#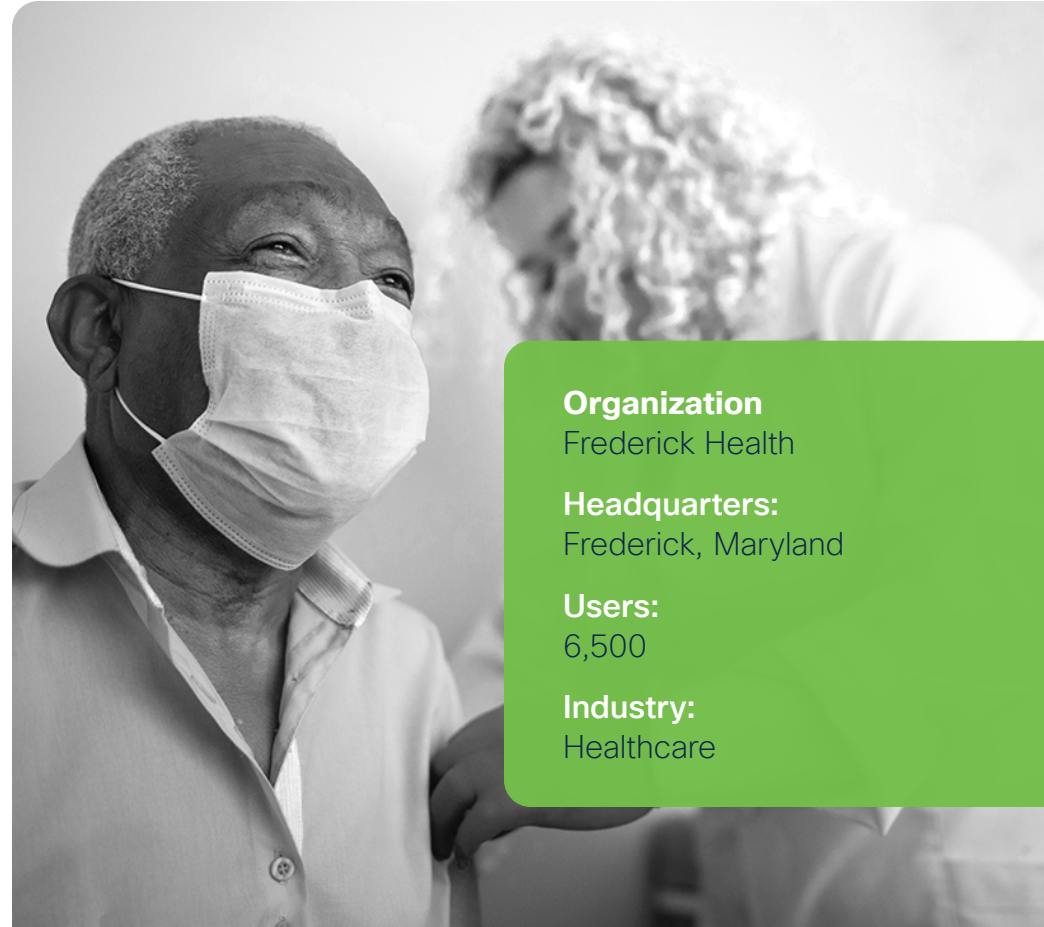 How Maryland's leading healthcare provider has adopted a SASE approach to improve security and build patient trust with Cisco Umbrella

Organization
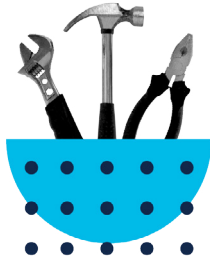Frederick Health

Headquarters:
Frederick, Maryland

Users:
6,500

Industry:
Healthcare

Objective

In an increasingly remote environment, protecting roaming users at distributed locations was a challenge for Frederick Health. To boost security protection on and off the network, safeguard patient data and address the complex access needs of the healthcare system's environment, Frederick Health opted for a SASE approach acquiring DNS-layer security, as well as secure web gateway and firewall functionality delivered from a single cloud security service.

Solution

Cisco Umbrella

Cisco Secure Email

Cisco SecureX

Impact

- Reduced alerts from antivirus and IPS solutions by at least 50%

- Protected users' web activity regardless of location by enabling the secure web gateway (full proxy for all traffic)

- Gained application visibility and control with layer 7 firewall to implement granular controls around granting access to users

- Improved management of web policies

Challenge

Reimaging security for a dynamic and complex healthcare environment

As the leading healthcare provider in Frederick County, Maryland, Frederick Health has expanded over the last two decades to keep pace with the 40% population increase. In addition to operating a hospital, the organization offers a network of primary care and specialty providers at more than a dozen locations. Recognized by the College of Healthcare Information Management Executives as one of the country's "Digital Health Most Wired" hospitals for several years, Frederick Health strives to use cutting-edge technology to better serve its patients.

With a growing number of remote users at distributed locations, boosting Frederick Health's security posture is a top challenge. "When you have more and more remote users, it's very hard to maintain visibility and control," a Frederick Health IT security analyst, shares. "Especially during the pandemic, with more employees working from home and remote locations, we needed additional layers of protection."

"Managing granular policies and proper access rights was a big challenge from the beginning," the IT security analyst says. "As a healthcare system, we're always concerned about HIPAA violations and personally identifiable information going out or being shared somewhere. This makes our environment hard to manage because some users need access to our storage or cloud storage environment, while most of the users do not." Frederick Health needed a secure and efficient solution at the cloud edge (SASE) that could provide granular controls for users no matter where they connect from. Frederick Health turned to Cisco to provide a secure access service edge (SASE) architecture to address these challenges.

> "As a healthcare system, we're always concerned about HIPAA violations and personally identifiable information going out or being shared somewhere."
>
> **IT Security Analyst, Frederick Health**

Frederick Health

Solution

The road to direct internet access

When Frederick Health decided to move to direct internet access (DIA), it needed to secure the DIA breakouts with a full proxy and protect internet activity regardless of location—from headquarters and branch offices to roaming devices. To support this move, Frederick Health chose Cisco Umbrella as a replacement for its previous on-prem proxy solution.

"We looked at the holistic Cisco portfolio today and where Cisco was going in terms of security going forward. It became clear that Umbrella was the right product for us, particularly its secure web gateway and cloud-delivered firewall functionality. The integrations Umbrella has with some of our existing solutions made our decision easier," a senior network engineer at Frederick Health says "Umbrella is a lot easier to manage than our previous proxy solution, especially when it comes to managing policies and granting access to users."

Frederick Memorial had integrated several Cisco solutions — Umbrella and Secure Email into the threat response feature of Cisco SecureX, which automatically aggregates data and threat intelligence from multiple security tools into a single console to accelerate investigations.

The reputation and efficacy of Cisco Talos also impressed the Frederick Health team. "The threat intelligence Talos provides is amazing," the senior network engineer shares. "Being able to restrict specific access for some users is also a win."

> "It became clear that Umbrella was the right product for us, particularly its secure web gateway and cloud-delivered firewall functionality. The integrations Umbrella has with some of our existing solutions made our decision easier."
>
> IT Security Analyst, Frederick Health

SECURE

Solution

The team saw additional value in the deployment simplicity of Umbrella's secure web gateway via Cisco AnyConnect for enabling full proxy for all traffic; protecting roaming users; and reducing risk by efficiently logging, inspecting, and controlling web traffic. "The last time I was researching, about a year ago, there were not that many products that would provide agent-based protection for remote users at exactly the same level as you would have for an on-premises environment," shared by the senior network engineer. "The Umbrella roaming module on AnyConnect gives us that confidence for remote users."

Another Cisco Umbrella feature that the networking team appreciates is the cloud-delivered firewall, which provides visibility and control for outbound internet

traffic across all ports and protocols. Umbrella logs all activity and uses IP, port, and protocol rules to block unwanted traffic. "The Layer 7 app control—the ability to control each application individually—is amazing functionality," he says. "We could not do this before we implemented Umbrella."

In addition, Frederick Memorial is actively involved in testing and sharing feedback on emerging features. "We've been fully participating in the rules-based web policies beta and helping develop those features. This capability makes Umbrella a unique solution," the IT security analyst notes. "We have a wonderful Customer Success team, and they've been doing a great job. They have taken all of our requests and made sure that everything we asked was implemented."

> "The Layer 7 app control—the ability to control each application individually—is amazing functionality. We could not do this before we implemented Umbrella."
>
> IT Security Analyst, Frederick Health

Results

Stopping threats before they get through the door

By efficiently logging, inspecting, and controlling web traffic—as well as blocking risky applications and user behavior—Frederick Health can better mitigate compliance and privacy risks.

Prior to having Umbrella, Frederick Health's security team received two to three legitimate malware alerts every day. "After we deployed Umbrella, we noticed a dramatic reduction in alerts on our other security solutions—by 50% or more," the senior network engineer notes. "Ever since we implemented Umbrella, threats aren't getting through anymore." Not only is Cisco Umbrella stopping threats before they enter the environment, but the reduction in alerts from antivirus and intrusion prevention tools filters out the noise, freeing up the team's time to focus on more sophisticated threats.

"If you think about securing your house from a burglar, you want to stop them before they even enter your home. Most of the other competing secure web gateways would let threats get into the network and then fight them inside, but Umbrella stops the threats before they even get in, and that's a big difference," he says. "You can't ask for anything better than that."

Cisco gives Frederick Health much more than confidence in security and the ability to protect remote users and meet HIPAA compliance requirements. "It's not just about improving security. It's also about giving people in our community the confidence to trust us with the information they're giving us, especially with all the prevalent ransomware and everything that's happening in the world today," the senior network engineer says. "The fact we've been using Umbrella and nothing has happened so far has given our community peace of mind and the confidence to come back to our facility for their healthcare needs."

> "After we deployed Umbrella, we noticed a dramatic reduction in alerts—by 50% or more. Ever since we implemented Umbrella, threats aren't getting through anymore."
>
> Senior Network Engineer, Frederick Health