PROTECT K–12 ENDPOINTS

SPOTLIGHTS

Industry

K-12 education

Use Case

Protect endpoints from zero-day malware and exploits

Business Benefits

- Prevent theft of student data and other PII
- Meet and exceed privacy regulations

Operational Benefits

- Improve efficiency with an endpoint offering that automates updates and malware threat prevention
- Improve experiences with transparency to end users – no resource-taxing scanning required

Security Benefits

- Pre-emptively block known and unknown attacks, including ransomware and exploits, at all endpoints

Business Drivers

K-12 schools and districts are embracing the power of the internet to engage students, improve learning outcomes and simplify administration. A key part of their digital strategy is how to effectively secure all the devices they own, from student notebooks to servers in the data center. Schools must meet student cyber safety and privacy requirements with limited cybersecurity budgets and staff.

Business Problem

K-12 educational institutions are frequent targets for cyberattacks. The range of data schools collect – including PII, financial information, medical records and retail transactions – is of great value to attackers. Servers, workstations, virtual desktops and other devices can suffer from vulnerable operating systems and applications – an easy way into the network for would-be attackers. Malware and new exploits that take advantage of vulnerabilities appear daily, and slow patch cycles make this even more concerning. New attack tactics to circumvent security controls also appear regularly. Antivirus technology or similarly outdated processes simply cannot protect assets from today's swiftly changing threat environment any longer.

K-12 educational institutions have more mobile devices than ever, including laptops for students and faculty, smart projectors, and other networked classroom learning aids – and they all need protection.

Traditional Approaches

In the past, schools have had little choice but to address their endpoint security requirements with antivirus protection. Unfortunately, breaches are happening more often, highlighting some problems with traditional endpoint products:

- **Modern threats change too quickly.** The advent of online forums where threat actors can buy and trade malware and malicious services that can quickly alter malware code has made it impossible for traditional antivirus point products to keep up. Attackers have also started to use more evasive techniques, such as fileless attacks. To that end, in 2017, Ponemon Institute projected that 35 percent of attacks would be fileless in 2018. This is significant as fileless attacks don't require users to take action, such as opening infected files, making them far more likely to succeed than file-based attacks. Meanwhile, many so-called "next-generation" antivirus products have focused on malware detection rather than exploit prevention. Others try to strike a balance, but they fall short on providing consistent prevention.

- **Traditional approaches rely on outdated methods**. Some vendors have begun adding machine learning to their endpoint security products. However, a deeper look reveals that many are underdeveloped, disabled by default or deliver only incremental improvements in malware coverage. Some vendors require multiple products with separate endpoint agents to compensate for the shortcomings of the new additions. In fact, technologies such as digital signatures, virus scanning and heuristic analysis remain at the core of "new" endpoint products offered by most traditional antivirus vendors.
- **The technologies operate in silos**. Most endpoint security products do not communicate with other network sensors, so they cannot leverage threat intelligence on new attacks initially targeting other environments. Network teams have fragmented views of threats.

Palo Alto Networks Approach

To protect today's modern school environments, Palo Alto Networks® Security Operating Platform automates collaboration and enforcement between endpoints, schools, district offices, cloud instances, and teachers and students working off-network. Palo Alto Networks Traps™ advanced endpoint protection prevents successful cyberattacks with a unique, multi-method approach across today's varied network environments. As part of the Security Operating Platform, Traps offers:

- **Persistent protection:** Traps protects endpoints whether they are online or offline, on a school network or off.
- **Diversity of threat prevention:** Traps employs a multi-method approach that prevents ransomware and other malware, exploits, and fileless attacks.
- **Unknown threat detection:** Traps shares threat intelligence with WildFire® malware prevention service, which analyzes and detects unknown threats.
- **Coordinated enforcement:** Once WildFire has detected a threat, it creates and automatically distributes protective measures to all Traps endpoints and other platform enforcement points, such as Palo Alto Networks next-generation firewalls, in as few as five minutes after initial discovery.
- **Automated response:** Traps works with next-generation firewall policies to isolate and quarantine suspect endpoints, minimizing the impact of an attack.

Schools around the world have chosen Traps for its:

- **End-user experience:** Traps is always on in the background, and students and staff need no training on its use. A lightweight agent minimizes impact on endpoint and network performance, improving user experiences. Automatic reprogramming of endpoint agents lessens the need for desktop teams to continually patch devices.
- **Simpler security operations:** Desktop and network staff can work together, sharing a unified view of traffic, threats and enforcement points with centralized logging. They can take advantage of automation, machine learning, and coordinated threat intelligence and enforcement to protect endpoints, as well as the networks they reside in, while generating fewer false positives, enabling them to focus on what matters.
- **Flexible deployment options:** Palo Alto Networks Endpoint Security Manager, or ESM, is available for on-premises deployments, while Traps management service is available in the cloud. Traps is supported on a wide variety of operating systems and endpoints, including Microsoft® Windows®, Apple® macOS®, Android® and Linux, as well as virtual desktop infrastructure. For a complete list of supported operating systems, please visit the Traps Compatibility Matrix page.

Real-World K–12 Education Deployment

A unified school district serving K-12 students moved from its traditional antivirus product to Traps. The district's endpoint protection had been struggling to keep up with advanced attacks, and the district had fallen victim to a number of viruses over the years, causing multiple issues on endpoints. Remediation required an IT technician to visit the site of the infected endpoint to manually wipe and reboot the machine – a tedious, time-consuming process that inhibited the end user's productivity and kept IT resources from being better spent elsewhere.

The district was considering a number of offerings from different vendors for a cybersecurity refresh when a Security Lifecycle Review from Palo Alto Networks highlighted intrusions that had previously gone undetected. Ultimately, the district chose the Palo Alto Networks Security Operating Platform to protect its endpoints, network perimeter and SaaS environments. After a demonstration of how Traps could prevent attacks the district itself was facing, as well as ransomware attacks being experienced by other schools, the district decided to deploy Traps on its workstations and servers.

The district was also in the process of rolling out a 1-to-1 computing initiative to certain grades, and wanted to secure thousands of Google® Chromebooks® that students use in classrooms every day and then take home with them. When the Chromebooks are on a school network, Palo Alto Networks firewalls with URL Filtering automatically protect students from accessing inappropriate content on the web, but the district wanted to ensure appropriate use of these school resources even after they leave the school network. GlobalProtect™ network security for endpoints extends and enforces the same security policies – including web content filtering – no matter where students travel. GlobalProtect also provides a secure VPN for students to access school resources while traveling. With GlobalProtect, the district can protect children from inappropriate traffic and meet compliance requirements that maintain student safety and privacy. GlobalProtect is available on-premises or as GlobalProtect cloud service.

Implementation Overview

Products deployed:

- Palo Alto Networks PA-3050 next-generation firewalls with Threat Prevention, URL Filtering, GlobalProtect and WildFire subscriptions
- Traps advanced endpoint protection
- Aperture™ SaaS security service
- GlobalProtect network security for endpoints

Customer implementation (high level):

- Traps deployed on 1,500 Windows and Mac® workstations and 31 Windows servers.
- GlobalProtect agent installed on 3,000 Google Chromebooks.

Business benefit:

- Exceeds regulatory requirements for keeping students and their data safe.

Operational benefit:

- Reduces complexity, eliminating the need for a managed security services provider to manage multiple vendors' interfaces; the district now manages its own systems.

Security benefit:

- Prevents malware and exploits, known and unknown, from impacting endpoints.

Services to Help You

Palo Alto Networks offers a number of services to help you maximize the value of your investment and protect your business. For more information on support services, professional services, and education and training opportunities, visit our Services Overview page. Additionally:

- **Our global Customer Support** provides timely, expert assistance to keep you up and running safely. Our support has been rated outstanding by third-party assessments. All Customer Support plans include online case management, online support resources, and license keys and upgrades; and Premium and Premium Plus support options offer additional resources.
- **Our Professional Services and Certified Professional Services Partners** deliver the tools, best practices and assistance you need to define an effective strategy, simplify operations and prevent successful cyberattacks.
- **Education and Training Services** help you expand knowledge and skills with world-class training, certification and accreditation, and digital learning options.
- **Cyber Range** is interactive cyber defense training that helps keep your IT network, infrastructure, OT, DevOps and SecOps teams razor-sharp.

Conclusion

Endpoints in K-12 education institutions are not only central to learning and day-to-day operations; they are a critical path to sensitive data. Malicious, unauthorized changes and access to endpoints can significantly affect operations. Traps and other elements of the Security Operating Platform protect these vital institutions against today's swiftly changing threat environment in a manner that is minimally disruptive and meets the productivity needs of the end users, whether students or faculty.

For further information on how Palo Alto Networks supports K-12 educational institution customers, please visit our K-12 industry page.

For further information on Traps:

- Visit our Advanced Endpoint Protection page.
- Read the 2018 NSS Labs Advanced Endpoint Protection Report.
- Participate in a Virtual Ultimate Test Drive for Traps from the comfort of your office.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com