MEDIGATE

AT A GLANCE

Eliminating the Telehealth Blindspot

Keeping Telehealth Devices and Patient Data Safe

Recent events have accelerated telehealth adoption by almost a decade. A recent report by Frost and Sullivan predicts that telehealth "uptake will increase by 64.3% nationwide this year." While improving the convenience and reach of care, telemedicine is also increasing the attack surface of healthcare delivery providers (HDOs). Every device that is used for telemedicine or has a telehealth application on it – from desktops to iPads and smartphones – is now a potential target for attackers. The sensitive personal health information (PHI) these devices have access to during the course of consults and the delivery of care is extremely valuable – medical data can go for as much as $1000 per record on the black market. It is imperative these telehealth devices are part of the HDO's larger security and compliance strategies to ensure patient data and care is effectively protected.

The Telehealth Blindspot

The problem is many of these devices are not managed by the HDO. Many have been rolled out to meet immediate needs, without considering the security impacts. Often IT and security teams are not even consulted, creating a huge blind spot around the presence of telehealth and telemedicine within the organization. Most hospitals have no idea what devices are being used to deliver these services and certainly have not implemented policies to protect them. Medigate can help provide visibility and control over their implementation.

Medigate Delivers Visibility and Control for Telehealth

Medigate's Medical Device and Asset Management Platform helps HDOs identify telehealth apps and the devices that access the app so they can include them in their clinical asset management and cybersecurity programs.

Visibility

The Medigate Platform continuously monitors the network, using its unique deep packet inspection (DPI) to provide complete visibility into the telehealth devices, including personal (BYOD) clinician mobile phones tablets and other devices as well as applications in the network.

For all connected medical, IoT and telehealth devices, Medigate can deliver details on the manufacturer, make, model, operating system (OS), embedded software/applications, and protocols, as well as location and utilization information. As a result, HDOs can pinpoint all the devices with apps on them that might be used to deliver telehealth services, such as:

- Telehealth apps: Amwell (formerly American Well), MDLive, MedChat, and InTouch
- Clinical communication apps: Heartbeat
- Video Conferencing: Zoom, Vidyo, and Skype for Business

Once the devices and applications that are active in the network are identified, appropriate measures can be taken to keep them safe.

Compliance

Medigate can integrate with an HDO's mobile device management (MDM) platform to identify what is managed or unmanaged within the network. By comparing the devices identified by Medigate with the devices being managed by the MDM, Medigate can automatically highlight those that are unmanaged, as well as those that are out of compliance with the organization's policies. This enables HDOs to ensure every device being used to deliver telehealth services, including BYOD, is brought into the management and security fold.

Risk Management & Anomaly Detection

Medigate also analyzes device and network communications, as well as medical protocols and workflow patterns, to accurately detect anomalous behavior and identify threats in real time. Once detected, the risk can be mitigated via integrations with the MDM and other components of the HDO's security infrastructure (e.g. firewalls, network access controls, etc.) to automate enforcement.

For example, it can detect when a device doesn't have a lock screen and passcode and have the MDM push that implementation or provide the list of devices being used for telehealth and have the MDM lock down those apps so they can't be used outside the hospital. Or it can alert on activity outside of normal clinical communication patterns, such as a telemedicine app that's talking to a server outside the country – and automatically block that traffic via the firewall.