VMware SASE: Deliver Patient-Centric Care from Anywhere

vmware SASE™

Benefits of VMware SASE for healthcare

- Provide **reliable, secure, and efficient delivery of healthcare data** such as EHR and imaging to, from, and between the cloud, data centers, pop-up clinics, hospitals, or home offices. Deliver exceptional patient experiences through fast, stable connectivity.
- **Facilitate HIPAA, PCI-DSS compliance** and protect healthcare workforce, network, application, and sensitive patient data against emerging threats from inside and out.
- **Turn up new sites quickly** or integrate newly acquired sites into the existing network with cloud-delivered zero touch deployment and unified network and security stack. Accelerate transformation of IT operations to an agile mode with proactive remediation and self-healing.
- **Future-proof network and security infrastructure** for long-term projects. Transition smoothly to SASE with a flexible architecture, leveraging services from VMware and a broad ecosystem of third-party solution providers, from analytics to security.

Over the last two years, there has been an acceleration in the use of technology to improve patient care. Patients discovered a preference for virtual care and digital services, and remote work is no longer just a trend. To meet rising patient expectations with a distributed workforce, modern-day health care organizations need a new architectural approach that provides secure, reliable and consistent access to patient data and applications.

Common use cases demand a change in architectural approach

Legacy architecture with a separate networking and security stack can no longer support the increasing demands of the modern-day healthcare organization. The following trends and evolution in healthcare highlight the need for a new architectural approach.

Telehealth and virtual care

Telehealth has become a must-have option to deliver care. It relies on video conferencing as a virtual connection point between a patient and a care provider. Video conferencing applications require a high level of reliable bandwidth. When a patient requires virtual care or physicians need to discuss patient cases for assessment and diagnosis, quality of service (QoS) is critical. Dropped calls or jitter-heavy connections are detrimental to providing high-quality care. Furthermore, physicians need a secure way to access patient data while delivering virtual care.

Distributed workforce

The healthcare workforce is becoming distributed with the rise in remote workers. Clinicians use virtual desktop infrastructure (VDI) so that they can use technology at the point of care to easily and securely access EMRs. In addition, non-clinical staff working remotely use cloud-based desktops and VDI to get work done. VDI supports multiple devices, including smartphones and tablets, and has robust security to comply with regulations including the Health Insurance Portability and Accountability Act (HIPAA). However, successful VDI deployments need reliable, optimized connectivity, which is often not available

in most clinics or branch offices. Remote workers using home broadband face unstable internet and VPN connections due to network issues. Healthcare organizations need a way beyond traditional WAN, VPN and security solutions to provide the workforce with secure and high-performance access to applications and data whether they are in the office or at home.

Cloud adoption

Moving applications and services to cloud is helping healthcare organizations meet new digital delivery demands of patients and physicians. Organizations turn to cloud-based storage and application delivery to enable clinicians with constant access to EMRs and sharing of high-resolution medical images, resulting in a need for creating and securing network connections across multi-cloud environments. Cloud applications require efficient, optimized access and an infrastructure specifically architected to support them. The traditional architecture is expensive and results in slow access.

Security and compliance

Healthcare organizations are embracing remote work to hire and retain top talent. But when the healthcare workforce accesses corporate networks and cloud services from home or a remote network, the increased number of devices and endpoints connecting to the network creates a larger surface area for attacks and may lead to data breaches and hacks. Healthcare IT needs a way to secure cloud access, home networks, employees' devices, and manage the risk of losing sensitive data. In addition, healthcare IT must ensure that each location adheres to the same HIPAA guidelines as primary care offices.

Healthcare offices and clinics often require patients to render payment at the time care is provided. This requires that offices provide either a payment device or an ATM connected to the network. Not only must this highly sensitive data be segmented from regular office traffic, but it must also comply with Payment Card Industry Data Security Standard (PCI DSS) regulations.

IoT device management

IoT devices such as MRI machines, infusion pumps, and light bulbs are part of the network. These devices need to be manually onboarded and are often unmanaged and unmonitored, with IT having no insights into their performance and behavior. IT needs a way to ensure IoT device performance and security.

Remote sites and pop-up clinics

Over the last two years, many healthcare providers had to quickly build pop-up clinics. In addition, mergers and acquisitions are a growth strategy for healthcare organizations, meaning that care often shifts to small remote or regional branch offices. These pop-up and remote sites require the same network connectivity and access to critical applications as hospitals and clinic buildings. Healthcare IT needs a way to integrate these new sites rapidly and provide them a reliable and secure network connection.

VMware SASE is foundational to digital healthcare

VMware SASE™ (Secure Access Service Edge) is a cloud-native platform that combines industry-leading SD-WAN capabilities with cloud-delivered security, including cloud web security, zero trust network access, and firewalling, to provide traditional care sites, remote offices, pop-up clinics, ambulances, or home offices with secure, optimized, and reliable access to applications and services deployed in public/private clouds, or SaaS.

Improve patient experience

With VMware SASE, healthcare IT can deliver digital experience to patients. Physicians get reliable and uninterrupted connectivity during telehealth calls with VMware SD-WAN Dynamic Multipath Optimization™ (DMPO)'s ability to aggregate all available links, including broadband, 5G, LTE, and MPLS circuits. DMPO uses application-aware per-packet link steering and on-demand remediation.

Healthcare organizations using mobile clinics to deliver care to underserved and remote communities', and pop-clinics to support increased patient volumes, can use 5G, LTE or satellite connectivity with VMware SD-WAN Edge devices to gain the same secure connectivity and access to critical applications as hospitals and clinic buildings. Furthermore, emergency responders in an ambulance can gain secure connectivity with VMware SD-WAN.

Empower your workforce

VMware SASE, designed on the idea that the cloud is the network, ensures the availability, security and performance of mission-critical healthcare applications for the healthcare workforce, no matter where they are. This is possible due to efficient routing of traffic through necessary security functions all with a single VMware SASE PoP. These PoPs have a global footprint and serve the world's major metropolitan areas. SASE PoPs provide a quick, secure, and high-quality on-ramp to SaaS and cloud services from any location or device. This cloud-ready network eliminates data center backhaul penalties and provides an optimized direct path to public and private enterprise clouds.

With VMware SASE, care teams across all locations get high-performance, reliable, and secure access to applications and data located anywhere (cloud, on-prem, SaaS, and edge), including in reduced-connectivity scenarios. This ensures that healthcare data is always accessible and transmittable, including the accelerated transfer of radiological images (PACS, DICOM, etc.), bolstering clinical and care team collaboration to provide vital care from any location.

Mitigate risk and ensure compliance

Protect healthcare workforce, network, application, and sensitive patient data against emerging threats from inside and out with VMware SASE's comprehensive suite of cloud-delivered security offerings. In each location, define security rules for incoming and outgoing data with an ICSA-compliant enterprise firewall residing on SD-WAN Edge. Not all healthcare traffic and applications are the same and need to be treated differently. Segment traffic

Learn more

- VMware SASE for healthcare: *sase.vmware.com/solutions/healthcare*
- VMware SASE: *sase.vmware.com*
- VMware SD-WAN: *sase.vmware.com/sd-wan*

from end to end to isolate various types (voice, data, HIPAA, PCI, etc.) with established profile templates ensuring separation of IoT and operational technology (OT) traffic from EMR traffic and meet compliance requirements.

Gain multiple benefits over traditional VPN solutions with the Zero Trust Network Access (ZTNA) framework-based offering, VMware Secure Access™. Protect healthcare workforce and infrastructure accessing SaaS and browser-based applications such as Salesforce Health Cloud or webmd.com from threats with VMware Cloud Web Security™ and gain visibility, control, and compliance. In addition, VMware SD-WAN integrates seamlessly with best-of-breed security vendors (including Palo Alto Networks, Zscaler, Symantec, and Check Point), allowing healthcare organizations to easily implement the security profile of their choice.

Simplify IT operations

Cloud-delivered VMware SASE centralizes monitoring, visibility, and control to enable zero-touch deployment across all healthcare locations while delivering automatic business policy and firmware updates, configurable rules, application prioritization, link performance, and capacity measurements. IT personnel can manage all network traffic and applications and remediate from a central location rather than a truck roll to remote sites. VMware SD-WAN Edges placed in each primary and remote office or clinic—or home office—automatically authenticate, connect, and receive configuration instructions with the centralized management portal once connected to the Internet in a zero-touch deployment. This enables healthcare organizations to quickly deploy new sites, as well as transition newly acquired locations into the overall network.

Gain actionable intelligence to ensure that devices such as laptops, workstations on wheels and IoT devices such as infusion pumps, patient monitoring devices at every location—whether a hospital or home—are getting the performance they need from WAN, LAN, SASE and applications with VMware Edge Network Intelligence™. Accelerate transformation of IT operations to an agile mode with proactive remediation and self-healing capabilities of VMware Edge Network Intelligence.

A complete SASE solution

VMware SASE delivers a complete solution for healthcare organizations. It provides reliable, secure, and efficient connections from clinics to applications in the cloud or in data centers, ensuring confidential access to sensitive information. Capabilities like centralized management, zero touch deployment, zero trust network access and the use of any link type means that sites can be connected quickly, data is always secure, and devices can be easily managed. Application visibility capabilities ensure performance and ease troubleshooting for reliable operations.

VMware SASE enables healthcare organizations with digital technology and future-proofs their networking and security stack.