K-12 BLUEPRINT

Creating Safe Learning Environments

School learning environments must meet academic needs for internet connectivity while simultaneously minimizing cyber risks. Meanwhile, on-premises data and cloud resources must all meet security protocols while meeting demanding performance requirements. And security policies for teachers, students and administrators must all be upheld and enforced across the district.

Keeping students and their data safe, while maintaining a modern and engaging learning environment, is a precarious juggling act. Legacy security systems leave much to be desired in dealing with the increasing sophistication and frequency of cyberattacks. Manual detection is usually a case of desperately mitigating the damage from an attack that has already happened, which can prove expensive in terms of time, money and resources. Comprehensive protection involves integrated and automated controls to detect and prevent threats at every stage of the attack lifecycle.

In Fighting (Plat)Form

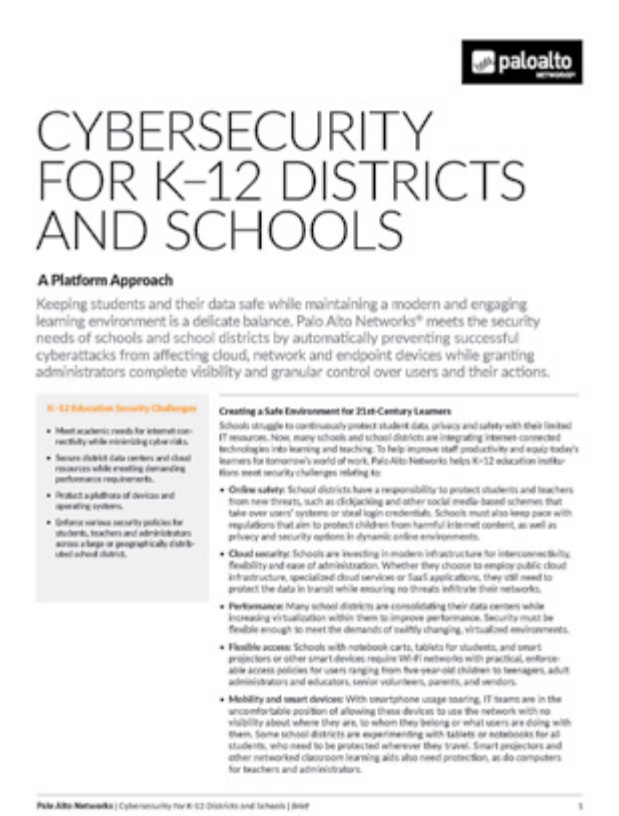
A security operating platform can do much to protect students from inappropriate content through content filtering on school-owned devices both inside and outside the network as well as BYOD (Bring Your Own Device) devices inside the school network. And this level of protection comes with simplified security operations due to automated threat intelligence. A security operating platform offers full visibility into all traffic and provides the context necessary to enforce dynamic security and reduce attacks. Detailed threat intelligence, analysis and protections prevent both known and unknown threats.

A Security Operating Platform typically provides the following overarching benefits:

- **Visibility** of all users and devices across the network, including endpoint, cloud and SaaS (Software as a Service) applications.
- **Reducing the attack surface** through integrated technologies.
- **Known threat prevention** across different security controls for quick identification and threat response.
- **Unknown threat detection** through the automated creation and delivery of near-real-time protections against new threats.

The elements of a security operating platform must be implemented in the correct positions within a security architecture while remaining agile and automatically sharing new threat data. It should also have the ability to automatically extend new protections based on this new data to stop the spread of an attack. In this way, schools can implement the latest learning applications and technologies safely and securely.

A New Approach to Security



paloalto

CYBERSECURITY FOR K–12 DISTRICTS AND SCHOOLS

A Platform Approach

Keeping students and their data safe while maintaining a modern and engaging learning environment is a delicate balance. Palo Alto Networks® meets the security needs of schools and school districts by automatically preventing successful cyberattacks from affecting cloud, network and endpoint devices while granting administrators complete visibility and granular control over users and their actions.

K–12 Education Security Challenges

- Meet academic needs for internet connectivity while minimizing cyber risks.
- Secure district data centers and cloud resources while meeting demanding performance requirements.
- Protect a plethora of devices and operating systems.
- Enforce various security policies for students, teachers and administrators across a large or geographically distributed school district.

Creating a Safe Environment for 21st-Century Learners

Schools struggle to continuously protect student data, privacy and safety with their limited IT resources. Now, many schools and school districts are integrating internet-connected technologies into learning and teaching. To help improve staff productivity and equip today's learners for tomorrow's world of work, Palo Alto Networks helps K–12 education institutions meet security challenges relating to:

- **Online safety:** School districts have a responsibility to protect students and teachers from new threats, such as clickjacking and other social media–based schemes that take over users' systems or steal login credentials. Schools must also keep pace with regulations that aim to protect children from harmful internet content, as well as privacy and security options in dynamic online environments.
- **Cloud security:** Schools are investing in modern infrastructure for interconnectivity, flexibility and ease of administration. Whether they choose to employ public cloud infrastructure, specialized cloud services or SaaS applications, they still need to protect the data in transit while ensuring no threats infiltrate their networks.
- **Performance:** Many school districts are consolidating their data centers while increasing virtualization within them to improve performance. Security must be flexible enough to meet the demands of swiftly changing, virtualized environments.
- **Flexible access:** Schools with notebook carts, tablets for students, and smart projectors or other smart devices require Wi-Fi networks with practical, enforceable access policies for users ranging from five-year-old children to teenagers, adult administrators and educators, senior volunteers, parents, and vendors.
- **Mobility and smart devices:** With smartphone usage soaring, IT teams are in the uncomfortable position of allowing these devices to use the network with no visibility about where they are, to whom they belong or what users are doing with them. Some school districts are experimenting with tablets or notebooks for all students, who need to be protected wherever they travel. Smart projectors and other networked classroom learning aids also need protection, as do computers for teachers and administrators.

Palo Alto Networks | Cybersecurity for K-12 Districts and Schools | Brief 1

Palo Alto Networks has released a brief entitled A Platform Approach: Cybersecurity for K-12 Districts and Schools that lays out the essential components of a safe, 21st century learning environment.

The brief addresses the responsibility school districts have in protecting students and teachers from new threats (such as "clickjacking": tricking a user into clicking on something different from what the user perceives, allowing others to take control of their computer) while keeping pace with regulations that aim to protect student data. There are also challenges to data security posed by specialized cloud services and virtualization, as well as flexible access and smart devices.

The Palo Alto Networks Security Operating Platform supports schools in their online safety efforts while helping IT teams to better support the 21st-century classroom. Schools and districts use Palo Alto Networks to gain visibility and control over their networks while preventing ransomware and malware from threatening critical information.

Students often unwittingly—or at times deliberately—put networks at risk. Palo Alto Networks automatically protects the network from threats with coordinated anti-malware and web content filtering. Advanced endpoint protection coordinates with threat intelligence to stop attacks the minute they are attempted.

The key is automation, with enforcement points and shared intelligence working together to prevent ever-changing cyberthreats. And cloud-delivered security services employ global intelligence to filter content as well as detect threats and attackers.

Schools and districts can explore the platform at a pace that makes sense to them: beginning by employing some elements, with the ability of expanding to grow their protection level without having to purchase, learn and manage a new system.

Security Operating Platforms arm schools against cyberthreats through integrated network, cloud and endpoint security technologies: decreasing a school's incident response time while increasing the reach and efficiency of their security teams.

Learn more

Learn more about data privacy for K-12 education at **CDW.**