



BURKE
REHABILITATION
MONTEFIORE HEALTH SYSTEM



FALLSTUDIE

Burke Rehabilitation Hospital Erforscht Das Grosse Potenzial Von Armis Solutions

Armis beleuchtet mit dem Netzwerk verbundene Geräte im IT- und Klinikbereich und überwacht den Datenverkehr, um Patientendaten besser zu schützen

Kundenprofil

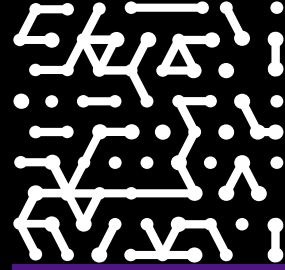
Anbieter von stationärer und ambulanter Rehabilitationsmedizin im Bundesstaat New York

Branche

Gesundheitswesen

IT-Umgebung

Das Burke Rehab Hospital hat einen Hauptstandort und 10 Satellitenstandorte in der Region. Die 1.100 Mitarbeiter der Organisation nutzen verwaltete Unternehmensgeräte, darunter verknüpfte medizinische Geräte, Server und Peripheriegeräte

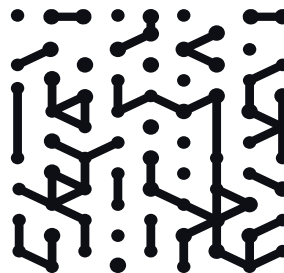


Einführung

Das Burke Rehab Hospital ist ein führender Anbieter von stationärer und ambulanter Rehabilitationspflege im Bundesstaat New York. Das Sicherheitsteam wusste, dass es seine Arbeit im Bereich der Netzwerksicherheit verbessern musste. Nach dem Einsatz von Armis konnte das Team den Einblick in die Geräte, die sich mit dem Netzwerk verbinden, erweitern, die Geräteauslastung im gesamten Unternehmen überwachen und den unverschlüsselten und verschlüsselten Datenverkehr sehen, um so zu erkennen und zu verhindern, dass Patientendaten exfiltriert werden. Burke Rehab entdeckt immer wieder neue Anwendungsfälle für Armis, die die Sicherheit verbessern und betriebliche Einblicke in das gesamte Unternehmen ermöglichen.

Das Burke Rehabilitation Hospital in White Plains, New York, ist Mitglied des Montefiore Health System-Netzwerks und gehört zu den führenden Einrichtungen für Rehabilitationsmedizin. Der seit über einem Jahrhundert tätige Gesundheitsdienstleister bietet seinen

Patienten stationäre Leistungen in seiner 150-Betten-Einrichtung für die Akutversorgung von Erwachsenen und ambulante Leistungen über ein ausgedehntes Netzwerk von Gesundheitseinrichtungen in der Region. Burke bietet Rehabilitationspflege für neurologische, muskuloskelettale, kardiale und pulmonale Erkrankungen an, die auf Krankheiten, Verletzungen oder Operationen zurückzuführen sind.



Sicherheitsteam setzt auf Armis zur Verbesserung der Netzwerksicherheit

Der Director of Network Operations and Security Brian Schultz, der seit 10 Jahren bei Burke Rehab arbeitet, ist immer auf der Suche nach innovativen und zuverlässigen Lösungen, um die Sicherheit der Organisation zu verbessern. Er ist eine praxisorientierte Führungskraft und leitet ein Team von 14 IT- und Sicherheitsexperten. Nachdem er eine Schulung des SANS-Instituts zum Thema Datenverkehr und Verhinderung von Eindringungsversuchen absolviert hatte, erfuhr er von Armis über einen Wiederverkäufer, der ihn über die vielen Fähigkeiten der Lösung informierte. Dieses Gespräch setzte die Weichen für einen Proof-of-Value (PoV) und den späteren Einsatz.

„Einer der Gründe, warum wir uns entschieden haben, Armis auszuprobieren, war, dass wir im Bereich der Netzwerksicherheit im Rückstand waren. Wir hatten keine Network Access Control (NAC)-Lösung – deren Implementierung wäre nur mit erheblichem Aufwand möglich gewesen – und wir hatten keinen Einblick in die Vorgänge im Netzwerk. Armis schien uns eine gute Alternative zu sein, weil wir damit sofort sehen konnten, was im Netzwerk vor sich ging“, sagt Schultz.

Warum „Packet Inspection“ unerlässlich ist

Schultz testete Armis gegen einen Konkurrenten und entdeckte, dass das konkurrierende Produkt nur Netzwerkdaten in Form von Logdateien lieferte, anstatt Netzwerkverkehrspakete zu untersuchen.

Die Armis Appliance hingegen befindet „out-of-band“ und nutzt Switch Port Analyzer (SPAN)-Ports, um den Datenverkehr passiv zu überwachen, ohne die Netzwerkleistung zu beeinträchtigen. Sie führt eine gründliche Paketuntersuchung durch und liefert Informationen über die Art des Datenverkehrs, der durch das Netzwerk fließt, einschließlich Anomalien und Identifizierung von verschlüsseltem und unverschlüsseltem Datenverkehr. Dies ist besonders wichtig im Gesundheitswesen, das strengen

Herausforderungen

- Keine Einsicht in die Geräte im Netzwerk
- Ausufernde Gerätevielfalt mit vielen klinischen Computergeräten, die wenig genutzt werden
- Mangelnde Fähigkeit, verdächtigen oder riskanten Datenverkehr zu erkennen, was zu einer schwachen Daten- und Netzwerksicherheit führt

Vorschriften zum Schutz der Patientendaten durch den Health Insurance Portability and Accountability Act (HIPAA) und anderer Behörden unterliegt. Armis kann zum Beispiel ein Gerät erkennen, das unverschlüsselte medizinische Bilder sendet. Es sendet dann eine Warnung an die Sicherheitsteams, damit sie weitere Maßnahmen ergreifen können, um das Risiko zu beseitigen.

„Wenn man Pakete sehen kann, ist das das Nonplusultra. Es macht keinen Sinn, sich Logdateien anzuschauen“, bemerkt Schultz. „Wir betrachten Armis als eine neue Möglichkeit, Einblicke in unser Netzwerk zu erhalten. Wir brauchen nur ein wenig Aufwand, um eine enorme Menge an Informationen zu erhalten. Vor Armis hätte der Aufwand, der nötig ist, um diese Daten zu sammeln, unsere Möglichkeiten überstiegen.“

Armis konzentriert sich auf IT und medizinische Geräte mit geringer Auslastung

Eine weitere wichtige IT-Initiative von Schultz ist die optimale Nutzung der Serverfarm. Er und sein Team nutzen Armis, um den Netzwerkverkehr auf den Servern im gesamten Unternehmen zu sehen und den Auslastungsgrad zu bestimmen. Mit diesen Informationen können sie Server, die nicht mehr benötigt werden, ausmustern. Vor Armis, so betont er, war es sehr zeitaufwändig, die Serverauslastung mit einem ihrer früheren Produkte zu überprüfen.

Als erfahrener Techniker, der sich intensiv mit den Abläufen im Hintergrund beschäftigt, weiß Schultz, dass Armis nützliche und kostensparende Informationen über die Geräteauslastung liefern kann. Das Armis-Team hat zum Beispiel eine Abfrage erstellt, mit der Schultz und sein Team sehen konnten, welche Vital Carts vom Klinikpersonal benutzt wurden. Vital Carts sind tragbare, digitale, mit dem Netzwerk verbundene Geräte, mit denen medizinisches Personal Patientendaten wie Blutdruck und Atemfrequenz erfassen kann. Diese Carts sind in der Regel mit Displays, Scannern und Druckern ausgestattet.

„Mit Armis konnten wir sehen, ob einige der Vital Carts, die in der Ecke zu verstauben schienen, tatsächlich benutzt wurden“, erklärt er.

Burke Rehab hat ein gemeinsam betriebenes Dienstmodell mit dem Netzwerk des Montefiore Hospitals und ist mit dem Netzwerk der

„Wir betrachten Armis als eine neue Möglichkeit, Einblicke in unser Netzwerk zu erhalten. Wir brauchen nur ein wenig Aufwand, um eine enorme Menge an Informationen zu erhalten. Vor Armis hätte der Aufwand, der nötig ist, um diese Daten zu sammeln, unsere Möglichkeiten überstiegen.“

Brian Schultz
Director of Network
Operations and Security
Burke Rehab Hospital



Mutterorganisation verbunden, um deren System für elektronische Patientenakten (EMR) zu nutzen. In diesem Zusammenhang bietet Armis einen Mehrwert, indem es ermittelt, wie effektiv die gemeinsam genutzten Geräte genutzt werden und wie hoch die Kosten sind.

Stärkere Sicherheit durch Schwachstellenerkennung und Integration mit Untersuchungstools

Armis hat auch bedeutende Apache Log4j-Schwachstellen in Java- Logging-Frameworks entdeckt. Diese Schwachstelle ermöglicht es Angreifern, einen Code aus der Ferne auf einem Zielgerät auszuführen, was bedeutet, dass sie Daten stehlen, Malware installieren oder die Kontrolle über das Gerät übernehmen können. Apache Log4j- Hacks sind besonders häufig bei medizinischen Geräten zu finden. Diese Schwachstelle hat die FDA sogar dazu veranlasst, dieses Problem bei den Herstellern von Medizinprodukten anzusprechen.

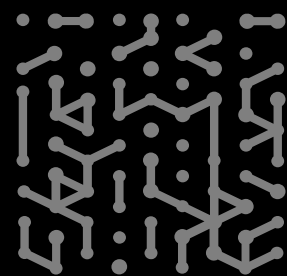
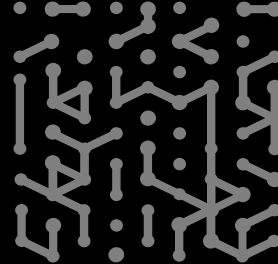
Schultz ist auch an grundlegenden Untersuchungen von Sicherheitsvorfällen beteiligt und nutzt zu diesem Zweck CrowdStrike. Während CrowdStrike zwar auf allen Geräten installiert ist, die Agenten verwenden können, gibt es dennoch blinde Flecken auf Geräten die keine Agenten verwenden können. Die Integration von CrowdStrike mit Armis hat zusätzliche Transparenz geschaffen und gründlichere Untersuchungen über einen größeren Querschnitt von Geräten ermöglicht.

Armis eröffnet Möglichkeiten für neue Anwendungsfälle

Schultz und sein Team befinden sich zwar noch in der Anfangsphase der Erforschung von Armis, aber sie sind sich bewusst, dass die potenziellen Anwendungsfälle für Armis nahezu grenzenlos sind. Derzeit konzentrieren sie sich darauf, das Netzwerk zu beleuchten und alte Geräte zu identifizieren, die nicht mehr voll ausgelastet sind, und freuen sich auf weitere kreative Anwendungen für die Lösung. Schultz plant zum Beispiel, Armis in naher Zukunft einzusetzen, um die Netzwerkleistung zu verwalten, indem er Abweichungen in den Netzwerkprotokollen überprüft, die Frühindikatoren für eine Datenexfiltration sein können.

Ergebnisse der Einführung von Armis

- Breitere Sichtbarkeit sowohl von abtrünnigen als auch neuen Internet of Things (IoT)- und medizinischen Geräten, die sich mit dem Netzwerk verbinden
- Einblicke in die Nutzung, um festzustellen, welche Geräte – von Servern über Peripheriegeräte bis hin zu medizinischen Geräten – wirklich einen Mehrwert für das Unternehmen darstellen und welche ausgemustert werden können
- Integration mit CrowdStrike, um bei verdächtigen Ereignissen gründlichere Untersuchungen zu ermöglichen
- Erkennung von verschlüsseltem und unverschlüsseltem Netzwerkverkehr zum besseren Schutz von Patientendaten und anderen vorgeschriebene Gesundheitsinformationen
- Großer Nutzen im Verhältnis zum Aufwand für den Einsatz und die Verwaltung von Armis



Armis ist die führende Plattform für Netzwerktransparenz und Sicherheit. Sie wurde speziell für die neuartigen Bedrohungen entwickelt, die durch vernetzte Geräte entstehen.

Fortune-1000-Unternehmen vertrauen auf den kontinuierlichen Schutz in Echtzeit, den unsere Lösungen bieten, um alle verwalteten, nicht verwalteten und IoT-Geräte, einschließlich medizinischer Geräte (IoMT), Betriebstechnologie (OT) und industrieller Kontrollsysteme (ICS), in vollem Kontext zu sehen.

Armis bietet ein einzigartiges passives Cybersecurity Asset Management, Risikomanagement und automatisierte Durchsetzung.

Armis ist ein privates Unternehmen mit Hauptsitz in Palo Alto, Kalifornien.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial

