SOLUTION BRIEF

VERSA NETWORKS

Versa Secure Web Gateway

Introduction

With critical data and corporate applications moving to the cloud, organizations looking to provide easier access for the unprecedented increase of “Work-from-Anywhere” users are faced with a growing attack surface area. To combat modern threats, enterprises are steadily implementing Secure Access Service Edge (SASE) to modernize and secure their ever-changing and distributed network of users and devices. Traditionally offered on-premises, Secure Web Gateway, one of the major services of SASE, are now also delivered via the cloud, becoming an essential service to securing all web traffic.

Securing the Modern Era of Connectivity and Communication

In today’s modern world, guests, employees, customers, and partners all require web access to stay connected, accomplish tasks, and collaborate. To enable the demand for better communication and connectivity, organizations are increasingly transitioning to multi-cloud and adopting 3rd party SaaS applications such as Office365, Salesforce, Box, Google, etc. According to Forrester, organizations are expected to be running up to 75% of their workload on cloud platforms by 2022.

Security is a top priority for organizations of all sizes and verticals because IT teams need to respond to a ever-changing landscape of new threats and attacks. Ensuring all users, devices, applications, and systems remain uncompromised, keeping intellectual property unexposed, and meeting compliance with regulatory standards are challenges enterprises need to tackle as the way data moves in and out of their network. To add to the ever expanding list of challenges, IT teams also need to provide uninterrupted and optimal user-experience to web applications to maintain business continuity and productivity.

The need for seamless user experience and hardened security accelerate the need for a new design for networking and security. As users connect directly to the web from any device and from any location, Secure Web Gateway (SWG), an essential component of SASE, is crucial to protecting users, the enterprise network, and any data that is being passed to and from the network.

The internet is a public place where anyone on any device can connect. Because it was designed to be open, the internet also exposes users to threat actors who look to compromise sensitive data for financial or political gain. These threat actors can range from script kiddies who buy their exploits all the way to advanced hackers who deploy zero-day attacks. Your organization needs to respond and stay on top of an ever-growing landscape of different threats and vulnerabilities.

Secure Web Gateway helps protect users from accessing malicious or suspicious websites. Protecting users from potential web threats means avoiding compromising an organization’s internal network where sensitive data is stored. Additionally, SWG also ensures all user web access is in compliance with an enterprise’s corporate policies. SWG plays a major role in the SASE architecture because it prevents sensitive data from being compromised while remaining compliant with the regulations that affect the organization’s bottom line.

Legacy SWG Solutions Aren’t Dynamic Enough

Some organizations still rely on their traditional network and security infrastructure to secure all internet traffic. Typically, there are expensive MPLS links that backhaul traffic to the datacenter or headquarters which slows traffic flow and interrupts the end user-experience and results in a less productive workforce and frustrated employees. Traditional network and security solutions often share the common trait of being anchored to physical sites and security policy is not dynamically applied to access the risk of the access attempt. This is the same for legacy SWGs. Legacy SWGs were simply not built for today’s modern, digital world of cloud and mobility.

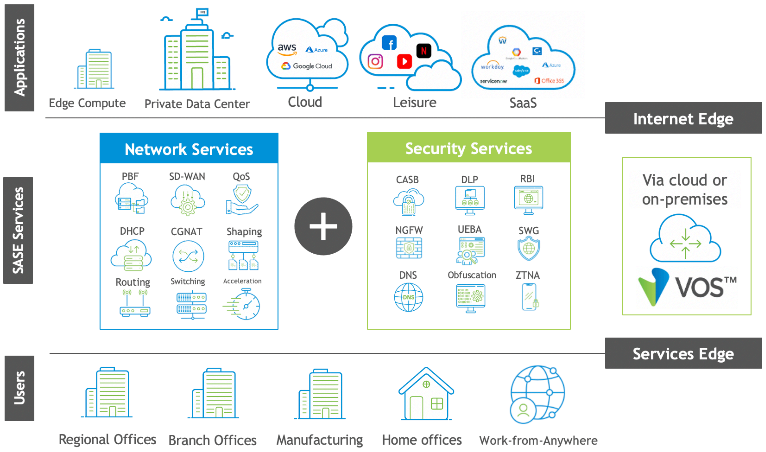
Originally, SWGs were made so that web traffic initiated on-premises through a hardware appliance that decrypted and inspected traffic for malicious activity. They required the use of VPNs to filter remote user traffic through the SWG appliance. Legacy, appliance-based SWGs do not scale, add friction to the user experience, and cost an extraordinary amount of time to deploy, configure, and manage. The complexity in traditional solutions resulted in poor configuration and human error that may increase the exposure to malicious actors. Furthermore, IT teams need to have a consistent level of visibility and control across the entire network, branch locations, and mobile users to remediate risk. This centralized visibility and real-time reporting was hard to achieve with point SWG appliances.

The Next Generation of Secure Web Gateway

In *The Future of Network Security is in the Cloud* 2019 report, Gartner defines SASE as the convergence of the WAN and security services (FWaaS, CASB, ZTNA, and SWG) into **a single, cloud-delivered service**. Following this framework, a modern Secure Web Gateway solution is offered directly from client to cloud, allowing for seamless and secure web access from any device to any application without the need for legacy appliances. SWG should be offered as a service delivered via the cloud, enabling ubiquitous and flexible security enforcement for all users and devices no matter their location. With this elastic approach, IT teams can provide their employees secure access to the internet with full visibility and control into real-time web traffic and activity.

Versa Networks: The Leader in SASE

Versa Networks has been delivering SASE capabilities several years before SASE became an industry term. Versa delivers a unique approach to networking and security challenges with a Single-Pass Parallel Processing architecture combining industry-leading SD-WAN, integrated full-stack security, advanced routing, and sophisticated analytics into a single software image. Moreover, Versa unites these benefits into a single, intuitive management interface, minimizing business friction, simplifying IT operations, and reducing appliance and management sprawl.



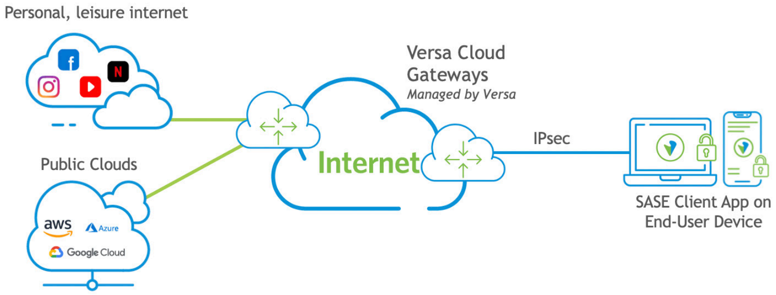
Versa's reimagination of network architecture enables services to not be chained together but rather built in a single pass software image with the highest levels of performance and security. Versa Secure Web Gateway leverages this distinctive approach at the forefront of its architectural design to allow for optimal performance and security. Versa SWG is unique in that it only decrypts a data packet once for both networking and security requirements, reducing the overall risk exposure.

Versa Secure Web Gateway

Versa Secure Web Gateway, a major service of Versa SASE, helps secure enterprise sites, home offices, and mobile users accessing distributed web applications without compromising security, network performance, and user experience. Versa Secure Web Gateway is flexible and scalable, allowing organizations to deploy on-premises, in the cloud, or a combination of both.

Versa Secure Web Gateways allow IT teams to:

1. **Secure** their users, devices, services, and sensitive data
2. **Prioritize** incidents to accelerate response time
3. **Easily scale** context-aware security without slowing performance



Versa Secure Web Gateway is the ideal solution for organizations looking to:

- **Ensure compliance** with industry and government regulations
- **Protect** against web-based threats and malware
- **Control** and authorize user access
- **Stay up-to-date** with security incidents
- **Identify** potential vulnerabilities and suspicious activities
- Take **real-time remediation** steps

Versa Secure Web Gateway helps organizations achieve these needs with a full set of enterprise-grade capabilities:

Optimizing and controlling web traffic

An organization can provide connectivity and access to a variety of users – employees, contactors, and guests. Users aren't always productive or responsible and can sometimes waste precious bandwidth using websites or web applications that are unrelated to their responsibilities during business hours. With URL filtering and traffic management, IT can simply manage web traffic by applying pre-set policies to automatically filter URLs, allowing or denying users access based on user groups, devices, types, location, and more. As a result, access can be contextually controlled, freeing up bandwidth for other prioritized uses.

Defending against evolving web threats

Malicious websites are everywhere. Defending against an evolving threat landscape is of utmost importance, given the high number of security breaches and ransomware recorded every year. Fortunately, with Versa Secure Web Gateway, organizations can prevent access to malicious websites, protecting their users from online cyberattacks. Versa SWG provides full-strength threat protection with detailed insights into applications, users, threats, and events allowing IT teams to consistent awareness to potential harm.

Preventing leakage on the web

Unfortunately, in addition to malicious harm on the web, the web also provides an opportunity for unauthorized transmission of private, sensitive data to an external recipient. A common example of this is users uploading sensitive files and sharing them across websites such as an email account. By implementing Versa SWG, private data such as credit card numbers and personal information like ID numbers, can be detected and prevented from being uploaded in real-time.

Protecting mobile workers

Work-from-Anywhere has exponentially grown in the last year. As the workforce expands and continues to be dispersed, protecting web access should be the forefront of any security strategy. Versa SWG offer protection to web applications hosted anywhere and everywhere, regardless of what device and location the user is accessing from. Without interrupting user experience, Versa SWG enables roaming users to authenticate seamlessly while security policies get dynamically applied to their devices, providing an office-like experience.

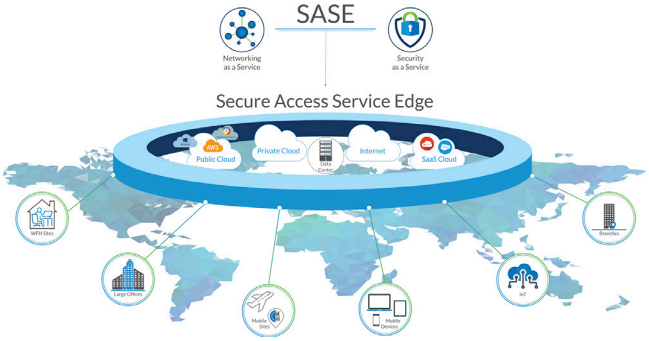
Inspecting traffic in real-time

Versa Secure Web Gateway continuously inspects web traffic in real-time, allowing IT teams to proactively enforce security policies suited to their compliance requirements. Versa SWG analyzes content against corporate policies and ensures any inappropriate content is blocked. Versa SWG also leverages shared threat intelligence across cloud applications and services in order to establish appropriate remediation given the context of the access attempt.

The Modern Secure Network

Versa Secure Web Gateway is an indispensable solution for today's web threats and is an integral part of Versa SASE. Versa Secure Web Gateway is ideal for organizations planning their SASE journey, providing flexibility, scalability, ease of use, industry certified security features, and redundancy, all in a single, unified solution.

Versa SASE is combines networking and security services such as, Software Defined-Wide Area Networking (SD-WAN), Zero Trust Network Access (ZTNA), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and more. Together, these cloud services provide enterprises of the modern world a secure architecture with context-aware, intent-based technologies, enforcing security no matter where devices, users, and applications are located.



About Versa

Versa Networks, the leader in SASE, combines extensive security, advanced networking, full-featured SD-WAN, genuine multitenancy, and sophisticated analytics to meet SASE requirements for small to extremely large enterprises and Service Providers. Versa Secure SD-WAN is available on-premises, hosted through Versa-powered Service Providers, cloud-delivered, and via the simplified Versa Titan cloud service designed for Lean IT. The company has transacted hundreds of thousands of software licenses globally through its global Service Providers, partners, and enterprises. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, Liberty Global Ventures, Princeville Global Fund and RPS Ventures.