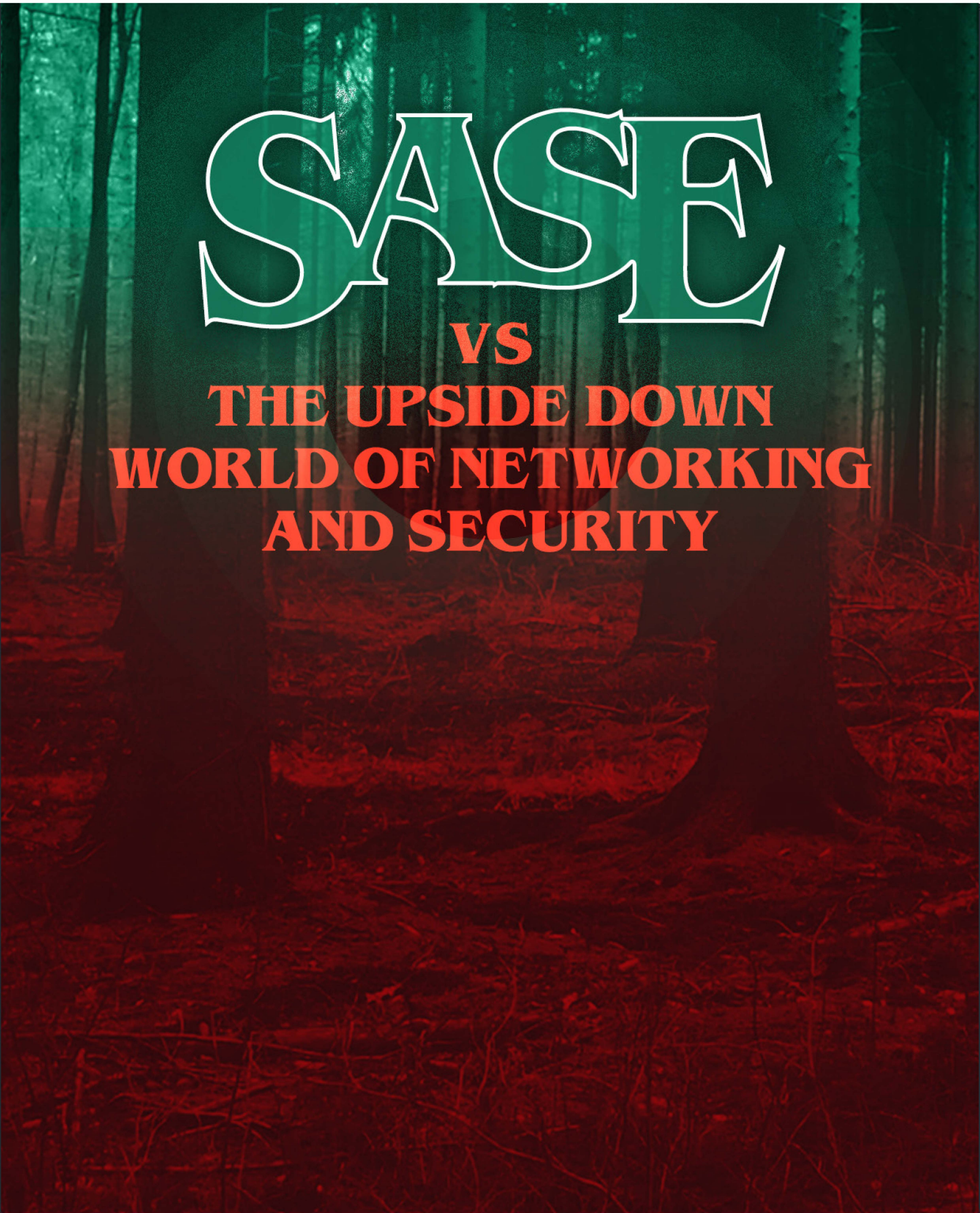
CATO NETWORKS

CLOUDTIVITY CONSULTING SERVICES LLC



What is SASE?

SASE (Secure Access Service Edge) is an enterprise networking category introduced by Gartner. A convergence of SD-WAN and network security solutions like ZTNA, CASB, and SWG, solutions provide enterprises with one, unified and cloud-native network and security service.

Before SASE, network and network security services were delivered through multiple point solutions, including legacy appliances. These legacy appliances operated in silos and required countless IT resources and attention to deploy, manage, maintain, and replace. Today, some enterprises are still trapped using these legacy appliances, despite their shortcomings.

The Upside Down World of Legacy Appliances vs. SASE

Examine the upside-down world of legacy appliances, where things are complicated and time-consuming, and see how they compare to Cato's SASE, which exists in the parallel, modern world.

We will cover five characteristics that exist in both dimensions:

- Network Device
- High Availability
- Security Updates
- The Hardware Refresh Cycle
- TLS Inspection

At the end of this eBook, you'll be able to rescue yourself from the upside-down world of legacy appliances. Or will you stay trapped...?

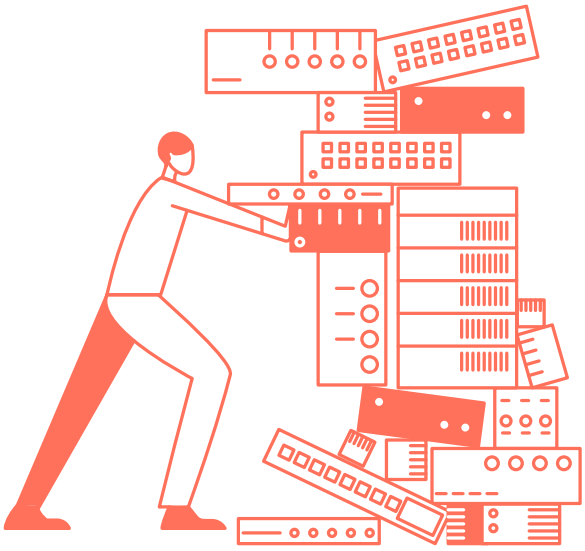
Characteristic #1:

Network Devices

Network devices are the physical appliances that build up the network to enable connectivity and security. In other words, they are the foundation of business information operations.

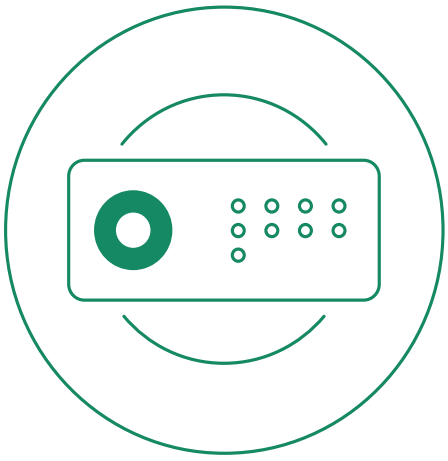
The Upside-Down World

In the upside-down dimension, legacy devices are heavy duty are incredibly high touch to maintain and monitor. And, to source and ship them, appliances rely on the availability of multiple physical components across the global supply chain. Additionally, deploying legacy appliances often requires flying an expert across the country or the globe to ensure proper installation and setup.



SASE World

In the modern world, Cato provides simple, lightweight appliances that can easily connect locations to services. The Cato socket devices easily pass through customs since they don't have direct security capabilities. Instead, they connect to services via the global Cato cloud. In addition, deployment is virtually zero-touch and just a few clicks. This means devices are up and running in just a few minutes and deployment can be done by business users.



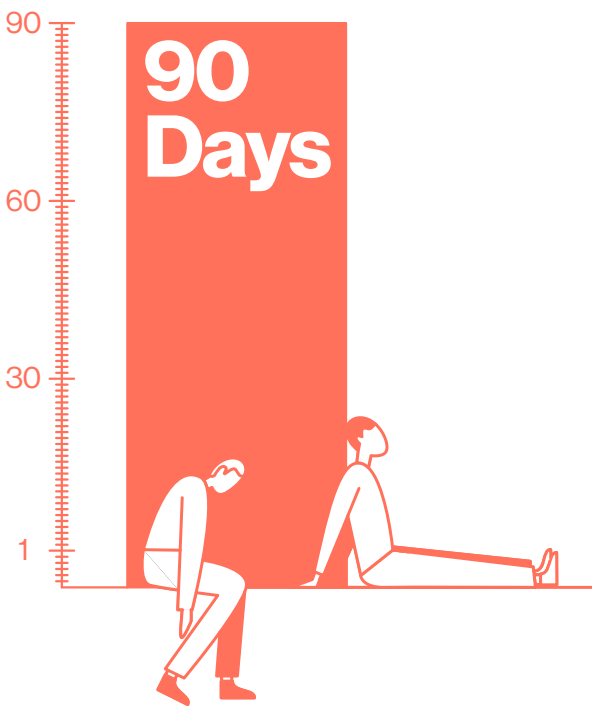
Characteristic #2:

High Availability

High availability means ensuring the system is always operating and accessible to all users. A single failure point due to outages, natural disasters, misconfigurations, or other reasons will not impact users' uptime. This is achieved by configuring multiple sites that can back each other up.

The Upside-Down World

Configuring new sites with legacy providers to ensure uptime is a costly and complex process in the upside-down dimension.



The process can take hours of work over the course of a few days. It often requires:

- Buying and deploying another firewall
- Configuring the failover interface
- Assigning the failover IP address
- Assigning an external IP address
- Assigning an internal IP address
- Verifying the primary configuration
- Configuring the secondary failover interface
- Assigning the secondary failover IP address
- Copying the configuration to secondary
- Additional secondary configuration address
- Copying the configuration to secondary
- Additional secondary configuration

Any mistake in this process could have dire consequences for the business.

SASE World

With Cato, on the other hand, admins can easily assign a second socket to a site using the Cato management application and have high availability up and running in a manner of minutes. This is a frictionless process with no complex configuration required.

The process is lightweight and significantly reduces cost, and removes the risk of someone accidentally taking down the network (and losing thousands or millions of dollars in business productivity, as a result.)

This process is also highly scalable and low cost, so high availability pairs can be deployed everywhere as OpEx rather than CapEx, and with no technical expertise required.

Maintenance is as easy as fine-tuning policies in the Cato management application, and sockets can easily move between sites as the business expands, with no additional overhead or support from Cato required.

Characteristic #3

Security Updates

Security updates are essential for businesses, but they also drive IT's attention away from their core business model. With a shrinking IT team and a growing number of cyber-attacks, businesses often find themselves pushing security tasks to the bottom of the list. How does each dimension deal with this challenge?

The Upside-Down World

In legacy environments, security tests can be cumbersome and complex, requiring IT teams to spend hours rolling out updates to production or rely on automatic updates to firewalls. However, both models are disruptive to the business. They require resources, and time and focus from IT teams, who are already juggling multiple, urgent and time-sensitive requests.

Additionally, automatic updates often don't work as expected, requiring IT teams to manually fix issues Since the number of hours in a day is limited, many of these actions can only be completed after-hours or via external consultants. As a result, many organizations find themselves lacking the proper security controls necessary.

SASE World

With Cato, no manual updates are required from IT.

Cato utilizes over 250+ security feeds, developed by our in-house security team, and evaluated by our proprietary system for accuracy and timeliness. The feeds are updated hourly and automatically by Cato SASE cloud.

These updates are based on common security feeds that are analyzed and compared to historical data. In addition, with Cato, there are rarely any false positives. This leaves IT with time and resources to work on business-critical projects (and even manage to drink a cup of coffee).

Cato enables organizations to shift their entire security paradigm and technology stack. Security and networking is automatically delivered via an automatic, cloud-delivered service of security experts, with no need for IT upkeep or additional expertise.

Characteristic #4

Hardware Refresh Cycle

The hardware refresh cycle is the process of evaluating and upgrading the hardware of the business. Reasons for replacing/adding hardware can be forced obsolescence, new capabilities, or requirements for increased capacity. Updated hardware ensures deploying the relevant technologies that will drive productivity, security and business agility, while meeting the business's needs.

The Upside-Down World

In legacy environments, the hardware refresh cycle is a time-consuming and slow process that typically consists of four steps:

Assessment

Testing the new functionalities, performing sizing exercises, and determining the project scope.

Purchase and Deployment

Negotiating the purchase, planning the deployment, and executing the deployment plan.

Maintenance

Managing policies across multiple devices and installing patches, plugins, and updates.

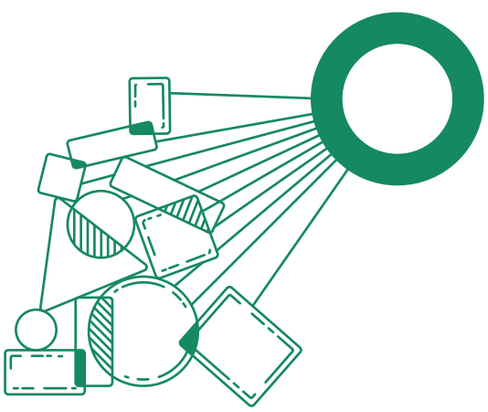
Repeat

Repairing every 3-5 years or when additional capacity is required.

Completing these steps is impacted and often slowed down by factors like global supply chain shortages, internal politics, budget approvals, IT bandwidth, and more.

SASE World

Cato's SASE cloud leverages a cloud-based platform and upgrades components and environments automatically.



This provides businesses with:

- (Near) infinite global capacity which is available on-demand
- Quick global connectivity, with no need for deployment
- The ability to easily adopt new features
- A low-cost subscription model for sockets
- Reduced administrative overhead
- Elimination of the expensive and time-consuming hardware refresh cycle
- Using an OpEx pricing model instead of CapEx pricing

These capabilities provide the business with agility and scalability, which have become more essential and in-demand since Covid-19. They also enable the business to respond on time to swift changes, like M&As.

Characteristic #5

TLS Inspection

TLS inspection is the security process of decrypting encrypted traffic, inspecting for security threats and then re-encrypting it. This is necessary to ensure that bad actors are not able to perform reconnaissance or progress laterally in the network.

The Upside-Down World

In legacy dimensions, TLS inspection requires:

- Sizing, purchasing, deploying, and configuring more firewalls.
- Managing and deploying security certificates.
- Backhauling traffic to firewalls for inspection.
- Spending time addressing user performance issues.
- Buying more firewalls as bandwidth and user count increase.

Appliances often can't handle the level of throughput required to enable advanced security functions like TLS inspection, requiring enterprises to choose between capacity and advanced security capabilities.

Additionally, IT teams are often required to prove the value of TLS inspection to ensure they get funding to perform the process.

SASE World

- An automatic certificate delivered by the Cato Client (for Windows).
- Defining exceptions at the click of a button (for privacy purposes).
- Enabling TLS inspection.

When it comes to TLS inspection, Cato allows for simple deployment at scale. Simply enable TLS inspection and traffic will be inspected according to your policies at any of Cato's 75+ global PoPs, allowing for a decentralized approach to inspection. There's no need to worry about capacity limitations, performance issues, or "breaking something" in your infrastructure. Just turn it on with the flip of a switch, and specify what traffic you want to bypass.

And if your network security team is limited in size or spread too thin as it is, TLS inspection can be set up and run properly with minimal resources required.

How to Get Out of the Upside-Down World

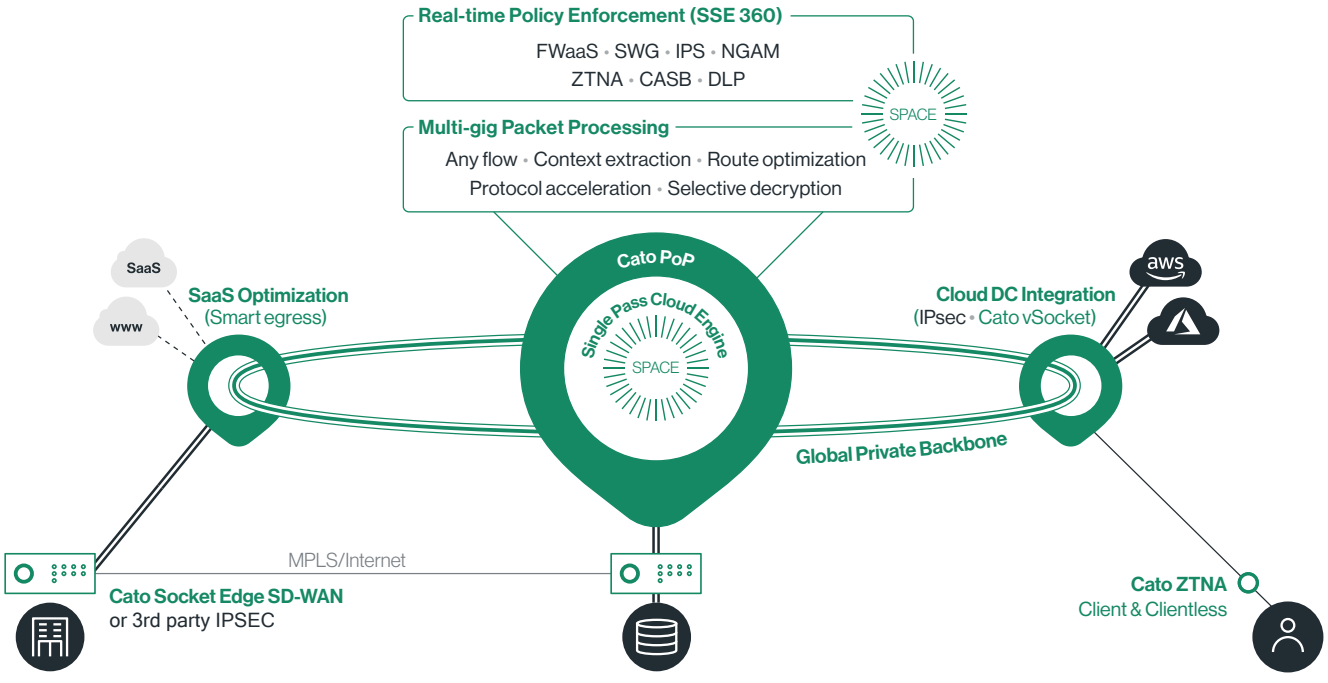
SASE improves business agility, provides a complete security stack, and simplifies both network and network security for enterprise IT teams and supports global remote work models. This all takes place through a solution that is easy to set up and use by IT and IS, making the experience simple and frictionless. SASE services provide a cloud-native architecture that connects and secures all resources and edges, anywhere in the world, based on identity-driven access.

By implementing SASE, enterprises can ensure they are never trapped in an upside-down world of cumbersome legacy appliances. Rather, they maintain control of their business and future, ready for whatever's next.

About Cato Networks

Cato provides the world's leading single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Cloud optimizes and secures application access for all users and locations everywhere. Using Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration. Cato enforces granular access policies, protects users against threats, and prevents sensitive data loss, all easily managed from a single pane of glass. With Cato your business is ready for whatever's next.

Cato SASE Cloud with SSE 360



For more details, please contact us

Kee Murray
Cloudtivity Consulting Services, LLC
Georgia, United States
770-833-6371
info@cloudtivityconsulting.com
https://cloudtivityconsulting.com/

Cato SASE Cloud

SSE 360

Secure Remote Access

Edge SD-WAN

Global Private Backbone

Multi-cloud / Hybrid-cloud

SaaS Optimization

Cato Management Application

Use Cases

MPLS Migration to SD-WAN

Secure Remote Access

Secure Branch Internet Access

Optimized Global Connectivity

Secure Hybrid-cloud and Multi-cloud

Work From Home

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.