



UNIFIED SECURITY TO IMPROVE COMPLIANCE AND PROTECT EPHI

HARMONY SASE FOR HEALTHCARE



Harmony
SASE

Security and networking professionals in the healthcare industry are under pressure to not only meet compliance requirements and safeguard Electronic Protected Health Information (ePHI), but to also provide efficient networking and data access to clinical teams, researchers, and others. Addressing these challenges is critical to prevent system slowdowns that impact patient care and to defend against the rising number of attacks on healthcare organizations.

Expanding Networks

As healthcare providers seek to deliver a more patient-centric care experience, they have embraced hybrid networking, complementing on-prem tools with the cloud. Spanning multiple environments and regions, healthcare networks are now more complex to defend than ever. Short-staffed IT teams are also tasked with managing multiple solutions for authentication, access control, encryption, and firewalls, opening up potential gaps in coverage.

Attractive Targets

Healthcare facilities and similar organizations are attractive targets for cybercriminals. Their repositories of patient data and expansive networks make them more susceptible to attacks.

The risk of ransomware is particularly notable. There were 630 such attacks impacting healthcare organizations in 2023, 460 of which were in the US. And the number of attacks nearly doubled from 2022 to 2023. Attackers recognize that the need to resume normal operations as quickly as possible increases the likelihood of a payout.

It doesn't stop with ransomware, however, as adversaries use a range of tactics in their pursuit of patient records, which command a premium price on the black market. From social engineering to credential stuffing to exploiting gaps in cloud configurations, attacks continue to evolve and place pressure on IT teams.

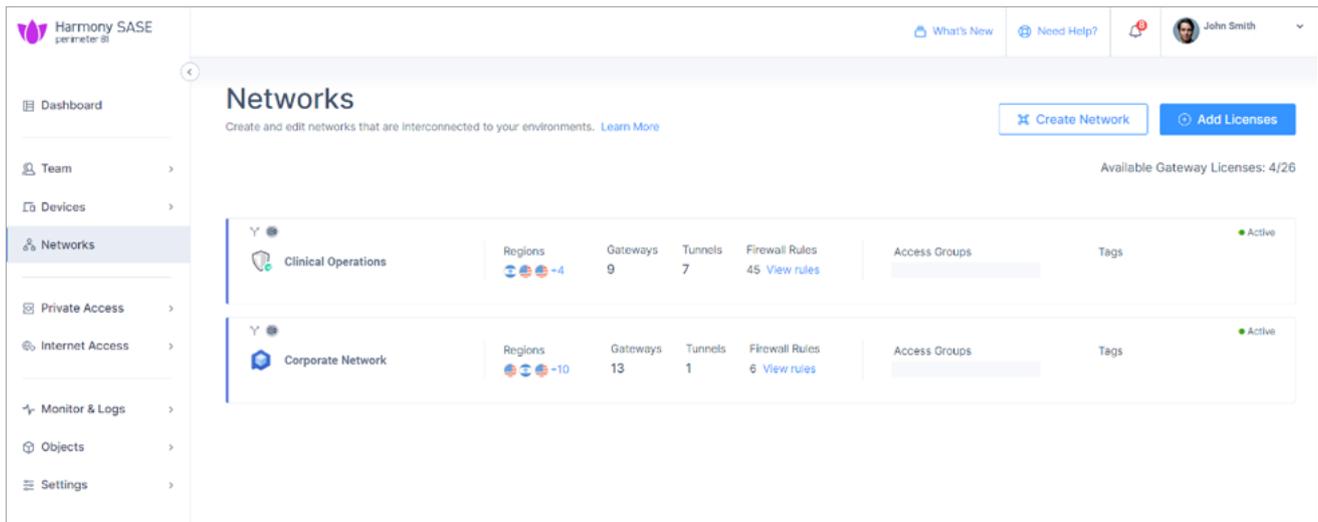
Addressing the Challenge with Harmony SASE

To address these complex challenges, organizations are turning to consolidated networking and security solutions like Harmony SASE. Hundreds of healthcare providers trust Harmony SASE because it delivers secure, streamlined access for users across the network, enabling compliant patient data protection.

Visibility is the First Step to Compliance...

Regulations such as HIPAA demand vigilance when it comes to how, where, and who accesses ePHI. This requires a level of visibility far more extensive than mere logging. What's needed instead is a real-time understanding of where sensitive data resides and who can access it.

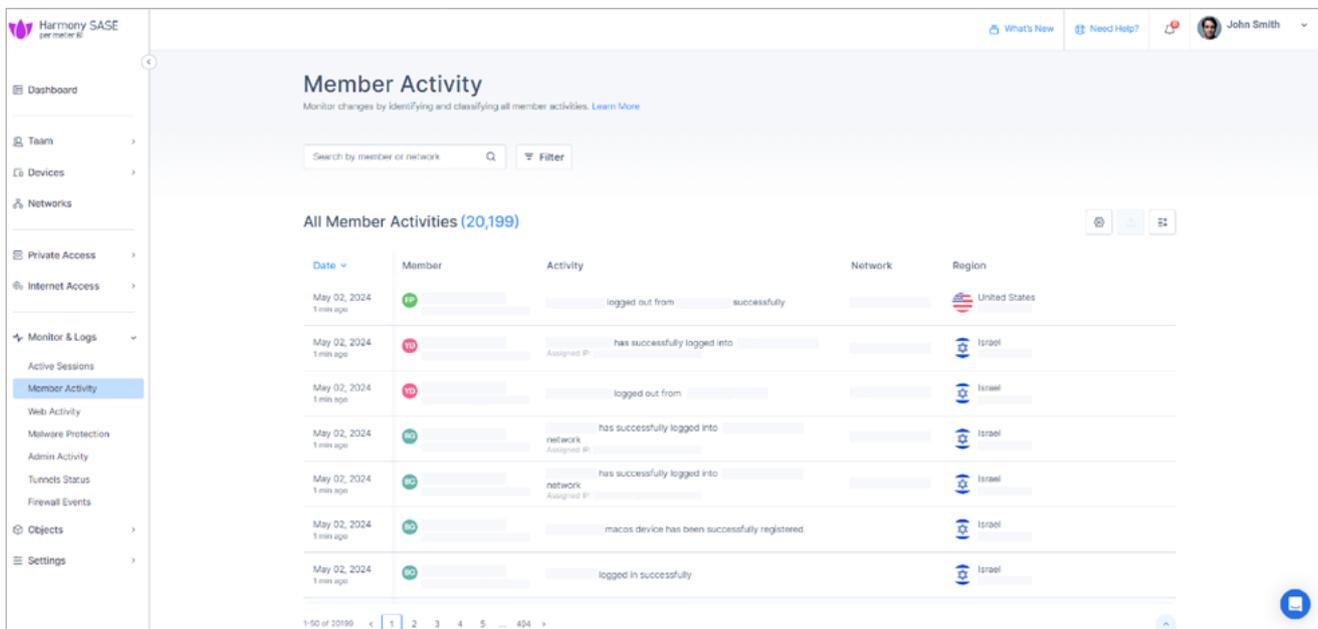
Harmony SASE provides a single pane-of-glass view of the network and activity taking place within it. IT teams can visualize the connection points to databases and applications housing patient data and implement the appropriate security controls.



Set up and view networks in a unified, easy-to-use dashboard

Whether your organization relies on a private or public cloud, on-premises resources or a mixture of both, Harmony SASE has you covered. Our platform integrates seamlessly, providing both visibility over these resources and extending security controls to the network's edge.

Administrators can view all users and endpoints, groups, associated policies, recent activity, and security posture in a single spot. Both our agent-based and agentless products work with Linux, MacOS, iOS, Android, and Windows.



View and download logs of user and system activity.

Boost visibility and compliance with holistic logs of network activity such as device posture and health, app connections and access, policy changes, gateway deployments, and more. You can also integrate with Splunk, Amazon S3, and Azure Sentinel for deep data analysis via SIEM.

...And Control is the Second

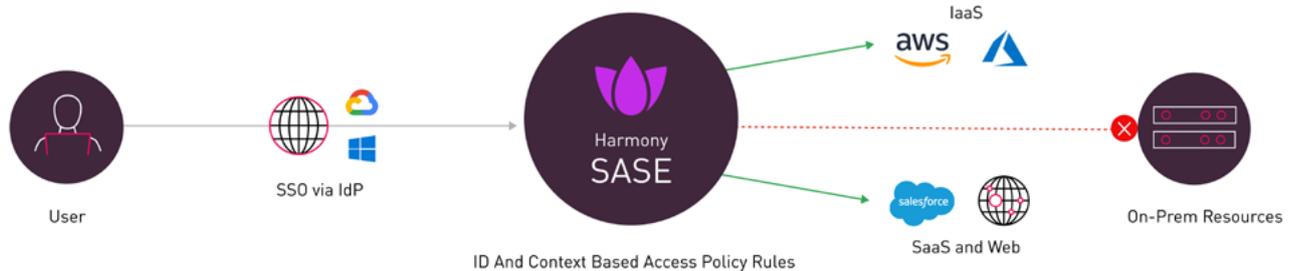
With visibility established, administrators can exercise control over network access, sensitive assets, and users. This helps to reduce the attack surface and, notably, demonstrate compliance with mandates such as the HIPAA Security Rule, which explicitly calls for control over access to sensitive systems.

Harmony SASE provides a unified platform to manage network security based on the principle of least privilege. It enables easy network segmentation by creating access policies for users and groups, which are applied when users

login via an Identity Provider (IdP) or any SAML 2.0 solution you choose, including Google, Azure, Okta and more.

Access policies created within Harmony SASE extend to resources in the cloud and on-prem networks via our agent. These are based on the permissions that groups of users need for their roles, but can also address location, device, and other variables.

Even traffic between network objects is controllable via firewall rules, which allow administrators to block or allow traffic between services, users, addresses, and more, further reducing the attack surface.



Achieve user-centric Zero Trust access with Harmony SASE

Your ability to control the network extends to the devices that attempt to make a connection. Device posture check rules enforce specific configurations and security settings for devices before they enter the network, and then periodically after the connection is established.

Additional security features to exert control over the network and protect patient data include:

- Automatic Wi-Fi security
- Multi-factor authentication
- Encrypted site-to-site gateways to protect patient medical data traversing the network

Harmony SASE is Stronger Network Security for Healthcare

Healthcare IT teams face a dual challenge of ensuring that clinicians and others can access

the applications and data they need to deliver quality patient care, while also safeguarding ePHI in compliance with stringent mandates.

This necessitates a network security solution that reduces complexity while improving data protection and compliance.

Harmony SASE empowers IT teams with streamlined visibility and control from a single management platform.

Administrators can connect care teams with the resources they need while reducing the risk of unauthorized data access or other incidents that can impact the delivery of care and result in HIPAA audit violations and fines.



Meet Harmony SASE

10x Faster Internet Security | Full Mesh Private Access | SaaS Security | Secure SD-WAN

Check Point's game-changing alternative delivers 10x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties.

Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

With Harmony SASE businesses can build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

To learn more, visit www.checkpoint.com/harmony/sase/ or [schedule a demo](#)

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com

© 2025 Check Point Software Technologies Ltd. All rights reserved.