GeoNet TELECOM

SASE: The Highly Secure SD-WAN Solution

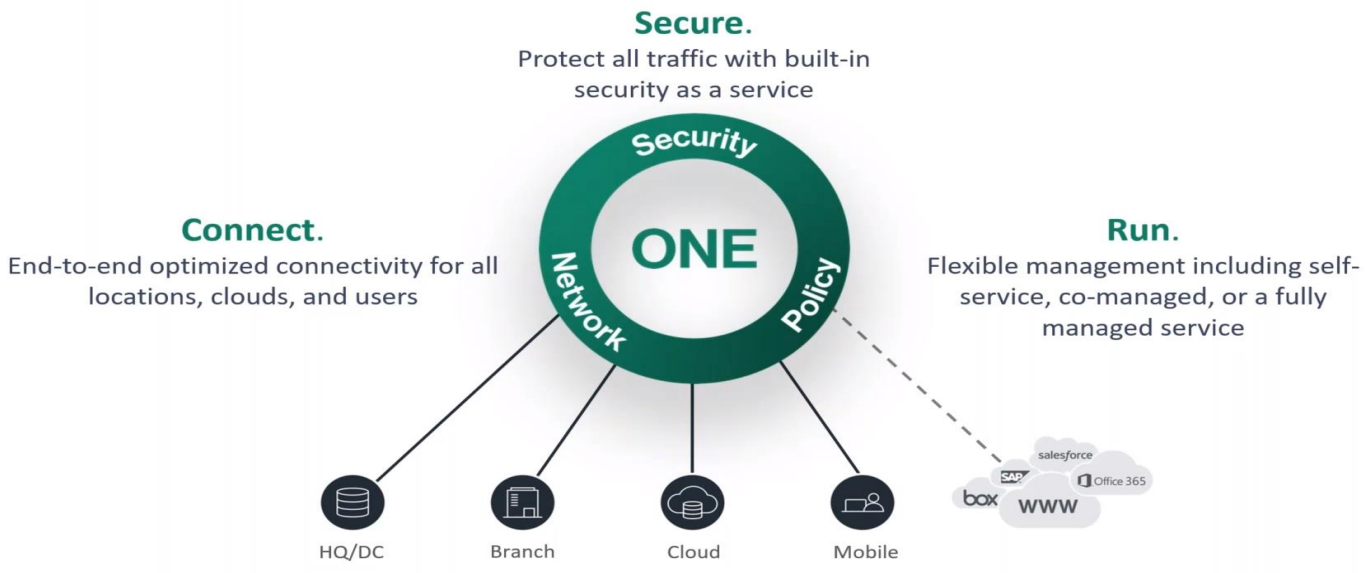
Solution Brief

The SASE Solution

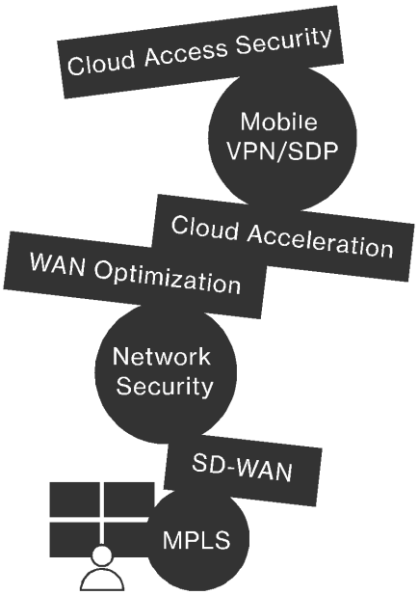
SASE: A New Networking and Security Architecture for Business

SASE stands for ‘Secure Access Service Edge’ and is a new enterprise networking technology category defined by Gartner, the world’s leading research and advisory company. It encompasses the centralized network management functions of SD-WAN along with extended cloud security, so not only can the security within your SD-WAN network be controlled but also, the security of your cloud services and all from one platform.

SASE details an architectural transformation of enterprise networking and security that will enable IT to provide a holistic, agile and adaptable service to the digital business.



The Network and Security Challenges of Digital Transformation



With businesses going digital, there is a lot of dependence on optimized access to applications and data, with on-premise and cloud solutions, and an increasingly mobile global workforce.

The old networks of the past built with expensive and rigid MPLS, are no longer sufficient to support digital transformation nor are they futureproof.

In fact, several point solutions are needed to cover your changing network, security, cloud, mobility, and global needs. It is difficult and resource-intensive to build such a complex network without assistance and can also be extremely costly using different service providers to do this. There has got to be a better way.

Digital business means a cloud-first, fast and agile business, something that is incompatible with legacy telcos and network services.

Legacy MPLS networks are limited because:

- MPLS is relatively expensive, rigid and not built for cloud access
- Direct and secure internet access is needed everywhere with MPLS networks as they possess limited capabilities
- MPLS is limited to physical locations, making cloud and mobile resources “second-class citizens”
- MPLS networks require discrete stand-alone appliances and solutions, complicating network management and lifecycle maintenance

Legacy telcos are not adequate partners because they are:

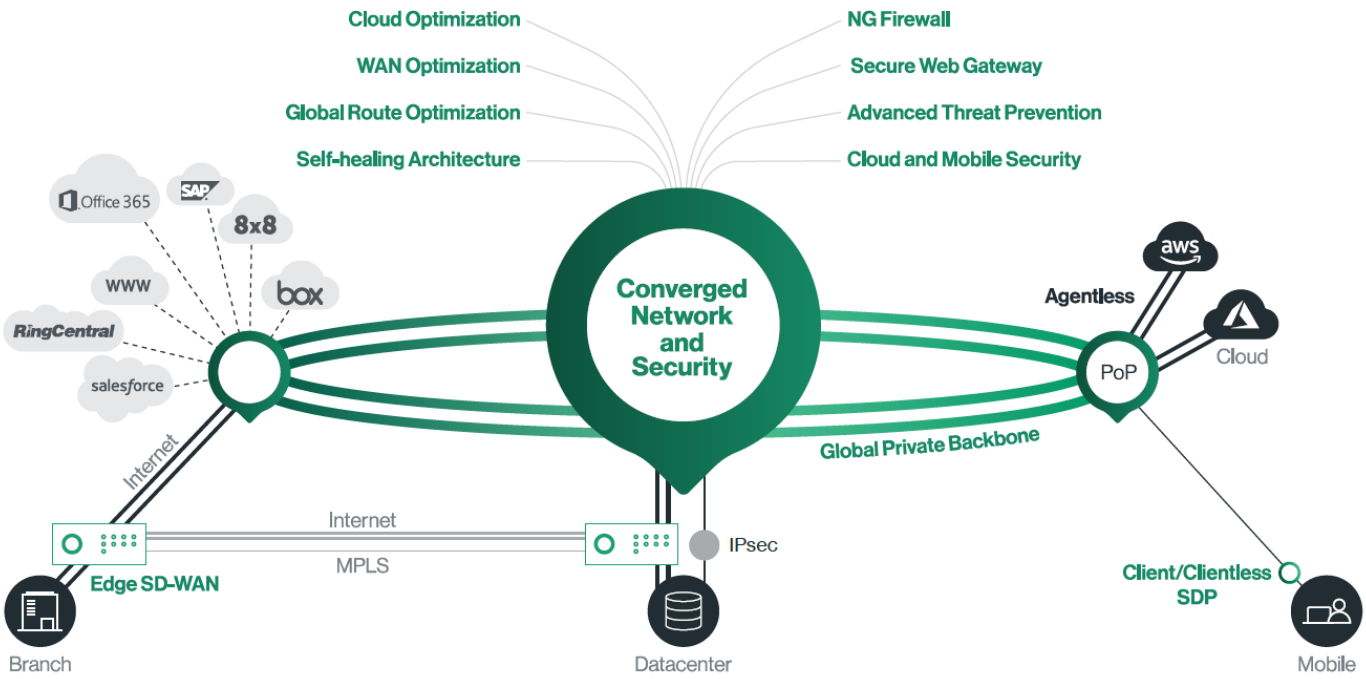
- Expensive relative to homegrown solutions
- Bureaucratic and slow to deploy new sites
- Slow in threat detection - relying on ticket-based services
- Unrefined with limited customer visibility and control

The Cloud-native Carrier

The ONLY managed SD-WAN service natively built with the global reach, self-service and agility of the cloud.

Our SASE cloud solution enables enterprises to move away from, a network built with rigid and expensive MPLS connectivity and which have a bundle of point solutions, to a simple, agile and affordable network.

It connects all enterprise network resources, such as branch locations, the mobile workforce, and physical and cloud data centers, into a global, secure and managed SD-WAN service. With all WAN and internet traffic consolidated in the cloud, our integrated security services protect the entire network at all times.



Global Private Backbone

This private global backbone is comprised of 50+ PoPs worldwide which are interconnected by multiple SLA-backed Tier-1 providers. All these PoPs run a cloud-native software stack. It is fully multi-tenanted, scalable and ubiquitous, performing all network functions - such as global route optimization, dynamic path selection, traffic optimization and end-to-end encryption - as well as implementing the inspection and enforcement functions needed by our security services.

WAN Optimization

WAN optimization is an integral part of the network software stack, utilizing TCP proxies and advanced congestion management algorithms to maximize throughput in key operations, such as file transfers.

Global Route Optimization

The proprietary routing algorithms factor in latency, packet loss and jitter. Unlike internet routing, our routing always favors performance over cost in selecting the optimal route for every network packet.

Encryption

Our end-to-end encryption uses the strongest industry-standard cipher suites and assures data confidentiality, privacy and secure multi-tenancy.

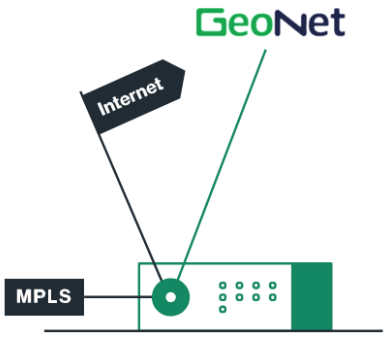
Self-healing Architecture

The cloud backbone is continuously monitored and measured. Self-healing capabilities guarantee 99.999% service availability. Elastic, scale-up cloud software design principles assure seamless service infrastructure growth without service downtime or disruptions.

Locations connect to the global, private backbone by establishing encrypted tunnels from a “socket”, being a zero-touch, SD-WAN Edge appliance, or any device that supports IPsec tunnels. Cloud data centers connect through an agentless configuration; mobile users can connect by running a SASE client or clientless.

SD-WAN Edge

Our SD-WAN Edge works with multiple internet circuits providing, reliable, high-performance access to our global private backbone. Traffic can also be routed over MPLS directly between sites (not through our PoPs), and across IPsec tunnels to third-party devices.



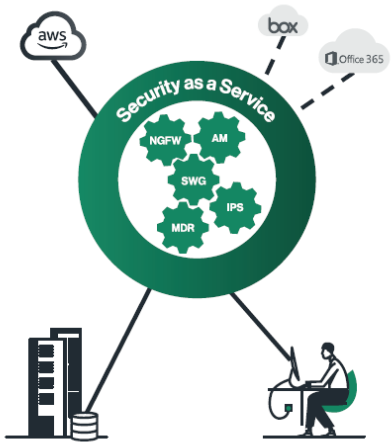
The socket (SD-WAN Edge device) is a zero-touch device ready to work in minutes once it has power and internet connectivity. Our sockets come in two models: X1500 for branch offices and X1700 for data centers. Both are continuously monitored and updated by our network operations center (NOC).

Our sockets include:

- **Link Aggregation** that balances inbound and outbound traffic across MPLS and multiple internet circuits (fiber, DSL, cable, 4G/LTE or 5G) to maximize bandwidth (active/active) and availability.
- **Dynamic Path Selection** that routes traffic across the optimum transport based on application, user and real-time link quality (jitter, latency and packet loss).
- **Application Identification** that uses our advanced Deep Packet Inspection (DPI) engine to automatically identify thousands of applications and millions of domains on the first packet.
- **Bandwidth Management Rules** ensure that more critical applications always receive the necessary upstream and downstream capacity, serving other applications on a best-effort basis.
- **Packet Loss Mitigation** techniques dynamically switch traffic to alternate, better performing link(s) and proactively duplicate packets on a per application basis. Our architecture eliminates middle-mile packet loss.
- **Routing Protocol Integration** that leverages BGP to make informed real-time routing decisions, easily integrating a company's existing routing infrastructure with our SD-WAN Edge.
- **High Availability (HA)** that carries no additional recurring charge and deployment is simple and completed in minutes. Sockets automatically connect to our best available PoP. Should the connection degrade or fail, the socket automatically reconnects to the best available PoP.

Security as a Service

Our security engines are built into the private global backbone and delivered as a service. No additional appliances need to be purchased or deployed. Security engines include an application-aware, next-generation firewall (NGFW); secure web gateway (SWG) with URL filtering; standard and next-generation anti-malware; and IPS managed by our SOC (Security Operation Center). These security engines form the basis of a comprehensive Managed Detection and Response (MDR) service that is provided as part of GeoNet's managed services offering. All engines seamlessly scale to process all customer traffic, encrypted and unencrypted, without the need for sizing, patching or upgrading appliances and point solutions. We protect user privacy and fully comply with GDPR. Inspected data is never stored on our hosted servers or shared with third-parties. Customers are able to exclude privacy-sensitive applications, such as banking and healthcare from inspection.



Next-generation Firewall

Our NGFW operates across every PoP protecting the entire organization with a unified application-aware and user-aware security policy - all without the cost and complexity of upgrading and maintaining individual firewall appliances.

Our NGFW uniquely provides:

- **Complete visibility -** inspecting all WAN and internet traffic for fixed and mobile users. There are no blind spots, no need to deploy multiple security appliances or tools.
- **Unlimited scalability -** applying security policies and inspecting any traffic mix (encrypted and unencrypted) at line rate. We ensure processing power and network capacity always meet committed service levels.
- **Unified security policy -** enforcing one granular policy and rule base that extends from one user to the entire business. The rule base is common to all security functions and traffic types. There is no need to associate policy with distinct appliances or point products.
- **Simple lifecycle management -** eliminating the need to size, upgrade, patch or refresh firewalls, customers are relieved of the ongoing "grunt" work of keeping their network security current against emerging threats and evolving business needs or paying additional costs for this to be done.

Secure Web Gateway

Secure Web Gateways (SWGs) protect against phishing, malware and other internet-borne threats. We converge SWG with NGFW, eliminating the need to maintain policies across multiple point solutions and the appliance lifecycle. Our integrated SWG provides dynamic site categorization, which includes an always current URL database enriched with information about phishing threats, malware delivery, botnets and other malicious content. Customers can set and enforce one set of web access policies for mobile and fixed users based on visibility into user activity thus reducing organizational risk.

Advanced Threat Prevention

Advanced Threat Prevention is a collection of network security and related defenses deployed to address current and emerging threats. IT organizations face the daunting task of maintaining complex infrastructures to identify and prevent advanced threats from penetrating networks. Our Advanced Threat Prevention solves this problem by inspecting encrypted and unencrypted traffic at line rate for malware and network-based threats.

TLS Inspection

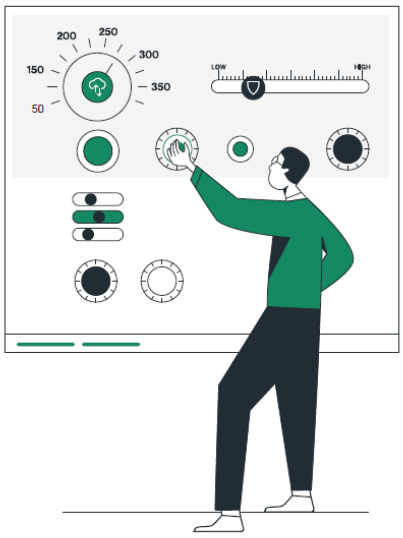
With most internet traffic encrypted, detecting and preventing threats delivered within SSL/TLS traffic is critical. However, inline SSL/TLS traffic inspection consumes significant processing resources. Appliance-based security solutions face resource limitations as their hardware is often inadequate, forcing hardware upgrades outside of the budgetary cycle. As noted, GeoNet security services benefit from infinite computing power of the cloud. We inspect all TLS-encrypted traffic flows without impact on user experience or application performance.

Malware Protection

Our network-based malware protection leverages multiple, multi-layered and tightly integrated anti-malware engines running in all our PoPs. The first layer includes a signature and heuristics-based inspection engine, which is kept up-to-date at all times based on global threat intelligence databases, scans files in transit across the backbone to protect against known malware. The second layer applies proven machine-learning algorithms from SentinalOne (endpoint protection platform) to identify and block unknown malware, such as zero-day attacks or polymorphic variants of known threats that are designed to evade signature-based inspection engines. With both layers, connected endpoints are deeply protected against network-delivered malware.

Intrusion Prevention

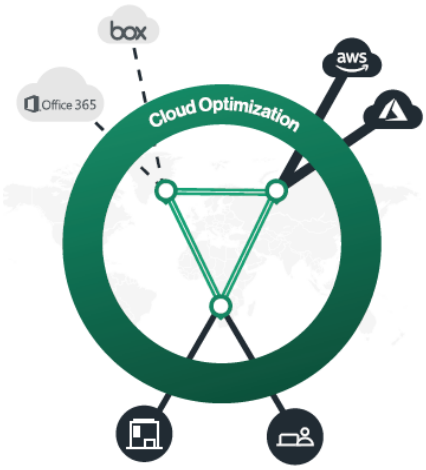
Our IPS leverages multiple layers and technologies to block network attacks. Network protocol validation detects protocol manipulations and malformed packets. Context-aware signatures and rules block attacks based on known CVEs, unknown attacks based on network traffic behavior and network scans. Internal and external reputation feeds enrich IPS intelligence. Geographic-based restrictions minimize the threat landscape.



Legacy IPS technology requires extensive skills and management effort. IT teams need to evaluate new signatures, determine which ones to activate, validate they will not disrupt the business, and consider the performance impact on the IPS appliance and the network. Those concerns simply do not exist with our IPS. Like all our security services, our Security Research Lab and SOC manage the IPS for you and ensure appropriate rules are applied against emerging threats with the proper validation and capacity analysis. Activation is simple. GeoNet customers only need to enable the IPS from their management console to benefit from its prevention power.

Cloud and Mobile Access and Optimization

Cloud Data Center Integration



We tightly couple cloud data centers into the SD-WAN effortlessly. All cloud providers - Amazon AWS, Microsoft Azure, Google Cloud and others - connect into our global backbone by establishing redundant IPsec tunnels, which typically only have to cross the physical data center shared with our PoP.

In this way, GeoNet delivers the optimum cloud experience. Cloud data center traffic routes over the optimum path across our global private backbone to our PoP. From there, traffic is typically sent across the data center network to the cloud data center. This architecture eliminates the need for premium cloud connectivity services, such as AWS DirectConnect or Microsoft Azure Express Route.

The integration is **agentless, not requiring any virtual appliances.** Leveraging the IPsec gateway connectivity available from all cloud providers, avoids additional VM costs as well as the risk of modifying production server network configurations. Like all other traffic, cloud data center traffic is subject to full security inspection by our security services.

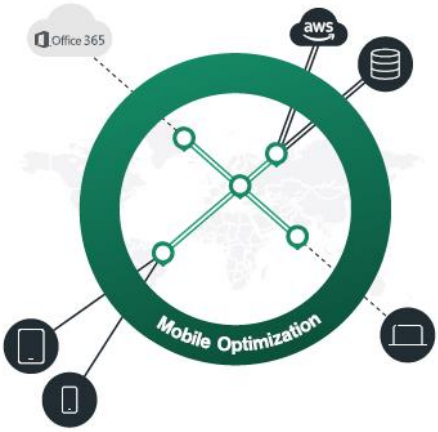
Cloud Application Acceleration

We also improve public cloud application performance, such as Office 365, Cloud ERP, UCaaS and Cloud Storage. Latency is reduced by optimally routing cloud application traffic across our global private backbone to our PoP closest to the cloud application provider's data center.

Our built-in WAN optimization maximizes end-to-end throughput to improve application performance, especially around bandwidth-intensive operations, such as file transfers.

All traffic and files exchanged with the cloud application are subject to full security inspection within our hosted cloud.

Mobile Access Optimization



We extend the full range of the network and security capabilities down to the mobile user.

Using a client or clientless browser access, users connect to our nearest PoP and their traffic is routed optimally over our global private backbone to applications on-premise or in the cloud.

Our **zero-trust SDP** (Software Defined Perimeter) mobile access model allows the most granular user access control down to specific applications. By contrast, legacy VPN solutions limit access to entire subnets.

All user activity is protected by GeoNet's built-in network security stack, ensuring enterprise-grade protection to all users everywhere.

CC2 Management Application

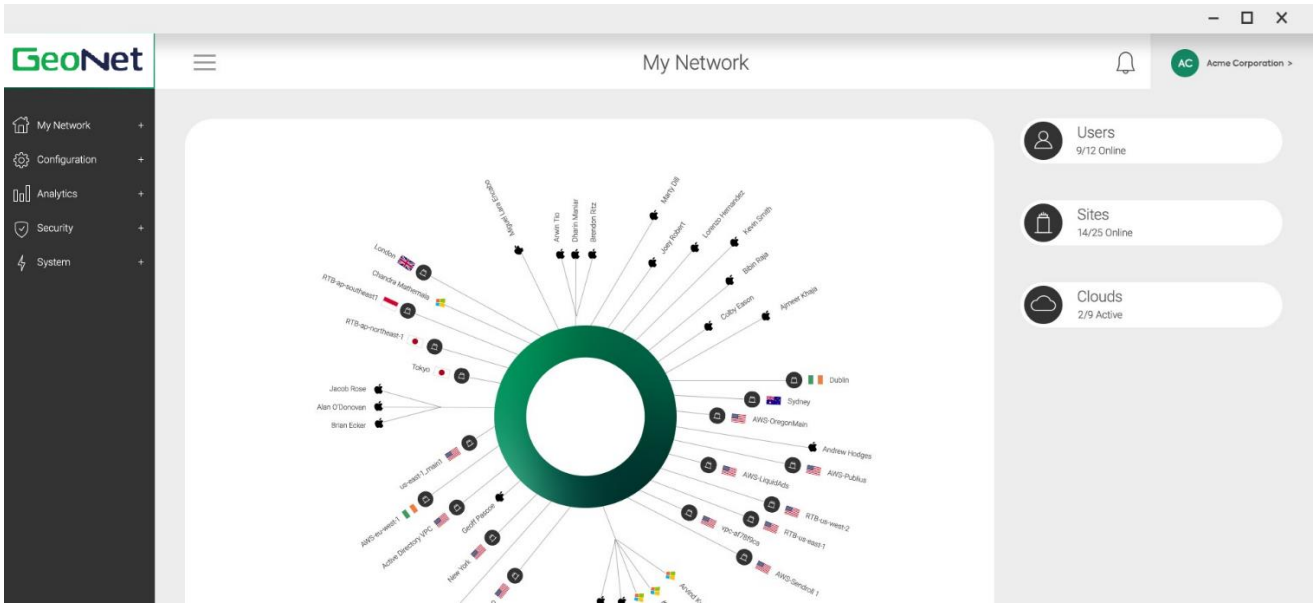
We provide a single-pane-of-glass into the complete enterprise network (sites, cloud resources and mobile users) for networking and security, through our cloud-based management application. Through the application, customers and providers can control all parts of the service, including network and security policy configuration, detailed network analytics and security event reporting.

The CC2 management console combines power and simplicity - administrators define granular network and security policies without a long learning curve or repetitive manual operations, now simplified by an intent-driven user interface.

Real-time and historical, analytics and reports - provide comprehensive network visibility, solving key challenges of access control, user experience, troubleshooting and shadow IT.

Collection and delivery of full network and security event logs - external analysis solutions like Security Information and Event Management (SIEM) are available, with the unique benefit of using a single interface for all events rather than manually aggregating data from multiple appliances and sources.

The management application is web-based and accessible over the internet with multi-factor authentication. All access and configuration changes are recorded in a centralized audit log.



Our management console provides a single-pane-of-glass, showing all connected sites, cloud resources and users.

Managed Services

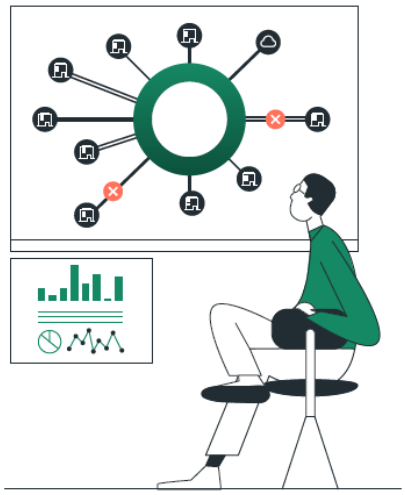
GeoNet offers a suite of managed services depending on the management model that best meets customer requirements. In all cases, we maintain the underlying platform, freeing customers from the associated costs and complexities of scaling, upgrading and managing the networking and security infrastructure.

With self-service management, customers control all aspects of their own networks. With co-management, customers can delegate configuration and troubleshooting tasks to the GeoNet NOC or a regional partner. Fully managed, transfers the responsibility for monitoring and managing the customer's network to the GeoNet NOC or a regional partner.

Multiple management models are a unique advantage of GeoNet over legacy telcos and managed network services providers which require customers to open tickets for any network change. In addition, to site deployment assistance, GeoNet and its partners offer the following managed services:

Intelligent Last-mile Management

GeoNet provides customers with a premium service to continuously monitor last-mile ISPs. In case of an outage (blackout) or performance degradation (brownout), GeoNet works with the ISP to resolve the issue by providing pertinent and detailed network information around the incident. This service helps customers that migrated from a fully managed MPLS network to quickly resolve network issues across their multiple, global ISPs without expending precious internal IT resources.



Managed Threat Detection and Response

As mentioned, GeoNet provides customers with a premium service to continuously monitor their networks for compromised endpoints.

Prevention is no longer sufficient to protect the corporate network. Detection is critical for complete defense against advanced attacks. However, such managed threat detection and response (MDR) services often come at high cost with significant deployment complexity.

Our MDR leverages the deep network visibility of the network to provide a zero-footprint detection of resident threats using a combination of machine learning algorithms that mine network traffic and a human verification of detected anomalies. Our experts then guide customers on remediating compromised endpoints.

Hands-free Management

Customers can choose GeoNet or one of its partners for complete hands-free management of their network. Change requests are submitted and tracked through a ticketing portal and addressed according to GeoNet's service SLA. Expert staff will perform all changes to networking and security policies as needed, to accommodate business and technical requirements.

Use Cases

MPLS Migration to SD-WAN

GeoNet enables customers to move away from expensive, rigid and capacity-constrained MPLS networks to multiple high-capacity internet links and GeoNet's last and middle-mile optimizations. Using GeoNet's SD-WAN Edge, customers boost usable capacity and improve resiliency at a lower cost per megabit. Customers with a global footprint, leverage an affordable global private backbone to replace global MPLS and the unpredictable internet, optimizing performance and maximizing throughput to resources on-premise and in the cloud.

Optimized Global Connectivity

GeoNet uses a global private backbone with built-in WAN and cloud optimization to deliver an SLA-backed, predictable and high-performance network experience everywhere. Customers who suffer from high latency and network inconsistency across their global locations use GeoNet to deliver a great user experience when accessing on-premise and cloud applications.

Secure Branch Internet Access

GeoNet provides a full network security stack built into our hosted cloud. By connecting all locations to our global private backbone through GeoNet SD-WAN Edge, all traffic, both internet and WAN, is fully protected by GeoNet's Security as a Service. There is no need to add the cost and complexity of point-security solutions, appliances or cloud services.

Cloud Acceleration and Control

GeoNet accelerates cloud access by routing all cloud traffic to our PoP closest to the cloud destination. As our PoPs share the data center footprint of major cloud providers, the latency between GeoNet and these providers is essentially zero. Cloud access optimization requires just a single application-level rule that determines where cloud application traffic should egress from our hosted Cloud. Gone are the pains and costs of deploying cloud appliances or establishing regional communication hubs all to extend the SD-WAN to the cloud.

Mobile Security and Optimization

Our global networking and security capabilities reach down to a single mobile user's laptop, smartphone, or tablet. No more treating mobile users like “second-class citizens” of your network and security infrastructure. Using our client or clientless browser access, users dynamically connect to the closest PoP, and their traffic is optimally routed over the global private backbone to on-premise or cloud applications. GeoNet's security as a service protects mobile users against threats everywhere and enforces application access control.

Complete WAN Transformation

Replacing MPLS and legacy WANs is not just an opportunity to connect your offices quickly and affordably. It is an opportunity to transform your entire organization, connecting every user to any resource from anywhere in the world. By transforming, not just upgrading their networks, companies have reduced WAN-related costs while still **doubling throughput and adding more locations,** with **decreased deployment times from months** to as a **little as 30 minutes,** and identified threats in their organizations missed by existing security appliances.

Yes, it is a radical vision but one that is reality. Hundreds of customers are already experiencing the power of this hosted cloud. **Validate it for yourself by speaking with us today.**

Enquiries

Please do not hesitate to contact us regarding this service with any questions or to register your interest.

Sales & Information:

Telephone: +44 20 3828 1190

Email: sales@geonettelecom.com

Address: 73 Park Lane, Croydon, CR0 1JG, United Kingdom

Website: www.geonettelecom.com