SOLUTION BRIEF

Secure Access for Healthcare

Reliable Wi-Fi for Uninterrupted Clinical Care

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.

Hospitals, clinics, and elder care facilities have countless ways to exploit 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.

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, retailers 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, without compromising the protection provided, with three distinctly different wireless offerings, each backed by world-class cybersecurity.

The Integrated Secure Access solution unifies network and security management through a “single pane of glass,” and provides superior visibility and control of applications. The Controller Secure Access solution supports high density and high mobility environments by offering several unique reliability and traffic isolation advantages. Fortinet’s Cloud-Managed Secure Access solution provides quick and easy wireless deployment to any size facility without requiring on-premise wireless controllers.

Secure Access Solution

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

- Choice of cloud-managed or two premise-managed WLAN deployment models to suit organizational preferences
- Rich set of options for guest access and BYOD onboarding
- Comprehensive threat protection consolidated on one appliance
- Full compliance with HIPAA and other Health IT regulations
- Exceptional visibility and control of applications and utilization
- Security devices kept up to date through regular signature updates from FortiGuard Labs

Healthcare WLAN Challenges

Plethoria of Mobile Changes

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 a top concern for healthcare networks, and WLAN vendors all have robust solutions to neutralize wireless protocol and RF threats, such as rogue APs, 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.

Mission-Critical Apps

Healthcare has more than its share of mission-critical applications, some of which are even life-critical. Wireless LANs 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 EHR, 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 VPN connectivity at remote sites is often a barrier.

Fortinet Secure Access 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 three distinctly different WLAN deployment models, Fortinet's Secure Access 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 current and evolving threats.

Integrated Secure Access

The Integrated solution is preferred by Health IT organizations that favor unified network and security management. In this solution, security and WLAN control are tightly integrated on a single platform and managed through a single pane of glass.

The Integrated solution is skewed toward ease of operation and superior visibility and control, through its seamless integration of security and wired and wireless infrastructure under a unified management interface. This solution is best suited to health networks with multiple locations such as clinics, community health centers, and assisted living facilities.

Controller Secure Access

The Controller WLAN solution is a best-of-breed Controller wireless offering which is preferred by Health IT organizations that like to manage networking and security separately, often using different vendor equipment for each.

In this solution, Wi-Fi and security are provided by different best-of-breed-components, each managed independently. The WLAN system uses a unique channel management approach, which enables rapid deployment and scaling, and offers several reliability and traffic isolation advantages.

This solution is best suited to large hospital campus deployments and is particularly effective at overcoming environmental interference from medical equipment.

Cloud-Managed Secure Access

The third WLAN solution is preferred by Health IT organizations with a large number of small sites requiring secure wireless networks. In this solution, security and WLAN control are tightly integrated in a cloud management platform allowing for centralized management and policies without the deployment of on-premise controllers.

The Cloud-Managed WLAN solution is skewed toward ease of operation and deployment, while still providing superior visibility and control of all wireless traffic.

This solution is best suited to health networks with many locations such as physician practices, clinics, community health centers, and assisted living facilities.

Fortinet Secure Access Solutions Overview

Integrated Secure Access Offering

What makes the Integrated Secure Access solution so unique is the unification of the network and security afforded by FortiGate. It simplifies day-to-day operations while providing superior visibility and control of users, devices, and applications at the lowest cost of ownership.

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.

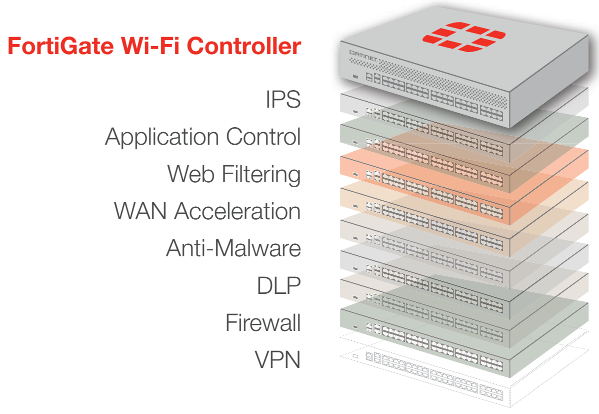

Figure 1: FortiGate consolidated security platform.

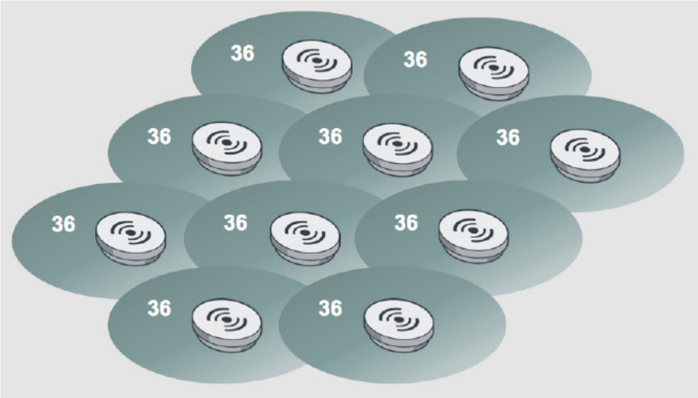

Figure 2: Fortinet virtual cell deployment model.

This enables effortless, secure onboarding of caregivers' personal devices and medical devices, and 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—by wire, wirelessly, or by VPN. Add high-density FortiSwitch PoE switches and those too can be managed as one, 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 802.11ac APs provides ample options for high-density indoor coverage as well as outdoor deployment in the most extreme conditions, using ruggedized outdoor models.

Key FortiGate Features For Healthcare

BYOD Onboarding

Guest access and seamless self-service onboarding utilizing 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.

Up-to-date Protection

Kept continually up to date through frequent automated updates from FortiGuard Labs, which researches the latest attacks to provide your network with immediate protection.

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

Can administer the same (or different) policies to the wired and wireless network and manage everything through a "single pane of glass," not a collection of separate management consoles.

No Hidden Licenses

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

Controller Secure Access Offering

What makes the Controller solution unique in the industry is its Wi-Fi channel management architecture, called Virtual Cell, which delivers compelling reliability, scalability, and ease of deployment advantages over the traditional multi-channel approach adopted by all other WLAN solutions.

Virtual Cell minimizes the complex, timeconsuming process of channel planning, which can take months for a large campus, through its unique single-channel deployment model which avoids the challenges of planning around co-channel interference.

In a Virtual Cell, all radios operate on the same channel, providing a layer of coverage across your campus, and they appear to clients as a single radio wherever they go. In addition, the network, not the client, controls how and when clients roam.

This unique approach renders co-channel interference harmless, ensures that caregivers' devices use the best available connection at all times, and enables seamless zero-handoff roaming. Clinicians can move freely from one point of care to another, always staying connected.

This network-based traffic control also makes it possible to perform real-time AP load balancing based on actual traffic, not crude, round-robin algorithms based on station count. It even governs station airtime so every client gets a fair turn on-air, and slow devices don't hog resources. With the constant movement of clinicians and wireless devices throughout the campus, this eliminates the problem of too many devices connecting to the same AP at the entrance to a department or clinical area.

Capacity scaling is a breeze and completely non-disruptive. Multiple Virtual Cells, each using a different channel, can be layered across the same coverage area to scale network capacity in high-density zones or facility-wide. And since adding new Virtual Cells does not require changes to existing cells, the stability and performance of mission-critical services is never at risk when you scale capacity.

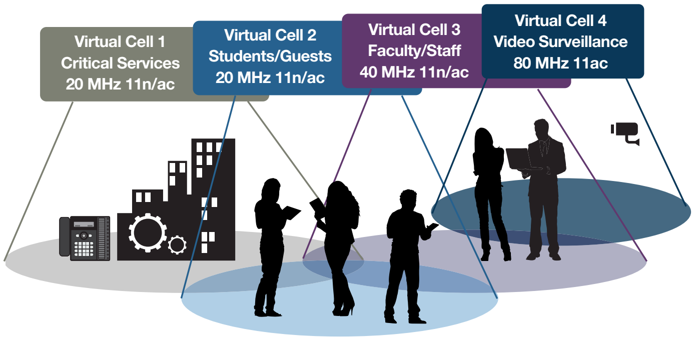

Figure 3: Enterprise-wide virtual cell layering.

Key Virtual Cell Features for Healthcare

Easiest Deployment

Deployment time shrinks to a fraction when you don't need site surveys or complicated channel plans. APs can be placed wherever it is convenient without fiddling with radio transmit power or worrying about co-channel interference.

Rapid Capacity Scaling

You can capacity incrementally simply by adding APs, or in multiples by layering Virtual Cells over the same coverage area, with absolutely no disruption to clinical services on existing cells or risk of reconfiguration errors.

Traffic Isolation

Virtual Cell layering can also provide total RF isolation for critical applications such as VoIP, heart monitors, location tracking, or by clinical function. This allows critical services or users to be assigned dedicated spectrum on the clearest channels, with immunity to congestion on other channels.

Reliable Connections

Network-directed roaming in 3 ms vs. 100+ ms makes voice calls more reliable and ensures all mission-critical apps, especially delay-sensitive, real-time services, stay connected as clinicians and patients move around.

Performance Flexibility

Virtual Cell is uniquely able to exploit 80 MHz wideband channels when the need for speed outweighs maximizing coverage and capacity.

Cloud-Managed Secure Access Offering

As the industry's only integrated nextgeneration firewall capabilities and access solution, Fortinet's Cloud Wi-Fi can be deployed in minutes and easily managed through FortiCloud provisioning and management portal. Simplify your Wi-Fi network 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 onpremise. 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 FortiCloud Provisioning and Management Service, and a new class of access points, the FortiAP-S series provides complete security at the network edge, with the convenience and low CAPEX of cloud management.

The FortiAP-S series access points (APs) perform real-time security processing on the AP itself. 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.

Cloud-Managed Secure Access Offering

Ease of Deployment

An entire wireless infrastructure can be deployed quickly and easily, without additional hardware, and without sacrificing security. Deployed access points are registered to FortiCloud 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

Is the comprehensive protection against wireless protocol and RF attacks, malware, keyloggers, viruses, and zero-day attacks at the users' entry point to the network? The closer security is to the end user, the better they are protected, and the better the network is protected.

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

Can administer the same (or different) policies to the wired and wireless network and manage everything through a "single pane of glass," not a collection of separate management consoles.

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 deployment model for their organizational needs, without compromising security.

January 24, 2020 9:42 AM

D:\Fortinet\Minor Changes\Re-color existing assets\sb-red-FA-secure-access-for-healthcare-1242020