FURTINET

# ATRIUS HEALTH USES NETWORK ACCESS CONTROL TO IDENTIFY AND CLOSE SECURITY GAPS

## INTRODUCTION

Atrius Health is a nonprofit, comprehensive ambulatory healthcare organization with 36 clinical locations throughout eastern Massachusetts. With more than 10,000 employees, including 900 physicians that cover 50 specialties, the organization provides comprehensive adult and pediatric care for over 740,000 patients. With a focus on technology and accountable care, Atrius Health strives to simplify healthcare services by providing on-site laboratories, medical scans, eye care and more.

## THE CHALLENGE

Atrius Health relies on electronic medical records (EMR) to provide instant access to patient data, ensuring seamless service across a wide range of providers and departments. While Atrius Health had multiple layers of network security, a reliable barrier for physical network connections was missing. If an unauthorized individual slipped into a room at a facility, they could connect a computer, get an IP address and access the network. As with any medical group, preventing data loss and ensuring HIPAA compliance is a major concern for the organization. Lack of complete visibility across the network could result in an easy path for data loss.

The second key challenge involved operational issues. Its many locations often acted as individual business centers, introducing new technology without consulting the IT group whose team was then tasked with supporting unfamiliar devices. This behavior also led to duplicate purchasing of networked equipment. The organization needed to gain visibility into the entire network to ensure efficient, centralized management.

## PREVENTING DATA LOSS AND ENSURING HIPAA COMPLIANCE THROUGH VISIBILITY

Atrius Health evaluated multiple Network Access Control (NAC) solutions to resolve these challenges. They chose the Fortinet NAC solution as they found it to be outstanding in both its technical capabilities as well as ease of management. With NAC, Atrius Health has a

> ““If you do not know about a device, there is no way to monitor and protect it. FortiNAC gives us a clear picture of the network and enables us to quickly find assets and shut down individual network ports.”
>
> – Rob Fountaine,
> Manager of Information Security,
> Atrius Health

Atrius Health

## DETAILS

**CUSTOMER:** Atrius Health

**INDUSTRY:** Healthcare

**LOCATION:** Newton, MA

## BUSINESS IMPACT

- Secured physical network connections to ensure HIPAA compliance and prevent data loss
- Gained complete visibility of all wired endpoints
- Detected and eliminated more than a dozen unregistered devices, including several unsecured wireless routers and hubs
- Reduced unnecessary and duplicate equipment expenses

## DEPLOYMENT

- Network Access Control

clear picture of every device connected to its network. Now if a user tries to connect an unregistered device to the network or even moves a computer from one port to another, the IT group is alerted and shuts down the IP address. “If you do not know about a device, there is no way to monitor and protect it. FortiNAC gives us a clear picture of the network and enables us to quickly find assets and shut down individual network ports. Adding this layer of visibility has helped us protect against data loss and ensure HIPAA compliance. I equate FortiNAC to having a lock on the doors and windows of your house. Without it, you are leaving your house wide open. We also no longer have to worry about lateral malware infections as we can just kill the port. Now, only authorized devices can connect to the network, and every port can be located and controlled.”

## SPEEDING REACTION AND QUARANTINE KEEPS CLINICIANS ON SCHEDULE

Atrius Health has a hierarchical IT organization with teams for different functional areas, often in disparate physical locations. Before implementing NAC, the network security team could not shut down a port without coordinating with the network team. “In the healthcare environment, you need to know if something is interrupting clinicians – their time and schedules are critical,” said Fountaine. Atrius Health decided to go with the persistent agent method, deploying agents to every endpoint and profiling each medical device that could not have an agent. Then it locked down the network, limiting access to only Atrius Health devices.

> **“MAKE EVERYTHING AS SIMPLE AS POSSIBLE. IMPLEMENT THE SYSTEM AND EVOLVE IT WITH TIME. IF YOU HAVE AN AGENT, YOU GET ACCESS. WITHOUT AN AGENT, YOU CAN STILL ACCESS THE SYSTEMS WITH THE LOGIN AND THE DOMAIN.”**

The next consideration was developing policies that weren’t overly complex. “I learned from the medical groups that projects can get bogged down in myriad of tiny policy decisions,” said Fountaine. His advice: “Make everything as simple as possible. Implement the system and evolve it with time. If you have an agent, you get access. Without an agent, you can still access the systems with the login and the domain.” Following this process enabled Atrius Health to quickly deploy NAC.

## THE RIGHT NETWORK ACCESS CONTROL SOLUTION

After installing NAC, Atrius Health found more than a dozen medical devices, wireless hubs and routers that were not on its asset list. Several unsecured wireless hubs and routers had been installed by clinical staff without IT approval, creating holes in network security. Also, the purchase of duplicate or unnecessary devices wasted money. By introducing visibility and control, Atrius Health secured the environment from potential data loss and ensure HIPAA compliance.

In addition to the NAC technology, Atrius Health was very impressed with the customer service. “Everything went smoothly during installation,” Fountaine shared. “The installation engineers were incredibly knowledgeable and helpful. Most impressive was the technical support — they have been spectacular.”

## FUTURE PLANS

Currently in the initial phase of its NAC implementation, Atrius Health is controlling access for both the network devices and temporary contractor access. Today, the NAC solution integrates with the Cisco switch, and in the future, Atrius Health plans to integrate with a SIEM solution to enable automated threat response. The NAC solution’s scalable design provides the flexibility Atrius Health needs to implement its solution in phases.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990