CATO NETWORKS | DATRIX

SASE

The Optimal Architecture to Secure and Connect the New Enterprise Perimeters

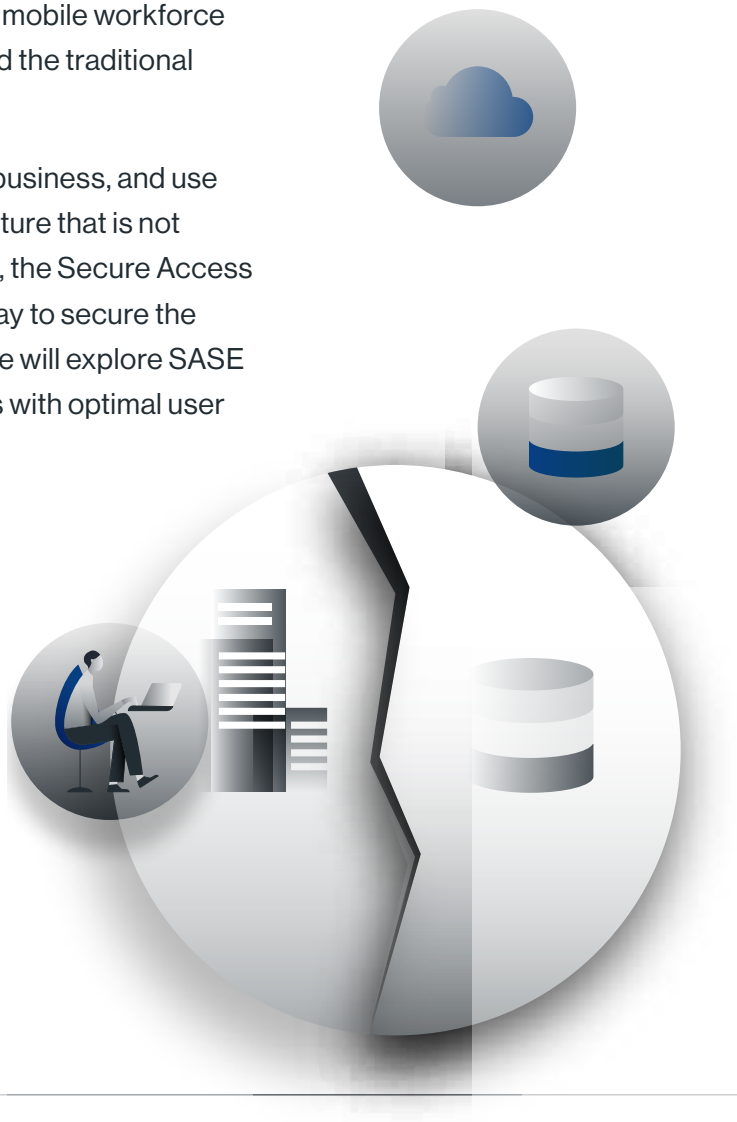
Introduction

The enterprise Perimeter has been the focus of networking and security leaders for decades. The basic planning assumption, and associated best practices, was that the Perimeter was drawn around the corporate datacentre that hosted all sensitive data and applications. IT has invested significant resources to secure all traffic coming into and going out of the Perimeter with network security technologies like firewalls, intrusion prevention systems, secure web gateways, and more.

Beyond security, the Perimeter was a clear physical boundary that requires optimal connectivity to the outside world: employees, partners, suppliers, and later distributed applications across regions and the cloud.

The single enterprise Perimeter paradigm came under pressure over the past decade. The datacentre Perimeter was stretched with the migration of many applications to cloud datacentres and public cloud services. The combination of cloud applications and the expanding mobile workforce created new traffic patterns that completely bypassed the traditional datacentre Perimeter.

This change in the way modern enterprises conduct business, and use cloud and mobile technology, requires a new architecture that is not based on a single Perimeter design. This architecture, the Secure Access Service Edge (SASE), was defined by Gartner, as a way to secure the new enterprise multi-Perimeters. In this document, we will explore SASE and how it can address a range of common use cases with optimal user experience and without compromising security.



What is SASE and How it Effortlessly Secures All Enterprise Perimeters

The Secure Access Service Edge (SASE) is a new enterprise networking technology category introduced by Gartner in 2019. SASE converges the functions of network and security point solutions into a unified, global cloud service. These include SD-WAN, Global Private Backbone, Secure Web Gateway, Firewall as a Service, and more. SASE architecture is marked by four main attributes. It is identity-driven, cloud-native, supports all edges, and is distributed globally.

SASE Architectural Attributes

Identity-driven

User and resource identity, not simply an IP address, drives SASE networking and security policies. This approach reduces operational overhead by letting companies develop one set of networking and security policies for users regardless of device or location.

Cloud-native

SASE is a cloud-first and cloud-native architecture. All networking and security functions are implemented in the cloud. Only capabilities that must be deployed at the edge, are delivered as simple edge clients. SASE architecture leverages key cloud capabilities including elasticity, adaptability, self-healing, and self-maintenance to uniformly deliver security and networking capabilities across the enterprise.

Supports All Edges

SASE creates one secure network for all company entities — datacentres, branch offices, cloud resources, and mobile users. For example, SD-WAN appliances support physical edges while mobile clients and clientless browser access connect users on the go, and while working from home.

Globally Distributed

To ensure the full networking and security capabilities are available everywhere and deliver the best possible experience to all edges, the SASE cloud is globally distributed across dozens of Point of Presence (PoPs). Enterprise edges connect to the nearest PoP so all traffic is secured and optimised at the PoP and across the global backbone of PoPs to its destination.

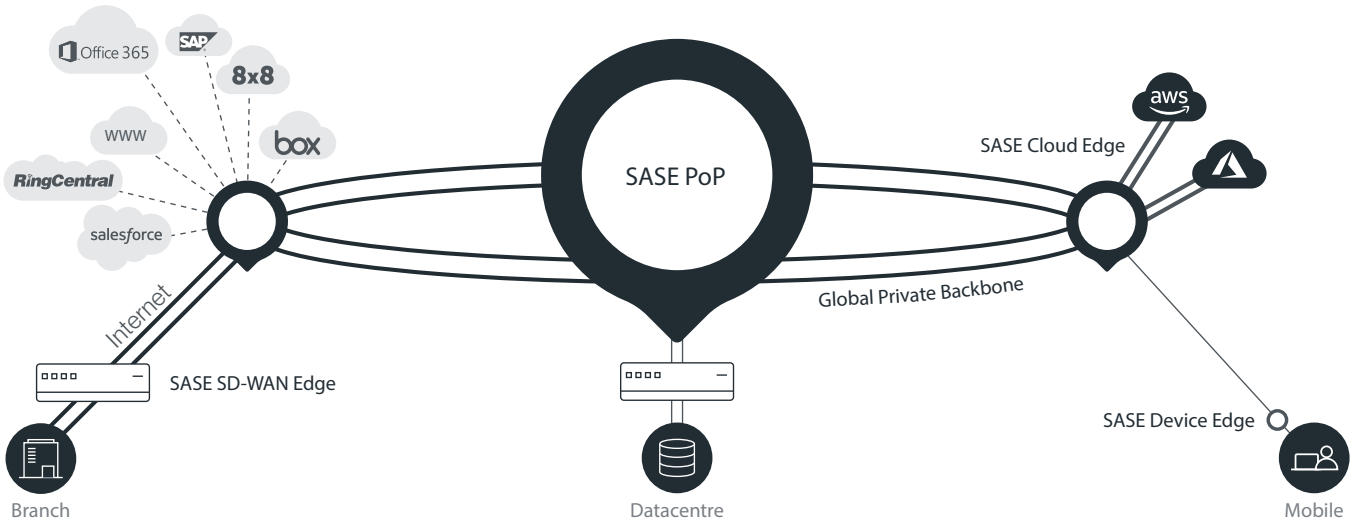
SASE is Optimised for Total Visibility and Control

SASE's cloud-first architecture is uniquely positioned to support the change to the enterprise Perimeters. How? The primary problem presented by the changes to the Perimeters is **restricted traffic visibility and inspection blind spots**. Traditional appliance-based security is optimised to secure a **single** traffic path. To ensure visibility and control of **all** traffic paths such as mobile-to-cloud or branch-to-cloud, enterprises had to force all traffic through their datacentre Perimeter – or go without security at all. This is a sub-optimal design that adds latency and pressures the datacentre security engines.

SASE architecture is built for **full visibility** to **all traffic** from **all edges** - physical, cloud, and mobile - including traffic between the edges (WAN), and from the edges to the Internet. SASE applies a rich set security and networking engines on that traffic, for **full inspection** for threat prevention and access control. This is why SASE has been touted, by Gartner, as the future of networking and security.

SASE CLOUD

Converged Traffic Optimisation, Access Control, Threat Prevention



SASE Components

SASE Cloud

A globally distributed cloud service that delivers the networking and security capabilities to all edges. The SASE cloud operates as a single entity and its internal structure is transparent to the end users.

SASE Edge

Designed to connect a specific edge to the SASE cloud. SASE clients include SD-WAN appliances for branches, IPSec-enabled firewalls and routers, and device agents for Windows, Mac, iOS, Android, and Linux.

SASE PoP

A specific instance within the SASE Cloud that hosts the resources needed to deliver the SASE capabilities including servers, network connectivity, and software. SASE PoPs are symmetrical, interchangeable, multi-tenant, and mostly stateless. They are built to serve any enterprise edge connected through them as an integral part of that particular enterprise network.

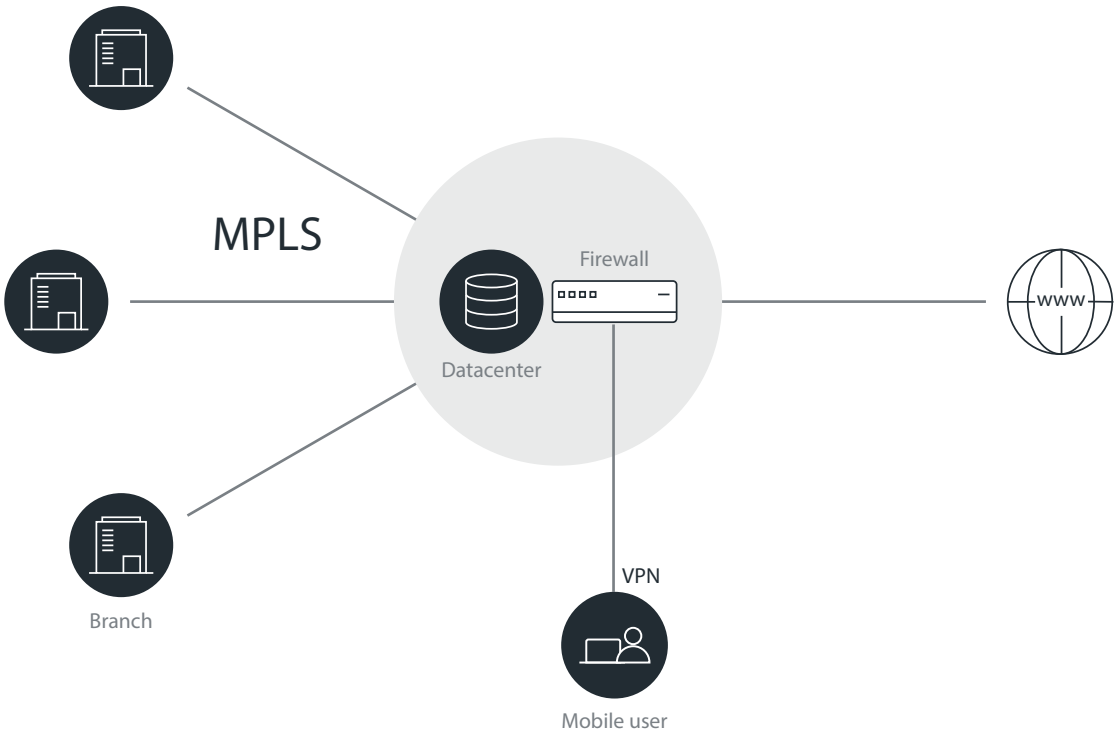
SASE Management

A cloud-based management application to configure all policies and view network and security analytics and real-time status.

The enterprise new Perimeter is, in fact, multiple Perimeters each representing a new line of sight, between users and applications. Enterprises think about these new Perimeters as separate gaps, that force the deployment of new network and security solutions for branches, users, and clouds. This piecemeal approach leads to immense complexity, inferior service, and weak security. A true SASE platform, built on a cloud-first architecture, has full visibility and control of all enterprise traffic. By design, SASE eliminates enterprise blind spots which makes it the ideal platform to optimally connect and secure the modern enterprise.

SASE Connects and Secure the Modern Enterprise

Let's take ACME Corp and its evolving enterprise infrastructure. From a rigid and static network design of branch-to-datacentre connectivity, ACME is in the midst of deploying its applications in new physical and cloud datacentres (IaaS) and migrating others to the public cloud (SaaS). Access requirements have evolved too. Users no longer need to access all applications from the branches and offices, but also need to connect from home and while on the road.



ACME Legacy Network

Use Cases

1 Securely Connect ACME Branches to Any Application

Before SASE

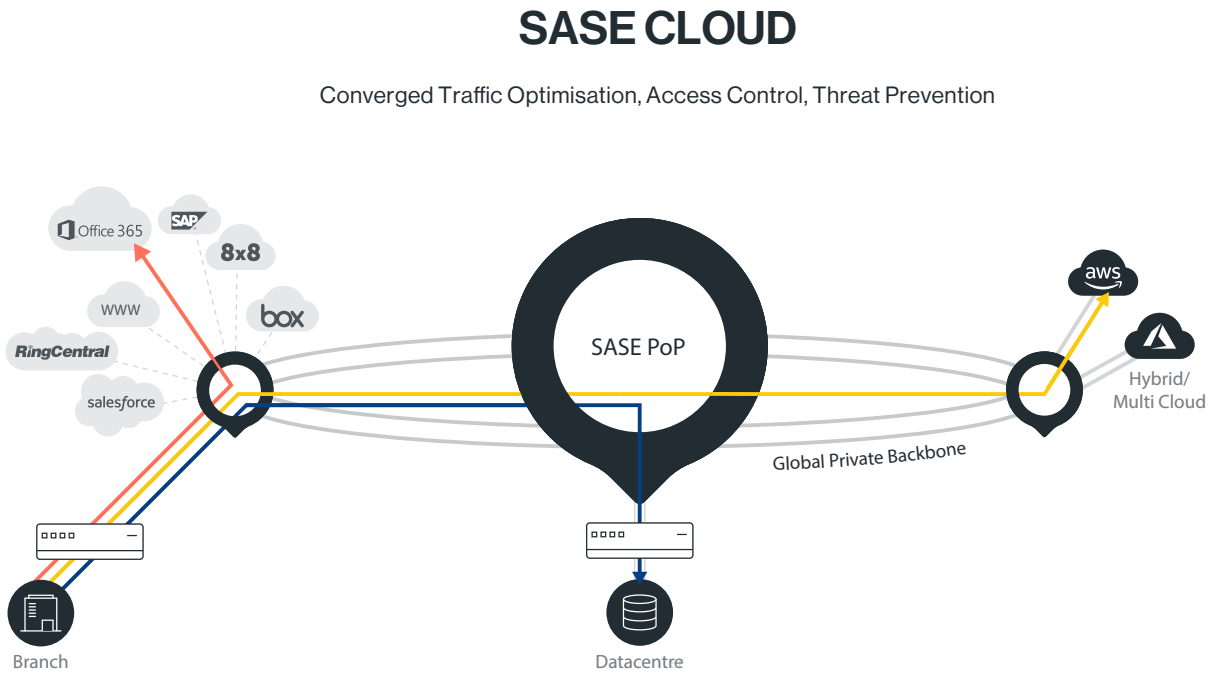
Trombone Effect and a Security Chokepoint

ACME needs to securely and optimally connect its branches to the applications – wherever they are. Branches are connected to the datacentre and from there to the cloud. This creates two problems. First, is the added latency, also known as the "Trombone Effect" of sending the traffic for inspection to a different physical location. Second, is the increased load on the datacentre firewalls as a result of the increase use of the cloud to host distributed applications.

With SASE

Optimal and Secure Branch to Application Access

ACME plugs all its branches into the SASE Cloud using edge SD-WAN appliances, and specifically to the SASE PoP nearest to each location All branch traffic, both WAN and Internet, is fully inspected at the SASE PoP, and then routed optimally to the target application via the nearest PoP to its location (on premises, in a cloud DC, or the public cloud). There is no "Trombone Effect", and there is no single security chokepoint.



2 Securely Connect ACME Remote Users to Any Application

Before SASE

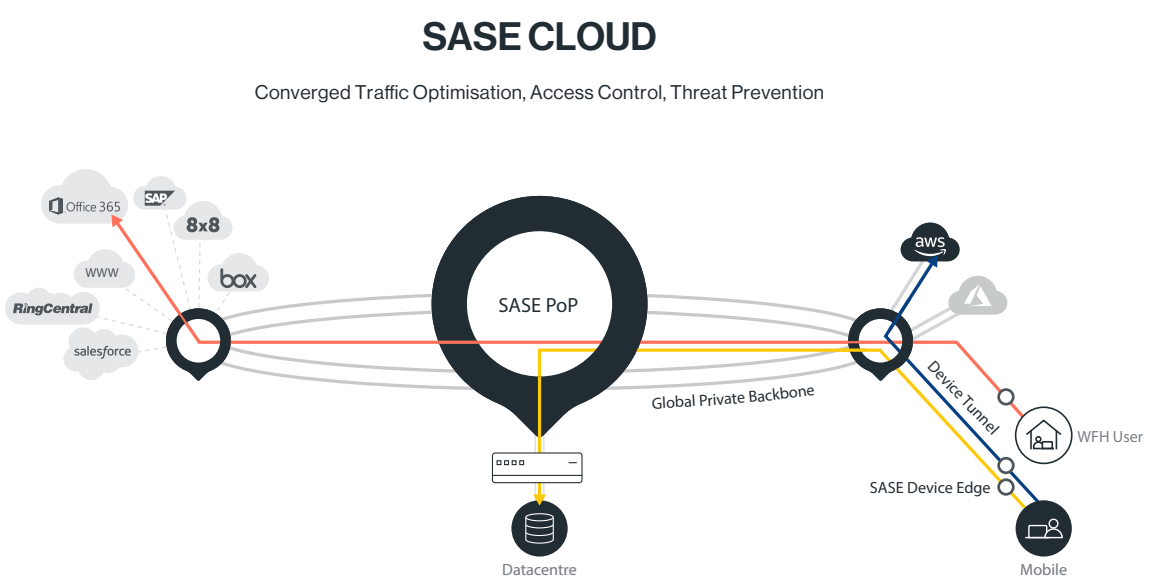
Trombone Effect and a Security Chokepoint

ACME wants to securely and optimally connect its remote users to the applications they need – wherever they are. Users currently use VPN clients to connect to the firewall in the datacentre, and from there to get to their applications. This created three problems. First, the use of the public Internet for VPN access created a bad user experience for global access from the user location to the datacentre Perimeter. Second, users where able to access public cloud applications directly, without any security enforcement or threat prevention applied. Third, in such case when the entire company had to work remotely, the current VPN infrastructure was unable to meet the sudden increase in traffic volume.

With SASE

Optimal and Secure User to Application Access

All ACME remote users connect to the nearest SASE PoP using SASE device clients or browser-based based clientless access. All user traffic, both WAN and Internet, is fully inspected at the PoP, and then routed optimally to the target application via the nearest SASE PoP to its location (on premises, in a cloud DC, or the public cloud). SASE addresses the three challenges described above. SASE global backbone optimises the traffic from the user location to the target application and delivers a better user experience versus the public Internet. All traffic is inspected at the PoP including WAN, Internet, and Cloud-bound traffic – so consistent security policy is enforced. And remote users' traffic is automatically load balanced within and across SASE PoPs to ensure unlimited scalability and the elimination of single point of failure and performance bottlenecks.



3 Optimally Connect ACME Branches Globally to a New Cloud ERP System

Before SASE

Static Global MPLS network into a Physical Datacentre

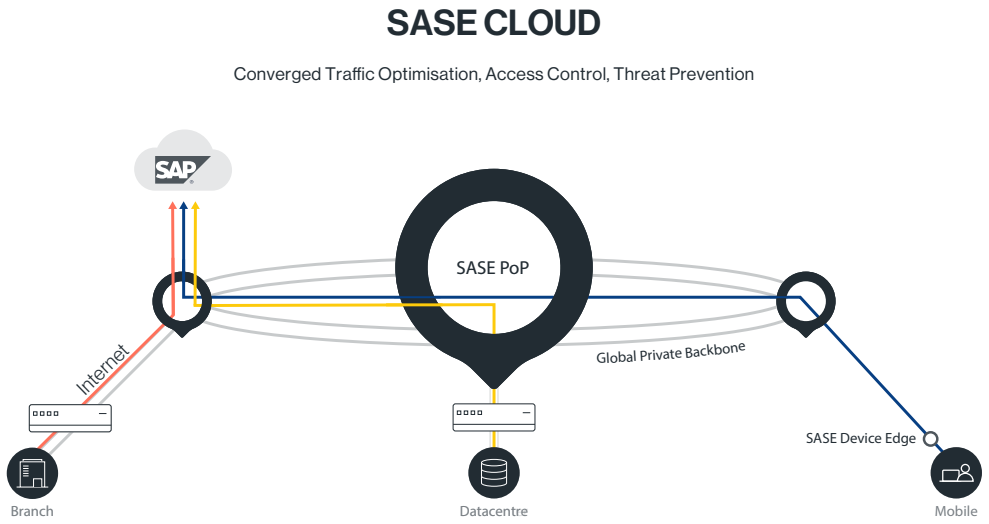
ACME's core business application is hosted in its datacentre in Germany. The entire MPLS network was built to optimise access to that datacentre globally. This was a hard-wired design. ACME decision to migrate its ERP to a cloud datacentre, to improve up time and simplify disaster recovery planning, had required a rethinking of the network. ACME didn't want to continue routing all traffic to its datacentre over MPLS and then send the traffic to the cloud.

With SASE

Optimised and Secure Global ERP Access for All Locations and Users

With SASE, ACME can eliminate the tight coupling of the network design and the business requirements. Such design can't respond to changes in business requirements (such as cloud migration for better availability and uptime) without a major overhaul of the network or a sub-optimal service.

ACME will plug its cloud datacentre to SASE on one-hand and all of its branches and users on the other hand. The SASE core will optimally egress all traffic to the cloud ERP system at the Frankfurt PoP from all edges. All traffic will be subject to full access control and deep packet inspection. This design will enable ACME to not only adapt to current requirements, but also to support future changes to the network such as migration between cloud providers, the distribution of the cloud ERP system across regions, and more.



4 Securely Connect ACME Multi-Cloud and On-Premise Datacentres (Future)

Before SASE

Complex Networking and Security Deployment

ACME is considering the use of multiple cloud providers in addition to its own datacentres. ACME would need to deploy virtual firewalls at the edge of each cloud provider and build a full mesh across its datacentres. Alternatively, it needs to use the native routing and security mechanisms of each provider, which required specialised and dedicated resources. To optimise access to each cloud provider, a premium connectivity service, like AWS Direct Connect and Azure ExpressRoute, would be required.

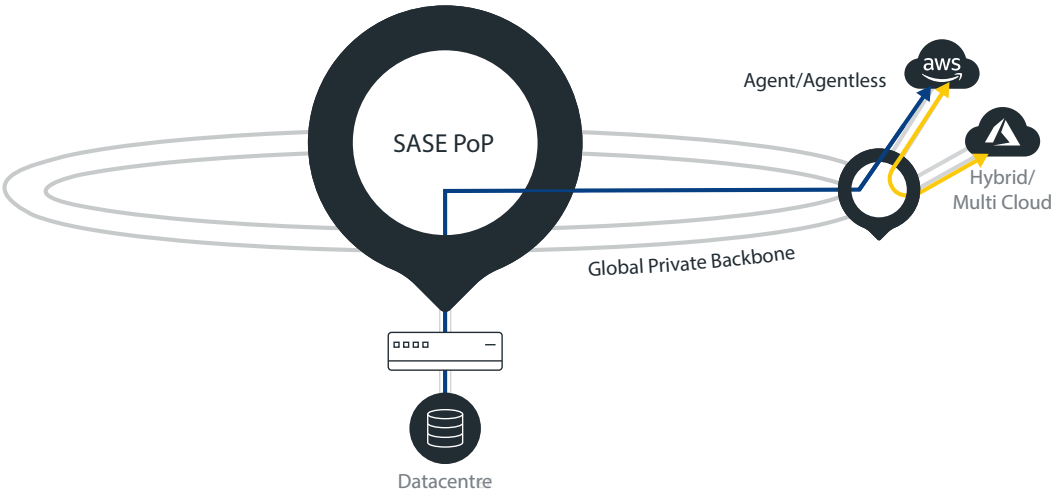
With SASE

Optimal and Secure Any-to-Any DC Connectivity

All ACME cloud and physical datacentres plug into the nearest SASE Cloud PoPs. Connectivity is established over IPSec tunnels or virtual edge SD-WAN appliances. Cloud-to-Cloud and Cloud-to-Physical DC Traffic is inspected inside the SASE PoP and the optimally routed across the SASE global backbone to the destination. Because SASE treats each datacentre as an edge, all edges including physical, cloud, or mobile, benefit from traffic optimisation without the use of premium connectivity options. Better yet, the centralisation of the security policy and enforcement within the SASE Cloud, ensures a consistent and coherent policy applies across all traffic independent of the underlying cloud provider native controls.

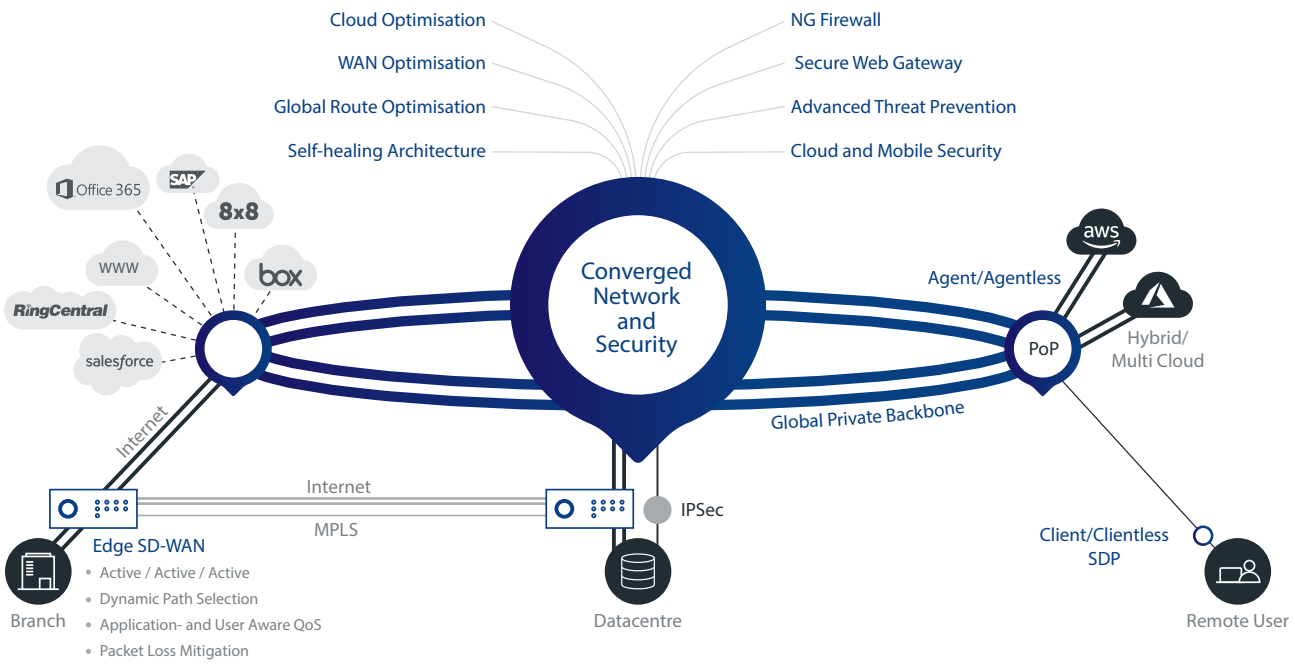
SASE CLOUD

Converged Traffic Optimisation, Access Control, Threat Prevention



About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimises and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimise global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacentres and mobile users into the network with a zero trust architecture. Using Cato, customers easily migrate from MPLS to SD-WAN, optimise connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacentres and mobile users into the network with a zero-trust architecture. With Cato, the network, and your business, are ready for whatever's next.



About Datrix

Established over 25 years ago, digital transformation is the driving force behind the evolution of Datrix services and solutions. Our professional and technical services teams adopt a consultative, client-centric approach that sees us design, build and manage superior solutions.

Our critical networking, communications and cyber security solutions are the preferred choice for the nation's key institutions, as well as public and private sector organisations seeking to address the business challenges of compliance, performance, availability and affordability.

+44 (0)20 7749 0800
enquiries@datrix.co.uk
sales@datrix.co.uk

London Head Office, Gray's Inn House
127 Clerkenwell Road, London EC1R 5DB