INSIGHTS | TECH BRIEF

Streamlining Healthcare Cybersecurity: The Case For Consolidating SASE

Hospital security protocols are crucial for ensuring a safe and secure environment for patients, staff, and visitors. Access control systems are in place to control the means of egress that ensures only authorized personnel can enter sensitive zones such as operating rooms, nurseries, and intensive care units. Meanwhile, visitors are typically restricted to designated hours and locations. There are safeguards utilized throughout hospital and clinic campuses including security personnel and physical barriers that prevent unauthorized entry and manage pedestrian traffic flow. Essentially, security is at the core of healthcare.

Healthcare And SASE

While the physical safeguards are easy to identify, the digital side of healthcare is an entirely different scenario. Given the sensitive nature of patient data and the critical importance of medical systems, it's clear why cybersecurity is a paramount concern to healthcare executives. The expansion and non-stop merging of healthcare organizations across multiple locations necessitates scalable, manageable, and flexible access controls to ensure consistent security regardless of location. This is precisely why a cloud-delivered Secure Access Service Edge (SASE) is ideally suited to meet the unique needs of today's healthcare industry.

With SASE, healthcare organizations can ensure secure access to patient records and medical systems from any location and on any device. SASE incorporates advanced threat detection and prevention capabilities that protect against cyberattacks such as ransomware and data breaches that could compromise patient confidentiality and disrupt life-saving healthcare services. By adopting SASE, healthcare IT leaders can strengthen their cybersecurity posture, mitigate risks, and maintain patient trust by effectively safeguarding sensitive information.

80%

of organizations are introducing innovations faster than their ability to secure themselves against cyberattacks.[1]

A Universal, Consistent Experience

Whether patients visit a healthcare facility for a regular checkup, outpatient surgery, emergency services, or a heart transplant, they expect a consistent, reliable experience across all locations and services. This expectation extends to digital users on the clinical and patient side as well. Organizations employing multiple cybersecurity solutions and vendors for both on-premises and off-site security face high operational costs and increased complexity. This often results in inconsistent cybersecurity measures for both on-site and remote users that can impact compliance and enlarge the attack surface. The importance of consistency is recognized across various industries, which is why businesses of all sizes are beginning to consolidate their security vendors, increasingly investing in companies capable of addressing as many of their security needs as possible.

According to a Gartner survey, by 2025, three-quarters of large organizations will be actively pursuing a strategy to consolidate their vendors. Organizations spread across multiple locations often struggle to provide a uniform security and application experience due to the use of multiple disjointed products. This challenge is particularly acute in the healthcare industry, which often lacks the high-level security talent necessary to architect and implement best-practice security strategies when dealing with numerous disparate security tools.

Additionally, there is the ongoing requirement to maintain, manage, and upgrade these complex systems, which is becoming increasingly unsustainable. On the other hand, a single-vendor approach makes it easier for organizations to purchase, deploy, and support SASE solutions. It also provides better integration and visibility while eliminating the elongated learning curves of having to master so many different tools.

Introducing Fortinet's SASE Solution

FortiSASE, a key component of Fortinet's comprehensive security solutions, can significantly enhance the Fortinet Security Fabric by ensuring secure access and robust endpoint security for every employee within an organization. For those utilizing existing FortiGate deployments, FortiSASE extends the capabilities of the security fabric to encompass real-time threat protection, sophisticated remote access, enhanced endpoint security, and continuous environmental monitoring.

This integration begins with a single agent that consolidates functions of the security fabric, SASE, and endpoint protection into a unified system. The Fortinet unified agent facilitates complete endpoint visibility using telemetry data that allows all components of the Fortinet Security Fabric to share a consistent view of all identified endpoints. This integration supports effective tracking and awareness, stringent compliance enforcement, and detailed reporting.

Management of this integrated system is streamlined through Fortinet FortiManager, which offers unparalleled visibility and control. This management platform enables consistent security policies across all network edges and user activities, significantly enhancing both the security posture and operational efficiency of the organization. By centralizing management, FortiSASE not only simplifies administrative tasks but also fortifies defenses, making it an indispensable solution for modern cybersecurity needs.

The Importance of Zero Trust

Zero Trust is nothing new to the healthcare industry. In the physical sense of a surgical room, strict protocols dictate that no clinical professional can complete a function without communicating it to their colleagues. Everyone from doctors, anesthesiologists, nurses, surgical techs, and trainees must verify their identity and go through rigorous hygiene procedures before entering the operating room. Access is strictly controlled to only those individuals who are essential to the operation and have the proper credentials.

In the digital sense, no end user or device should be trusted by default from inside or outside the network. Access to digital resources should be granted based on strict identity verification, least privilege access, and continuous authentication. Like a surgical room's controlled access to ensure a sterile environment and prevent infections/mishaps, Zero Trust aims to minimize risks and protect sensitive data from unauthorized access, breaches and ransomware attacks.

Fortinet's Universal Zero Trust Network Access (ZTNA) solution offers the industry's most versatile Zero Trust application that ensures only the right people can access the right assets regardless of user location or where the application is hosted. Integrated directly within the Fortinet operating system, ZTNA enables the enforcement of Zero Trust policies for employees, whether they are working from the main office, a branch location, or remotely.

Zero Trust architecture involves controlling traffic around critical data and assets by creating micro perimeters. A segmentation gateway at these micro perimeters scrutinizes all entries of people and data, acting as a critical checkpoint. Fortinet ZTNA enhances security further with features such as endpoint verification, least privilege access, multi-factor authentication (MFA), and micro segmentation. This comprehensive approach ensures that healthcare facilities can secure their data and critical systems with the same rigor applied to their patient care areas.

Further Consolidation With WEI

Healthcare organizations are enhancing their control over users and devices across multiple locations by adopting Fortinet's FortiSASE solution with integrated ZTNA and expanded cloud-based security. They value its straightforward licensing structure, ease of management, and seamless integration capabilities. Despite these advances, many healthcare providers are still catching up with securing their rapidly advancing digital transformations. Despite these advances, many healthcare providers are still catching up with securing their rapidly advancing digital transformations.

Talk to WEI today

If you're not familiar with the extensive benefits of a cloud-based SASE solution for securing widespread enterprises, WEI security engineers are ready to assist. As the most comprehensive Fortinet partner in the northeastern United States, our deep technical bench is fully trained and authorized in Fortinet technologies.

We encourage you to allow WEI and Fortinet to demonstrate how consolidating your security solutions with leading next-generation SASE solution can benefit your organization.

Sources:

1. Accenture Security and the Ponemon Institute, The Cost of CyberCrime – Ninth Annual Cost of Cybercrime study: https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.