FURTINET

FORTINAC PROVIDES EVOLVED NETWORK ACCESS CONTROL FOR HEALTHCARE

EXECUTIVE SUMMARY

Technology is transforming healthcare, and the rapid growth in connected devices is at the forefront. This includes smart, connected medical devices (heart-rate monitors, insulin pumps, MRI machines, and ultrasound devices), Internet of Medical Things (IoMT) devices (HVAC sensors, security cameras, lighting, and printers), and personal mobile devices of staff, patients, and visitors. All of these greatly expand an organization's attack surface and multiply the odds that one or more devices are noncompliant with security requirements. A third-generation network access control (NAC) solution—such as the Fortinet FortiNAC—helps ensure that only devices that meet set policies and regulatory compliance standards can connect to the network, while providing visibility, control, and automated responses that reduce the burden on healthcare IT staff.

IOMT AND BYOD GROWTH IS CHANGING HEALTHCARE NETWORKS

IoMT devices are designed to improve healthcare efficiency by generating, collecting, analyzing, and transmitting data via the internet. Specific benefits include improving diagnoses and drug management, controlling costs, facilitating broadband-enabled remote patient monitoring, and engaging and empowering patients in their own care. With a rapidly growing number of devices already in use, the IoMT market is estimated to reach $158.1 billion by 2022.[2]

More than 500,000 connected medical technologies are currently available for improving patient outcomes.[1]

But the critical factor to consider with this kind of transformative growth is interoperability. Adding multiple connected solutions from disparate vendors creates complexities that can jeopardize security and effective data sharing. With no common IoMT operating system and no adherence to standard security protocols built into these devices, each one offers the potential to expose a critical security gap.

Healthcare connectivity demands have also been impacted by widespread adoption of bring-your-own-device (BYOD) policies. Workplace use of personal mobile devices is now a way of life for doctors, professors, medical students, and staff—not to mention guests, contractors, and patients. Organizations must be able to ensure these devices meet minimum security standards before connecting to the network and then continuously monitor all devices post-connect.

NEW SECURITY CHALLENGES PUT DATA AT RISK

Between 2009 and 2017, there were 2,181 healthcare data breaches that involved 500 records or more. Those breaches resulted in the theft or exposure of 176,709,305 healthcare records—more than 50% of the population of the United States. Healthcare data breaches are now being reported at a rate of more than one per day.[3]

Beyond the high frequency of attacks, healthcare organizations also have the highest costs associated with data breaches at $408 per lost or stolen record—nearly three times higher than the cross-industry average ($148). The associated costs of a major healthcare breach can be as high as $350 million.[4] More importantly, these kinds of incidents can have a direct impact on disruption of clinical services and severely hinder operations in the provider environment.

THE NEED FOR ENHANCED NETWORK ACCESS CONTROL

Healthcare security architects need improved access controls to protect devices and the broader network from threats. Access controls can also support compliance with increasingly strict privacy laws and industry regulations. To address these challenges, NAC has evolved to provide more robust capabilities. Effective NAC solutions must now be able to see where each device is, what it does, and how it connects to other devices across the network topology.

A third-generation NAC solution validates an endpoint device's configuration when it attempts to join the network. Ensuring the integrity of wired and wireless devices before they connect to the network minimizes the risk of vulnerability and the spread of exploits. If the configuration is found to be noncompliant with the organization's set policies, the connection is either prevented or the device is forced to an isolated or limited-access VLAN. Users are then automatically warned that their device must be remediated and access will be granted only after corrective measures have been taken.

FORTINAC—SECURING DEVICE-BASED RISKS FOR HEALTHCARE

To fully secure BYOD and IoMT endpoints across a healthcare infrastructure, the Fortinet FortiNAC coordinates endpoint visibility, control, and automated responses.

VISIBILITY

Since it is impossible to protect the network from unseen threats, visibility is a crucial first step in securing IoMT and other endpoint devices. While a firewall provides the first line of defense in visibility, securing the network for IoMT requires a deeper line of protection within the network. Unlike first- or second-generation NAC solutions, FortiNAC identifies headless devices each time a device connects to the network. For new devices, FortiNAC notifies the device sponsor to authorize the device onto the network. It then records every action taken by the device. Fortinet's NAC solution also simplifies management—ensuring that if a device is compromised it can be quickly located, even if the device is in a remote location.

CONTROL

FortiNAC provides granular control of endpoint access policies and permissions. Healthcare organizations can protect sensitive data by providing employees (either by role or by user) with only enough network access to do their job. In addition, FortiNAC simplifies and supports network segmentation right to the network edge.

> **To fully secure BYOD and IoMT endpoints across a healthcare infrastructure, the Fortinet FortiNAC coordinates endpoint visibility, control, and automated responses.**

Organizations can also create separate VLANs for IoMT devices that limit cross-talk and secure the network from the spread of lateral (or east-west) virus attacks. As an integrated part of the broader Fortinet Security Fabric architecture, FortiNAC helps provide end-to-end control of the entire network, including satellite medical offices and clinics. It also helps eliminate common audit failures due to Shadow IT (devices and applications managed without direct involvement or oversight of the organization's IT staff).

AUTOMATED RESPONSES

FortiNAC provides real-time automated threat responses that can immediately quarantine an IoMT device that acts suspiciously. For example, if an IoMT device starts pinging a DNS server, it will be tracked and an alert will be generated. The port where the IoMT device connects to the network can also be locked down pending a review by an analyst. Additionally, once a device is isolated, FortiNAC automatically delivers all the contextual information to a security analyst. By eliminating the manual processes of an analyst having to compile and coordinate this information, time to resolution is shortened and the burden on strained IT resources is reduced.

HIPAA COMPLIANCE MANAGEMENT

More than 95% of large hospitals have progressed to meaningful use of electronic health records (EHRs),[5] and 38% of hospital chief information officers (CIOs) cite EHR integration with other systems as a top priority.[6] The objective of healthcare providers and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) is to ensure that—as these records become more widely used, shared, and interoperable—there are sufficient security controls in place to guarantee both regulatory compliance and patient privacy.

> **The penalties for HIPAA violations can be severe, with multimillion-dollar fines possible when violations have been allowed to persist for several years or when multiple violations of HIPAA rules have been allowed to occur.**[7]

Because of the value attached to EHRs, smart medical devices pose critical security threats to hospitals and healthcare institutions. In fact, there has been a 525% increase in medical device cybersecurity vulnerabilities reported by the U.S. government, with the trend threatening to climb even further in the years to come.[8] Unsecured IoMT and other endpoint devices allow hackers a backdoor onto the network, risking protected health information (PHI) disclosures and HIPAA fines.

To help meet HIPAA security requirements, the Fortinet FortiNAC solution integrates advanced device visibility and access control capabilities into the Fortinet Security Fabric. These technologies address many of the HIPAA compliance requirements, as well as compatibility with other best-of-breed security solutions, to form a cohesive security architecture. FortiNAC records 100% of network access actions for a complete log that helps automate audits and reduce the time and labor burdens on IT security staff.

FORTINAC DELIVERS GREATER EFFICIENCY, BETTER PROTECTION

Endpoint devices (including IoMT) will remain a prime target for cyber criminals as long as they offer an easy, exploitable pathway to valuable data. As an integrated part of the broader security architecture, a third-generation NAC solution can provide comprehensive history tracking and forensic information. This is used to enable critical functions such as breach prevention, detection, and remediation. FortiNAC also enables healthcare organizations to verify that connecting devices meet compliance requirements. Automated processes—such as for provisioning or providing contextual data to accompany an alert—reduce the burden on IT staff for greater operational efficiency and productivity.

And when it comes to maintaining unfailing quality of care for patients, FortiNAC enables healthcare organizations to protect against operational outages due to things like distributed denial-of-service (DDoS) or ransomware attacks. FortiNAC uses dynamic role-based network access control to create network segments that keep compromised devices from causing extended problems across the organization. Automated containment responses across the integrated Fortinet Security Fabric go even further to protect enterprises from the onslaught of sophisticated, endpoint-targeted attacks.

CASE STUDY: ATRIUS HEALTH

Atrius Health (Massachusetts, USA) provides comprehensive care for over 740,000 patients across 36 locations. Atrius Health needed reliable controls for their physical network connections. If an unauthorized individual slipped into a room at a facility, they could connect a computer, obtain an IP address, and access the network.

As with any medical group, preventing data loss and ensuring HIPAA compliance is a major concern for Atrius Health. They also needed to conveniently see everything connected to the network—all devices and all activities at all times.

Ultimately, Atrius Health chose FortiNAC on the basis of its technical capabilities and ease of management. After installing FortiNAC, Atrius Health found more than a dozen medical devices, wireless hubs, and routers that were not on its asset list.

"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."

- *Rob Fountaine,*
  Manager of Information Security,
  Atrius Health

Atrius Health

[1] “Medtech and the Internet of Medical Things,” Deloitte, July 2018.

[2] Ibid.

[3] “Healthcare Data Breach Statistics,” HIPAA Journal, August 2018.

[4] Heather Landi, “Healthcare Data Breach Costs Remain Highest at $408 Per Record,” Healthcare Informatics, July 13, 2018.

[5] “Hospital Progress to Meaningful Use,” Health IT Dashboard, August 2017.

[6] Jessica Kent, “40% of CIOs to Deploy a Healthcare Analytics Platform in 2018,” Health IT Analytics, December 22, 2017.

[7] “What are the Penalties for HIPAA Violations?,” HIPAA Journal, June 24, 2015

[8] Jasmine Pennic, “12 Defining Healthcare Trends to Watch in 2018, “HIT Consultant, December 18, 2017.

FORTINET®

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