SOLUTION BRIEF

Deliver Secure, Reliable Wireless for Healthcare With Fortinet

Executive Summary

Healthcare professionals are the epitome of a mobile workforce: constantly on the move and 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.

Hospitals, clinics, and elder care facilities have countless ways to use wireless technology for better patient outcomes, and to improve operational efficiency. From accessing patient records with computers on wheels or handheld tablets, to getting telemetry from medical devices, nurse call systems, and location-tracking applications, Wi-Fi is now at the heart of patient care.

Wireless local-area network (WLAN) reliability is of course paramount. But there are a growing number of wireless devices accessing the network, many of them headless (with no user interface). That means that access control and application security are now critical success factors for any healthcare network.

To address these changes, healthcare providers must balance the need for security with the flexibility of allowing almost any type of device onto the network. Only Fortinet can offer health IT organizations a choice of WLAN and security deployment models with different wireless management options, each backed by world-class cybersecurity.

Our Wi-Fi LAN edge solution unifies network and security management through a "single pane of glass," and provides superior visibility and control of applications. Fortinet's cloud-managed wireless solution provides quick and easy wireless deployment to any size facility without requiring on-premises wireless controllers.

Healthcare WLAN Challenges

Plethora of mobile devices

Today's caregivers have a veritable arsenal of mobile devices at their disposal, many of which are personal. They must all be onboarded securely and in compliance with HIPAA and other healthcare standards.

From smartphones to Wi-Fi phones to voice pendants, clinicians often carry three or four mobile devices each, and use any number of other Wi-Fi-enabled medical devices from medical-grade tablets to infusion pumps. Many of those devices are owned by the physician, while others are issued, and still others are shared. Each presents different security challenges that must be addressed.

Escalating mobile threats

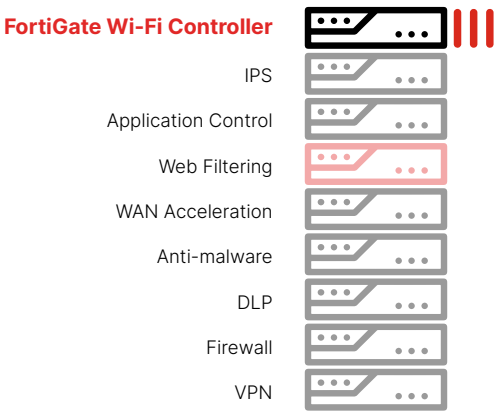
Protecting patient data and regulatory compliance have always been top concerns for healthcare organizations. WLAN vendors all have robust solutions to neutralize wireless protocol and radio-frequency (RF) threats, such as rogue access points (APs), distributed denial-of-service (DDoS) and man-in-the-middle attacks, and more.

However, there is a growing vulnerability to malware resulting from the explosion of mobile devices in clinical environments. With that expanded connectivity, and widespread reliance on the internet for updates and remote management, new security measures are required to offer continuous protection across this ever-growing attack surface.

Secure Wireless Solution

Fortinet gives health IT organizations WLAN solutions that provide seamless mobility within and between healthcare facilities of all sizes, while assuring mission-critical apps perform flawlessly. Plus, patient data, devices, and applications are fully protected from the latest cyber threats.

- Choice of cloud-managed or premises-managed WLAN deployment models to suit organizational preferences
- Rich set of options for guest access and bring-your-own-device (BYOD) onboarding
- Comprehensive threat protection consolidated on one appliance
- Compliance with HIPAA and other health IT regulations
- Exceptional visibility and control of applications and utilization
- Security devices kept up to date through regular updates from FortiGuard Labs



Mission-critical apps

Healthcare has more than its share of mission-critical applications, some of which are even life-critical. WLANs must deliver those applications without a glitch at every point of care, even in RF-hostile places such as elevators and radiology units.

Bandwidth demands from video, imaging, telemedicine, and spiraling patient and guest usage are putting critical electronic health record (EHR), Voice over Internet Protocol (VoIP), and telemetry applications at risk. Resources must be managed with surgical precision. Bandwidth management and application controls are crucial for prioritizing mission-critical apps while blocking or throttling others.

Rural and community clinics

Whether clinicians are at a hospital or at a remote clinic, they demand a consistent experience every time. They need seamless access to centralized medical records, local and remote clinical applications, and many other resources.

This secure mobility between locations requires sophisticated identity management integrated with a comprehensive security solution. But remote-care delivery must still make economic sense, and the cost and complexity of provisioning and maintaining secure Wi-Fi access and virtual private network (VPN) connectivity at remote sites is often a barrier.

Fortinet Secure Wi-Fi Solution

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.

With a choice of WLAN deployment models, Fortinet's secure wireless solution allows health IT organizations to select the best match for their operational needs, without compromising security.

Certified by Dräger, Welch Allyn, Ascom, Vocera, and other medical device manufacturers, all Fortinet solutions enable healthcare organizations to safely onboard caregivers' personal devices, as well as medical equipment of every type. Whether it's IV pumps, patient trackers, heart monitors, or remote presence robots, they all enjoy comprehensive protection from known and evolving threats.

FortiGate-managed Wi-Fi offering

What makes the FortiGate-managed Wi-Fi solution unique is the unification of the network and security afforded by our industry-leading security appliance. It simplifies day-to-day operations while providing superior visibility and control of users, devices, and applications at the lowest total cost of ownership (TCO).

FortiGate unifies security and network management by consolidating all the functions of firewall, intrusion prevention, anti-malware, VPN, WAN optimization, web filtering, application control, and WLAN controller on a single, high-performance platform.

This enables effortless, secure onboarding of caregivers' personal devices and medical devices. It also provides captive portal services for guest access as part of a complete cybersecurity portfolio. With security and network management unified through a "single pane of glass," any security measure can be applied to any user or device whether connected by wire, wirelessly, or by VPN. Add high-density FortiSwitch Power over Ethernet (PoE) switches and those too can be managed through the FortiGate.

The FortiGate family scales to meet the Wi-Fi, LAN, WAN, and security needs of any size hospital, clinic, community health center, or assisted living facility. For high-availability deployments, it supports both active/passive and active/active controller failover configurations. For small sites, FortiWiFi appliances combine an entry-level FortiGate with a full-featured AP, making a network in a box equipped with a VPN and a comprehensive security suite.

A full range of Wi-Fi 6 APs provides ample options for high-density indoor coverage. APs for outdoor deployment, even in the most extreme conditions, are also available, with ruggedized outdoor models.

Key FortiGate features for healthcare

Bring-your-own-device (BYOD) onboarding. Guest access and seamless self-service onboarding utilize customizable captive portals, device integrity checks, virus scan, and a broad choice of user authentication options.

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

Up-to-date protection. Near real-time automated updates from FortiGuard Labs, which researches the latest attacks and creates new defenses, provide the network with protection against the latest threats.

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 is managed through a "single pane of glass."

No hidden licenses. All security services are included as standard. There are no costly surprises as new security features are activated—only added protection.

Internet-of-Things (IoT) onboarding. Onboard NAC features allow for easy onboarding of the variety of IoT devices found in a medical setting and ensure that each is put into the proper security context.

Standalone cloud-managed Wi-Fi offering

Fortinet's Cloud Wi-Fi can be deployed in minutes and easily managed through FortiLAN Cloud provisioning and management portal. Wi-Fi networks are simplified with a secure cloud deployment. Fortinet's cloud Wi-Fi solutions offer advanced security protection at the edge without the complexity of installing WLAN controllers and management servers on-premises. Cloud Wi-Fi security includes intrusion prevention, L7 application control, antivirus, anti-botnet, and web filtering.

Fortinet's cloud-managed WLAN solution is unlike any other cloud Wi-Fi offering. Based on the FortiLAN Cloud Provisioning and Management Service, the FortiAP-U series provides complete security at the network edge, with the convenience and low CapEx of cloud management.

The FortiAP-U series APs can perform real-time security processing on the AP. Combining Wi-Fi access and network security into the compact footprint of a single AP provides an exceptionally elegant and affordable solution for secure Wi-Fi at the remote sites of distributed enterprises.

Standalone management is preferred by health IT organizations with a large number of small sites requiring secure wireless networks. This solution is skewed toward ease of operation and deployment, while still providing superior visibility and control of all wireless traffic.

Key cloud-managed secure Wi-Fi features

Ease of deployment. An entire wireless infrastructure can be deployed quickly and easily, without additional hardware, and without sacrificing security. Deployed APs are registered to FortiLAN Cloud and immediately adopt the organization's defined security policies. This seamless security posture ensures that all clinical locations are properly secured at deployment, leaving no unplanned security gaps.

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

Up-to-date protection. Cutting-edge automated network protection updates from Fortinet's accomplished security research team, FortiGuard Labs, assures some of the fastest response times in the industry to new vulnerabilities, attacks, viruses, botnets, and other threats.

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 is managed through a "single pane of glass."

No hidden licenses. All security services are included as standard. There are no costly surprises as new security features are activated—only added protection.

Summary

The mobile revolution and IoT are bringing about an explosion of devices on healthcare networks. To protect patient data and deliver the best possible care, health networks need holistic, end-to-end cybersecurity at every point of care and in every facility, from clinics to hospital campuses.

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 wireless deployment model for their organizational needs, without compromising security.

September 29, 2021 2:44 AM
485442-B-0-EN