CATO NETWORKS

MOUNTAIN PATH SOLUTIONS

Integrate Point Solutions with Sweat and Tears or

Choose the SASE Way

Network and Security Challenges: What Changed?

Historically, IT solved emerging business needs with point solutions, and as more network and security products piled up, IT was expected to manage and maintain them all. This responsibility forged the perception that only by managing everything on their own, could IT teams fully control enterprise network and security. But as businesses evolved and networks expanded to include cloud applications and remote users, handling all this became too complicated, too expensive, too slow.

The price enterprises pay for point products, isn't just the obvious financial cost, but the complexity and burden of dealing with vendor evaluation, procurement, integration, maintenance and troubleshooting of multiple individual components. This complexity entails hidden costs and results in lack of control. Admittedly, IT teams find themselves busy agonizing over how to handle network and security, and unintentionally slowing down the business instead of moving it forward.

Weighed Down by Point Solutions

Let's look at an IT stack built of these four segments: network, security, cloud and mobile. Each segment is traditionally comprised of point products that continue piling up, as IT attempts to address evolving business needs.

Network

Whether a network is built on legacy MPLS and WAN optimizers, or whether MPLS has already been replaced with a more modern SD-WAN and private backbone, it still lacks the ability to natively support cloud and mobile, which are becoming the enterprise's new center of gravity.

Security

To ensure network security, enterprises need to either route traffic through security products like NGFW, UTM, and SWG; or backhaul traffic to a datacenter or in the cloud. However, each of these options has its limitations and shortcomings: Security products need to be installed on-premises at each site, and then managed and maintained accordingly. And, backhauling traffic creates latency that impacts performance and user experience.

Cloud

Networks have evolved with the rise of cloud services. Yet traditional security appliances weren't designed to secure cloud infrastructure and applications, so once again IT is required to deploy additional point solutions: CASB for governing cloud application access and avoiding Shadow IT, and virtual NGFWs for securing cloud datacenters.

Mobile

The need to support mobile users has only intensified post COVID-19 outbreak, and IT is compelled to install additional solutions such as Software-defined Perimeter (SDP)/Zero Trust Network Access (ZTNA), or at times even settle for a legacy bandage in the form of stacking up multiple VPN Concentrators.

Supporting the modern business with point solutions is complex and expensive, entailing inevitable management, maintenance and scaling challenges. This raises the question of the options available for IT teams that rightfully demand cost saving, optimization and agility – without having to compromise or give up control over network and security.

SASE:
The Right Way Forward

According to Gartner, Secure Access Service Edge (SASE) is the direction enterprises should take to avoid the hassle of managing a legacy network built on a never-ending pile of point products. SASE delivers the full set of networking and security capabilities through a converged, global, cloud-native, and PoP-based architecture. SASE supports all enterprise edges (physical, cloud, mobile) and is centrally managed from the cloud.

SASE eliminates the complexity, rigidity, and costs (the hidden ones as well) associated with managing numerous point products. The SASE architecture focuses on convergence, creating an agile, scalable and elastic platform that can support the business today and into the future.

> **"Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets."**
>
> "Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge, 2019"
>
> By: Joe Skorupa, Neil MacDonald | Gartner

The Wonders of the SASE Architecture

SASE delivers end-to-end visibility for all network users, applications and activity, at all locations. No more rigid and costly connectivity, fragmented and complex IT infrastructure, or restricted visibility and control. The SASE architecture is streamlined and simplified, enabling IT to regain control of the network, ensure optimal security posture, and accelerate business growth.

We all realize the clear benefits of cost saving, simplicity and scalability gained from IT moving key business services and applications (e.g., SFDC, Office 365 and AWS) to the cloud. It only makes sense that networking and security, as the underlying infrastructure for all applications, data, branches and users, should move to the cloud as well.

But, moving networking and security to the cloud wasn't possible before SASE. Well, now it is, and the value to be gained is huge:

Agility

Supported by the SASE architecture, IT can deliver optimized networking and strong security to all locations, applications and users regardless of where they are. Provisioning of new resources and capabilities is fast and simple. Just deploy the right edge client and plug into the SASE platform and corporate policies drive your network and security experience.

Collaboration

IT teams can leverage the convergence of network and security to manage all features and policies in a single interface, using a common terminology, and gaining deep visibility into network and security events. Cross team collaboration improves the overall service delivery to the business that often involves a combination of availability, performance, and security requirements.

Efficiency

With SASE, IT teams are relieved of the grunt work to maintain on-premises infrastructure. Physical topology, redundancy, scaling, sizing, and upgrading is dramatically reduced. IT can achieve better service to the business, while focusing precious resources and skills on business-specific problems rather than the grunt work of generic infrastructure maintenance.

Cost reduction

The simplification of the network and security stack, as well as the consolidation of multiple point products, enables both vendors and customers to reduce the overall costs of keeping the infrastructure running.

Business continuity

With or without the trigger of a sudden global crisis, enterprises have come to realize that enabling all employees to work remotely, from anywhere, and at any given time, has become a critical pillar of their business continuity plan (BCP). The elasticity of the SASE's cloud-native architecture makes it possible to instantly shift to a work-from-anywhere model.

Two Myths that Get in the Way of Taking the SASE Direction

IT can move networking and security functions to a SASE provider without giving away control – just like moving applications to the cloud. It can be that simple. But first, let's break these two myths:

1 Spending Time and Money on Maintenance is Unavoidable

In the past, costly and time-consuming maintenance was an integral part of any IT work routine. However, with a SASE platform, all the mundane maintenance inherent in legacy networks and security products, is eliminated. The SASE provider handles all maintenance of the underlying platform, freeing IT from the costs and complexities associated with scaling, upgrading, and otherwise handling the networking and security infrastructure.

2 Offloading Management Means Giving Up Control

With legacy networks, outsourcing management indeed meant losing control, visibility, and the agility necessary for effectively supporting the business. Hence, IT teams would unwillingly choose to manage network and security in-house, even when they lacked sufficient resources and skills. And, things only became more complicated when IT needed to support cloud and mobile. SASE enables offloading management, while control over network and security functions always remains with IT.

Choosing the Management Style that Suits you Best

SASE enables flexible management models. Services can be managed by the user, the SASE provider, or its local partners. This allows IT teams to choose the management style fit for their business, while control over network and security functions always remains with IT.

1 Self-Service Management

If you consider yourself a DIY addict, this management model is for you as IT controls all aspects of the enterprise network. SASE enables a simple management experience, where you can control your entire network from a full-featured, self-service portal. You provision new users, configure and change firewall and access policies, add routes, adjust QoS policies, and more — without the SASE provider's involvement.

Special Advice for DIY Addicts

Even the most enthusiastic DIY IT teams can see the logic and value in offloading the following:

Edge device configuration and setup should take minutes, not hours or days. The SASE provider does that with zero-touch provisioning for networking and security. And, it doesn't come at the expense of the ability to control bandwidth management, routing, and QoS.

Without adequate in-house expertise and resources, having to keep the security stack updated at all times turns into an unnecessary burden on IT. Let the SASE provider handle this, while you still control access and have the ability to monitor and audit network security.

Making sure all remote and mobile employees have secure access to enterprise resources requires building a complex remote access infrastructure. The SASE provider handles this, and at scale, allowing IT to add more users and access permissions instantly, per need.

2 Co-Management

If you like to leave your options open, co-management is for you. IT teams can make any pressing changes themselves, while the SASE provider or its local partners assume responsibility for ongoing, time-consuming tasks.

3 Full Management

If you prefer the full management model, you can rely on the SASE provider or its local partners. They'll monitor and manage your network, with 24x7x365 NOC team support and a formalized SLA and ticket-based process.

You can choose any of the management models, with the option to switch between them at any time, based on your business needs and goals.

Regaining Control with SASE

SASE allows you to focus on core activities, ensure business continuity (even at times of a global crisis), and facilitate growth. SASE eliminates the complexity associated with handling multiple point products and services. Fragmented management and limited visibility are no longer complications you need to worry about.

You can choose from flexible management models, while always staying in control of the enterprise's most critical infrastructure assets – network and security. The converged SASE architecture creates an agile, scalable and elastic platform that can support the business today, while ensuring your network is ready for whatever the future may unfold.

Appendix

What Keeps You Up at Night?

There seems to be a direct correlation between the amount of components legacy networks necessitate and the volume of challenges IT faces. There are two ways to handle this – integrate point products or SASE. We recommend the SASE way; it overcomes the challenges that keep IT awake. See how below:

Challenge	Point Solutions	SASE
Cost model	Requires enterprises to invest capital expenditure (CAPEX) in purchasing hardware and software licenses, all of which have to then be managed and maintained in-house.	As a managed service, SASE eliminates the need for any CAPEX purchases and in-house management and maintenance. All costs are transformed to operational expenditure (OPEX).
Management	Whether managing the network in-house or outsourced, IT is burdened with the responsibility of handling a complex and fragmented infrastructure. Without a single point of management, IT has no way to effectively control network and security.	SASE converges all networking and security functions into a single cloud service that's centrally managed. This eliminates the complexity associated with handling numerous point products. Furthermore, SASE customers can select the management model that best serves their needs.
Integration overhead	Stacking multiple point products requires extensive integration efforts, as well as scaling challenges implicit in physical appliances. Implementing new features entails upgrading software and risking downtime. In addition, IT needs to spend resources on addressing a full range of high availability and failover scenarios.	SASE overcomes the cost of integrating location-bound point products and enables scaling as necessary, and wherever necessary. All new features, and enhancements are made available to every resource (branch, datacenter, cloud instance, mobile/remote user) and are automatically installed by the SASE provider.
Reliability and availability	Relying on a network that's based on disparate components is getting increasingly challenging. In the case of failure in equipment components, manual intervention is required – many times this means using external expertise.	High availability is inherently designed into SASE's self-healing architecture. SASE withstands outages and the application layer is left unaffected. All edges automatically seek the nearest PoP and migrate to the next available PoP if the current PoP is unreachable. This eliminates pre-planning or manual intervention.
Compute limitations	Branch appliances are bound by their processing power, which too often reaches its limits ahead of time, forcing an unplanned investment in appliance refresh. This can be due to a sharp increase in users and/or network traffic, or because of new security capabilities such as decrypting traffic that consume additional processing.	Cloud-native services are elastic and scalable by design. As such, a SASE platform isn't subject to the compute limitations of branch appliances. This guarantees a continuous and unlimited services to all users. The worries of sizing and upgrading that belong to the old appliance world, are eliminated.
Visibility	Visibility into legacy networks is fragmented by the numerous components. Each appliance has its own set of monitoring capabilities, creating silos and blind spots within the network. The result is limited network visibility and potential security holes created by oversight or policy misalignments.	With a single, converged network and security stack, SASE provides full visibility into all users and traffic. There are no blind spots, and there's no need to deploy dedicated monitoring tools. IT can govern security through unified, enterprise-wide policy enforcement.
Troubleshooting	When network and security are built from multiple products loosely integrated, troubleshooting complexity is multiplied. Finding the root cause of a problem across multiple products and then fixing it, is time consuming and resource intensive.	SASE converges all network and security capabilities, storing all events in a common data repository. SASE's monitoring and troubleshooting tools are converged as well. As such, finding the root cause of a problem, and the steps needed to fix it, are significantly simpler and faster.

Additional Reading

Whitepaper
A Practical Guide to SASE Migration

Whitepaper
The Optimal Architecture to Secure and Connect the New Enterprise Perimeter

eBook
The Network for the Digital Business Starts with SASE

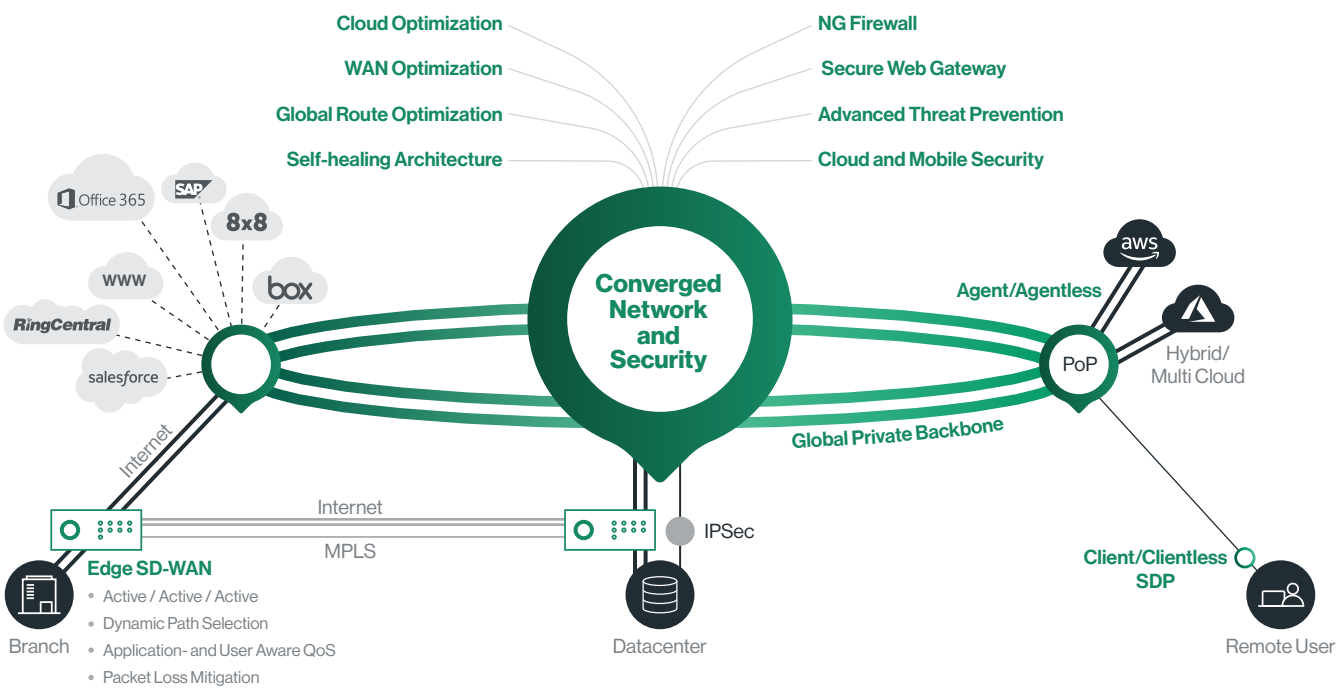
eBook
MPLS, SD-WAN, Internet and SASE

Webinar
Why SASE is the Future of SD-WAN & Security

RFP Template
SASE RFP Made Easy – Get the Template

About Cato Networks

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



For more details, please contact us

Stuart Preston
Mountain Path Solutions, LLC
Gilbert, Arizona, United States
(480) 801-7471
stuart@mountainpathsolutions.com
http://mountainpathsolutions.com/

MOUNTAIN PATH
SOLUTIONS

Cato. The Network for Whatever's Next.

Cato Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Datacenter Integration

Cloud Application Acceleration

Secure Remote Access

Cato Management Application

Managed Services

Managed Threat Detection and Response (MDR)

Intelligent Last-Mile Management

Hands-Free Management

Site Deployment

ISO 27001 Certified

SOC2 Approved

GDPR Compliant