Healthcare's essential guide to preventing cybersecurity breaches

Outsmarting threats with a Zero Trust approach

eBook

MENLO SECURITY

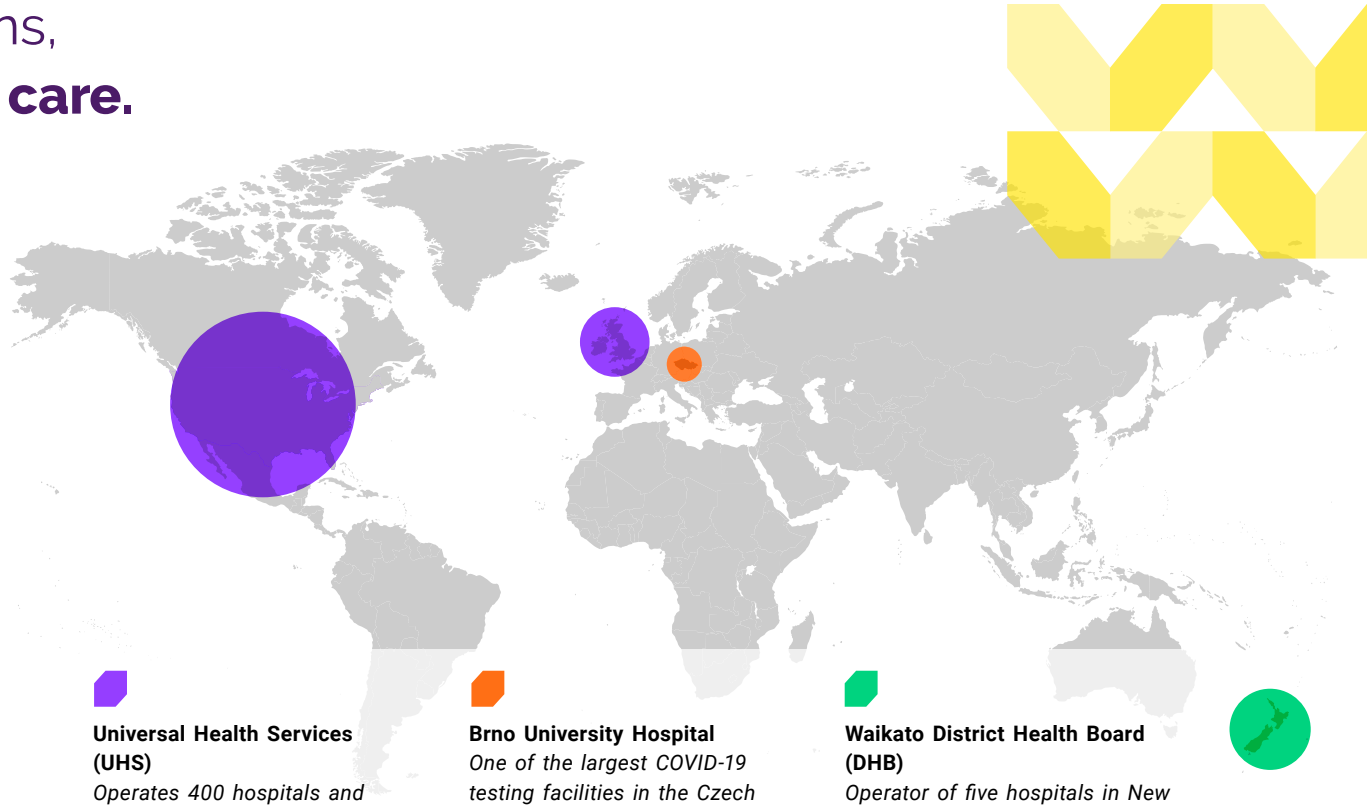
For healthcare organizations, **cybersecurity is an act of care.**

Across the globe, the healthcare sector continues to top the list of most targeted industries. Compared to other high-ranking industries that experience security incident that result in temporary disruption, penalties, and reputational damages—which are repairable over time—breaches can result in life or death implications for healthcare organizations.

As cybercrime continues to climb, the importance of healthcare cybersecurity has not only increased, but has fundamentally changed how and where organizations need protection. Today's healthcare technology innovations have introduced connected, network systems and wireless technologies capable of providing life-saving functions, enhancing provider productivity, and improving affordability. Devices, both corporate-issued and personal, are used within the confines of the network and at places with less secure WiFi, such as homes and coffee shops—all while the ecosystem expands as third parties supplement core services, leveraging cloud-connected technologies.

When you can't uphold "do no harm"

For the international healthcare community, ransomware cyberattacks have ground hospitals to a stop—forcing them to redirect ambulances and relocate patients in need of surgery to nearby competitor facilities.



Universal Health Services (UHS)
Operates 400 hospitals and behavioral health facilities in the U.S. and U.K

According to the UHS earnings report, due to the significant incremental labor expense needed to restore IT operations after the incident, and delayed administrative functions like billing that reduced operating cash flows, they experienced a pre-tax impact of approximately $67 million during 2020.[1]

Brno University Hospital
One of the largest COVID-19 testing facilities in the Czech Republic

At the time, the COVID-19 pandemic had only just begun to spread in the Czech Republic. Within two days of the attack, confirmed cases nearly doubled, highlighting the importance of working testing laboratories.[2]

Waikato District Health Board (DHB)
Operator of five hospitals in New Zealand

According to the DHB, hospital discharges were completed by hand and personal mobile phone numbers were used in place of the inoperable pager system that alerts multiple doctors when a patient suffers a cardiac arrest.[3]

1 https://threatpost.com/post-cyberattack-universal-health-services-faces-67m-in-losses/164424/
2 https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak
3 https://www.healthcareitnews.com/news/apac/waikato-dhb-making-good-progress-bringing-systems-back-online-says-chief-executive

According to the Center for Disease Control and Prevention, there was a

154% increase

in telehealth visits during the last week of March 2020 compared with the same period in 2019.[4]

By 2026, the Global Telemedicine Market is projected to grow up to

US$ 218.49 Billion.[5]

Ransomware attacks were responsible for almost

50%

of all healthcare data breaches in 2020.[6]

Virtual health revolution:
More care, more attacks.

In 2020, patient caseload volumes soared to heights never experienced before. Creating chaos of overwhelmed hospitals, mental health providers being booked solid for months, and payors inundated with claims. And to navigate it all, simply continuing with normal operations wasn't a sustainable option. Instead, a virtual health revolution began that could only be rapidly facilitated through cloud adoption.

Despite the attention given to the acceleration of telehealth, work-from-home models boomed across all types of healthcare organizations (HCOs). Dispersed healthcare professionals responsible for research collaboration, patient scheduling, and more all worked from managed and unmanaged devices—increasing the number of endpoints used for critical work. And as endpoints proliferated, so did the security risks. Working outside of the network on less secure WiFi, accessing cloud-hosted electronic health records, logging into web-based payor portals, and doing so on non-IT issued devices became a necessity.

Later in the year, the FBI and U.S. Department of Health and Human Services issued a joint alert that cybercriminals were taking new aim at healthcare providers and public health agencies. The agencies warned that malicious cyber actors were currently and soon planning to infect systems with ransomware for financial gain on a scale not yet seen before.

At home there is no IT manager to control the security of WiFi networks, which often leads to weaker protocols. For example, WEP instead of WPA-2.

4 https://www.cdc.gov/mmwr/volumes/69/wr/mm6943a3.htm
5 https://www.medgadget.com/2021/06/telemedicine-market-global-forecast-impact-of-covid-19-industry-trends-growth-opportunity-company-overview-financial-insight.html
6 https://www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf

A time to thrive

Traditional detect-and-remediate cybersecurity practices may keep HCOs breathing, but the approach falls short if organizations want to thrive. As breaches and incidents continue to rise, even with the best solutions, protection is a step behind by solving yesterday's issues.

Uncover a breach that has been active for months? Your detect-and-remediate solution will allow you to address the problem—eventually—but it depletes time and resources, and still does not undo the sensitive data leak.

Reactive, perimeter-based security is not a strategy. And it's not working...

- New malware variants emerge daily, constant patching and updating of attack signatures would have to be perfect and immediate to wholly protect.
- Traditional cybersecurity products and services protect the perimeter of the network, but these on-premises products often fail because they aren't located where the data, devices or users are.
- Attacks often start with people, through social engineering schemes like phishing emails that exploit human behavior, rather than technology. Traditional security products cannot change the way we operate online.

...especially now.

As HCOs quickly adopted work from home practices, digital transformation projects accelerated to cater to the distributed workforce and expanded the attack surface. IT teams had no choice but to force security to the backseat as hastened deployments required favoring operability over protection, which created security gaps and further increased cyber risk.

93% of healthcare organizations reported having some employees working remotely.[7]

2020 Healthcare Attacks

655 incidents, 427 with confirmed data disclosure[8]

Data Compromised

77% Personal · 67% Medical
18% Other · 18% Credentials

7 https://www.intelligentcio.com/north-america/2021/05/04/study-shows-future-of-healthcare-is-shaped-by-hybrid-cloud/
8 https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Stop defending the perimeter.
Relocate and isolate the target.

Rather than continuing with old practices that rely on on-premises proxies to block sites that are either known to be malicious or are considered bad for productivity, new cloud-based security solutions and frameworks are available to not only protect online work, but serve as business enablers.

Given the recent architecture changes and move to work in the cloud, now is the time for HCOs to take full advantage to dig out of the difficulties created by the pandemic. By moving security closer to the user and delivering security services via the cloud, HCOs can begin to proactively protect systems and data across the network at scale, including edge and Internet of Medical Things (IoMT) devices all with transparent security that doesn't impact the user experience.

Zero Trust eliminates malware for good.

HCOS can isolate users from risky online resources, including the most exploited vectors: phishing emails, malicious websites and infected downloads.

Using a proactive approach with Zero Trust, you can protect from malware, ransomware, spyware, and zero-day attacks 100% of the time.

The concept of a Zero Trust approach assumes that all traffic—inbound and outbound—is inherently bad. Because it cannot be "trusted," isolation-based security solutions separate content and users, while still providing the expected end user experience and protecting productivity and business continuity.

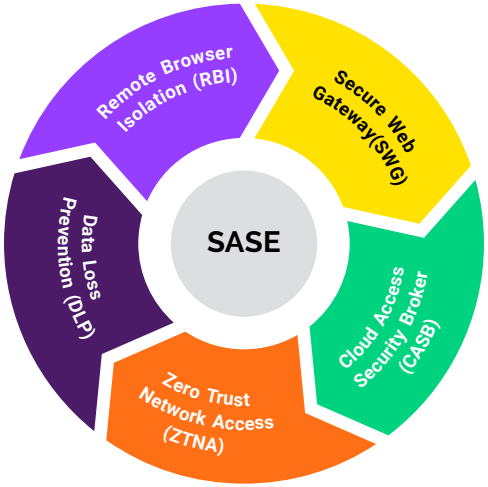
- Inbound traffic: content is cleaned and safely delivered from the cloud to the user's browser
- Outbound traffic: a least-privileged approach supported by continuous authentication, authorization, and risk evaluation for every request ensures users are granted limited access so they only touch what they need

To provide new work-from-home employees with access to IT resources, healthcare increased its investment in cloud.

56%
Public cloud[9]

51%
Hybrid cloud[10]

46%
Private cloud[11]



"A logical starting point for the journey to SASE is focusing on eliminating attacks on users with an emphasis on where they spend the most of their working day–in a web browser."[12]

— Enterprise Strategy Group

Foundational elements for a secure cloud.

As HCOs increased work-from-home, people, data, devices, and applications went "everywhere," sparking IT teams to use VPNs to provide access and mitigate risks. Unfortunately, many quickly found that VPNs didn't scale efficiently and resulted in bottlenecks, hampered productivity, and compromised security.

While many HCOs signed up for the long list of cloud transformation promises, to actually reap the benefits of cloud-first operations requires being "security first." Because of this, many HCO's moving to the cloud are turning to a secure access service edge (SASE) framework.

SASE tightly integrates software-defined wide area networking (SD-WAN) capabilities with network security functions and meshes with connectivity like 5G to build a framework for dynamic and secure access.

No SASE without SWG

Despite SASE being the latest trendy acronym in security, it relies on a time-tested technology: secure web gateways (SWG).

SWGs are proxies that block unsecured malicious traffic from coming out of or going into an organization's network to shield users from web-based threats. But today's cloud-based SWGs are a far cry from the traditional on-premise proxies still in use today. Offering scalability with minimal effort and allowing users to connect securely to the Internet no matter where they are working or from what device, cloud-based SWGs are better matched for the current operations and security needs of HCOs.

9 https://www.intelligentcio.com/north-america/2021/05/04/study-shows-future-of-healthcare-is-shaped-by-hybrid-cloud/
10 https://www.intelligentcio.com/north-america/2021/05/04/study-shows-future-of-healthcare-is-shaped-by-hybrid-cloud/
11 https://www.intelligentcio.com/north-america/2021/05/04/study-shows-future-of-healthcare-is-shaped-by-hybrid-cloud/
12 https://resources.menlosecurity.com/white-papers/a-pragmatic-path-to-sase-with-menlo-security

Isolate all work.
No matter the device or location.

Much like the cloud, today, remote and mobile connectivity are central to day-to-day operations. The concern is that HCOs don't issue all devices and don't have total control over the networks managed and unmanaged devices connect to.

Despite the significance of mobile and remote access, growing scale of regulatory penalties, and patient and employee sensitivity to data breaches, security is often shirked for the sake of efficiency.

Whether it is a contractor recording patient data on a BYOD tablet or an exhausted resident clicking a link in their email from their smartphone at home, bad actors have honed in on unmanaged and unknown devices both inside and outside of the network as a treasure trove of data and vulnerabilities.

And *when* breaches occur, the experience is not one of mere inconvenience. It ripples through the environment, disrupting everything in its path from the patient experience, productivity, operations, and brand trust.

Everywhere threats go, eliminate them.

SWGs with isolation aren't just for inside the network on corporate-issued devices—it goes where the threats go. As the number of end users accessing web applications via mobile devices continues to increase, isolation provides a way to eliminate the possibility malware might be downloaded (especially by that weary resident that falls for a phishing scheme) by keeping everything in the cloud and off the device. And while doing this, security remains invisible to ensure a seamless user experience.

SWGs work for everyone, not just employees. Securely enable contractor devices to access your network for greater attack prevention.

85% of HCOs

report that within five years, mobile will be their primary means of accessing cloud-based services.[13]

of healthcare organizations admit to going around mobile security measures. And those organizations were nearly twice as likely to experience a compromise than those that did not sacrifice mobile security.[14]

13 https://www.verizon.com/business/resources/reports/mobile-security-index/2021/foreword/
14 https://www.verizon.com/business/resources/reports/mobile-security-index/2021/foreword/

Prevent the expected.

Epidemiologists predicted another pandemic, much like security experts expect new and sophisticated cyberattacks to target the healthcare industry. And for both, the outcomes are largely dependent on the coordinated prevention methods.

For HCOs, cloud-based SWGs are the first place to start to make online work a safe space for everyone accessing your assets, whether on a managed or unmanaged device, while also enabling virtual health for better patient outcomes. Instead of simply moving your existing security stack to the cloud, cloud-based SWGs act as the central aggregation point through which all traffic flows, while providing full visibility into traffic—all without adding latency.

5 cloud-based SWG must haves

While HCOs were thrown into abrupt shifts in work and technologies, distributed workforces that need unfettered access to the Internet will always be here in some capacity. So finding the right cloud-based SWG to accommodate modern workforce requirements is key. When evaluating your options, consider these five must haves:

1 Global elasticity

Patients, providers, and other healthcare workers can now be anywhere in the world. Ensure that your cloud-based SWG allows you to scale wherever they are through the cloud at the press of a button. That means no provisioning, additional configurations, calling vendors, or new contracts.

2 Single point of control

Through a single management console security teams should have centralized control and visibility into who the user is, what they are trying to access, and what groups they belong to. With this information security teams should then be able to apply security policies to any or all users instantly, and enable web security for hundreds of thousands of users in short order.

3 Works with existing and future environments

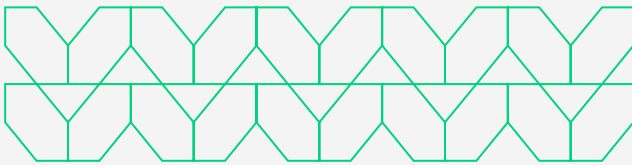
Adopting a cloud-based SWG doesn't mean your on-premises solution is completely obsolete. Be sure to find a solution that works with your existing infrastructure and is adaptable as your organization, or world around it, evolves.

4 Preserves the user experience

The best security is one that users don't go around, is transparent, and even improves productivity. When evaluating a cloud-based SWG, check that it meets these standards and doesn't have any latency or lag, while also supporting and fully securing all kinds of documents, electronic health records, videos, etc.

5 Leverages Zero Trust to eliminate malware

A primary reason to adopt a cloud-based SWG is threat prevention. As we have already seen, attacks like ransomware can bypass legacy SWGs and dramatically impact the ability to care for patients. Before adopting a cloud-based SWG, ensure that it takes a Zero Trust approach to eliminating malware through technology like isolation, which creates a protective layer around users as they navigate the web, blocking not only known and existing threats but unknown and future threats as well.



Malware shouldn't stop hearts in the hospital, or out.

Hospitals hit with ransomware were suddenly locked out of systems fundamental to providing critical care to cardiac patients, while giving a figurative heart attack to the security team.

It's time to make this a memory.

HCOs already rally around the goal of bettering wellness. So why not expand the definition of wellness to include patient data, overall security, and the well-being of security teams that support it all?

The Menlo Security Cloud Platform powered by an Elastic Isolation Core™ ensures HCOs can reach their goals and eliminate malware, ransomware, and zero-day attacks without overburdening security analysts or creating bottlenecks.

Completely secure work from online threats.

Menlo's SWG delivers 100% security by using an isolation-by-default approach so that all web and email traffic is automatically isolated in a remote browser in the cloud—cutting off any access to endpoint devices.

Boost productivity, don't stifle it.

Menlo's Adaptive Clientless Rendering™ (ACR) technology efficiently delivers authorized content to the end user's browser with no impact on user experience or productivity, and with no need for special client software or plug-ins. Security is invisible, operating in the background while essential workers go full-speed ahead.

Free security ops teams from constant threat response.

The Menlo Security SWG allows HCOs to employ an isolate or isolate-read-only policy instead of the standard block policy, resulting in a truly preventive approach to security, as opposed to the reactive stance that organizations take by focusing on detection and response.

Outsmart and outpace adversaries

The Menlo Security SWG powered by an Elastic Isolation Core™ converges all SWG capabilities into a single cloud native platform—including CASB, DLP, RBI, Proxy, FWaaS, and Private Access—to provide extensible APIs and a single interface for policy management, reporting, and threat analytics. As the only solution to deliver on the promise of the secure access service edge (SASE), Menlo provides the most secure Zero Trust approach to preventing malicious attacks, by making security invisible to end users while they work online, and by removing the operational burden for security teams.

Stop ransomware, malware and zero days across your HCO now.

Put an end to the threats posed by phishing, ransomware, and malicious websites, protecting productivity for all users.

menlosecurity.com/secure-web-gateway

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

MENLO SECURITY