Next-Generation Security Platform for Lower Education/K-12 Districts and Schools

LOWER EDUCATION/K-12 CHALLENGES:

- Allay parents' concerns and protect student information
- Serve diverse device requirements across numerous platforms and operating systems
- Serve academic cloud and other online initiatives such as YouTube for schools and Google Safe search
- Serve schools' academic needs with swiftly aging and outdated infrastructure
- Ensure security of the school's network regardless of the level of end user knowledge — whether teacher, administrator, or student
- Provide security for district data centers, many of which are virtualizing, with demanding performance requirements
- Many school networks are centralized at the district level, making granular controls and policies harder to enforce

MANAGING THE DELICATE BALANCE BETWEEN FREEDOM OF LEARNING AND CYBER SAFETY

Most schools and school districts are taking huge leaps forward in technology reliance to meet their academic needs. Frequently, school programs aim to develop technologically-skilled students, offer high-level visibility around the integration of modern devices, mobile device access, and Internet connectivity into every aspect of learning and engagement.

While there is no doubt this high-tech focus increases student and teacher productivity and prepares students for the future, it also creates a unique set of challenges for the IT teams who support these classrooms. They are dealing with antiquated networks. They must protect student data. They must anticipate that their students and teachers are not familiar with all aspects of cyber threats. They must safeguard against cyber risk across a myriad of technology initiatives, while delivering the freedom educators and parents expect from these initiatives:

- **Data center infrastructure:** School districts often run centralized data centers which provide connectivity between school campuses and administration offices. As IT teams deliver on technology programs (for example, replacing antiquated hard lines with WiFi or installing Voice over IP), they must invest in modern infrastructure built for interconnectivity, flexibility and ease of administration. Whether they choose to leverage public cloud infrastructure, specialized cloud services, virtualized or physical data center servers, they have to design security controls from wherever the data center is, across networks to school campuses, and every point in between.
- **Wi-Fi deployments:** The demand to use tablets, notebook carts, smartphones and wireless projectors can't be addressed with networks that were not built to support and secure that kind of traffic. IT teams have to build access policies that are practical and enforceable for a user community ranging from five year old children to college-bound teenagers, adult administrators and educators, senior volunteers, parents and vendors.
- **Networked devices:** With the rise of social networking, instant messaging, file sharing and multimedia applications, IT teams have to allow more freedom around device usage while maintaining visibility about where the device resides, its IP address and who is responsible for it. This extends beyond mobile phones and smartphones, to networked printers, storage (including USB and other removable devices), or any other gear that communicates over the network.
- **YouTube for Schools, Facebook or other Social Media initiatives:** Students and teachers tend to have implicit trust when they are in their online communities. For this reason, IT teams have to figure out how to create guardrails that protect users from "clickjacking" schemes which take over users' systems to a self-described "hilarious video" link that tricks users into giving up login credentials. IT also has to keep pace with privacy and security options in these highly dynamic online environments, (e.g., choosing whether to use YouTube for Schools or run YouTube in safety mode).

paloalto networks.

- New applications or services: Web applications and the browsers used to access them can be the weakest link in a network. Peer-to-Peer (P2P) seems relatively harmless to users without understanding that organizational assets used in potentially illegal ways can expose a school to liability, and that P2P programs can be used to transfer every type of file. Exploitation of vulnerabilities in commonly used programs, such as Adobe Reader and QuickTime, is also on the rise. E-mail and webmail communications through internal e-mail servers or webmail applications can errantly expose information to possible interception.

THE PALO ALTO NETWORKS® ENTERPRISE SECURITY PLATFORM

To address these challenges and effectively secure these education networks, a disruptive, comprehensive approach — a platform approach — is necessary. Palo Alto Networks Enterprise Security Platform eliminates complexities involved with point products — firewall, IPS, IDS, URL filtering, endpoint antivirus, and more. The Enterprise Security Platform realizes this vision of comprehensive security by integrating the power of three core elements:

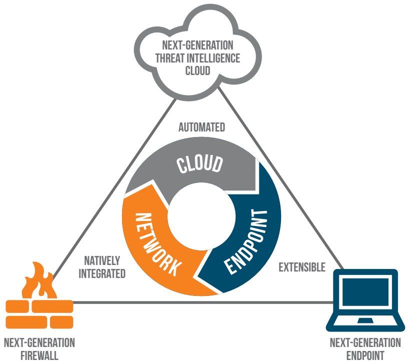

Figure 1: Palo Alto Networks Next-Generation Enterprise Security Platform.

- The next generation firewall with its innovative layer-7 classification engine not only provides granular traffic visibility but as the enforcing device allows users to segment their network using intuitive school-appropriate policies that reduce the threat footprint. It further secures the allowed traffic by natively blocking known threats such as viruses and spyware and by sandboxing unknown threats which are quickly analyzed and stopped with automatically generated protections. Security can also be extended to virtual and mobile environments.
- The advanced endpoint prevention, Traps, ensures that the point of entry for most threats, the host, is secure. It uses a disruptive approach to prevention, stopping the underlying techniques used by exploits and malware in their attack chain. This is unlike the ineffective and burdensome approach used by traditional endpoint solutions which only look at the ever growing repository of known signatures, strings, and behaviors to try to deter zero-day attacks.
- The threat intelligence cloud analyzes and correlates intelligence from all platform security functions — URL Filtering, mobile security, IPS/threat prevention and the virtual execution engine or sandbox, WildFire™ — and validated community input. WildFire immediately discovers previously unknown malware and communicates the results to the platform to automatically generate signatures. All threat intelligence is distributed to the network and endpoints to ensure they are protected. Known, zero-day and advanced attacks, including APTs, can all be prevented from endpoint to data center. This is all done automatically, reducing operational burden and shortening an organization's response time.

HOW SCHOOLS AND SCHOOL DISTRICTS BENEFIT FROM THE ENTERPRISE SECURITY PLATFORM

Palo Alto Networks Next-Generation Enterprise Security Platform helps educational institutions all over the world deploy new technologies (cloud, mobile, online course delivery and virtualization) without compromising security or network bandwidth. We make it easier for IT teams to:

Adopt a platform approach

- Protect student data and school networks by detecting, analyzing and preventing both known and zero-day threats from one consolidated platform.
- Supports all of the school's key network security needs including URL filtering, anti-malware, mobile device management, and IPS/IDS.
- Increase return on security investments with the ability to correlate threat insights across security functions all within the same platform.
- Maintain security regardless of how aged or modern the school's or district's infrastructure, or knowledge level of the school's or district's users.
- Handle complex modern data center network scenarios, including advanced packet-forwarding decisions.
- Coalesce all visibility, policy control, logging, reporting and forensics features within one platform across the school and/or district. This simplifies school operations, taking full advantage of this contextual awareness to provide a closed-loop feedback platform for the school's network and data center security.

Enable freedom of devices and other specific use cases

- Serve diverse device requirements across numerous platforms and operating systems, maintaining security policies and even device-context access to keep the school's data and network secure.

[1] Gartner Group Magic Quadrant 'leader' for Enterprise Firewalls 2014 and several years in a row.

- We support and secure data center consolidation, virtualization, hybrid cloud and overall cloud projects by providing IT the ability to customize data center access — across school districts, onto campuses and into administration offices.

Secure user, application and Internet access

- Instead of the traditional “allow all or block all” approach, IT teams can deploy flexible, policy-based control (based on groups of users, applications, categories of URLs, customized white or blacklists created from local lookups of the most frequently accessed URLs and a cloud-based database of the latest URLs) with Palo Alto Networks application visibility and URL filtering.
- Give access to the variety of users to whom schools must provide network access, with customizable security permissions and access privileges.
- Provide the ability to enforce policies and comply with regulations — providing more control over the applications, content and users on their network.

Accelerate integration

- To integrate easily into an existing physical data center network, Palo Alto Networks platforms support a range of network modes, including L2, L3, Virtual Wire and mixed mode. In a virtualized computing environment, the Palo Alto Networks VM-Series of virtualized firewalls allows customers to deploy the exact same next-generation firewall and advanced threat prevention features used in our physical appliances in private, public or hybrid cloud computing environments.
- A rich set of native management features streamlines policy deployment so that security keeps pace with the changes in the physical or virtual environment with security policies applied consistently and cohesively.
- Centralized logging and reporting capabilities that give visibility into virtualized applications, users and content across the school’s or district’s network.

RESPOND TO YOUR SCHOOL AND SCHOOL DISTRICT SECURITY NEEDS

Take action today and find out what protocols, applications and risks exist in your academic environment. The Palo Alto Networks Next-Generation Enterprise Security Platform provides the security required for today’s academic demands. With more than 19,000 customers in over 120 countries across multiple industries, more than 75 of the Fortune 100 and the most advanced governments rely on Palo Alto Networks to improve their cybersecurity posture. Sign up for a free **Application and Visibility Risk Report** for your school network. This free and non-disruptive process will help you discover unknowns on your network and where you are most at risk.

paloalto networks®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com