FORTINET

CREATE SAFER SCHOOLS AND CAMPUSES WITH PHYSICAL AND CYBER SECURITY SOLUTIONS FROM FORTINET

WHITE PAPER

EXECUTIVE SUMMARY

Violence in U.S. schools and campuses is not uncommon. In fact, almost 75% of public schools experience at least one incident of violence per year.[1] Although bullying is the most common form of violence, fatalities, though rare, are occurring with more frequency and are particularly devastating.[2] Today, many schools have in place surveillance cameras, metal detectors, and other devices to safeguard the well-being of all students and staff, but a new approach is needed. One of the top recommendations from a recent study identifies the use of new or nontraditional technologies as a top priority in addressing school safety and violence issues.[3] Integration of these technologies is key, where physical and cyber security solutions seamlessly work together to detect and minimize violence in schools and on campuses.

SCHOOL SAFETY IS A PROBLEM

With violence on the rise, something clearly needs to change to ensure the safety of students and staff at our nation's schools. Not only is there an urgency to shrink the window in response times to acts of school violence, there is also a critical need to implement self-sufficient technologies, which allow schools to respond to a crisis in the first few minutes prior to the arrival of law enforcement and other professional responders. All technologies—both hardware and software—must integrate. Specifically, the processes of merging physical and cyber security solutions as well as new technologies must create a holistic approach to school safety that can prevent, reduce, and effectively respond to school violence.

Funding is also part of the overall equation. Although financial restraints might imply roadblocks to adequate security, the opposite might be true.[4] Schools can leverage federal funding initiatives such as the Student, Teachers, and Officers Preventing (STOP) School Violence Act of 2018 and E-rate for secure telecommunications and internet access to address physical and cyber security issues at schools and campuses.

CONSIDERATIONS DRIVING SOLUTIONS

There are four considerations, in general, that are driving the need for implementing nontraditional technologies to address school safety, and in particular, prevent violence on school grounds:

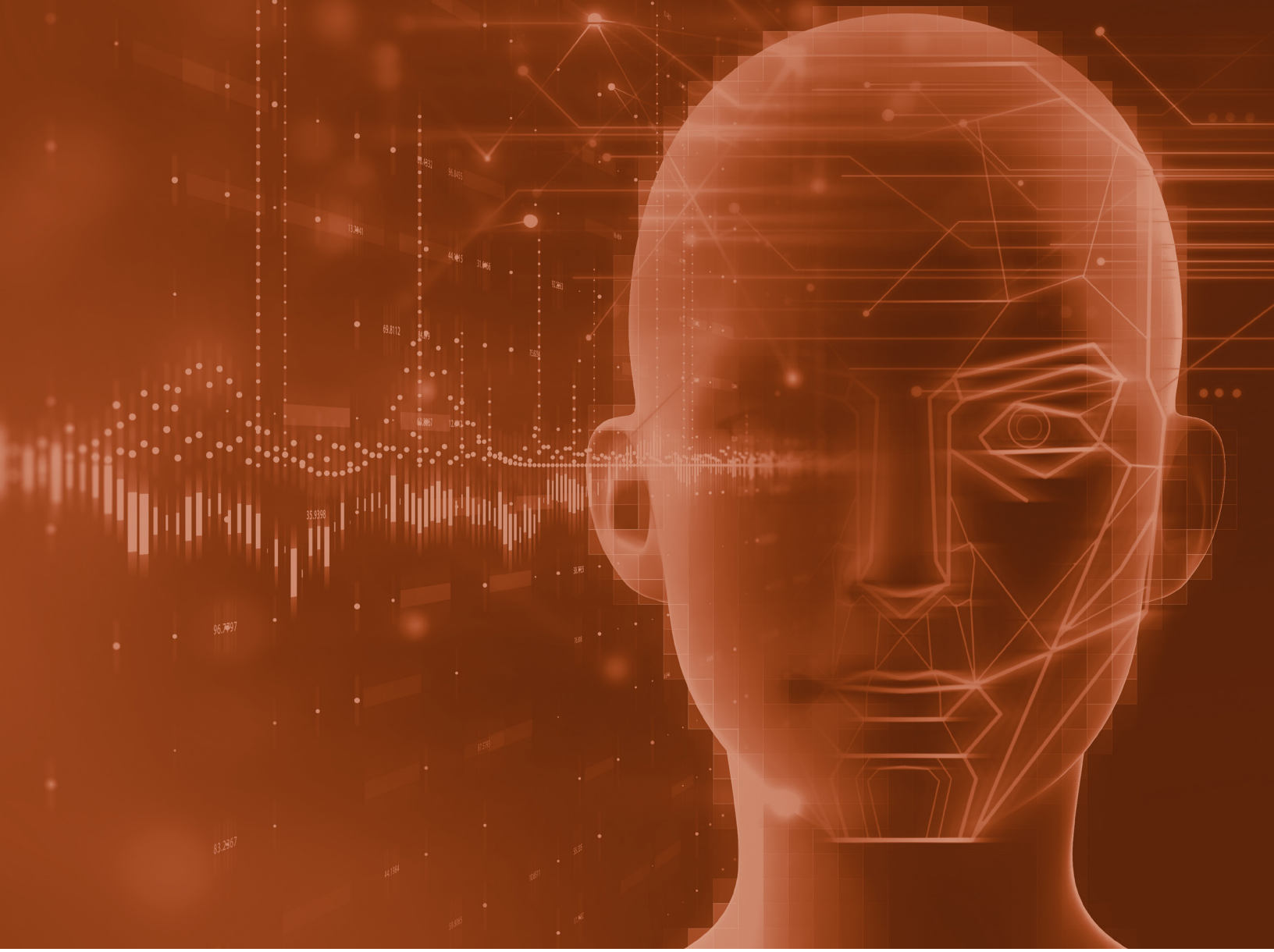
- Violence across the spectrum
- Integrating physical security into the network
- Facial and device recognition and object detection
- Children's Internet Protection Act (CIPA) and other regulations

VIOLENCE ACROSS THE SPECTRUM

Most schools experience some form of violence at least once a year. Cyber and physical bullying, assault, cyber and verbal threats, and weapon carrying are the most common type of violence.[5] Any solution must address the full spectrum of violence.[6] Proactive responses can be facilitated by monitoring real-time data aggregation (e.g., from video surveillance and social media), making intervention possible before emergencies occur.[7] For tier-one violence incidents, which require medical and/or security requests, the length of emergency response time needs to decrease, even at urban schools, which historically have shorter response times. Longer response times—usually the case at suburban and rural schools—generally require a greater need for self-sufficient technologies that enable responses to crises within the first few minutes before law enforcement and other professional responders arrive. Because of the wide spectrum of violence, a targeted response to threats is key.[8]

INTEGRATING PHYSICAL SECURITY INTO THE NETWORK

There is growing recognition across multiple industry segments that keeping physical and cyber security separate is a mistake.[9] Running security cameras and recording devices (the "physical" security of the equation) need to reside on next-general firewalls (NGFWs) (the "cyber" security part of the equation), which keep them safe from ransomware, botnets, and other forms of hacking. At the same time, the combination enables schools to ensure that their physical security devices have sustained high-performance network bandwidth. And in the event of a malicious intrusion of the physical security devices, network segmentation quarantines infected cameras and prevents the malicious intrusion from spreading to other cameras or areas of the network. Integration of physical security also enables schools to monitor and block network access (e.g., email and web) for students (e.g., an expelled student) and third parties deemed violent or dangerous.



FACIAL AND DEVICE RECOGNITION AND OBJECT DETECTION

Facial recognition enables schools and educational institutions to upload photos or images of a student or other perpetrators and pinpoint or flag every location where the student or perpetrator has been detected on campus at any given time. Depending on the severity of the incident or risk of the individual in question, facial recognition allows school officials or other authorities to send notifications, alerts, and alarms to appropriate personnel. In addition, photos and videos of pedophiles, sex offenders, expelled students, et al. can be uploaded, enabling schools to receive real-time alerts, determine their location, and rapidly remove them from school premises. Object recognition enables schools and institutions to identify weapons, backpacks, and other objects that could be used by students or others to carry out violent acts. As with facial recognition, schools can activate notifications, alerts, and alarms in real time using object recognition. And when physical and cyber security systems are integrated, they can also activate technological controls such as dedicating higher network bandwidth for specified devices, applications, and users.

CHILDREN'S INTERNET PROTECTION ACT AND OTHER REGULATIONS

E-rate includes funding initiatives from the Federal Communications Commission (FCC) that provide technology discounts for telecommunications and internet access to schools and public libraries. K-12 schools that receive discounts for internet access or internal connections through the E-rate program are required by CIPA to adopt and implement various protection measures to prevent and monitor access to content deemed obscene or harmful to students and minors.[10]

Schools that seek discounts offered by the E-rate program must provide ways to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and teaching about cyberbullying awareness and response.[11]

STOP appropriates $50 million per year to improve school security through the use of technologies, including developing threat assessment systems designed to stop would-be killers before they commit acts of violence.[12]

WHAT TO LOOK FOR IN A SOLUTION

The previous section highlights several points that should be carefully considered by IT managers and school administrators when assessing and then implementing physical and cyber security solutions. This section provides guidance on what to look for in physical and cyber security solutions that are designed to prevent or respond to violence on schools and campuses.

INTEGRATE PHYSICAL DEVICES INTO THE NETWORK

Schools need surveillance solutions that integrate into the network. This ensures that the cameras and recording devices have dedicated network bandwidth without any degradation in performance or interruption in connectivity. Integration of physical and cyber security also means that physical cameras and recording systems are protected from cyberattacks.

There are three key points to consider when integrating camera and recording solutions into your network:

- Dedicated network bandwidth to ensure 100% availability and streaming of video
- Rapid, easy deployment, including auto-recognition, of each camera and recorder
- Perimeter firewall protection, including segmentation and threat protection, of all cameras from external attacks

Integrating physical devices into the network allows for prioritization of bandwidth for cameras and also facilitates the deployment of each camera and recording system (e.g., enabling plug and play into the network). At the same time, this also ensures that physical devices are protected from malicious attacks.

AVOID OFF-THE-SHELF CAMERAS AND RECORDING DEVICES

There are a number of reasons educational institutions should steer away from off-the-shelf cameras and recording devices:

- They cannot provide facial and object recognition.
- They do not integrate into network security.
- They cannot provide historic and present location of object or person.
- They lack the “network intelligence” for high-performance bandwidth and speed.
- They often do not have the much-needed recording and playback features.
- They are not built to scale.

In addition to the above, with many institutions requiring hundreds or thousands of cameras and recording devices, they must be easily and quickly deployable. Off-the-shelf, stand-alone physical devices cannot be integrated into the NGFW infrastructure and require longer deployment cycles.

USE FAST AND INTELLIGENT BIOMETRICS

Incorporating fast and intelligent biometrics allows educational institutions to leverage machine learning and full integration with recording systems. This significantly decreases retrieval cycle times. That means seconds versus minutes (often 10 or more) with many camera and recording surveillance systems. With seconds often counting when it comes to many school violence incidents, solutions that cannot meet these requirements put students, faculty, and others at greater risk. For example, fast and intelligent biometrics allow law enforcement to respond more quickly if they know the specifics of who and what to look for.[13]

FUTURE-PROOF FOR FURTHER INTEGRATION

Integration with network security allows for additional integration of other security capabilities such as flagging web and email behavior on secure networks. It also enables institutions to enact physical security measures commensurate with the level of security risk.

And what about tomorrow’s landscape? Regulations such as CIPA are just part of the equation. The Jeanne Clery Act requires colleges and universities that participate in Title IV federal student financial aid programs to provide timely warnings of crimes to the student body and staff; to publicize campus crime and safety policies; and to collect, report, and disseminate campus crime data, including statistics for the preceding three calendar years, and details about efforts taken to improve campus safety.[14] Educational institutions must have a comprehensive and integrated security solution that addresses the ever-evolving attack surface, the complexity of managing security and compliance, including the growing number of state and federal laws and regulations designed to protect students and staff on U.S. schools and campuses.

THE FORTINET SOLUTION

Fortinet approaches school safety from the perspective that both physical and cyber security must be taken into account and moreover integrated for optimal protection. Fortinet offers a network-based security surveillance system for education with high-level features that are secure, simple to use, and deliver optimal price-performance results. The combination of FortiCamera and FortiRecorder with FortiGate NGFWs is a critical linchpin. FortiSwitch and FortiAP wireless access add better visibility and an easier-to-manage physical and cyber infrastructure.

When it comes to physical security, FortiCamera and FortiRecorder combine to provide network-based video security while simplifying Internet Protocol video surveillance. With FortiCamera, educational institutions can see everything: doors, hallways, and other public areas—any location they need to monitor and keep an eye on. FortiRecorder employs facial and object recognition, capturing the images for easy monitoring, storage, and retrieval. IT administrators or even facilities management personnel simply plug in the cameras, connect FortiRecorder, open a web browser or client application, and the physical monitoring is all set.

When it comes to capabilities, FortiCamera and FortiRecorder deliver short biometric retrieval cycles and use machine learning to constantly improve accuracy of video identification. This provides schools and campuses with motion or audio detection notifications instantly. You can also choose camera profiles and schedules and get a real-time overview through a dashboard.

FortiSwitch allows educational institutions to enable security features to protect their infrastructure with no decrease in speeds by aggregating and extending security features into and meeting the requirements of bandwidth-intensive data-center networks. FortiAP supports the demand for plug-and-play deployment for data, voice, and video applications. When it comes to integration, FortiCamera and FortiRecorder are integrated into FortiGate NGFWs, FortiAPs, and FortiSwitches and can be easily and quickly deployed to thousands of locations.

Fortinet's key capabilities include:

- Rapid, easy deployment via automatic discovery and provisioning when cameras are added to the network
- Priority and quality-of-service-based queuing of traffic
- Integrated SD-WAN capabilities built into FortiGate NGFWs that auto-provision and deliver least-cost routing and highest-priority routes.
- Decision-making at a network level rather than at a camera level
- Camera-policy enforcement

But capability is more than simply implementing physical and cyber security solutions. As educational institutions demand more capabilities from fewer components to save money and reduce complexity, they also expect reliability, continuity, and quick access. The Fortinet solution integrates physical and cyber security to allow IT to consolidate endpoints and manage network access from a single pane of glass, thereby increasing visibility, control, and reporting—important for managing access to and monitoring the internet, as required by CIPA and other regulations.

Integrating physical and cyber security solutions is enhanced when integrated with NGFWs. Seamless integration ensures that security devices—such as cameras and other recording devices—and software on the physical devices can be standardized on one platform, minimizing risk to cyber threats and other malicious activity. This is particularly important because 99% of firewall breaches are caused by firewall misconfigurations, not flaws in the firewall.

When it comes to NGFW infrastructure, FortiGate NGFWs provide high performance, consolidated advanced security, and granular visibility for broad protection across the entire digital attack surface. That's what Fortinet defines as the Fortinet Security Fabric, an architectural approach that's built around three keystones—broad, integrated, and automated—to unify security technologies deployed across the network into a single, integrated security system.

To stop or reduce violence in schools, it's imperative that physical and cyber security technological components communicate with each other, share continuous threat intelligence, and are easy to manage. FortiGate NGFWs reduce complexity and improve overall security posture by providing full visibility of users, devices, applications, and threats across the network. And as the different solutions from Fortinet are part of the Fortinet Security Fabric, threat intelligence is applied between the different pieces in real time.

CONCLUSION

Every year the vast majority of K-12 and higher educational institutions experience at least one incident of violence, which ranges across a wide spectrum. With incident detection and response time critical factors in mitigating the potential implications of safety incidents, an integrated physical and cyber security solution is pivotal.[15] Off-the-shelf camera and recording solutions are inadequate, failing to provide the requisite scalability, ease of deployment, intelligence, and cybersecurity protections. Unless all components can be easily integrated and managed—and are compliant with CIPA and other laws and regulations—it becomes nearly impossible to focus on one of the critical roles that educational institutions must play today: protecting students and staff from acts of violence on schools and campuses.

FortiCamera and FortiRecorder, combined with FortiGate NGFWs, FortiSwitch devices, and FortiAP wireless access points, integrate physical and cyber security for a high-performance, easily accessible surveillance camera system. The Fortinet Security Fabric lets educational institutions keep an eye on the distributed network to detect advanced threats and quickly adapt to the evolving network architecture and threat landscape. Fortinet provides a powerful, scalable, reliable, and highly secure solution that helps meet the aggressive, evolving requirements of school safety issues to detect and minimize violence in the school environment.

[1] S. Robers, J. Kemp, A. Rathbun, and R. E. Morgan, "Indicators of School Crime and Safety: 2013," U.S. Department of Education, U.S. Department of Justice, and Office of Justice Programs, June 2014.

[2] Heather L. Schwartz, Rajeev Ramchand, Dionne Barnes-Proby, et al., "The Role of Technology in Improving K-12 School Safety," A Project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver, 2016.

[3] "The Role of Technology in Improving K-12 School Safety."

[4] Kenneth S. Trump, "Keeping Schools Safe During Tight Budget Times," National School Safety and Security Services, September 2010.

[5] "Indicators of School Crime and Safety: 2013."

[6] "The Role of Technology in Improving K-12 School Safety."

[7] Ibid.

[8] Ibid.

[9] "The Case for Integrating Physical and Cyber Security," Wall Street Journal, February 8, 2018.

[10] Children's Internet Protection Act (CIPA), https://www.fcc.gov/consumers/guides/childrens-internet-protection-act, accessed April 16, 2018.

[11] "Protecting Children in the 21st Century Act Amendment,"https://www.fcc.gov/document/protecting-children-21st-century-act-amendment, accessed April 16, 2018.

[12] H.R. 4909: STOP School Violence Act of 2018, https://www.govtrack.us/congress/bills/115/hr4909/summary, accessed April 18, 2018.

[13] "The Role of Technology in Improving K-12 School Safety."

[14] "Summary of the Jeanne Clery Act," https://clerycenter.org/policy-resources/the-clery-act/, accessed April 25, 2018.

[15] Ibid.

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

May 1, 2018 3:54 PM

182382-0-A-EN

wp-creating-safer-school-with-fortinet-050118-354pm