Unified SASE for Healthcare

Modernizing healthcare information security

By moving away from a hardware-centric IT architecture and legacy wide-area networks, resource-constrained healthcare providers can navigate the performance and security challenges brought on by an expanding attack surface, compliance adherence, and poor network visibility. Versa's Secure Access Service Edge platform, or SASE, is a modern approach that combines security and networking services to underpin an improved care delivery model for healthcare providers.

Versa Unified SASE is the most scalable solution to allow seamless access and secure thousands or even millions of connected users and devices, regardless of their location inside or outside of the corporate network. Access to records and networks can now be governed by granular policies that deliver consistent security through a central management console – creating the necessary conditions to practice a proactive, rather than reactive, security model.

Versa Unified SASE includes the comprehensive, integrated functionality of a Software-Defined Wide Area Network (SD-WAN), Zero Trust Network Access (ZTNA), Secure Web Gateways (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Remote Browser Isolation (RBI). These services are delivered in a single software stack via the cloud, on-premises, or as a combination of both, allowing providers to flexibly adopt the blended infrastructure best suited to their needs without sacrificing security, performance, reliability, or control.

Complete access control

Versa's SASE enables healthcare providers to bring cloud platforms, data centers, branches, remote users and mobile users under one umbrella, protecting them with a unified Zero Trust security policy pushed to every user on any device at any location. It allows provider security teams to dynamically roll out organization-wide policy updates in a single instance. Having centralized control over security policies helps eliminate fragmentation, blind spots, and policy misconfigurations, and severely limits an attacker's ability to compromise devices and move laterally in the provider network.

Holistic network visibility

Through a single-pane-of-glass interface, the Versa platform offers complete visibility into users, devices, and applications across the entire network – whether on-premises or in the cloud. It automatically classifies application traffic on all ports to determine if any unsanctioned applications are being run on non-standard ports. This readily available information helps security administrators make appropriate policy changes quickly to minimize security risks. By making network-wide security information available in one centralized location, Versa allows providers to derive critical insights on potential threats, remediate those threats faster, and make better-informed decisions when troubleshooting.

Simplified administration and management

Since Versa's SASE platform operates from the cloud and delivers all its capabilities in a single unified framework, it eliminates the need for stand-alone point security products deployed for different requirements, reducing intensive capital investment in disparate products along with the administrative burden and dedicated IT resources required to deploy, configure, and manage disparate solutions and devices at each separate branch. Instead, IT staff can manage network and security policies in a consistent manner

through a single interface. This allows them to streamline security update rollouts, ensuring they not only stay ahead of emerging threat actors, but also react quickly to any regulatory changes.

Optimized application performance

Secure SD-WAN, part of the Versa Unified SASE architecture, helps providers leverage multiple transport routes such as MPLS, broadband, and 5G LTE to meet evolving bandwidth demands. Versa's architecture also embeds application awareness and traffic-steering capabilities which analyze and monitor traffic patterns and evaluate conditions like latency, jitter, and packet loss in real time. It then intelligently and dynamically sends traffic over the ideal transport route so that even bandwidth-heavy applications like EHRs and telehealth applications run seamlessly and reliably. As an additional benefit, organizations are effectively pushing their security to the network edge, closer to where the applications and data reside, eliminating data center backhauling and providing more robust application access to employees and patients without compromising security.

Integrated security and compliance

Versa Unified SASE integrates a broad set of security capabilities, including stateful and next-generation firewalls, malware protection, URL and content filtering, IPS and anti-virus scanning, DDoS and VPN/next-generation VPN. The secure SD-WAN consolidates all enterprise connectivity circuits (e.g., broadband, LTE, MPLS, etc.) into a single virtualized network, making it easier for security enforcement teams to monitor and manage the entire application suite and network landscape, as well as dynamically apply role-based access and manage configurations and enforce security policies through one centrally managed console.

Seamless UCaaS telehealth experience

Telemedicine, mhealth or mobile health kiosks depend heavily on the public internet to connect to corporate networks. However, the public internet is notorious for being unreliable for enterprise connectivity, and is susceptible to problems like packet loss, security, jitter and network latency. The problem compounds when the internet is used for media-rich applications like video conferencing or VoIP. When patients are being diagnosed (or in some cases even medical surgeries aided) via video conferencing or video calls, a seamless and reliable video and voice experience is essential.

Reduced cost and complexity

Versa's SASE integrates low-cost internet and broadband alongside MPLS to reduce the cost associated with increasing bandwidth demand. Healthcare providers can now rely on secure internet connectivity to cloud-based applications and switch over to the more reliable MPLS for mission-critical traffic. By automating and software-defining the WAN, Versa Unified SASE also helps healthcare providers cut down on the cost of resources (hardware and human) required to manage and run the networks. All these factors significantly bring down the Capex and Opex. A cloud-based subscription model means enterprises can avoid capital expenditures and shift capacity demands with ease. A centralized software-defined approach to network management also gives IT staff greater visibility and control over the corporate network, with lower administrative costs

More flexibility for the cloud

Versa Unified SASE lets IT teams proactively set up application transport policies and network routes to cope with traffic spikes, instead of having to upgrade circuits and bandwidth. By leveraging low-cost broadband and making it more secure and enterprise-ready, the SD-WAN helps healthcare providers be prepared for the possibility of natural disasters or pandemic emergencies that can lead to rapidly increased demand for healthcare services.

Support for business growth

Whether the healthcare provider decides to expand to new geographical locations by opening new branch offices or through acquisitions and mergers, IT's role is critical in quickly bringing a new location on board. Versa Unified SASE's centralized administration and console makes it easy to add new services and locations and adjust policies remotely for immediate results, without having to worry about the cost, resources, and logistics associated with setting up new IT infrastructure.

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