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.

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.

Only Fortinet offers health IT organizations a choice of WLAN and security deployment models with different wireless management options, each backed by world-class cybersecurity.

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.

Improperly secured BYOD devices can compromise healthcare organizations' internal IT networks. Every device that connects to the network is a potential risk, particularly if those devices lack security updates and aren't subject to stringent security controls.[1]

From smartphones to Wi-Fi phones to voice pendants, clinicians often carry three or four mobile devices, often with differing levels of IT ownership. Patient care may also require the use of a number of other Wi-Fi-enabled medical devices, ranging from medical-grade tablets to infusion pumps. Each device presents different security challenges that must be addressed.

Escalating mobile threats

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 ensure continuous protection across this ever-growing attack surface.

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 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.

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.

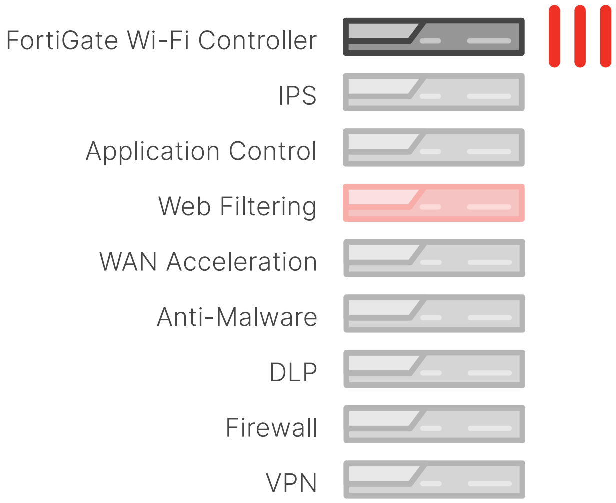

Figure 1: FortiGate built-in security and networking components

Fortinet Secure Wi-Fi Solutions

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 key industry vendors such as Dräger, Welch Allyn, Ascom, and Vocera, Fortinet solutions enable healthcare organizations to safely onboard caregivers' personal devices and medical equipment of every type. Everything from IV pumps to patient trackers to heart monitors to remote presence robots is protected from known and evolving threats.

FortiOS-Managed Wi-Fi Offerings

The FortiOS-managed Wi-Fi solution converges networking and security to simplify day-to-day operations while providing superior visibility and control of users, devices, and applications at the lowest total cost of ownership. FortiOS 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 in 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 regardless of how it is connected. FortiSwitch Power over Ethernet switches can also be added and managed through FortiOS.

The FortiGate hardware family scales to meet the Wi-Fi, LAN, WAN, and security needs of any size hospital, clinic, community health center, and 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.

With hardware, virtual machine (VM), and as-a-Service form factors, healthcare companies can install their controller and security solution where it makes most sense and still have secure networking at all edges.

A full range of Wi-Fi 7 APs provides ample options for high-density indoor coverage. APs for outdoor deployment, even in the most extreme conditions, are also available, with ruggedized models.

Key FortiOS hardware, VM, as-a-Service, and SASE features

Bring-your-own-device 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, let 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.

Internet-of-Things (IoT) onboarding: Onboard network access control 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.

Virtual patching: The FortiGuard services running on the FortiGate can recognize devices (often IoT devices) that have known vulnerabilities. The system can then virtually patch the device by putting compensating controls in place to prevent exploitation of the vulnerability until IT updates the firmware.

Standalone Cloud-Managed Wi-Fi Offering

Fortinet Cloud Wi-Fi can be deployed in minutes and easily managed through the FortiLAN Cloud provisioning and management portal. Wi-Fi networks are simplified with a secure cloud deployment. Fortinet 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 series provides complete security at the network edge with the convenience and low CapEx of cloud management.

The FortiAP series APs 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.

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: 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.

Summary

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.

Fortinet provides a total solution for uninterrupted care at any size healthcare facility. Our WLAN solutions offer seamless mobility within and between healthcare facilities, while protecting against all manner of cyberthreats. With Fortinet, health IT organizations can select the best wireless deployment model for their organizational needs without compromising security.

[1] 5 BYOD Security Risks in Healthcare, LINQ, February 28, 2023.