



Solution Benefits

In the classroom, walking along a corridor, outside on the field, Fortinet protects Student and Staff sensitive data 24/7 with:

- Comprehensive Security: Industry's most advanced cybersecurity platform
- Secure unified access for all users
- Access Control: Full access and network control for student owned devices (BYOD)
- Web Filtering: Block student access to adult content and malicious websites
- Application Control: Policy-based control over any application usage
- No Surprises: Complete feature-set without hidden license fees
- Real-time Security Services: Up to date security

Securing K-12 Schools

Enabling a Safe Learning Environment

K-12 Education Network Security Challenges

With the number of security breaches rising in Education over the past 10 years, K-12 institutions have become prime targets for cyber attackers. In 2015 alone, according to the Gemalto Breach Level Index, educational institutions around the world experienced a total of 150 breaches with 19.3 million records being compromised. One reason for such a large number of breaches is the unique challenges that K-12 schools face, challenges that the typical enterprise doesn't encounter.

Market Drivers

- BYOD plus ubiquitous Wi-Fi have dramatically changed the learning experience.
- In today's interactive classrooms, schools must be vigilant about cybersecurity and have a duty to control student access to online resources.

Student Protection

Whereas businesses have adults to manage, schools need to consider students, who, in most cases, are minors and are often not subject to the same legal obligations as adults in the event of unauthorized network access. Most students, belonging to the social media generation, are unaware of network related security threats and are more likely to expose devices and the school network to threats by downloading malware or using unsecure networks.

Managing Bandwidth

There is only so much bandwidth to go around. Application usage needs to be controlled, so that priority applications such as internal communications or education related sites receive a guaranteed service level at the expense of less important traffic. But application priority is not absolute, it is relative. Schools are increasingly looking to apply unique policies for certain user groups, devices or applications.

Network Segregation	Tight Budgets
<p>In order to preserve data integrity, schools must segregate students from staff and in particular prevent students from accessing the school’s internal network.</p>	<p>Schools are rarely granted the budgets and IT expertise that large corporations have to invest in networking and network security.</p>
Onboarding New Devices	Inappropriate Websites
<p>The mobile revolution has brought with it a slew of ‘smart’ devices that have revolutionized learning but at the cost of security. Schools have embraced Bring Your Own Device (BYOD) in order to stretch their capital budget and realize the goal of interactive learning.</p>	<p>Schools have both a legal and moral obligation to protect students from sites containing inappropriate content or malware. In addition to blocking obvious adult and malicious content, 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.</p>
New Mobile Threat Vectors	
<p>Wi-Fi networks and mobile platforms, including Bring Your Own Device (BYOD), are prime attack targets. Most threats originate from students visiting malicious websites or downloading infected games and applications and then sharing them. These threats then propagate through a school’s network potentially infecting it. With BYOD in particular, schools fail to realize that each device introduced to the network is a possible attack vector and a potential source of malware.</p>	

The Consequences

Although the challenges of securing K-12 schools are great, the consequences of an unsecure school network are even greater. In 2015, data breaches in K-12 schools have occurred primarily due to hacking, stolen mobile devices, and email phishing. The consequences of these breaches have taken on the form of stolen academic records, individual data and tests as well as academic record modification. Furthermore, education has the second highest cost per capita after healthcare with the Ponemon Institute estimating this cost to be as high as \$300 per capita.

The Optimal Solution

These data breaches highlight the need for an effective and comprehensive cybersecurity solution for K-12 schools. To deal with the unique challenges facing K-12 schools, the solution should have certain characteristics including:

- Unify wired and wireless access with network security.
- Provide an access security framework that includes real-time malware and virus protection with frequent signature updates so that real-time traffic is protected.
- Screen and on board mobile devices securely.
- Have simple tools that provide full user, application, and device visibility with granular control over those devices and apps. Fortinet not only provides a model solution but does so with three unique offerings to ensure that each school has the solution most aligned to its needs.

Fortinet Secures K-12 Schools Secure Access Solution

Fortinet’s Secure Access solution (Figure 1) takes network security from the core and extends it to the access layer regardless of the access type or connection method. Where most vendors approach the problem with a one size fits all solution, Fortinet understands that schools require flexibility and addresses this need by offering three distinct deployment options. All three guarantee optimum security and share the same core security functions, features, and services. However, each model differs in its wireless capability giving schools the choice to deploy that which best fits their wireless requirements, budgets, and organizational structure.

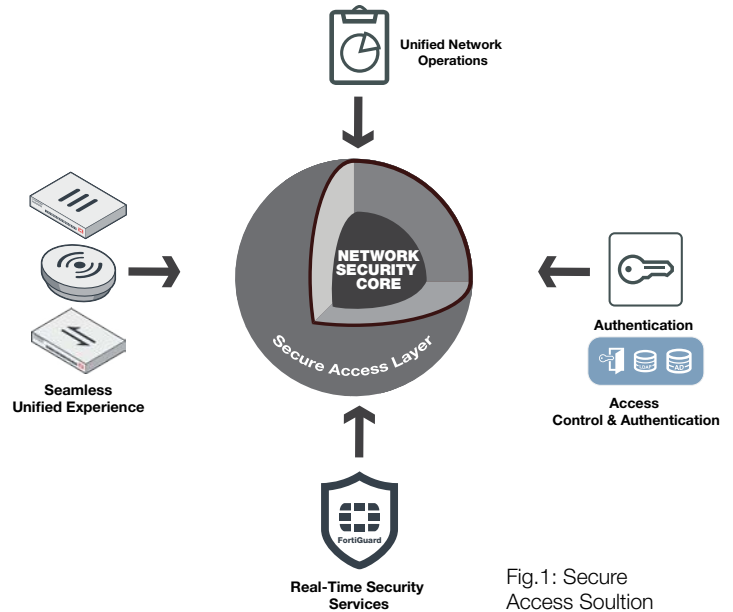
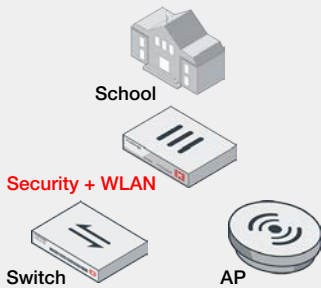
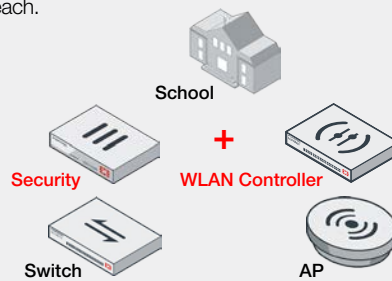


Fig.1: Secure Access Solution

The **Integrated option** is best suited to schools that favor a **consolidated network and security approach**. Security and access are tightly integrated on a single platform, the FortiGate, and managed as a single entity.



The **Controller option** is for those schools with **wide scale wireless requirements** that exceed the scalability of the Integrated option. It offers the most flexible wireless channel configuration and layering to simplify deployment while increasing performance, traffic segmentation, capacity, and reach.



The **Cloud option** integrates **wireless access and security onto the AP** providing a secure wireless solution at an affordable price. It is ideal for smaller K-12 schools and school districts with multiple small locations.



Integrated Option Highlights

Key Features for K-12 Education

<p>BYOD Onboarding</p> <p>Guest access and self-service device onboarding uses customized captive portals, device integrity checks, virus scan and a broad choice of user authentication options.</p>	<p>Application Control</p> <p>Complete application visibility and precision control of the network with signatures for over 4,000 applications allowing schools to prioritize any application at a group, user or device level.</p>
<p>Secure Unified Access</p> <p>With a common security structure throughout the access layer, security differences between wired and wireless access methods are eliminated.</p>	<p>Unified Management</p> <p>Cybersecurity, network and access are managed through a single management interface.</p>
<p>Continuous Protection</p> <p>The various security services are maintained by frequent automated updates from FortiGuard, Fortinet’s Global Threat Intelligence.</p>	<p>No Hidden Costs</p> <p>The different security services can be licensed either individually or in a cost effective bundle. There is no licensing cost for wireless access.</p>
<p>Web URL Filtering</p> <p>Compliant web filters based on more than 75 web content categories, and more than 47 million rated websites are updated via FortiGuard Labs.</p>	

Controller Option Highlights

Key Wireless Features for K-12 Education

Ease of Deployment Deployment time is reduced since site surveys and channel planning are no longer required. APs can be placed anywhere without tuning radio transmit power settings or worrying about co-channel interference.	Traffic Isolation Virtual Cell layering provides total RF isolation for applications such as VoIP and alarm systems. This ensures the availability of critical services and provides users dedicated bandwidth that is immune to congestion.
Rapid Capacity Scaling Capacity can be scaled incrementally simply by adding APs by layering multiple Virtual Cells using different channels over the same coverage area.	More Reliable Connections Network-directed roaming is quasi instantaneous making voice calls more reliable and ensuring students always stay connected when roaming.

Cloud Option Highlights

Key Cloud Features for K-12 Education

Security at the Wireless Edge Wi-Fi access and cybersecurity are combined onto the AP for a comprehensive and affordable WLAN solution.	Application Control Complete application visibility and precision control of the network with signatures for over 4,000 applications allowing schools to prioritize any application at a group, user or device level.
Ease of Management APs are easily provisioned and managed remotely through FortiCloud, Fortinet's cloud based management system.	Continuous Protection Up-to-date security through regular signature updates from FortiGuard Labs
Role based Access Role-based access control allows for separate access profiles for different groups within a school (e.g. faculty, students).	Cost Effective FortiCloud is free and there is no recurring management license per AP.

The Secure Access Solution is an integral part of the family of solution sets offered by Fortinet. These solutions are a realization of our technology vision, the Fortinet Security Fabric, which is designed to address the security issues and challenges of the enterprise network, including K-12 education. The Fortinet Security Fabric includes the key capabilities for a complete cybersecurity solution by providing broad, powerful, and automated security throughout a school network.

Summary

Fortinet's Secure Access enables schools to deploy cybersecurity more effectively in order to protect what matters most to them – their students and school's sensitive data. The solution is uniquely suited to the needs of K-12 institutions, where budgets are tight and resources are in short supply. Regardless of their network architecture or organizational structure, schools can select the best fit for their needs from the three Secure Access deployment options.



1.800.800.0019
www.connection.com/Fortinet-ps