LogRhythm

Use Case

Securing Telehealth Systems and Patient Data

While telehealth has been around for a number of years, it gained significant traction during the global pandemic of 2020. As the number of affected individuals increased and uncertainty led to fear, the benefits of telehealth became clear. It enables at-risk populations to see physicians without endangering themselves or others. And telehealth can extend the reach of healthcare, particularly mental health services, to rural areas.

Unfortunately, the technology used to deliver telehealth can pose a security risk. As an IT system used to interface with patients, a telehealth solution handles real patient data, including personally identifiable information. The adoption of these technology solutions will only continue to increase, and healthcare organizations need to address the security concerns sooner rather than later.

The Challenge: Protecting Patient Data

The risk associated with telehealth comes down to protecting patients and their data. Telehealth exposure is similar to the risk of exfiltrated electronic health record (EHR) data—but now the following are also at risk: a patient's face (if it's video), pictures of the patient, what the patient's home or workplace looks like, children, etc. Telehealth systems provide additional data that will further increase the value of stolen EHR data, making it a prime target for cyberattackers.

Healthcare organizations also face regulatory compliance implications if they do not properly secure their telehealth systems and the data in them. Health Insurance Portability and Accountability Act (HIPAA) Breach Notification rule specifies a 500-record threshold of compromised individuals before the organization is required to report the breach within 60 days, make public statements, take out advertisements, and add banners to the website—all shining a light on the fact that patient data in the organization's care was breached. Any size of breach could be subject to fines depending on the circumstances of the breach and how quickly authorities are notified. It's therefore imperative that organizations have the ability to detect and respond to attacks in a timely manner.

Telehealth is not new. In fact, it's common for a large healthcare organization to have several telehealth initiatives running simultaneously. In a perfect world, these initiatives are consolidated under a single vendor. However, telehealth initiatives tend to spring up at various times, each outsourced to a different cloud or managed services provider. It's even likely that some of these initiatives are running without your approval or oversight. Uncovering these telehealth initiatives is the first challenge in protecting patient data.

The second challenge posed by telehealth solutions relates to the authentication and access controls used to access the technology. These systems are often set up with generic logins that don't tie back to the organization's core authentication structure. For example, the system access controls may be tied to the room rather than the individual user. As a result, the IT organization loses its ability to attribute a user back to the system, creating a nonrepudiation problem and potential regulatory compliance violation.

How to Gain Visibility and Control

Network monitoring provides the network and application visibility you need to address telehealth-related security risks. Whether the telehealth solutions are in the cloud or on-premises, the network and the services must be monitored in real-time from a centralized point. A security information and event management (SIEM) platform allows healthcare organizations to see the traffic flowing to and from all the systems in the IT environment and attribute traffic logs to cloud providers, enabling IT to identify the telehealth systems in use.

LogRhythm SIEM offers comprehensive, single pane-of-glass visibility into legacy systems and cloud-based solutions, including telehealth and telemedicine. LogRhythm can help bridge detection and response for security threats by correlating that with health records violations and other healthcare operational technology, such as medical devices and physical security. As a result, LogRhythm enables you to quickly respond to threats and prevent breaches of EHR data.

LogRhythm SIEM also monitors cloud services for alignment to compliance requirements. LogRhythm's prebuilt Health Care Compliance Automation Module provides a comprehensive security framework that helps protect your patients and improve your organization's security posture. The module features capabilities to help you comply with HIPAA and HITECH guidelines, including:

- Analysis rules built to monitor your environment, staff, and vendors for risks and policy violations associated with HIPAA and HITECH guidelines
- Investigation queries designed to answer and address key questions associated with investigations and regulatory requirements
- Prebuilt reports that directly map to HIPAA directives

When integrated with LogRhythm SIEM, LogRhythm NDR provides real-time visibility and security analytics you need to monitor your organization's entire network. LogRhythm NDR delivers rich data and deep insights to help you detect and investigate to advanced threats, including data extraction.

Confidently Secure Healthcare Data

LogRhythm knows healthcare. Our Health Care Compliance Automation Module and deep integrations with other health IT systems help take some of the challenges out of securing your healthcare systems and environments. We're also among ten technology providers and industry experts chosen to collaborate to participate in an initiative from the National Cybersecurity Center of Excellence — Securing Telehealth Remote Patient Monitoring Ecosystem. The project aims to provide a reference architecture that will address the security and privacy risks for healthcare delivery organizations leveraging telehealth capabilities. LogRhythm SIEM — along with LogRhythm NDR — will be core to the detection and response capabilities of the architecture.

To see how LogRhythm can help solve the unique challenges of securing telehealth systems, schedule a demo today.

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224

www.logrhythm.com