Versa SASE for Healthcare

The start of year 2022 marked the second full year since the outbreak of COVID-19 was declared a global pandemic. Today, a worldwide healthcare ecosystem continues to shoulder the burden of curbing the virus's damage.

Despite many country's advancements in vaccine development, treatments, and social protocols within the last two years, COVID-19 continues to be a crisis for healthcare providers around the world, accounting for the lion share of the ecosystem's resources and attention.

One trend within the sector points to a countermeasure against some of these challenges, one born both out of convenience and necessity. With a growing number of patients ushering in a pattern of "healthcare consumerization", providers are re-examining how they can provide services in new ways. This shift in HCDM (health care delivery model) coined by Deloitte refers to more healthcare providers looking at virtual and digital means to deliver services, expertise, and care, converging traditional and new channels to serve the most patients possible in ways more convenient.

While HCDM continues to be a concept re-thought by healthcare providers to make use of technology when treating and caring for patients, migration to virtual services potentially exacerbates the ever-present threat of cybercrime within the collective ecosystem.

An Increasingly Vulnerable Sector

Healthcare providers are very familiar with breaches and online attacks. Cybercriminals have historically utilized ransomware attacks to acquire and hold hostage sensitive patient data from providers. In the worst-case scenarios, internet connected systems storing patients' health data are leveraged to demand cash payouts from hospitals with no other option than to recover system control by paying the ransomware price to attackers.

As of December 2021, global cases surpassed the 270 million mark. More than half the world's population remains unvaccinated, with rates dropping below 5% in developing countries. And in United States, 55% of frontline healthcare

In September 2020, a ransomware attack run on a German hospital made emergency care facilities and digital infrastructure inoperable, resulting in direct threats to patient lives. This incident rang an alarm bell for many providers that had long deprioritized adopting cybersecurity technology and had prolonged the development of companywide incident response plans.

These kinds of attacks are widespread throughout healthcare, as cybercriminals continue to take advantage of providers shifting to virtual care in their struggle to manage case load during times of resource shortage.

Recent significant incidents include attacks that disrupted life-saving operations and disabled access to medical records for key staff, resulting in hundreds of employees furloughed and a self-reported millions of dollars in damages per day.

According to healthitsecurity.com, 560 companies in the healthcare sector were victims of a breach, impacted by 80 separate incidents in 2020. PHI and other sensitive data was stolen in multiple incidents, and published online in at least twelve of those incidents. And as reported by Verizon in their 2021 Data Breach Report, the sector saw 655 incidents, 472 of which were reported with confirmed data disclosure.

This data infers a mounting volume of attacks on healthcare providers in coming years. And as more providers adopt virtual and online channels to serve patients out of necessity, an expanding surface of distributed systems and data means compounding targets for attackers.

While the ecosystem deals with its fragility and current challenges, criminals will continue to see companies within this space as prime targets for exploitation unless providers address key challenges related to the security of their systems, data, devices, and applications.

Growing Attack Surface

For attackers, the growing number of providers adopting online channels to provide patient care and services means increasing device complexity on those provider networks, which can be exploited in attacks. Providers must also consider how their employees access records and systems from their own devices and home networks, as well as how those devices and networks are segmented by access policies.

Hospitals and other care providers often have multiple locations accessing the same systems and records within singular private networks, which, if not governed by intelligent dynamic context, attackers can exploit gaps and then laterally move within the network to find sensitive data.

Organizations using static access policies for records and systems allow criminals to identify security gaps and launch malware attacks in the network if a single device is compromised, despite perimeter security controls like stateful firewalls.

HIPAA and Other Regulations

The healthcare sector, being one of the most regulated, faces unique challenges when dealing with compliance frameworks.

HIPAA has governed how providers must approach patient privacy and medical record security for over twenty years, while more recently the HITECH Act expanded IT compliance standards originally set by HIPAA with the adoption of EHR practices. The Interoperability and Patient Access Final Rule passed by the CMS also drew a narrow scope on how patients should be able to access and control their electronic health information.

While the adoption of NIST CSF and participation in organizations such as H-ISAC can help providers better comply with relevant regulations, variables such as violation fines, shifting requirements, and the increase in general availability of patient records online all contribute to the growing complexity in navigating these regulations. A single violation of HIPAA alone can cost a provider up to $50,000 depending on severity, not accounting for the cost in other damages of an incident or breach even properly disclosed.

For providers without rigorous, organization-wide access policies to patient records, heavy regulation fines remain a very real possibility on top of financial loss caused by a malicious actor.

Limited Visibility of In-Network Threats

Despite their shifts toward incorporating cloud and mobile channels to provide IT services, many providers have yet to shift away from hardware-centric architecture and legacy wide-area-networks because of budget and staffing limitations when modernizing their technology stack.

Networks like this were designed to secure data stored within a provider's perimeter. In order to further secure data and devices within their perimeters, many providers adopt security products ad-hoc along network points to combat threats.

The unfortunate result is more network fragmentation, where integration and interoperability limitations create obscurity and management complexity, denying providers holistic network visibility into the who, what, and when of their network access points. Amidst pressure to deliver critical patient services, providers run thin of time and resources to operate and maintain these disparate products.

Versa SASE: Modernizing Healthcare Information Security

By adopting the proper technology, resource-constrained healthcare providers can navigate the challenges brought on by an expanding attack surface, necessary compliance adherence, and obscured network visibility, all while dealing with the new trends that drive patients and employees toward cloud services.

Versa Secure Access Service Edge, or SASE, is a modern approach that combines security and networking services to enable seamless asset access for users. Versa SASE is the simplest and most scalable solution to secure millions of connected access points in and out of provider resources, regardless of their locations. Access to records and networks can now be governed granular policies that deliver consistent security through a central management console – giving providers the advantages of a proactive, rather than reactive, security model.

Versa SASE includes security and networking services, and at its core is comprised of Software-Defined Wide Area Networking (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 blended combination of both. Providers can leverage these capabilities to adopt infrastructure best suited for them without sacrificing security, performance, reliability, or control.

Complete Access Control

Versa SASE enables healthcare providers to bring cloud platforms, data centers, branches, remote and mobile users under one umbrella, protecting them with a unified security policy pushed to every user on any device and 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 laterally move in the provider network.

Holistic Network Visibility

Through a single-pane-of-glass interface, Versa SASE 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 providers make appropriate policy changes quickly to minimize security risks. By making network-wide security information available in one centralized location, Versa SASE enables providers to derive critical insights on potential threats, remediate those threats faster, and make better-informed decisions when troubleshooting.

Simplified Administration and Management

As Versa SASE 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.

Operating and managing point products by branch takes dedicated IT resources that are costly to upkeep. Because it fulfills a multitude of security requirements with a single security stack, Versa SASE saves providers what could be intensive capital investment in disparate products and IT staff. The administrative burden of deploying, configuring, and managing these devices at each separate branch is removed.

Instead, IT staff can manage network and security policies in a consistent, ubiquitous manner through a single pane of glass. 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 challenges that would result in fines and damages.

Optimized Application Performance

Secure SD-WAN, part of the Versa SASE architecture, helps providers leverage multiple transport routes such as MPLS, broadband, and 5G LTE to meet evolving bandwidth demands. Versa SASE architecture also embeds application awareness and dynamic traffic steering capabilities which analyze and monitor traffic patterns like latency, jitter, and packet loss in real-time.

From this analysis, it intelligently routes traffic over the ideal transport route so that bandwidth heavy applications like EHRs and telehealth applications run seamlessly and reliably. As an additional benefit, providers shift their security to the cloud, closer to where applications and data reside, eliminating data center backhauling and providing access to employees and patients without compromising security.

An Improved Care Delivery Model

As healthcare providers continue to deal with the ongoing COVID-19 crisis and the challenges unique to their ecosystem, malicious actors will continue to exploit security gaps and vulnerabilities.

Now, with Versa SASE, access policy and security tooling can allow providers easier resource access for all health care workers, more service delivery instead of less, and complete network visibility and policy management through a uniform, centralized management console. The dynamic model of securing user and device access when risk is detected allows a distributed workforce to support more patients in a time when support is most needed.

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com