CATO NETWORKS

SOMMITA TECHNOLOGY GROUP, LLC

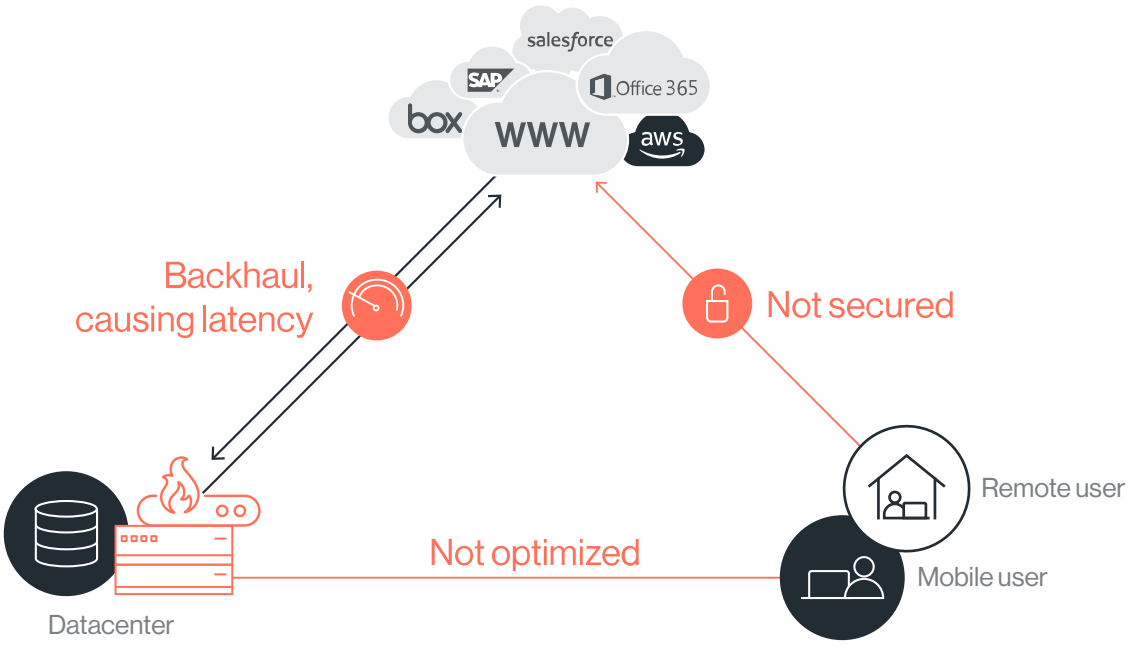
GUIDE TO
Zero Trust Network Access (ZTNA) Delivered as Part of a SASE Platform

Secure Remote Access Doesn't Have to be Complicated

Today's reality and evolving business environment are challenging IT like never before. As more enterprises look to deploy work-from-home capabilities at scale, remote access is turning into a fundamental business requirement. You need a new way to deliver secure remote access to all your employees, worldwide. And you need it now.

Say Goodbye to VPN

For over 20 years, enterprises have relied on virtual private network (VPN) to connect mobile and remote users to applications and other network resources. However, the way we do business has changed, revealing many shortcomings with legacy VPN – such as limited scalability, availability, performance and security.



Legacy VPN Limitations

Scalability

VPN wasn't designed to continuously connect entire enterprises to critical applications. And in an all-encompassing, work-from-anywhere scenario, such as a global health crisis, legacy VPN can't support the extreme load, resulting in slow response time and poor user productivity.

Performance

VPN uses the unpredictable public Internet, which isn't optimized for global access and requires backhauling traffic to a datacenter and then to the cloud. This turns VPN into a chokepoint of network traffic into the datacenter, adding latency and creating a trombone effect.

Availability

VPN requires that each of its components be manually configured for high availability, resulting in additional expense and complexity. This in itself is a non-trivial, costly and time-consuming project.

Security

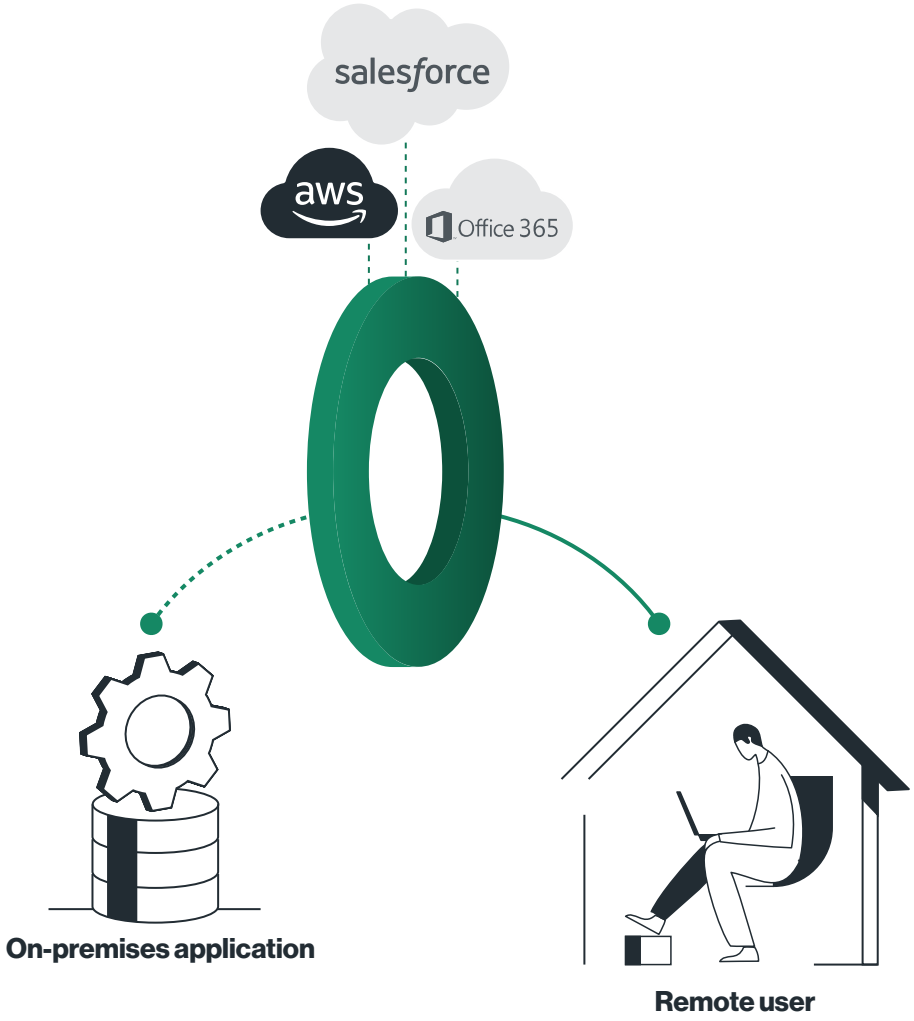
VPN provides access at network level rather than application level. This increases the attack surface and degrades the enterprise security posture, as users are just a password away from undesired access to entire networks.

Networking and security have come a long way since the introduction of VPN. A new approach is needed to address legacy VPN pitfalls, alongside equipping the digital business with a viable solution for securely delivering enterprise-wide remote access.

Say Hello to ZTNA

Zero Trust Network Access (ZTNA) also known as Software-defined perimeter (SDP), is a new approach for securing remote access to business applications, both on-premises and in the cloud. In today's work-from-home reality, ZTNA is taking on the lead role – replacing legacy VPN, which is hardly suited for supporting the shift to the cloud and increase in remote users.

Being a cloud service, ZTNA eliminates the scalability limitations of legacy VPN and enables instant scale – if demand increases – without having to install additional servers or software. ZTNA also delivers enhanced security, providing remote access to specific applications, with granular access control and monitoring capabilities.



ZTNA and VPN Challenges

ZTNA presents a better alternative than VPN, nevertheless, when deployed as a stand-alone solution, it fails to address the critical issues of threat prevention and performance optimization.

Threat Prevention

Continuous threat prevention is critical for ensuring that remote users, who are connected to your enterprise network and business applications, don't introduce threats such as malware and ransomware; or unknowingly serve as a means for hackers to penetrate your network and steal sensitive information.

Performance Optimization

In a work-from-everywhere environment with users accessing applications and data from various locations, performance optimization is essential for delivering employees an experience similar to the office. Without addressing the issue of optimization, traffic must be backhauled to the datacenter, and remote users will suffer from poor performance, badly affecting their productivity.

Whether using VPN appliances or a ZTNA cloud service, the challenges of integrating them into the corporate network remain. Despite the criticality of threat prevention and performance optimization, lagacy VPN and ZTNA alone can't solve these issues.

When ZTNA Meets SASE

ZTNA is an integral part of Gartner's Secure Access Service Edge (SASE) framework, which implements a unified, cloud-native approach, promoting shorter rollout times, unlimited scalability, ongoing threat prevention and optimized performance worldwide. ZTNA is defined by Gartner as a core component of SASE, presenting an ideal alternative for legacy VPN and delivering these key advantages:

Global, Unlimited Scalability

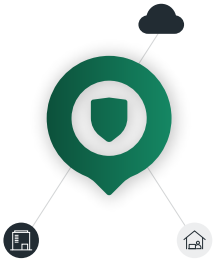
The SASE's cloud-native and globally distributed architecture supports an unlimited number of users worldwide. Users can easily move from the office to their homes, and work on the go with access being consistently secured and optimized.

Performance Optimization

Rather than using the unpredictable public Internet to connect remote users to your applications, a SASE platform, with a private backbone and built-in WAN optimization, ensures optimal performance to each user and application.

High Availability by Design

All enterprise resources establish a tunnel to the nearest SASE PoP. Each PoP is built from redundant compute nodes for local resiliency, and multiple regional PoPs dynamically support each other. Available PoPs are automatically identified to deliver ongoing service, so you don't have to worry about high availability configuration and redundancy planning.



Integrated Security Stack

All traffic passes through a full network security stack that is built into SASE. Multi-factor authentication, full access control, and threat prevention are applied as well. Because a SASE service is globally distributed, it avoids latency associated with forcing traffic to specific security chokepoints on the network.

Flexible Deployment Options

Consider having to deploy VPN for thousands of new users in multiple locations. This would require extensive resources and time you can't necessarily afford – especially not during a crisis when instant deployment is essential. Based on your specific business needs, you can gradually implement ZTNA as part of a full SASE migration, or deploy just ZTNA without delay. SASE provides secure connectivity at the network layer, eliminating the need to install additional software on your application servers. Instead, all you need to do is the following:

1

Connect your physical datacenter's network to the SASE platform using an IPsec tunnel or Edge SD-WAN device provided by the SASE vendor.

2

Define a policy enforcing remote users' authentication, as well as the applications they're allowed to access.

3

Provide client-based access for supporting all business applications, or clientless access (URL) for specific web applications.

By avoiding software installation on your application servers, risk is minimized and downtime is prevented. The availability of clientless access eliminates VPN deployment time and effort altogether, allowing you to complete the above in just hours, as opposed to days or weeks. From this point forward, you can provide granular access to specific applications for your entire remote workforce.

Built-in Business Continuity

The elasticity of the SASE cloud-native architecture makes it possible to instantly move all your employees to work from remote. Built-in high availability reduces the cost related to the scalability and redundancy needed to support your business continuity plan (BCP). This is why ZTNA, integrated into SASE, has become a vital tool for ensuring that your entire workforce is always ready to continue business as usual.

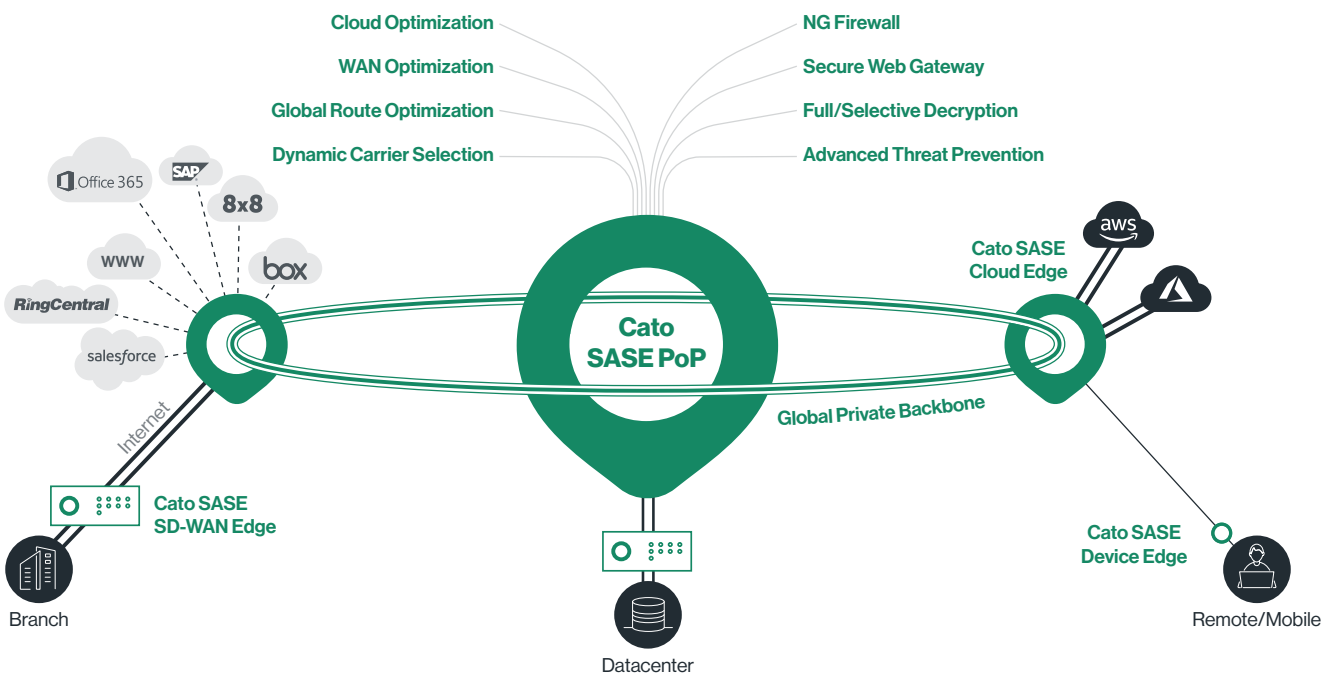
> "SASE services will converge a number of disparate network and network security services including SD-WAN, secure web gateway, CASB, SDP, DNS protection and FWaaS."
>
> *Hype Cycle for Enterprise Networking 2019* | **Gartner**

The Legacy Way vs. The Cato Way

	Legacy VPN	Cato
Scalability	VPN requires specialized hardware appliances and regional concentrators to cover a global workforce. Because of its appliance-based architecture, VPN isn't scalable and is subject to capacity constraints, especially with a sudden increase in work-from-home users.	ZTNA seamlessly scales to support optimized and secure access to an unlimited number of users, on any device, and from any location. There's no need to set up any additional infrastructure.
Access and Authentication	VPN provides secure connection to networks as a whole. Granting access to applications entails giving users unrestricted access to the network. This expands the attack surface, increasing the risk of compromise and data breach.	ZTNA enforces multi-factor authentication and granular application access policies, which restrict access to approved applications, whether on premises or in the cloud. This way, users don't get access to the network layer, reducing risk significantly.
User Experience	With VPN, traffic is backhauled to the datacenter, making access painfully slow for users, while repetitive logins and authentications only add to their frustration. This occurs even when infrastructure is sized properly, due to the unpredictability, latency, and packet loss of the public Internet.	With ZTNA you can simplify and speed up the user experience, so working at home feels just like working from the office. Users can connect to all applications and resources with a single login, whether spread across multiple clouds or in private datacenters.
Threat Prevention	VPN doesn't provide continuous deep packet inspection (DPI) to protect against threats, post authentication. This results in compromised endpoints and the propagation of threats inside the enterprise network.	ZTNA provides continuous protection against threats, applying DPI for threat prevention to all traffic, regardless of its source or destination. Threat protection is seamlessly extended to Internet and application access, both on premises and in the cloud.
Performance	VPN doesn't enable performance optimization and requires remote users to access resources across the public Internet. The increased latency and packet loss of public Internet routing, undermines the user experience.	With ZTNA, remote users access resources via a global private backbone, and not the unpredictable public Internet. This delivers a consistent and optimized experience, where mobile and remote users are first-class citizens on the enterprise network.

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 SASE Cloud, customers easily migrate from MPLS to SD-WAN, improve connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud data centers and remote users into the network with a zero-trust architecture. With Cato, your network and business are ready for whatever's next.



Cato SASE. Ready for Whatever's Next

Cato SASE Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Secure Remote Access
- Unified Management Application

Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management
- Site Deployment

SOC2 Approved

ISO 27001 Certified

GDPR Compliant

Gartner peerinsights™ Customer first

CATO NETWORKS

Contact Sommita