Versa Secure Internet Access

Introduction

SASE (Secure Access Service Edge) has transformed traditional WAN, Internet, and cloud user experience for large-scale enterprises as well as small-to-medium size businesses. Versa Networks has been leading this transformation by providing integrated SD-WAN, security, routing features in a single platform, with centralized management and monitoring, analytics and reporting, and automation on the WAN Edge.

Today, organizations are faced with the following reality:

- Digital transformation accelerated the migration of enterprise applications and workloads from an enterprise datacenter to a variety of public clouds and/or SaaS services.
- Many networking functions, including security functions, running on-premises are now expected to run on the private or public cloud or on all of these locations, all while being consumed as a service.
- Users are connecting from everywhere. COVID-19 has changed the workplace dynamics to a new normal where employees can work from anywhere. Hybrid workstyle is the norm.
- High-performing and omni-present cloud connectivity have gained importance as applications move to the cloud for flexibility and scalability.
- As-a-service is the new norm for IT organizations for elasticity, flexibility and for continuously updated services.

Challenges

Legacy firewall solutions may be too rigid, aging out, and reactive. Security solutions based on legacy firewalls, are often times anchored to physical sites and users need the same level of security regardless of where they connect from: a branch office, HQ, a home office or on the road.

Maintaining legacy networking equipment and disparate point solutions for networking and security on-premises or on the cloud create complexity and security gaps. There is no single pane-of-glass or single policy enforcement capacity that is applicable to networking, security functions whether on-premises, on-cloud or on both.

Versa Secure Internet Access (VSIA)

Versa's cloud-managed, cloud-delivered Secure Internet Access (VSIA) solution helps secure enterprise sites, home offices, and traveling users accessing distributed applications without compromising security and user experience. With Versa Secure Gateway, customers can achieve a full suite of security features:

- Enterprise-grade device and user authentication with Multi-Factor Authentication (MFA). User, Group, and Device level access control and policies.
- Identification of thousands of applications with features like DPI, URL, protocol and port numbers, destination IP addresses and more, combined with comprehensive policy-based control.
- Stateful firewall, DOS protection, CGNAT with ALG support.
- Web filtering to prevent traffic from going to undesired, out of compliance, illegal, or virus or malware spreading sites.
- URL traffic management for millions of sites managed simply by categorization into 83 classes by type, risk and other factors, including encrypted HTTPS flows.
- Comprehensive Unified Threat Management including market-leading NG-IPS, antivirus, file filtering, malware protection, and sandboxing capabilities.
- SSL-TLS Proxy to terminate encrypted sessions and to apply detailed security scans to ensure no vulnerability or malware hides within encrypted flows while enforcing applicable security policies as defined by the Network Administrator.

- DNS Proxy, DNS Security to secure and manage DNS inquiries and resolutions.
- Cloud based CASB to provide compliance and protection from data loss.
- Identifying and securing sanctioned and unsanctioned IoT devices is a must un today's Enterprise networks of sorts
- Identity Proxy and integration with 3rd party Identity Management services along with an Enterprise's own Identity Management systems.
- Rich set of routing protocols supported natively to enable traffic routing and management decisions, from carrier class networking heritage of Versa Networks.
- Industry first, native SD-WAN support by VSIA to provide integrated Secure WAN Edge solution for Enterprise branch, HQ, and DC WAN sites, giving enterprises the ability to choose placement and management of security functions on-premises, on cloud, or both, all managed through a single pane of glass.
- Flexibility to deploy customer-selected mixes of thin branch & thick cloud, thick branch & thin cloud, or other options of functional placement based on corporate, regulatory, and market requirement.
- Seamless integration option with Versa Secure Private Access (VSPA) to provide comprehensive security to Versa clients while using encrypted, private access to the network.
- Versa Analytics: detailed insights into network, application, threats, and events, and correlates this information with SD-WAN and routing analytics. These insights can also be exported to 3rd party SIEMS and accessed via Restful API.
- Granular visibility and control of the detailed application usage and behavior to analyze and police user access of specific application features like file uploads, email attachments etc.
- Data Loss Prevention with pattern-based match, Exact Data Match.

Versa Secure Internet Access is part of the Versa Secure Access Service Edge (SASE) solution, integrating full-stack security, identity management, cloud application security, and SSL encryption/decryption into a simple, hassle-free service that runs in the cloud, on-premises, or in a mix of these locations.

Solution Focused on User and Application Experience

Versa Secure Internet Access is a cloud-delivered Versa SASE solution providing integrated critical features focused on improving user experience while accessing internet applications, composed of:

- Intelligent Gateway Selection ensures that remote users always connect to closest and healthy Versa Cloud Gateways. The Versa Cloud Gateways distribute real time health and load information. Intelligent client monitors network performance towards the gateways. Client is guided to the closest healthy gateway.
- SD-WAN Lite from the Client: Versa Client supports Application Aware Policy and Traffic Steering based on FQDN and Application to ensure that unnecessary traffic is offloaded at the device. Performance based Intelligent Gateway selection and Seamless handover to alternate circuits ensures that the user experience is always maintained.
- Single Pass Architecture: Versa's single pass architecture for all security, networking, and SD-WAN functions without creating complex Network Function service chains. This architecture features a single OS delivering services through a single pass which eliminates shortcomings of discrete network functions especially when managing and securing encrypted flows via proxy. A single pass architecture for SD-WAN and VSIA ensures that the data packets spend least amount of time in the Cloud Gateways which reduces the impact on the application experience.

VSIA provides multi-faceted defense for protection of users, data and the network:

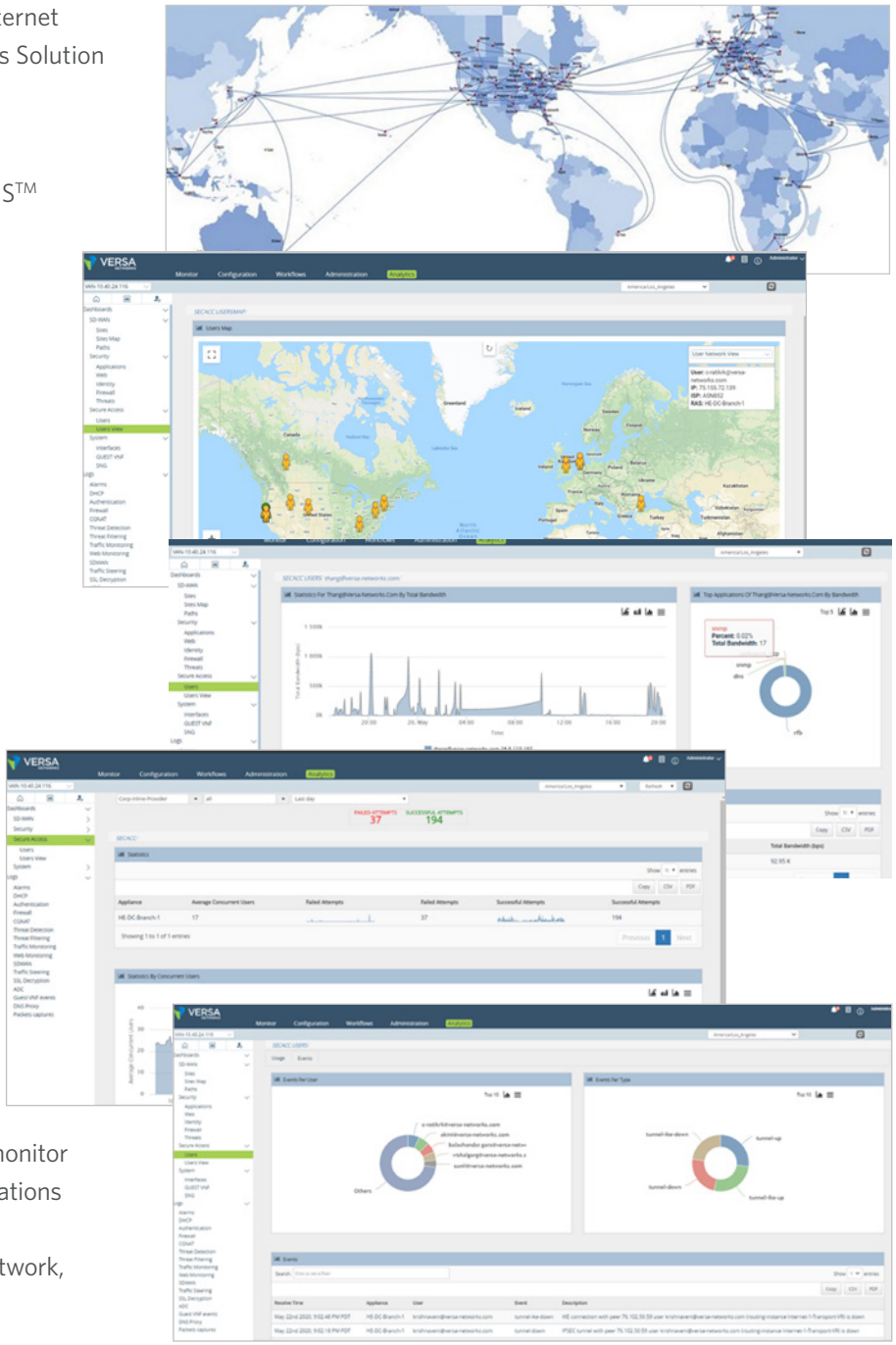
- SSL Decryption decrypts user traffic for deep scanning and re-encrypts when forwarded to the application.
- Deep scanning for threats using URL filtering and reputation, CASB, IPS, anti-malware, Zero Day protection, DLP
- Policies influenced by the end-user device status and posture. This is a key aspect of Zero-Trust security as the end device environment (e.g., absence of AV software) can be used to restrict users for accessing confidential information. This improves the security posture of the enterprise and reduces the risk of intrusion
- AI/ML based security policies based on user risk profile which is determined based on applying AI/ML analysis to user location, user activity, application access activity, time of day and other parameters.

Admins and analysts enjoy a single portal for SD-WAN, SD-Security and VSIA to provide a unified policy environment across networking and security solutions for the enterprise.

- **A software stack** deployed in the most demanding networks globally, including top service providers and enterprise networks.
- **Versa's single pass architecture** for all security, networking, and SD-WAN functions without creating complex Network Function service chains. This architecture features a single OS delivering services through a single pass which eliminates shortcomings of discrete network functions especially when managing and securing encrypted flows via proxy.
- **A single pane-of-glass** for management, provisioning, and analytics of all networking and security functions.
- **Low latency** across cloud functions, combined with optimized traffic management capabilities which provide the best application and Internet experience to customers.
- **A single, native policy language** for networking and security functions, greatly simplifying the tasks Network Administrators need to perform.
- **An always-on experience** with maintenance by expert Versa staff.
- **Highly scalable** and extensible architecture that allows users to work from anywhere.

Versa Secure Internet Access

A distributed solution to connect users to the Internet and to SaaS clouds. Versa Secure Internet Access Solution consists of:



Versa Cloud Gateways

Points of Presence based on industry leading VOS™ platform. They are globally distributed to provide reliable secure on-ramps for access to enterprise applications. Gateways authenticate users, authorize application access, and secure enterprise network from external threats. Versa Cloud Gateways integrate advanced routing, comprehensive security, and market-leading SD-WAN, with secure access. The Versa Cloud Gateways securely connect to and integrate with an Enterprise's existing network and datacenter infrastructure.

Versa SASE Client

A software agent/application that runs on and extends SD-WAN to client devices. Versa Client creates a secure and encrypted connection from remote devices to the Versa Cloud Gateway. Upon authentication and access authorization through the Versa Cloud Gateway, users with Versa Client can securely connect to enterprise applications in both the public and private cloud.

Versa SASE Portal

Provides enterprise administrators the ability to monitor and manage granular visibility of users and applications in a centralized location. Versa Self Service Portal provides real-time and historical reporting at a network, application, and user level.

Key Service Capabilities

Comprehensive and Intelligent Security

Versa Secure Internet Access is a key pillar of Versa SASE solution. VSIA provides a comprehensive protection for data residing on-premises as well as in the cloud. VSIA comes integrated with automated signature and vulnerability updates, log analysis, and configuration and policy updates.

VSIA leverages shared threat intelligence across customer and cloud-hosted applications to proactively establish appropriate protection mechanisms, providing maximum levels of protection.

A Single Pane of Glass Combining VSIA, SD-WAN, and VSPA

VSIA service comes with an intuitive portal for provisioning, managing, and monitoring of security, routing, and SD-WAN services. VSIA portal provides centralized visibility and control for internal, inbound and outbound traffic. VSIA eliminates the need for organizations to deal with operational upkeep and other day-to-day tasks, reducing IT complexity and costs.

VSIA solution comes with a unified policy framework with single-touch deployment including sites that are leveraging Versa Secure SD-WAN. Versa policy framework covers devices and applications independent of deployment and access, providing a simpler policy deployment, configuration, and management through an automated and centralized policy engine.

3rd Party Labs-Tested and Approved Security Resiliency

VSIA uses both carrier-grade and enterprise scaled security engines that have proven to be resilient and very effective. In addition, Versa security solutions have been tested and certified by Cyber-Ratings (aka NSS-Labs) and other acclaimed 3rd party testing labs.

Consistent and Assured User Experience

Versa Secure Internet Access supports geolocation, user, and application policy to ensure clients connecting to the closest designated gateway are based on current user location. VSIA customers can connect to multiple gateways based on enterprise policies and the best available gateway using real-time network information.

Once connected to Versa Cloud Gateways, clients can safely browse Internet whether they are connecting from home, traveling or connecting from Enterprise office locations using VSIA service.

If combined with Versa Secure Private Access (VSPA), enterprise-hosted applications can be accessed directly from the Versa Cloud Gateways delivering privacy, control, and enhanced performance. Through the combination of VSIA and VSPA services, applications avoid hair pinning to the enterprise DC only to break out into the cloud again, thus improving the overall application experience. This method also reduces the number of resources required at the Enterprise data center.

Use cases

Remote Worker – for connecting remote users (client/clientless) via cloud VPN or an on-prem solution to the corporate network. Apply Zero Trust principles to provide access to internet resources.

Branch and Corporate office transformation – enterprises who are migrating to the cloud and need to connect corporate offices to each other, distributed security for connectivity to the Internet, and to enterprise data center. Apply security on the edge, and in the cloud to protect data and applications hosted in private data centers, public cloud or by SaaS provider.

Security Transformation – for connecting branches, remote users, and cloud-based applications either as cloud-hosted SSE or on-premises implementation or a combination of both.

Single-Vendor SASE (SD-WAN and SSE) – to secure and connect users, applications, and devices anywhere, anytime. Single Pane of Management and Visibility across SDWAN, VSIA and VSPA solutions.

Cyber Threat Protection - protect data and resources from malware, ransomware, and Zero-Day exploits. Protect traffic bound for the internet (VSIA) or internal applications (VSPA)

Internal Threat Protection - protect data from internal or compromised users and devices. Apply Zero-Trust policies for users, devices and applications accessing internal or internet applications.

Service Tiers

VSIA Features (all features are provided inline and through the VersaONE single-pass architecture)	Essential	Professional	Elite
Secure internet access	✓	✓	✓
Cloud-based applications and SaaS access with traffic optimization	✓	✓	✓
Protection for HTTP and HTTPS flows, and broad spectrum of common protocols	✓	✓	✓
Connection from enterprise sites via SD-WAN overlay, IPSec, GRE-based tunnels	✓	✓	✓
VPN client application-based end-user device connectivity	✓	✓	✓
Connections to multiple Versa Cloud Gateways	✓	✓	✓
User and device authentication via enterprise authentication servers, 3rd-party Identity Management services	✓	✓	✓
Security policies based endpoint posture of the user device	✓	✓	✓
Rich set of routing protocols *(see feature matrix for details and options)*	✓	✓	✓
IKEv2 IPSec, Perfect Forward Secrecy (PFS), and encryption option	✓	✓	✓
Bandwidth control and traffic priority management	✓	✓	✓
Built-in stateful firewall and DOS protection	✓	✓	✓
Deep packet inspection, URL-based, destination IP address-based, and more	✓	✓	✓
Categorization (83 categories) and policy control of web applications	✓	✓	✓
Multi-dimensional policy engine based on application, user, SD-WAN, location, and scheduled traffic	✓	✓	✓
DNS proxy, DNS Security, DNS anomaly checking, Global DNS threat intelligence, transparent and split proxy	✓	✓	✓
URL identification, classification, and policy-based management for millions of URLs	✓	✓	✓
Web filtering for company compliance, prevention of malicious sites, illegal sites, and more	✓	✓	✓
Identification and policy-based traffic management of encrypted HTTPS flows	✓	✓	✓
Captive portal, integrated with proxy functions	✓	✓	✓
Real-time security updates to protect against the latest threats	✓	✓	✓
Streaming to 3rd-party analytics server	✓	✓	✓
Forward proxy, SSL/TLS proxy, and transparent proxy with granular policy level control		✓	✓
SSL/TLS proxy with support for SSLv3 and TLSv1.3. Explicit and transparent proxy support.		✓	✓
NG-Intrusion detection and prevention (NG-IDS/IPS)		✓	✓
Network-based anti-virus protection		✓	✓
Malware and ransomware scanning and protection - inline		✓	✓
File scanning and filtering, whitelist, blacklist support		✓	✓
Cloud application visibility and control via inline CASB – extensive coverage for cloud-based applications – Forward proxy-based		✓	✓
Granular cloud application behavior control *(email, streaming, conferencing, file sharing, video streaming, etc.)* via inline CASB		✓	✓
XoT Security - Device identification, classification, traffic baselining, anomaly detection and security for IOT, BYOD, XoT devices		Optional	✓
BYOD/Clientless SaaS application access management. Including inspection of content for compliance, and malware		Optional	✓
Network Data Loss Prevention / Data Leak Prevention		Optional	✓
Data Loss Prevention: Exact data match for matching structured data, indexed data match for documents and binary		Optional	✓
Data Loss Prevention: Optical Character Recognition		Optional	✓
Advanced Threat Protection including Zero-Day vulnerability protection, multiple malware engine scanning and multi-sandboxing detonation and analysis		Optional	Limited
CASB: Out-of-band, API-based; Inline, API-based; and hybrid operation		Optional	Limited

For bundling of Versa Secure Internet Access with other VersaONE platform services, please reach out to your Versa account representative.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com