CUSTOMER CASE STUDY

UNIVERSAL MH/DD/SAS "Caring People, Caring for People"

UNIVERSAL MENTAL HEALTH SERVICES (UMHS)

Eliminates Branch Firewalls

Leslie W. Cothren,
Information Technology Director at UMHS

Background

UMHS is dedicated to helping individuals and families affected by mental illness, developmental disabilities and substance abuse in achieving their full potential to live, work and grow in the community

The organization is a comprehensive community human service organization based in North Carolina that strives to provide integrated and quality services to its clients. UMHS is nationally accredited by the Commission on Accreditation of Rehabilitation Facilities (CARF) International and it has 13 locations, with a total of approximately 900 employees.

Challenge

UMHS network was originally designed to have all 12 branches connected via MPLS and backhauling to a primary datacenter with one central firewall. However, after the process began, UMHS realized that MPLS was too expensive to deploy in all locations. Additionally, some locations were outside of the MPLS provider's service area. This then forced the organization to connect 5 branches via SonicWALL Firewalls with site-to-site VPN's. This resulted in a mesh of two network architectures that was more complex to run and manage.

Running this environment proved to be challenging, especially due to the burdens of updating the hardware and maintaining firewall software. It was labor intensive and updates didn't always go smoothly. "Specifically I remember updating the firmware on some devices that caused us to lose connectivity. This created a disruption in our record keeping as our branches send key reports directly to our headquarters. Employees generally scan records using copiers, and those records are then stored directly into the appropriate folder at corporate. Additionally, because we deal with sensitive issues like abuse and drug use, employees need free access to internet resources. Policy management was difficult because SonicWALL does not offer agile options to balance the blocking of banned websites while still providing access to necessary information".

Solution

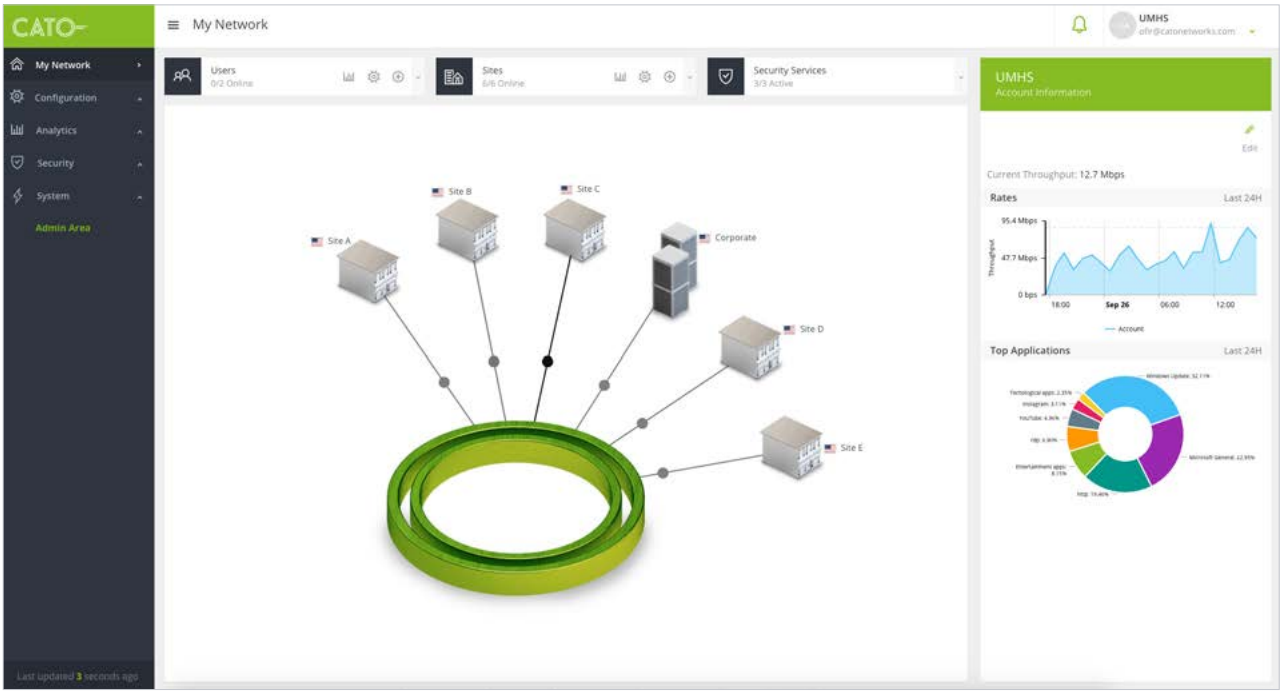
UMHS came across Cato opportunistically. “I was at an industry event, and there was a quite a bit of excitement around Cato’s booth and its services. I decided to visit the booth to see what the buzz was all about.” After a thorough review of the services, UMHS selected Cato to replace all of its SonicWall Firewalls.

The first step was to establish an IPSEC tunnel to Cato from the datacenter firewall. Than, each branch location had a Cato Socket replace the SonicWalls firewalls.

Now connected to the Cato network, UMHS has eliminated connectivity issues, saved money and simplified its policy management. Cato protects all connected locations and seamlessly scales to secure all traffic, without the need for unplanned hardware upgrades and resource-intensive software patches. It also coexists with the MPLS-based network.

As a healthcare organization, security and agility are two of the biggest drivers when it comes to providing good customer service. With Cato, UMHS is now armed with the ability to clearly see all network traffic and application usage, create policies and enforce them across all branches, and identify security gaps and policy violations. Cato has given the organization a completely new perspective on how easy network security can be.

“Transitioning to Cato was so easy. I joke that it was like pressing the Staples’ Easy Button. Cato gave me the Sockets and set up the static IP addresses, I plugged them in and things just started working. Setup took about five minutes at each location.”



Future Plans

UMHS is so satisfied with the decision to switch its firewalls to Cato that it plans to migrate all locations using MPLS as soon as their contracts expire. A cost analysis done by the organization shows that this change will save thousands of dollars by having all of its 13 locations connected to the Cato Cloud.

About Cato

Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data.

The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure Internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures into the enterprise network. Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.

For more information:

www.CatoNetworks.com

@CatoNetworks

Where do you want to start?

SECURE AND OPTIMIZED SD-WAN

SLA-BACKED, AFFORDABLE WAN

SECURE DIRECT INTERNET ACCESS

APPLIANCE ELIMINATION

HYBRID CLOUD NETWORK INTEGRATION

MOBILE WORKFORCE, SECURE CLOUD ACCESS