SECURING DIVERSE NETWORK ENVIRONMENTS FOR K-12 SCHOOL DISTRICTS

EXECUTIVE SUMMARY

Cybersecurity is rarely one of the top considerations when planning for K-12 school technology needs—but times are changing. From January 2016 through November 2018, there were 386 cyber incidents in U.S. public schools alone.[1] These attacks resulted in the disclosure of personal information, the loss of taxpayer dollars, reduced instructional time, and increased identity theft. School districts must define and implement a comprehensive security architecture that provides end-to-end network visibility, dynamic access control, and automated threat responses. As part of the Fortinet Security Fabric, FortiNAC offers an ideal network access control (NAC) solution. Its compatibility with a wide range of third-party security solutions helps schools secure sensitive data while maximizing limited budgets.

BALANCING THE NEEDS OF THE HIGHLY DIVERSE K-12 COMMUNITY

Cybercriminals are now targeting vulnerable K-12 schools to steal personal information and using ransomware to shut down access for financial gain. Securing today's primary and secondary school networks require:

- Knowing and controlling who has access to the network
- Ensuring appropriate access restrictions
- Constantly monitoring all activity
- Automatically quarantining devices that behave suspiciously

Securing the K-12 network is challenging. Schools must protect school-owned devices such as tablets, laptops, lab devices, and integrated smart boards while at the same time securing access for students, teachers, and staff with BYOD laptops, smart phones, and e-readers. In addition, there has been a dramatic rise in Internet of Things (IoT) devices being introduced to school networks. Many districts now use things like internet-enabled printers, security cameras, and HVAC sensors. While IoT devices are fantastic at streamlining operations and automating systems, most of these products lack built-in security and therefore require compensating protection.

K-12 SCHOOL NETWORKS CAN CONTAIN VALUABLE DATA, SUCH AS:

- **Personal data of students and parents**—for example, contact details and social security numbers
- **Employment records for faculty and staff**—for example, personal details, social security numbers, tax information, and banking information for direct deposits

FORTINAC PROVIDES:

- Complete visibility and automated onboarding onto the appropriate VLAN for all endpoints, including BYOD and IoT
- Pre-connect and post-connect device monitoring
- Granular network access controls to enforce minimum security requirements (OS, antivirus)
- Custom access levels by device, user, age group, or role
- Automated threat responses to quarantine suspicious devices

Another security challenge facing schools is the dramatic difference in access needs between younger primary students and older secondary students who often take distance-learning courses for college credit in their junior and senior years. Faculty must have continuous, secured access as well. Teachers rely on online solutions to manage homework assignments and grades, as well as sources for the digital content that enhances today's smart classrooms.

Unfortunately, threats don't always originate outside the network. Some attacks come from within the firewall, where digitally savvy students insert malware to record passwords or hack into the network to gain access to grades. It is now essential that schools have complete visibility into every connected device and action taken within the network.

Protecting today's K-12 environments requires securing appropriate access for large volumes of varied devices in one simple solution. Schools must incorporate access and device controls with simple, seamless onboarding to ensure a productive and secure learning environment that meets the needs of all students and teachers.

COMPREHENSIVE SECURITY WITH CUSTOMIZABLE CONTROLS

As part of the Fortinet Security Fabric architecture, FortiNAC offers a network access control (NAC) solution that provides:

VISIBILITY

With thousands of endpoint devices, identifying "who, what, when, and where" is critical to protecting all devices on the network. FortiNAC provides the deepest level of network endpoint visibility that also delivers contextual information to speed incident review. It profiles every endpoint and infrastructure device on the network, provides contextual awareness about the device, user, and applications, and monitors all activity. From identifying rogue devices to speeding forensic investigations, complete visibility is now a necessity for schools.

CONTROL

FortiNAC provides simple, automated on-boarding and highly customizable dynamic access controls. Network access can be assigned using automated, pre-defined profiles—saving a significant amount of time when provisioning access for the diverse needs of students, faculty, and staff. FortiNAC provides granular control of endpoint access policies and permissions by role or by user to ensure that users only receive the necessary level of access.

FortiNAC integrates with other Fortinet solutions as well as third-party security products to help schools to set and enforce minimum security requirements for current operating system patches, antivirus software, and more.

FortiNAC integrates with other Fortinet solutions as well as third-party security products to help schools to set and enforce minimum security requirements for current operating system patches, antivirus software, and more. Using a pre-connect scan, FortiNAC only grants access to devices that meet established requirements and can automatically direct users to a self-remediation page for those that don't qualify. FortiNAC also provides continuous post-connect scanning to look for devices and or users that act suspiciously or fall out of network compliance.

AUTOMATED THREAT RESPONSES

FortiNAC's automated threat response can immediately quarantine suspicious devices/users, triage events, and speed forensic reviews by delivering all contextual information along with the alert. By leveraging contextual awareness from the broader Fortinet Security Fabric, FortiNAC helps analyze and prioritize security alerts. It streamlines multi-step workflows and integrates with ticketing systems to provide real-time endpoint containment. This speeds time-to-resolution and reduces the burden on limited IT resources.

FortiNAC also acts as a compensating control for IoT devices with weak security. It monitors these devices for unusual behavior and automatically quarantines those that act suspiciously. For example, if an IoT device starts pinging a DNS server, it is tracked, an alert is generated, and the port can be immediately locked down while awaiting analyst review.

By leveraging contextual awareness from the broader Fortinet Security Fabric, FortiNAC helps analyze and prioritize security alerts.

K-12 CASE STUDY: ABBOTSFORD SCHOOL DISTRICT

The Abbotsford School District in British Columbia, Canada is comprised of about 18,500 students and 2,100 faculty and staff across 46 schools. If you combine every classroom across the district, its network supports approximately 10,000 unique devices on a given day.

Not long ago, student personal devices were depleting network bandwidth needed to support institutional operations. Moreover, access for school-owned devices was constantly being compromised, allowing unknown devices onto the network. According to Shelley Wilcox, the director of Technology at Abbotsford School District, "[The district] needed a solution that would give us better control of our network—a solution that would tell us who's trying to connect and can automatically route them to the right network. We also needed to be able to track devices as they moved around the district and locate them if used inappropriately."

FortiNAC now helps Abbotsford schools identify all endpoint devices as they connect to the network. It performs compliance checks to ensure devices meet security standards and automatically puts them on the appropriate VLAN—one for school-owned devices used in the classroom and labs; a BYOD network for teachers, staff, and special-needs students; and a BYOD network for students and guests. "Now you can walk into any facility and FortiNAC will automatically recognize your device and put you on the right network," says Wilcox.

In addition to controlling access, FortiNAC detects and identifies devices that are already on the network. "We discovered more than 1,000 unregistered, rogue devices which we can now register or block, since authentication occurs through active directory," Wilcox says. He notes that this kind of visibility and access control are very helpful when investigating an incident. "When you have a powerful tool in the pocket of every kid, you can't see everything all the time," Wilcox observes. "Now, using FortiNAC with our firewall, we know exactly what is on the network. We can identify the device, where it is, what it's doing, and who is using it. It's a very powerful combination."

FortiNAC also eliminates the need to manage multiple service set identifiers (SSIDs) at each school, and Wilcox no longer needs to send teams to different schools to reset compromised SSID passwords—something that was very time-consuming for the IT department. "Schools thank us because we're no longer constantly resetting passwords that students had hacked and texted to everyone, and their networks are no longer overwhelmed," says Wilcox.

"Using Fortinet's NAC solution, we have much higher security because we know exactly what's on the network, how each device is connected, where it's located, and who is using it. FortiNAC enables us to provide better security and increased user satisfaction, and that's huge."

- Shelley Wilcox
Director of Technology
Abbotsford School District

DETAILS

CUSTOMER: Abbotsford School District
INDUSTRY: Education
LOCATION: Abbotsford, British Columbia, Canada

BUSINESS IMPACT

- Automatically provisions network access based on predefined BYOD policies
- Ensures that only authorized users and devices can access the network
- Remediates noncompliant devices
- Integrates with firewalls to help remediate devices on the network if cyber abuse or inappropriate activity is identified
- Tracks all devices across the school district
- Cuts administrative overhead and improves the user experience

SOLUTIONS

- FortiNAC Network Access Control

SEAMLESS PROTECTION

FortiNAC offers unparalleled visibility, control, and automated threat responses for educational network access. Beyond those core capabilities, FortiNAC can be deployed as a hard¬ware appliance, a virtual appliance, or a cloud service—offering school security architects a flexible, third-generation NAC solution that can adapt to the unique needs of any network environment. Designed for flexibility and simple, central management, FortiNAC helps lower total cost of ownership (TCO) by not requiring a server in every deployment location and can be seamlessly integrated with existing network technology investments.

FortiNAC offers unparalleled visibility, control, and automated threat responses for educational network access.

[1] "The K-12 Cyber Incident Map," K-12 Cybersecurity Resource Center, November 2, 2018.

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
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

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

310350-0-0-EN
November 16, 2018 2:15 PM
D:\Fortinet\Work\November 2018\111418\sb-cybersecurity-threats-K-12-school-networks