CHARTING THE SECURITY JOURNEY FOR K-12 SCHOOLS

EXECUTIVE SUMMARY

The role of IT leaders in the K-12 environment is changing, from a technology focus to a more strategic focus on the enablement of eLearning and digital transformation. In their new roles, technology directors are undergoing much more scrutiny, as network security and regulatory compliance make up a larger part of their responsibilities.

Because K-12 network security breaches have gained such a high profile, nearly all technology products now feature some form of security provision. There are also dedicated security solutions from a variety of vendors. Unfortunately, a piecemeal approach to security creates a hodgepodge of technologies, which are hard to coordinate and don't allow IT to deal effectively with persistent, accelerating, and pervasive threats.

It is up to each school district to develop a strategy for broad, integrated, and automated network security. Network security design should adhere to best practices, such as those promoted by the SANS Institute[1] and the Consortium for School Networking (CoSN).[2] The resulting security architecture must be agile enough to keep pace with perpetual changes in education, regulation, and cyber crime. And, most important, it must be practical to implement and maintain, given the district's budget, staffing, and time constraints. As a longtime solution partner of schools, Fortinet offers IT leaders a proven model for such a strategy.

More than 330 K-12 cybersecurity incidents were reported in the U.S. in the last two years.[3]

ABOUT FORTINET

- The fastest-growing enterprise network security company in the world
- Serving more than 340,000 customers worldwide, including 2,200+ school districts
- Most comprehensive portfolio of E-rate eligible security, wireless, and network access technologies
- #1 most-adopted network security solution

KEY SECURITY PRIORITIES FOR K-12

In CoSN's 2018 K-12 IT Leadership Survey Report, privacy and security tied with broadband and network capacity as IT leaders' number one priorities.[4] Whether driven by enthusiasm for eLearning technology or by fear of being the next breach victims in the news, K-12 technology directors are juggling complex, and often conflicting, objectives:

Protect network users, systems, and data. Cyberattacks against K-12 schools and districts are growing in both frequency and severity. For example, in Flathead County, Montana, late last year, the Columbia Falls school district was closed for three days after hackers demanded $150,000 in bitcoin in exchange for not publishing stolen school records.[5]

While ransomware, phishing attacks, and malware threaten school district networks from the outside, K-12 technology directors must contend with internal mayhem as well. Malicious and prankster hacking, distributed denial of service (DDoS), and cyberbullying are all in their purview.

Enable education's digital transformation. Cyber-criminal attraction to the K-12 environment is hardly surprising, considering that education is moving inexorably toward increasing openness, sharing, mobility, and flexibility. Teachers are encouraged to adopt new, often cloud-based, eLearning technologies; students are welcome to bring their own laptops and smartphones; and facility management staff are making campuses more comfortable, efficient, and secure with networked HVAC, lighting, facility monitoring, cameras, and alarms.

To support all this, IT is expected to provide a cost-effective, high-speed, and highly available network. Security, therefore, must protect without hampering user experience or productivity.

Maintain compliance and enforce policies. They may have "technology" in their titles, but K-12 IT leaders increasingly find themselves addressing "people issues" with cyber-awareness campaigns, cyber-hygiene education, and continual revisions to data-use policies.[6] Nevertheless, training can take time, and cyber threats are continuous. IT must have safety nets in place, such as advanced threat detection and automated, real-time response to mitigate the effects of malicious actors and imprudent user behavior.

K-12 school districts also face unique regulation and compliance requirements, such as the Children's Internet Protection Act (CIPA), the Family Educational Rights and Privacy Act (FERPA), and the Children's Online Privacy Protection Act (COPPA), designed to protect children and sensitive personal data. CIPA, for example, requires schools to have technology and policies in place that protect students from harmful materials, including those that are obscene and pornographic.[7] Website filtering and application control are two ways IT can restrict what students are able to access over school networks or through school-provided laptops.

Do it all with limited resources. K-12 IT teams remain resource- and budget-constrained. Some districts share a chief information security officer; others have none. In many cases, districts are managing older or end-of-life network equipment. Their security infrastructure may offer only limited visibility and control across the entire network, which poses both security and compliance risks.

With more than 2,200 school districts as customers, Fortinet understands the challenges of security in K-12 education. The security roadmap offered here adapts the Fortinet Security Fabric to the unique needs of the K-12 environment, helping technology directors manage the complex challenges mentioned above.

Many school districts have implemented the Fortinet Security Fabric as a foundation on which to build their network security strategies. Example implementations are available on the Fortinet website.

WHAT IS THE FORTINET SECURITY FABRIC?

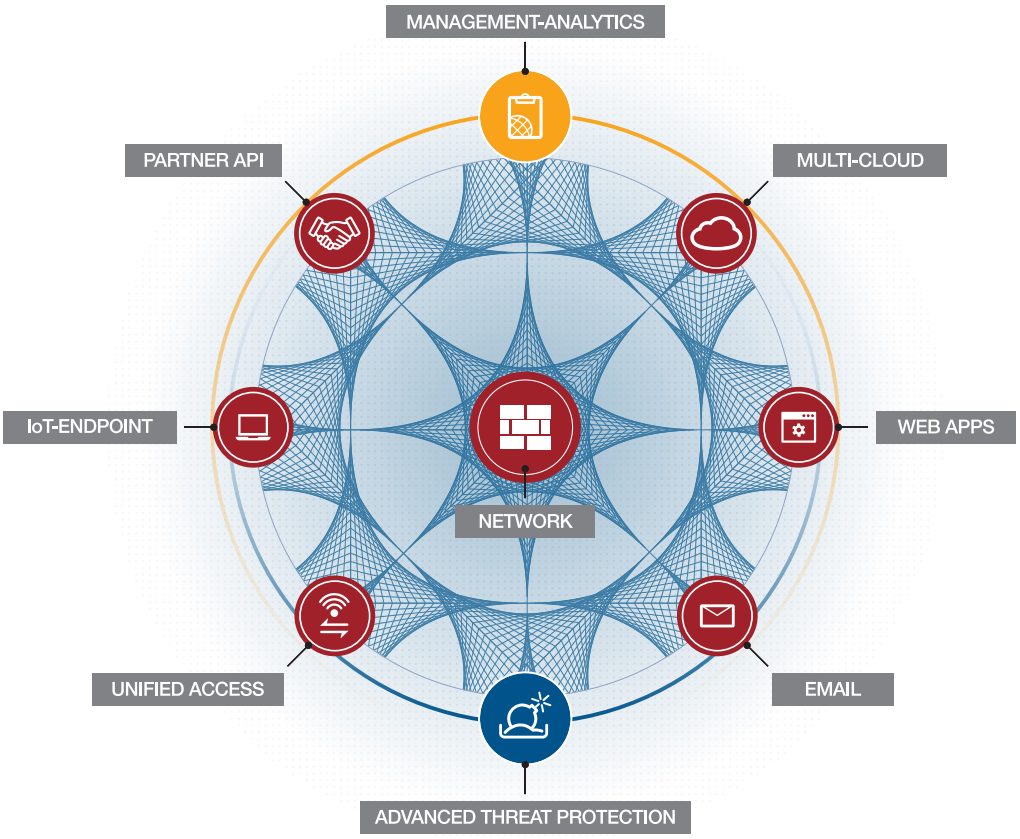
The Fortinet Security Fabric weaves all of Fortinet's powerful security components into a cohesive, automated, end-to-end security solution. The fabric has three key attributes:

Broad. It scales easily and provides security coverage across the entire attack surface. The fabric also enables better visibility across the entire network and extends protection to school-issued devices even while off campus.

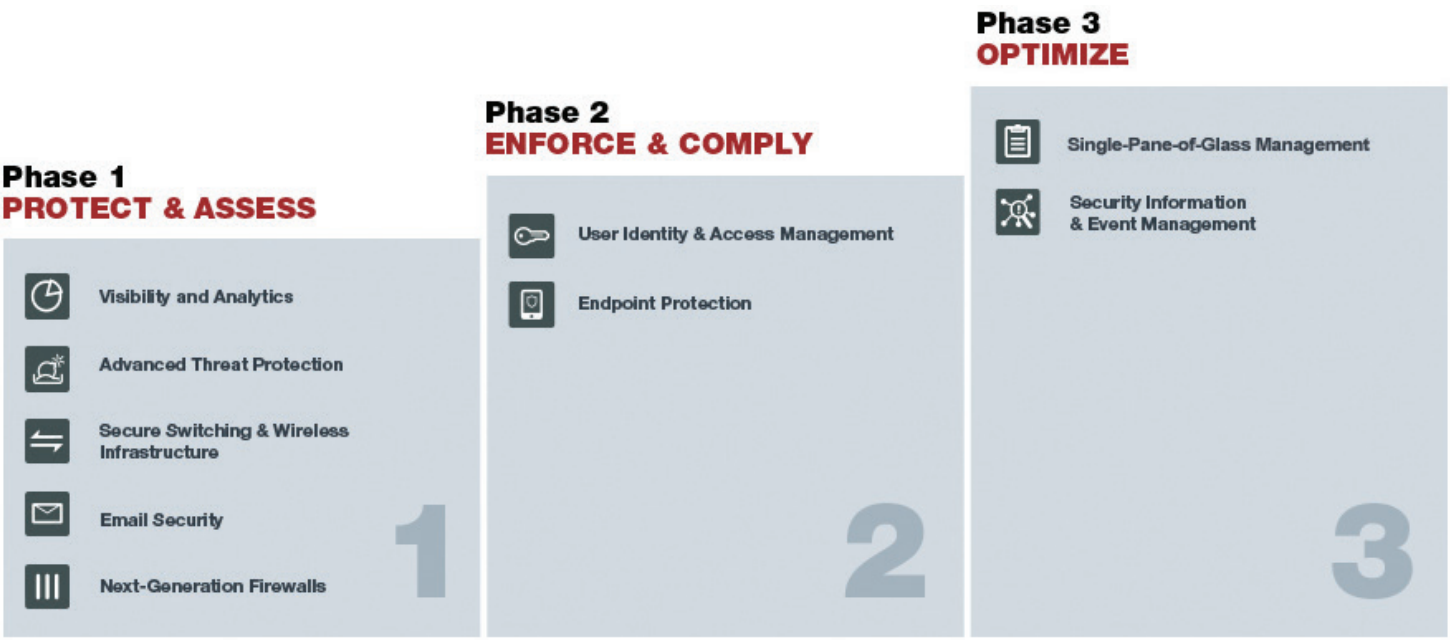
Integrated. The Security Fabric works as a complete, unified system, providing protection across all K-12 devices and systems, such as Chromebooks, learning management systems, and Internet of Things (IoT) devices.

Automated. The synchronized response of the Fortinet Security Fabric facilitates fast and coordinated response to threats. It relieves IT of the burden of manual monitoring, logging, and reporting while providing real-time threat intelligence to capture known and unknown threats and prevent their further intrusion.

As K-12 IT teams build their security roadmap and begin their journey, employing a fabric approach will ensure that each new component integrates completely with the overall security solution. That synergy is key to providing comprehensive security coverage for users, devices, and applications across the entire network.



THE SECURITY JOURNEY



FORTINET PARTNERS WITH K-12 SCHOOL DISTRICTS AT EVERY PHASE OF THEIR SECURITY JOURNEYS.

The roadmap to a K-12 Security Fabric helps districts move quickly and confidently toward a defensible and compliant security infrastructure. It consists of three phases:

1. Protect networked assets and assess vulnerabilities
2. Enforce policies and comply with regulations
3. Optimize operations

Accommodating districts that differ in their network complexity, IT staffing, and budget constraints, Fortinet offers easy-to-acquire and fully supported security technology that integrates with many third-party products.

PHASE 1: PROTECT AND ASSESS

The initial priority in the security journey is to build a foundational security infrastructure that will provide visibility and control across the district and prevent, detect, and mitigate threats in real time.

PERIMETER NETWORK SECURITY: FORTINET NEXT-GENERATION FIREWALLS (NGFWS)

FortiGate NGFWs offer all-in-one threat prevention, including firewall, antivirus, application control, and intrusion prevention capabilities. This eliminates the need for school districts to deploy and manage separate point products, such as a secure web gateway (SWG) or intrusion prevention system (IPS). FortiGate NGFWs also perform secure sockets layer (SSL) packet decryption and inspection, enabling CIPA compliance in the completely SSL-encrypted Google Chrome environment.

Even with all the threat prevention and SSL inspection features turned on, FortiGate NGFWs sustain excellent throughput for educational and administrative applications and consistently score high in third-party performance tests. This is due to the continually refined FortiOS operating system and Fortinet's unique security processing units, which deliver superior performance compared with off-the-shelf CPUs.

OBJECTIVES IN PHASE 1

- Gain visibility and insight into network vulnerabilities
- Defend the network edge, district data centers, and Internet service provider (ISP) interfaces
- Consolidate function-specific hardware into multifunction appliances
- Detect and respond to zero-day and other advanced threats
- Optimize wide-area network (WAN) bandwidth for cloud and mobile apps while controlling network costs
- Provision secure Wi-Fi access across the district

A final consideration for perimeter security is the implementation of software-defined wide-area networking (SD-WAN). Educators are increasingly looking to Software-as-a-Service (SaaS) subscriptions to roll out eLearning programs. The problem is that traditional security provisions, based on backhauling traffic through the data center, introduce unacceptable latency into cloud-based applications. Dedicated, managed MPLS connections are expensive, and they may not be fully utilized if the applications they support are not in continuous use. Fortinet's SD-WAN solution, implemented in the secure environment of the FortiGate NGFW, provides application-level control over WAN traffic and helps make efficient and economical use of all available WAN services.

EMAIL SECURITY

School and district office staff may dread their overflowing inboxes, but email remains a key productivity tool. Teachers also rely heavily on email to communicate with parents and students. So, it doesn't bode well for K-12 districts that email is the most common vector for malware attacks, with nearly two-thirds of malware installed through email attachments.[8]

FortiMail email security supplements and supports cyber-awareness training by enabling students, faculty, and staff to engage with their email applications, unencumbered by threats, bullying, and other distractions. FortiMail inspects student, faculty, and staff email to filter out unwanted messages such as spam, malicious missives with phishing, malware, and imposter intent, as well as messages that contain content that may constitute a potential CIPA liability. Even if an employee falls prey to an attack such as an email phishing scam while accessing email from a home computer, a data loss prevention (DLP) feature in the FortiOS operating system enables FortiMail to prevent sensitive information, such as W-2s, from leaving the network.

ADVANCED THREAT PROTECTION

By the time news breaks about one district falling prey to a new cyber threat, other districts' networks could already be infected. That's why advanced threat protection is a must. Advanced threat protection is designed to thwart all types of threats, even previously unknown, highly evasive, or transient ones, which may be present for only a few seconds.

As soon as a possible threat is detected by a FortiGate, FortiWeb, FortiMail, or FortiClient device, **FortiSandbox** quarantines the suspicious files and inspects them at a deeper level in an isolated environment. It then shares information about the detected threats in real time with all threat prevention devices on the distributed network, immunizing the entire district. It also reports to the threat research team at FortiGuard Labs to benefit the global community.

LOCAL AREA NETWORKS (LANS): SECURE SWITCHING AND WIRELESS INFRASTRUCTURE

K-12 school campuses are becoming saturated with Wi-Fi users. In addition to cellphones and school-issued tablets and Chromebooks, more schools are expanding BYOD policies, allowing users to connect to the network from their own devices. And these users don't stay put. As they roam the campus, or connect and disconnect from the network, the attack surface fluctuates rapidly. To maintain both network availability and security under these conditions, Fortinet offers a Secure Unified Access solution:

- **FortiAP** wireless access points to easily provision secure Wi-Fi to meet growing demand
- **FortiWLC** wireless controllers to optimize client distribution and RF channel utilization
- **FortiWLM** wireless LAN managers to provide service-level assurance across the network
- **FortiSwitch** to extend the protection of the FortiGate NGFW quickly and cost-effectively to new LAN segments such as computer labs or portable classrooms

The integration of the switching and wireless products with the FortiGate NGFW enables IT to apply common security policies throughout the network.

VISIBILITY AND ANALYTICS

FortiAnalyzer is a software tool that IT teams can use both to provision Fortinet devices and to analyze the data that these devices collect. With FortiAnalyzer's **FortiView**, staff can see all the deployed devices across the district and gain critical insights into threats across the entire attack surface. With FortiAnalyzer's situation awareness, real-time threat intelligence, and actionable analytics, one IT staff member can manage hundreds of security nodes.

FORTISANDBOX IS INDEPENDENTLY TOP-RATED

- NSS Labs "Recommended" for breach detection[9]
- ICSA Labs certified for advanced threat defense[10]

PHASE 2: ENFORCE AND COMPLY

Once a solid security foundation is successfully established, IT teams can easily extend it with tools that support the implementation of district cybersecurity policies and enable compliance with CIPA, FERPA, and COPPA regulations.

USER IDENTITY AND ACCESS MANAGEMENT

Users of K-12 district networks are diverse and highly mobile, making access management challenging. Students, faculty, and staff all have different rights to access data and applications. Contractors must access the network to maintain and repair networked operational technology, such as HVAC, lighting, and fire alarms. Schools may also wish to provide visitors Internet access while ensuring that they cannot access applications and data on the school network.

FortiAuthenticator simplifies and centralizes the management of user identity information and provides secure, role-based network access with user identification and session tracking.

It can be used in a variety of ways. For example, to help districts comply with CIPA regulations, FortiAuthenticator integrates with Chromebooks in the classroom, enabling seamless single sign-on for students. For more secure site-to-site VPN connectivity between school campuses or with the district office, FortiAuthenticator streamlines certificate management, making it more feasible to use certificates instead of the riskier pre-shared keys for VPN authentication.

FortiAuthenticator maintains a user identity management database, where it stores user login credentials, IP addresses, and group details, which can be shared with multiple FortiGate NGFWs. Per-user authentication levels accommodate different access control needs for student teachers versus full-time faculty, school site staff versus district-level staff, or even students in good standing as opposed to those who must be restricted in their network access.

ENDPOINT PROTECTION

Because K-12 network users are highly mobile and vary in their levels of caution and compliance, it's risky to rely solely on cybersecurity training to secure endpoints and to keep them from becoming attack vectors. FortiClient detects and blocks malicious objects from web, email, network, and personal storage targeting endpoint devices. **FortiClient** delivers easy-to-manage, automated, fully customizable endpoint security for a wide range of devices, including Chromebooks.

FortiClient also provides web filtering at the host, allowing schools and districts to take measures against cyberbullying. Access controls also help restrict access to gaming applications such as Roblox and prohibit the download or installation of gaming applications on local machines.

OBJECTIVES IN PHASE 2

- Strengthen and simplify user identity management
- Enforce content filtering and user access policies
- Secure endpoints, including Chromebooks
- Automate security provisioning across the district

CIPA COMPLIANCE WITH FORTINET SOLUTIONS

- Granular controls for application use and web content filtering
- Antivirus, intrusion prevention, and data loss prevention to protect against malicious content, unlawful activities, and disclosure of sensitive data

PHASE THREE: OPTIMIZE

While eLearning and the overall digital transformation of the K-12 environment are expanding rapidly, IT staffing and budgets are not. One security architect said at a recent CoSN conference that he sees "roughly 500,000 attacks per hour on the school networks he monitors—far more than a small IT team can be expected to handle with 100 percent success."[11] Technology directors who want to implement tight network security must streamline their operations so that a few IT team members can provision and competently manage security from the district office.

SINGLE-PANE-OF-GLASS MANAGEMENT

The cloud- or appliance-based **FortiManager** provides centralized security management, giving administrators full control over the entire school or district security architecture. Easy-to-use tools accelerate the deployment of security policies, updates, configurations, and revisions, while the centralized, single-pane-of-glass management console provides complete visibility into the school's security posture.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Just as the technology director's role has merged network and security operations, the management of these functions is merging as well. SIEM systems, typically part of a security operations center, can be equally at home in the network operations center. **FortiSIEM** provides real-time analysis of security alerts generated by applications and network hardware. It also provides rapid detection and remediation of security events while aiding security, performance, and compliance management.

OBJECTIVES OF PHASE 3

- Provide greater visibility into the security infrastructure
- Accelerate and simplify security administration

A PROVEN PARTNER FOR THE K-12 SECURITY JOURNEY

Districts that have reached this point in their security journey with Fortinet will have a well-established Security Fabric that supports a highly resilient cyber program for their digitally transforming schools.

The advantage of the Security Fabric is not just in its holistic nature but also in the quality of each of its components. K-12 technology directors will find that Fortinet Security Fabric components rank with leading best-of-breed security point products and platforms.

Fortinet frequently participates in third-party tests, consistently earning top scores. Fortinet has earned "Recommended" ratings for eight different products in tests by NSS Labs, an independent research and testing organization. This is more than any other network security vendor. Fortinet also regularly receives certifications from ICSA Labs, Virus Bulletin, and more. These unbiased validations let IT administrators know which products perform the best and deliver the lowest total cost of ownership (TCO), helping them make informed decisions.

Similarly, research and advisory firm Gartner provides insights on technology and vendors to help business leaders make purchasing decisions. Multiple Fortinet solutions can be found in Gartner Magic Quadrants, including Enterprise Network Firewall, Unified Threat Management (UTM), Wired and Wireless LAN, and Web Application Firewall.

By combining its Security Fabric approach with a prioritized long-term execution plan, Fortinet makes it easier for K-12 schools and districts to map and implement their security journeys. With world-class support, including consulting and advisory services for the E-rate program, as well as a talented partner community and a low TCO, Fortinet is the ideal K-12 security partner.

FORTINET'S E-RATE ELIGIBLE PRODUCTS

Fortinet offers multiple solutions that are eligible for category 2 funding from the E-rate program:

- FortiGate
- FortiAP
- FortiSwitch
- FortiCache

[1] "The CIS Critical Security Controls for Effective Cyber Defense," SANS Institute, accessed May 8, 2018.

[2] CoSN Cybersecurity Leadership Initiative, CoSN, accessed May 8, 2018.

[3] K-12 Cybersecurity Resource Center, EdTech Strategies, accessed May 7, 2018.

[4] Paula Maylahn, "2018 K-12 IT Leadership Survey Report," CoSN, 2018.

[5] Maritsa Georgiou, "Schools re-examine cybersecurity measures after Flathead hacking," nbcmontana.com, September 22, 2017.

[6] Ryan Johnston, "People, plans and passwords: School IT managers outline best cybersecurity practices," edscoop.com, February 15, 2018.

[7] Children's Internet Protection Act (CIPA), Federal Communications Commission website, accessed May 9, 2018.

[8] "2017 Data Breach Investigations Report," Verizon, April 2017.

[9] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, May 2018.

[10] "Q1 2018 Advanced Threat Defense Certification Testing Report: Fortinet, Inc. Advanced Threat Protection Solution," ICSA Labs, April 2, 2018.

[11] Ryan Johnston, "People, plans and passwords: School IT managers outline best cybersecurity practices," edscoop.com, February 15, 2018.

[12] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, May 2018.

[13] E-rate is the common name for the Universal Service Schools and Libraries Program, which helps ensure that schools and libraries can obtain high-speed Internet access and telecommunications at affordable rates.

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
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

June 28, 2018 12:29 PM
173251-0-A-EN
wp-charting-the-security-k-12-school-062818-1229pm