CASE STUDY

FortiSASE Secures Remote Employee's Data and Long Beach's Most Vulnerable Residents

In Long Beach, California, in the 1940s, mental health help was hard to find. Families had a variety of problems, and children were often caught in the middle. Some students went to local schools anxious, fearful, or even aggressive. But for lower-income residents, assistance with these issues was usually out of reach.

That is why a visionary group of public-school teachers and counselors founded The Guidance Center. Now, more than 70 years later, the nonprofit agency provides evidence-based mental health services to disadvantaged children in the local community. The program's services have been highly successful through the years in helping improve local kids' mental health.

Behind the scenes, the three-person IT team abides by its own equivalent of the Hippocratic Oath. "If our data were compromised, that would have a significant impact on our clients and our reputation," says Ian Adduru, IT Director. "We must do whatever it takes to protect the data we collect. They come to us for help and it is our responsibility to protect them."

The New Remote Worker Environment Introduces Risk

When the COVID-19 pandemic arrived, most of The Guidance Center's staff began working from home. The organization was already using mostly cloud-based clinical applications like Microsoft 365 for cloud communications and file storage. "We do not have a local server store data anymore," Adduru says. "We have pushed more and more data to the cloud, because that is where the future lies." But at the time, employees were safely behind the office's firewall. Now, Adduru's lean team was suddenly responsible for securing 200 remote workers, their data, and the network traffic they required to do their jobs.

"The key challenge with remote work is that it can be difficult to secure users' connections," Adduru says. "We initially worried that staff would work from public Wi-Fi somewhere like a coffee shop." Fears of unencrypted data shared over public Wi-Fi led to his team turning off Wi-Fi on all the organization's client machines. "We required every employee—even the CEO—to plug in with an Ethernet cord. Everyone wanted Wi-Fi, but we could not risk allowing them to work from an unsecure connection."

Lessons Learned Searching for a Solution

What The Guidance Center needed was a solution that would encrypt data from the laptop to the cloud and ensure proper security was being enforced as that data traveled. In fact, this was not just a nice-to-have: The Mental Health Services Division of the California Department of Health Care Services requires encryption of patient data, both on local systems and in transit. "We needed to make sure that wherever staff may go to use Wi-Fi, their data would be encrypted," Adduru

"I know our environment is secure. I made our end users sign an agreement that they would not connect in public places. But even if they do, I am confident our remote users' internet access is going to be secure even over public Wi-Fi with FortiSASE".

– Ian Adduru, IT Director,
The Guidance Center

Details

Customer: The Guidance Center

Industry: Healthcare

Location: Long Beach, California

Number of endpoints: 200

Business Impact

- High performance and user experience while enabling enterprise-grade security delivered from the cloud to remote users
- Encryption of data in transit meets compliance requirements of California Department of Health Care Services

explains. "Any Wi-Fi is going to get hacked because it is out in the open. But if we keep the data encrypted, the attacker cannot access our PII [personally identifiable information]."

The Guidance Center considered a proposal from a managed service provider (MSP) that would have installed a larger firewall at headquarters. "But it did not make sense for our remote users' cloud connectivity to rely on our building," Adduru says. "That would create a single point of failure: If our building suddenly lost power, for example, all access would shut off."

Instead, the organization decided to deploy a secure access service edge, or SASE, solution. Adduru talked to two different vendors that claimed to offer what he wanted. "Both promised they would encrypt our traffic," he says. "For one, when I looked at their IPsec connections, I saw that rather than encrypting, they were just changing the DNS. The other one defaulted to encryption but provided a backdoor for users to avoid the encryption. The vendor denied this, but we discovered it during testing. For each of these projects, we spent some money and more than a month deploying, only to find out in testing that they did not work the way the vendors said they did."

That is when Adduru discovered Fortinet's approach to quick and easy remote security, FortiSASE, a firewall-as-a-service, maintained by Fortinet so customers only have to implement and maintain their policies like web security and application controls. Adduru's team thoroughly tested FortiSASE, and they were pleased with the results.

FortiClient: Trusted Encryption

Adduru's team deployed FortiClient endpoint protection on the laptop of each clinician and staff member. Whenever a user connects to a cloud application, his or her system establishes an encrypted tunnel to FortiSASE, which then establishes a secure Hypertext Transfer Protocol Secure (HTTPS) connection to the SaaS solution.

"Fortinet truly encrypts data, and users cannot bypass it to establish unsecure Wi-Fi connections," hAdduru says. "FortiClient establishes a VPN connection from the user's device to the FortiSASE network, which maintains and enforces security as it moves through the internet. Our testing revealed that with FortiSASE, we could confidently answer 'yes' when the Department of Mental Health asks whether our data is encrypted in transmission."

FortiSASE: High-Performance, Cloud-based Firewall-as-a-Service

"Performance was one of my main concerns before we deployed," Adduru says. "I thought that having people connect to SaaS apps through FortiSASE might bog down their connection. But other than 'don't block my YouTube' type comments, we have received no feedback. It is like our end users do not even notice the security solution is there, which means it is working perfectly."

The as-a-service part of the solution also sat extremely well for Adduru and team: "FortiSASE is easier to manage and patch than on-premises firewalls because FortiSASE is in the cloud. Fortinet patches the equipment. If we had to add a physical security device in each individual's office, managing those devices would take a huge amount of time," Adduru points out. "Any time the vendor decided the devices were outdated, we would need to roll out new updates and new devices."

Finally, the ease of user segmentation further secures and creates a more efficient network for the IT team. "At one point, we blocked YouTube, and everybody was calling IT to complain," Adduru says. "But we do not want people using their Guidance Center laptops for entertainment and personal use. Some users do have a legitimate need to access certain sites. For example, HR and marketing may need access to social media. FortiSASE makes it easy to place them in a separate group and properly manage their restrictions vs. other groups."

Business Impact (contd.)

- IT team and senior management have confidence they are effectively protecting the data of the community's disadvantaged children

Solutions

- FortiSASE
- FortiClient

"Performance was one of my main concerns before we deployed, but we have received no feedback. It is like our end users do not even notice the security solution is there, which means it is working perfectly."

– Ian Adduru, IT Director,
The Guidance Center

Ultimately, Adduru estimates, the total cost of ownership for FortiSASE is less than half that of other solutions The Guidance Center considered. And unless it is blocking a site they shouldn't have access to, it has proven transparent to the organization's end users.

Most important, Adduru concludes, "I know our environment is secure. I made our end users sign an agreement that they would not connect in public places like coffee shops or airports. But even if they do I am confident our remote users internet access is going to be secure even over public Wi-Fi with FortiSASE." For an organization charged with protecting some of the community's most vulnerable people, that confidence is mission-critical.

www.fortinet.com

October 31, 2022 4:47 PM

123456-0-0-EN