The Kahan Center
FOR PAIN MANAGEMENT

Private Healthcare Practice Ramps Up Secure Telehealth Services While Remaining Compliant

The Kahan Center for Pain Management in Annapolis, Maryland serves the greater Baltimore and Washington Metro areas. Offering the most advanced treatment in pain medicine and management available, their core focus is to improve their patients' quality of life, taking a whole-body approach. Brian Kahan, D.O., has owned the healthcare practice for 22 years, and also manages their IT department and IT vendor relationships to keep his systems up and running smoothly and securely.

Executive Summary

▶ **Company**
- The Kahan Center for Pain Management

▶ **Industry**
- Healthcare

▶ **Solution**
- Pulse Access Suite Plus
- Pulse Connect Secure (PCS)

▶ **Challenge**
- Continue secure remote access with increased use of telehealth services

▶ **Results**
- Comprehensive and continuous endpoint security posture assessments for both mobile and desktop devices to ensure security during expanded telehealth sessions

As a locally owned, specialized medical clinic, one might assume they don't require the technical infrastructure of a larger enterprise. Yet, with the advancements and acceptance of practices like telehealth and telemedicine, smaller operations like The Kahan Center can take advantage of the many benefits experienced by their larger counterparts.

With the need to protect patient records due to compliance mandates like HIPAA, and the constant threat of ransomware, patient data breaches, and increased need for securing remote work, Dr. Kahan and his team know they have to stay vigilant in protecting their threat landscape. Dr. Kahan explains a little on his experience as a Pulse user, and growing his Pulse Secure footprint:

> *"We found out about Pulse around 10 years ago through our IT department. We started off as a small practice and as we grew, we needed a server. When we finally migrated to a server that required remote hosting and having people log into servers from different areas, we looked into how to make it secure. How are we going to support a VPN? And that's where we found Pulse. We've migrated to the cloud since then, and so we're still using Pulse Secure to be our VPN to log in to the cloud and do everything from remote destinations."*

By moving to a cloud infrastructure in Microsoft Azure, The Kahan Center is able to adapt their secure access framework to support their evolving environments while maintaining the same user experience, compliance, and performance capabilities. Pulse appliances, deployed within Azure offer the following features:

- Always-on and application-specific VPN with lockdown
- Split-VPN tunneling
- Single-sign on (SSO) interoperability
- Unified operational visibility
- Device compliance checking
- Integrated enterprise mobility management
- Rich user and device auditing
- Multifactorial authentication

⟨S⟩ Pulse Secure®

Healthcare in the Crosshairs

In 2019, the healthcare sector saw a jaw-dropping 41.4 million patient records breached in 572 attacks, fueled by a 49% increase in hacking according to the Protenus Breach Barometer who analyze breaches reported to the Department of Health and Human Services, the media, or other sources. And just in October, 2020, Universal Health Services, one of the largest U.S. health systems suffered a ransomware attack that affected all of it's U.S. care sites and hospitals. Furthermore, data from the Ponemon Institute shows that the number of small and medium-sized business that experienced data breaches increased to 63% in 2019.

41.4M
Patient record breached

49%
Increase in hacking

As a potentially attractive target to bad actors, Dr. Kahan knows he must work diligently to stay ahead of any potential compromise. And, as a security-conscious vertical, with stringent requirements, he needs an always-on VPN, continuous posture assessments, and compliance to the various data regulatory bodies such as HIPAA for the management of his electronic health records (EHR).

While staying compliant is one thing, another key assertion is the difference between meeting regulatory compliance and bolstering security. While a company may diligently adhere to certain geographical and empirical mandates and standards, it is by no means a surety that a company is impervious to an attack.

When the restrictions and limitations of in-person visits began due to Covid-19, Dr. Kahan and his team had to thoroughly assess their network and security posture, and what was needed to harden their position as end-users started working remotely:

> *"We had to make sure that we were secure because our electronic medical record programs are hosted on the cloud. We've had our own experiences with ransomware attacks so that was really important. That kind of changed things too and over the last seven months that we've been working on this, we've had to really secure our infrastructure and make sure that we were not susceptible to any risk. Sadly, a lot of healthcare facilities are getting hit; that seems to be a hot item right now."*

Telehealth and Telemedicine Gets Ready for Primetime

With the arrival of a global pandemic and the resultant stay-at-home orders instituted across the country, physicians and medical teams turned to telemedicine and/or telehealth to communicate and stay connected with their patients. Having the ability for real-time, face-to-face audio/video communication allows patients and their doctors to connect from remote locations.

Telehealth is a bit different than telemedicine in that it refers to a broader scope of remote heath care services including non-clinical services, while telemedicine refers specifically to remote clinical services. The American Medical Association outlines some areas where telemedicine can offer new ways to deliver care including:

- Real-time, audio-video communication tools (telehealth) that connect physicians and patients in different locations.
- Store-and-forward technologies that collect images and data to be transmitted and interpreted later.
- Remote patient-monitoring tools such as blood pressure monitors, Bluetooth-enabled digital scales and other wearable devices that can communicate biometric data for review (which may involve the use of mobile health apps).
- Verbal/Audio-only and virtual check-ins via patient portals, messaging technologies, etc.

As a top target for cyberattacks, Dr. Kahan knows he needs to apply rigorous controls to accommodate all the different types of users according to their privileges by role and from different locations. The need to apply access privilege management capabilities ensures users only have access to those resources that are deemed necessary for that session, according to administrator-defined policies.

When users log into Pulse Connect Secure, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings.

As such, Pulse Secure's security framework helps extend visibility across users, locations, networks, and devices to enable consistent policies across the Kahan's Center's network and cloud resources. The ability to automatically detect and to continuously profile both managed and agentless devices on his network allows Dr. Kahan to provide secure remote access while serving his patients.

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites and a SaaS platform that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 24,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

in   linkedin.com/company/pulse-secure

f   www.facebook.com/pulsesecure1

twitter.com/PulseSecure

@   info@pulsesecure.net