SECURE ACCESS

Only Fortinet gives schools a choice of two alternative premises-managed WLAN solutions to cost-effectively support BYOD, guard against wireless protocol and RF attack, malware and viruses, and fully control application usage.

Secure Access for K-12 Education

Uninterrupted Learning with Secure Wi-Fi

Affordable laptops and tablets plus ubiquitous Wi-Fi can turn the dream of one-to-one computing into reality, but not without challenges in security and application control.

In today's flipped classrooms, where students direct their own education on their mobile devices, schools must be ever vigilant about cybersecurity and have a duty to control which online resources, games and apps students are permitted to access.

As Wi-Fi technology has evolved, different enterprise WLAN architectures have emerged and feature sets have matured. From a performance and connectivity perspective, there is little to separate vendors. However, in the era before us, holistic security is as important as coverage and capacity, and vast differences exist between WLAN vendors' capabilities.

With a choice of two premises-managed and one cloud-managed wireless offerings, all backed by world-class cybersecurity, Fortinet leads the way. School districts, charter schools and private schools can select a deployment model that best fits their IT organization, without compromising on the level of security protection.

For schools, Fortinet recommends either its *Integrated* or *Infrastructure* Secure Access solutions. Both have powerful benefits that provide a secure, reliable wireless deployment. The *Integrated* solution simplifies management by unifying network and application security through a single pane of glass and providing the most visibility and control of applications. The *Infrastructure* solution simplifies deployment and scaling through its unique channel management approach, and offers several unique reliability and traffic isolation advantages.

- Choice of 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
- Exceptional visibility and control of applications and utilization
- Security kept up to date through regular signature updates from FortiGuard Labs
- No feature gouging. All security features included as standard. No hidden feature-licensing shocks

Flipped Classroom Challenges

Onboarding New Devices

As the mobile revolution unfolded, many schools purchased their own laptops and tablets. Nowadays, we are seeing more schools embrace BYOD in order to stretch their capital budget and realize the goal of one-to-one computing.

But every new device introduced to the network is a potential harbinger of malware, so it must be screened and onboarded securely. To accomplish this, an automated self-service solution is essential to prevent skyrocketing support costs.

New Mobile Threat Vectors

Securing the network from intruders and from unauthorized or contaminated devices is only part of the story. Wi-Fi networks and mobile platforms are prime attack targets, and new threats, mostly at the application layer, are continuously evolving and on the rise.

Threats find their way behind your perimeter defenses, embedded in content – games, apps and other files – downloaded from the Internet. Therefore your access security framework must include real-time malware and virus protection with frequent signature updates.

Risky or Inappropriate Websites

Children are easily lured to websites containing inappropriate content or malware. Schools have both a legal and moral obligation to protect students from such sites.

In addition to blocking obvious adult and malicious content, depending on student age group and school policies, schools may also need to selectively block social, gaming and other sites. However, selective blocking is difficult to accomplish without sufficient user and content visibility.

Managing Your Bandwidth

Merely segregating students from staff is not enough. Schools are increasingly looking to apply unique policies for certain groups of users, devices or applications to block nuisance applications such as Facebook. Additionally, it is vital for schools to prioritize critical apps such as VoIP or Common Criteria testing, while relegating other traffic to best-effort service.

To do this, you first need visibility of your users, applications and devices and control over how, where and when those devices and apps are used. Second, your access infrastructure must be capable of accurately enforcing relative priorities and bandwidth caps for hundreds of apps and devices simultaneously.

Fortinet Secure Access Architecture

Fortinet recognizes that while all school districts, charter schools and private schools face similar challenges with tight budgets and IT staff in short supply, they don't always tackle networking and security matters the same way. They often differ in their preferred network architecture and organizational structure.

With a choice of three distinctly different WLAN deployment models, including the industry's most secure cloud offering, Fortinet's Secure Access Architecture lets schools select the best fit for their organization, without compromising security.

For school districts and independent schools, Fortinet recommends either of its two premises-managed solutions. Both provide effortless onboarding, granular control of application usage and priorities, and complete protection from current and evolving threats. The differences lie in how these and other capabilities are implemented.

Integrated Secure Access

The *Integrated* solution is best suited to schools 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.

Infrastructure Secure Access

The second solution offering is a best-of-breed *Infrastructure* wireless offering, which is better suited to schools that prefer to treat networking and security separately, and believe different equipment should be used 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 Virtual Cell architecture that enables rapid deployment and scaling, and offers several unique reliability and traffic isolation advantages.

Fortinet Secure Access Solutions Overview

Integrated Secure Access Offering

What makes the *Integrated* Secure Access solution so unique is the unification of network and security management 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.

A leader in Gartner's Magic Quadrant for Unified Threat Management (UTM) since 2009, FortiGate consolidates the functions of Firewall, VPN, Intrusion Prevention, Anti-malware, WAN Acceleration, VPN, Web Content Filtering, Application Control and WLAN Controller on a single, easy-to-manage platform.

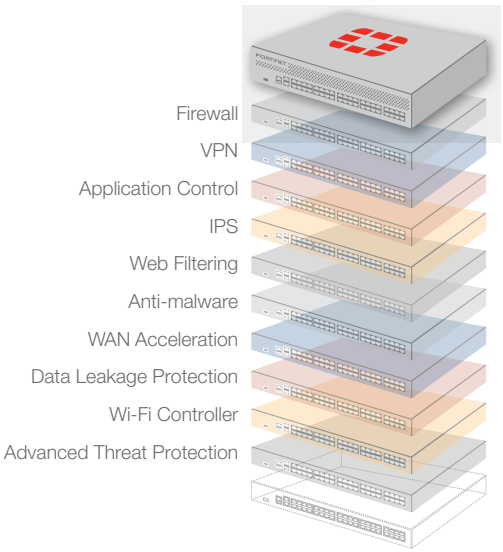

Fig 1: FortiGate Consolidated Security Platform

This cuts complexity, eliminates gaps left by point products and maximizes your control, allowing you to manage the network and its users, devices and applications through a "single pane of glass."

Fortinet has a full range of 802.11ac APs, from single radio to dual radio 3x3 MIMO devices. These include plenum-rated models for concealed deployment above classroom ceilings, tamper-proof smoke detector style models for discrete installation in classrooms and hallways, removing the temptation for students to tamper with them, and ruggedized outdoor models suitable for deployment in school sports fields and other outdoor areas.

When coupled with Fortinet's switch line, end-to-end configuration is a breeze. The FortiSwitch Secure Access Switch series with high-density 802.11at Power over Ethernet (PoE) powers anything from WLAN APs to surveillance cameras.

FortiSwitch administration and access port security is all managed from the same FortiGate "single-pane-of-glass" management console, providing equal visibility and control regardless of how users and devices connect to the network, wired or wireless.

Key FortiGate Features for K-12 Education

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, key loggers, 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.

Web URL Filtering

CIPA (US HR4577) and BECTA (UK) compliant web filters based on more than 75 web content categories, and more than 47 million rated websites – updated via FortiGuard Labs.

Application Control

Complete application visibility and precision control of the network with signatures for over 4,000 applications lets schools prioritize, throttle or block literally any 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.

Infrastructure Secure Access Offering

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

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

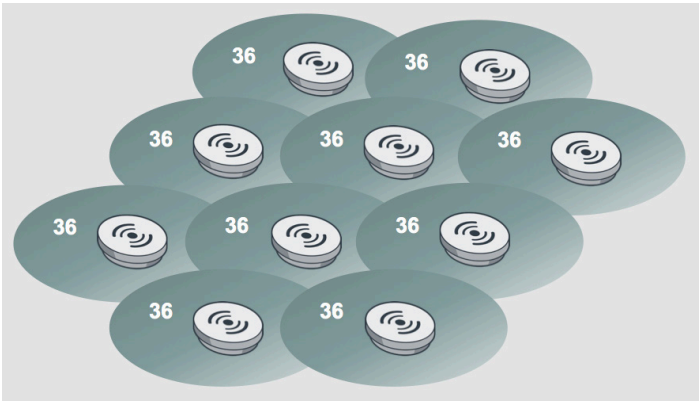

Figure 2: Fortinet Virtual Cell Deployment Model

In a Virtual Cell, all radios operate on the same channel, providing a layer of coverage across your campus and appearing 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 clients always use the best connection available to them and enables uninterrupted learning while roaming.

For serious capacity scaling or to wirelessly segment users and applications, multiple Virtual Cells can each use a different channel, while occupying the same coverage area by adding additional sets of APs. Layering cells in this way can be limited to a small zone or it can span your entire campus.

Layering new Virtual Cells does not require changes to existing cells, so the stability and performance of your existing environment is never at risk when you scale capacity.

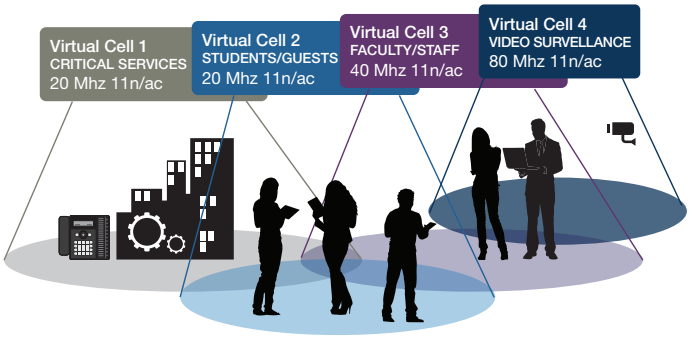

Figure 3: Enterprise-wide Virtual Cell Layering

FortiGate provides an access security overlay featuring the comprehensive portfolio of security services mentioned earlier. While some granularity is lost by giving up the network management from the FortiGate to a different appliance, it still delivers more complete threat protection and greater operational efficiency than competing solutions based on multiple security appliances.

Key Virtual Cell Features for K-12 Education

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 settings or worrying about co-channel interference between APs.

Rapid Capacity Scaling

Capacity can be scaled incrementally simply by adding APs, or in order of multiples by layering multiple Virtual Cells using different channels over the same coverage area.

Traffic Isolation

Virtual Cell layering can also provide total RF isolation for applications such as VoIP and alarm systems, or for teachers and staff, to ensure critical services or to give users dedicated bandwidth that is immune to congestion on other channels.

More Reliable Connections

Network-directed roaming is almost instantaneous (3ms vs. 100+ms). This makes voice calls more reliable and ensures students always stay connected when on the move.

Summary

The mobile revolution and BYOD are bringing about one-to-one computing in schools. But it doesn't just mean giving everyone uncontrolled access to the Internet. Digital natives they may be, but they are still kids, needing protection from themselves and from others.

The perennial problems of insufficient budget and too few IT staff have driven schools to focus on capacity and coverage. But the flood of student-owned devices joining a school's network now makes holistic access security an acute need.

With Fortinet, schools can support BYOD, guard against malicious attacks, malware and viruses, and completely control application usage. With a choice of two different Wi-Fi deployment models, Fortinet enables schools to select the architecture and topology that best suits their organization without compromising security.

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
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

March 1, 2016