HEALTHCARE IT TRANSFORMATION

Healthcare professionals are the epitome of a mobile workforce: constantly on the move, yet highly dependent on fast, accurate information. They need a secure wireless solution that performs flawlessly on the array of devices they rely on every day.

But healthcare IT is a lot bigger than that. A seemingly infinite number of devices used in patient care are now networked and access to them must be always available and secure. These devices also must be discovered by network security and protected, along with the entire infrastructure supporting the delivery of critical clinical applications.

In addition, all data and patient records, regardless of where they are stored or how they are transmitted, must be protected. This is already often a daunting task, which becomes increasingly complex as new technologies such as virtualization, cloud, and mobility become commonplace.

To address healthcare IT transformation, organizations must balance security with the flexibility of allowing almost any type of device onto the network. With critical medical devices on the network, a reliable wireless LAN (WLAN) can actually be a matter of life and death. Given that many of these Internet of Things (IoT) devices do not have innate security, effective access control and application security are now key to the success of any healthcare network.

Fortinet understands the challenges today’s health IT organizations face and we address them with a choice of WLAN and security deployment models, each delivering high-performance Wi-Fi and proven cybersecurity.

HIGHLIGHTS INCLUDE:

- Choice of three WLAN deployment models to suit organizational preferences
- Rich set of options for guest access and BYOD onboarding
- Consolidated, comprehensive threat protection
- Easy to demonstrate compliance with HIPAA, PCI DSS, GDPR, and other regulations
- Ability to discover and understand everything connected to the network
- Up-to-date threat protection with near real-time signature updates from FortiGuard Labs

TOP HEALTHCARE WLAN CHALLENGES

IOT

Securing IoT is a common challenge across industries, but in healthcare, a compromised IoT device can be deadly. From IV pumps to patient wearables, the number of connected devices continues to expand rapidly. Unfortunately, IoT devices are typically built to get to market as quickly and inexpensively as possible, which leaves security out. Not only does this make them vulnerable but it’s also difficult to detect when they’ve been compromised.

In addition, categorizing IoT devices connecting to the network adds a great deal of complexity. It’s not always clear which to trust, and sorting through them is problematic, especially in a wireless environment.

GUEST ACCESS

Wireless access is expected everywhere, especially in places people may spend a lot of time waiting, like hospitals. The staff doesn’t have time to help patients and visitors get connected, so onboarding must be intuitive.

More importantly, guest devices could be infected and spread the infection to the network. They also could slow down the network, impacting health-critical applications. Guests must be separated from the business network so there is no chance of them accessing data or affecting network performance.
COMPLIANCE

IoT and guest devices complicate security posture, which in turn complicates compliance. Attack vectors are expanded, IT can’t completely lock down patient information without impacting electronic charting, and there tends to be a lot of extra “noise” in the network to sort through.

In addition, compiling logs and information from multiple systems is extremely time-consuming for IT staff.

FORTINET’S SECURE UNIFIED ACCESS SOLUTION

Fortinet’s Secure Unified Access solution secures network connectivity, both wired and wireless. It includes LAN and WLAN infrastructure products as well as identity and access management products. It allows security policies to be extended from the network to the edge, where potentially unsecure or compromised laptops, mobile phones, and IoT devices connect.

While capacity and coverage requirements vary from hospitals to clinics and everything in between, security, reliability, and manageability are equally important to all. It can be very difficult to successfully deploy security solutions across all of these environments, as most solutions are built for one environment and do not scale well from the data center to the physician’s office.

Certified by Dräger, Welch Allyn, Ascom, Vocera, and other medical device manufacturers, Fortinet solutions enable healthcare organizations to safely onboard caregivers’ personal devices, as well as medical equipment of every type.

With a choice of three distinctly different WLAN deployment models, based on flexible controller options, Fortinet’s Secure Unified Access solution allows health IT organizations to select the best match for their operational needs, without compromising security. Solutions are scalable and flexible, to fit any size healthcare organization.

MANAGEMENT OVERVIEW

FORTIGATE INTEGRATED WIRELESS MANAGEMENT

Our Integrated Wireless Management solution leverages FortiGate NGFWs already deployed. Every FortiGate comes with a built-in controller. No additional equipment or licenses are required. In addition, the same management interface as the firewall is used, so there is no need to learn a new one.

DEDICATED CONTROLLER WIRELESS MANAGEMENT

Very large sites with hundreds to thousands of access points, like large hospitals, may prefer to segment firewall management from wireless management. FortiWLC can handle larger scale and more complex radio frequency deployments.

CLOUD-BASED WIRELESS MANAGEMENT

FortiCloud is recommended for smaller sites without a FortiGate installed, but it can scale to thousands of access points.

KEY FEATURES

BYOD ONBOARDING:

Guest access and self-service onboarding are easy with customizable captive portals, device integrity checks, virus scan, and a broad choice of user authentication options.

SECURITY THREAT MANAGEMENT:

Comprehensive protection against wireless protocol and RF attacks, malware, keyloggers, viruses, and zero-day attacks across all devices and operating systems is included.

UP-TO-DATE PROTECTION:

The threat experts at FortiGuard Labs work 24x7 to deliver timely automated network protection updates, assuring protection from even the newest attacks.

With a choice of three distinctly different WLAN deployment models, based on flexible controller options, Fortinet's Secure Unified Access solution allows health IT organizations to select the best match for their operational needs, without compromising security. Solutions are scalable and flexible, to fit any size healthcare organization.
APPLICATION CONTROL:
Complete application visibility and precision control of the network, with signatures for over 4,000 applications, lets hospitals and clinics prioritize, throttle, or block applications at a group, user, or device level.

UNIFIED MANAGEMENT:
The same or different policies can be administered to the wired and wireless network, and everything can be managed through a “single pane of glass.”

NO HIDDEN LICENSES:
All security services are included as standard. There are no costly surprises as you activate new security features—only added protection.

Complete application visibility and precision control of the network, with signatures for over 4,000 applications, lets hospitals and clinics prioritize, throttle, or block applications at a group, user, or device level.

And of course, everything else you’d expect in a wireless solution including:
- Wave 2 operation on 802.3af
- 802.3az power-efficient Ethernet (Wave 2 FAP)
- Fast-roaming 802.11 r/k/v
- Bonjour genius
- Channel utilization (duty-cycle measurement)
- QoS profiles (per SSID/per client)
- Automatic channel selection
- Probe response suppression
- Broadcast/multicast management
- Multiple PSK for WPA2 personal
- Fast failover for controller redundancy
- Rogue detection and suppression
- WIDS
- Frequency and AP load balancing
- Mesh wireless network
- Remote APs
- Onboard BT/BLE
- Location tracking (with FortiPresence)

HOW FORTINET SOLVES HEALTHCARE’S CHALLENGES
To address today’s biggest healthcare network challenges, Fortinet takes a holistic and automated approach. The Fortinet Security Fabric is a security architecture that provides broad visibility and protection of the digital attack surface, integrated detection of advanced threats, and automated response. The Security Fabric enables the following:

SECURING IOT
Rogue and compromised IoT and BYOD devices can be difficult to identify and extremely time-consuming to deal with if they must be sorted through manually. FortiGate and the Security Fabric can discover and understand what is connected to the network. In addition, endpoints can be automatically quarantined if they generate an indicator of compromise (IOC). This ensures infected devices are neutralized quickly.

With management platforms such as FortiManager, configuring and managing large numbers of headless devices is much easier, and performance for many purpose-built devices is improved with Virtual Cell by removing roaming as a client choice.

SOLVING GUEST ACCESS
A guest network can be directly segmented at the wireless controller to keep guests and their devices away from healthcare data.

Onboarding is easy with seamless self-service via any of our identity and access management products with a guest portal, such as FortiAuthenticator.

SIMPLIFYING COMPLIANCE
Fortinet makes demonstrating compliance far simpler. With segmentation enforcement of wireless traffic and automatic quarantine of compromised endpoints (regardless of what side of the network they enter), IT just needs to generate automated reports. Management platforms automate logging and reporting for showing compliance.

FortiGate and the Security Fabric can discover and understand what is connected to the network. In addition, endpoints can be automatically quarantined if they generate an indicator of compromise (IOC). This ensures infected devices are neutralized quickly.
SCALABLE FOR ENVIRONMENTS OF EVERY SIZE

There are three controller options and flexible form factors (hardware, virtual machine, or hosted) to suit any environment.

LARGE HOSPITALS

Large, complex environments can benefit from dedicated RF management. The FortiWLC WLAN controller and FortiWLM WLAN manager allow for customized, dedicated RF control and management. Virtual Cell can be enabled to support mobile IoT devices that have unreliable roaming behaviors.

SMALL PRACTICES, REMOTE OFFICES, CLINICS

There are many deployment options for small environments as well. The most common is to use a FortiGate NGFW or FortiWiFi UTM to manage APs directly. This results in low equipment overhead and simplified management.

AND EVERYTHING IN BETWEEN

With three completely scalable management options to choose from, Fortinet Secure Access is ideal for mid-sized locations as well.

COMPLETE AND FLEXIBLE WI-FI AND SECURITY SOLUTION

Healthcare networks are becoming increasingly complex, and as IoT in healthcare explodes, the attack surface expands. As a recognized leader in cybersecurity, Fortinet can provide a total solution for uninterrupted care at any size healthcare facility. With Fortinet, health IT organizations can select the best deployment model for their organizational needs, without compromising security.