CYBERSECURITY REFERENCE BLUEPRINT FOR K-12 IT

IT network and security teams in K-12 institutions around the world must keep students and their data safe while providing appropriate network security for diverse groups of users. They must also detect and block a rising volume of ransomware and other threats while ensuring high performance and availability as well as complying with policies and regulations. The Cybersecurity Reference Blueprint for K-12 IT provides a framework to help school IT teams keep students and data safe in modern learning environments using principles of Zero Trust, automation, and integrated security services to stop threats and simplify security administration.

I. SECURITY CONCERNS FOR K-12 INSTITUTIONS

Cybersecurity is the number one concern for K-12 IT leaders.[1] New multimedia content, e-learning tools that complement traditional learning, and staff and students who take advantage of bring-your-own-device (BYOD) policies all require protection from modern cyberthreats. The increasing use of cloud storage and software-as-a-service (SaaS) applications, while increasing efficiency and productivity, has also introduced new threat vectors. Navigating and monitoring this changing minefield is a difficult and time-consuming task for security teams, some of which are attempting to repel dozens to thousands of attacks per day.

Reams of student and staff online data, combined with limited IT resources, have made K-12 institutions an increasingly popular target for ransomware and phishing.[2] Hackers infiltrate networks, disrupt operations by encrypting data, and extract ransom payments in exchange for decryption keys.

An effective security strategy incorporates key security principles to address this type of exposure and damage, while improving the visibility and control of IT and security teams. This paper discusses how Palo Alto Networks technology enables schools to implement these principles to detect and prevent threats to networks, devices, and information—both on-premises and in the cloud—while monitoring policy effectiveness as well as reducing complexity and unnecessary overhead. The end goals: efficiently manage a high-performance learning environment; protect students, staff, and their data; and ensure ongoing compliance with policies and regulations.

II. REFERENCE BLUEPRINT GOALS AND SECURITY PRINCIPLES

This Cybersecurity Reference Blueprint for K-12 Education IT describes a framework that enables education security and IT professionals to meet their stated goals:

- Meet academic needs for internet connectivity while keeping students safe.
- Prevent data breaches and the loss of sensitive information.
- Maintain high availability and performance while continuously scanning for and preventing new threats.
- Identify best practices for cybersecurity deployment and management.
- Comply with regulations relating to personal data, protection of children, and more.

Like most industries, schools must protect their staff, computers, and servers from cyberthreats. Unlike most industries, however, most K-12 network users are children, not employees, who require protection from inappropriate content as well as cyberthreats. These children and the staff who serve them may even be allowed to connect their own laptops, tablets, and smartphones to campus networks. Many K-12 institutions are now evaluating how to protect student-owned devices—and be protected from the risks of those devices—without impacting network performance or significantly adding to the workload of their overburdened IT teams.

Several types of cyberthreats impact K-12 networks: opportunistic malware with no specific targeted victim; exploits of vulnerable applications; and, increasingly, targeted attacks. Using some key security principles, K-12 institutions can prevent these threats, minimize network interruption or downtime, and protect against unauthorized access and leakage of sensitive data. These core security principles include:

- Complete visibility into traffic to reduce the network's threat footprint, enforce usage policies, and assist with capacity planning and appropriate access controls.
- A Zero Trust security approach designed to prevent data breaches and improve defenses against modern cyberthreats.
- Coordinated protection across endpoints, in data centers, in remote locations, and at major internet gateways and cloud locations.
- Advanced protection against zero-day and known malware attacks.
- Automation that shares and distributes threat intelligence in addition to coordinating actions between systems.

Subsequent sections address each of these principles in detail.

III. CORE SECURITY PRINCIPLES

Gain Complete Visibility

Schools cannot protect against threats they cannot see. Visibility into the applications traversing the network—including how often they are being used, who is using them, and how much bandwidth they are consuming—helps IT teams make informed policy decisions. They can use this visibility to make contextual, policy-based decisions about which applications should or should not be allowed; who should be able to use certain applications; what they are allowed to do and under what

1. "CoSN's 2019 K-12 IT Leadership Survey Report," Consortium for School Networking, accessed December 18, 2019, https://cosn.org/sites/default/files/_CoSN_ITLdrship_Report_2019_Final.pdf.

2. "K-12 Cybersecurity Lessons Learned From 'Constant Barrage of Attacks,'" Education Week, March 19, 2019, https://www.edweek.org/ew/articles/technology/2019/03/20/k-12-cybersecurity-lessons-learned-from-constant-barrage.html.

circumstances; and what different groups of users need while controlling the risk to the network. Schools can choose to block applications that carry the highest risk, such as peer-to-peer apps that can lead to data exposure or proxy server apps that bypass web filtering. Next-generation security can also ensure that downloaded applications are not carrying risky payloads. In contrast, port-based policies applied with traditional security products cannot distinguish risky or unauthorized applications or users, and therefore cannot effectively protect the network.

By integrating security platform information with user repositories, IT teams can identify users and user groups instead of only devices or IP addresses. This enables IT teams to build security policies that limit certain applications to particular users or groups.

Application-based policies can help control access by allowing IT teams to:

- Identify risky applications and traffic, such as:
  - SaaS storage apps that allow data transfer and exfiltration
  - Suspicious DNS requests
  - P2P applications, such as Tor and BitTorrent®
  - Proxy avoidance tools, such as UltraSurf, Psiphon™, or tunneling services
- Look for other dynamics within the environment, such as:
  - Port scanners and/or vulnerability scanners
  - Unapproved third-party networks
- Build groups for traffic to always block:
  - IP ranges, including geolocation for regions you don't need to communicate with
- Identify, monitor, and analyze all SSL/TLS-encrypted traffic, especially from external websites. Malware authors are increasingly delivering encrypted malware payloads. With some exceptions based on privacy policies, schools should examine encrypted traffic for malware or inappropriate usage.

Implement Zero Trust

In a typical attack against a K-12 institution, attackers send emails with infected attachments that, when opened, spread malware through the network. Other emails may invite recipients to follow malicious links to credential phishing sites. The end results can be data breaches, financial loss, operational disruption, and/or compliance violations.

Taking a Zero Trust approach to network security makes it very difficult for these attacks to succeed by requiring your network to continually verify all users, devices, and applications as well as segment user groups, devices, and/or data types into zones. Zero Trust enforces security controls at every entry and exit point of a zone. You can control which users or applications have access to the zone as well as what can enter or exit the zone. Ideally, Zero Trust zones include data and resources with the same trust level and similar functionality, such as payment systems or student information systems with shared protocols and transaction types. This minimizes the number of allowed pathways into and out of a given zone, reducing the potential for malicious insiders and other threats to gain access. Scanning traffic that enters and exits zones prevents the spread of malware as well as other threats and can prevent exfiltration of sensitive data.

Segmenting your systems into Zero Trust zones reduces risk in three ways:

- Limits the scope of vulnerability by separating vulnerable devices, such as old servers that cannot be patched from others, or those containing sensitive data such as student health records.
- Limits data exfiltration by limiting the amount of data that is compromised in a breach.
- Limits the scope of compliance since only the devices, workstations, and servers in a particular zone are subject to compliance audits.

Examples of Zero Trust zones include:

- Applications and databases containing private or regulated information (e.g., payroll and payment systems).
- School Wi-Fi internet access.
- Smart machines and sensors, such as building and facilities management systems.
- Physical safety systems, such as internet-connected smoke detectors and alarms.

Protect Cloud Environments and SaaS Apps

Most K-12 institutions are already running SaaS applications, such as G Suite™ or Microsoft Office 365®. Many are also implementing private and public cloud architectures. A Zero Trust network architecture should inspect and apply security policies to both north-south traffic entering and exiting cloud and SaaS apps and east-west (virtual machine segmentation) traffic between applications. Here are a few more considerations for cloud environments:

- **Reliability:** Consider active/active high availability for north-south boundary appliances to continuously synchronize their configuration and session information, ensuring that performance does not degrade and no traffic is lost in the event of a hardware failure.

- **Orchestration and management:** Ensure policies can keep pace with the rate of change in your virtualized workloads and multi-cloud environments.
- **Policy consistency:** Centrally define and consistently apply policies to all devices to reduce complexity and avoid gaps in threat protection. Use centralized management to serve as a single point of management for all security appliances, both physical and virtual.

Protect Endpoints

K-12 education networks deal with a plethora of devices—some managed by the school or district and many not. An effective security strategy extends Zero Trust to all endpoints, including virtual and physical desktops, laptops, and servers, regardless of patch status, signature or software-update levels, or ownership. IT teams have a duty to prevent ransomware and other malware from affecting either school- or student-owned devices.

The main threats affecting managed endpoints include executable malware and exploits that target specific application vulnerabilities. To protect against them:

1. Employ a lightweight agent to continually monitor for exploit techniques and malicious executable files.
2. Apply policy-based restrictions to prevent the spread of threats. Set up policies restricting specific scenarios. For example, you may want to prevent the execution of files in the Microsoft Outlook® temporary directory or of a specific file type directly from a USB drive.
3. Connect traveling, school-owned mobile devices to the institution network via a VPN.

Through user identification and Zero Trust, you can identify many devices not owned by your institution, grant or deny them access to certain applications, and monitor and prevent the spread of threats. For example, you may want to grant a teacher's personal laptop access to the zone that contains student assessment software. However, through usage policies, you may want to prevent that teacher from uploading executable files to the zone or using the upload option of Dropbox® to exfiltrate data.

Thwart Targeted, Advanced, and Zero-Day Attacks

Advanced attacks and zero-day ransomware can strike swiftly, so discovery and remediation to repel attacks must be equally swift. Automation is critical to immediately discover and prevent zero-day threats as well as repel both the initial attack and subsequent similar attempts. Any unknown file attempting to enter a trusted perimeter or network zone should be inspected within an advanced malware execution environment. Once zero-day attacks are recognized and analyzed, only automatic generation and delivery of signatures is fast enough to ensure zero-day attacks don't get past your security.

Coordinate Reporting and Threat Intelligence

With new ransomware, phishing, and millions of other potential threats a day, coordinated cybersecurity between endpoints, data centers, network perimeters, and cloud environments reduces the danger cyberthreats pose. Manual coordination, for example emailing or calling another team to confer, wastes valuable time that attackers can use to exploit your network and/or exfiltrate data, which can take just minutes.[3] The only way to preemptively mitigate threats is to automate collaboration, coordination, and reporting across networks, endpoints and clouds without relying on the human factor. Collaboration and coordination must extend to any potential attack vector (URLs, known and unknown threats) at any zone or location. For example, your security ecosystem should immediately flag and block users from sending information, such as their user credentials, to brand-new or suspicious URLs.

IV. SECURITY REFERENCE BLUEPRINT FOR K-12 IT

Let's explore how you can implement these security principles to stop threats from harming your students, staff, data, and learning system availability. This section provides a high-level reference blueprint for K-12 IT, demonstrating how Palo Alto Networks integrated innovations work together to automatically secure K-12 network, endpoint, and cloud environments.

While your unique network requirements will ultimately determine your architecture decisions, the example blueprint in figure 1 shows a large school or district with its own connection to the internet as well as its own data center and administrative offices.

Implementing Zero Trust in K-12

The growing use of cloud apps, platforms, and storage in K-12 environments has eroded the typical idea of a network perimeter (see figure 1). Through one-to-one computing initiatives, students can access e-learning and the internet from school, home, or anywhere. Many internet-connected devices in schools, such as fire detection and alarm systems, building management, and security systems, are remotely managed by third parties. With so many unknowns, all these locations and communication paths need coordinated cybersecurity. Fortunately, schools can use Palo Alto Networks Next-Generation Firewalls to implement Zero Trust, reduce risk, and consistently protect data, operations, staff, and students—inside the traditional perimeter or not.

3. "Verizon 2019 Data Breach Investigations Report," Verizon, May 2019, https://enterprise.verizon.com/resources/reports/dbir.

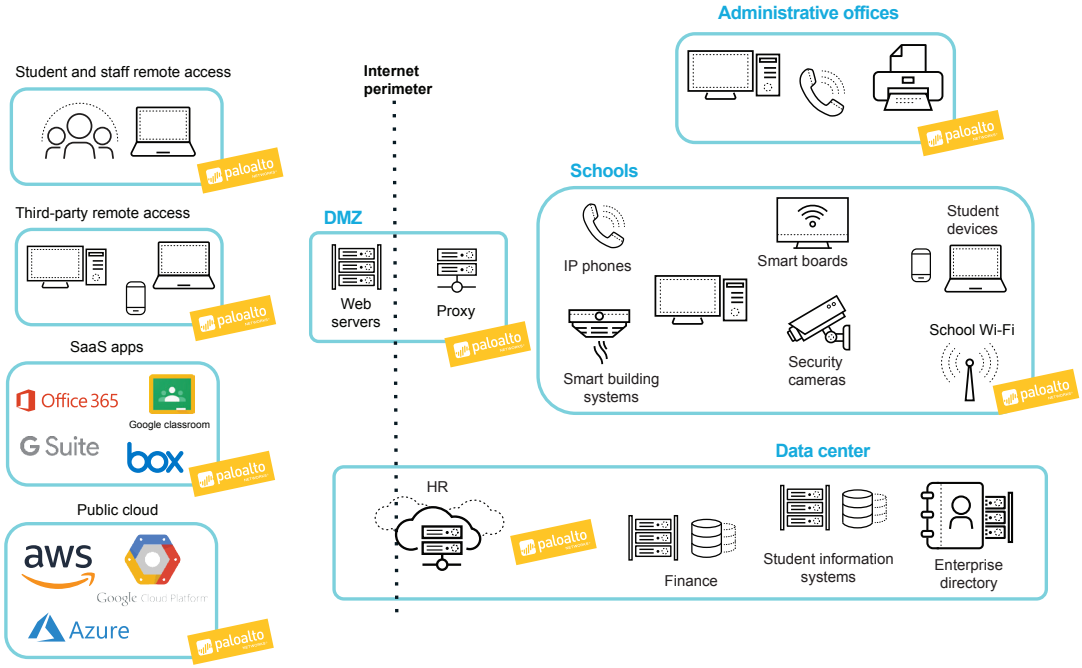

Figure 1: Security Reference Blueprint for K-12 IT

Figure 2 shows a typical school district with different Zero Trust zones, arranged by criticality of data. Palo Alto Networks Next-Generation Firewalls, whether physical or virtualized, create Zero Trust zones by scanning all north-south and east-west traffic entering and leaving zones. The firewalls enforce security policies around users, applications, and content to prevent data leakage and the spread of malicious payloads.

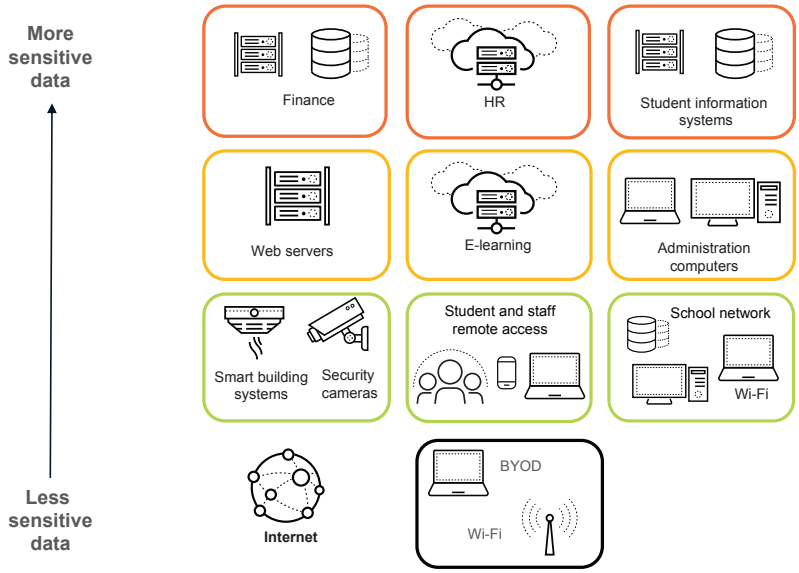

Figure 2: Implementing Zero Trust for K-12 IT

Palo Alto Networks Next-Generation Firewalls support the following integrated capabilities, which work together to protect your students, operations, and data:

- **User-ID™ technology** enables schools to create and view policies, reports, and forensics based on users and groups—not IP addresses. User-ID leverages information stored in a wide range of repositories to identify users on your networks.
- **App-ID™ technology** identifies and controls more than 3,000 applications, irrespective of port, protocol, SSL encryption, or evasive tactics. Schools can foster education and research while controlling access to applications.
- **SSL Decryption** improves visibility into potential threats while eliminating the management overhead and performance impact of separate decryption appliances.

- **WildFire® malware prevention service** detects and then automatically blocks zero-day threats. The malware execution environment detonates new malware, creates protections for all Next-Generation Firewalls, and distributes them automatically in as few as five minutes following the discovery of new malware anywhere in the world.
- **URL Filtering** hosts information about hundreds of millions of websites and more than 75 URL categories, categorized by risk level and automatically, continuously updated. Administrators can enforce internet surfing policies such as Safe Search, create alerts and perform actions based on keyword searches, control bandwidth for designated categories, and more. The service discovers and shares new malicious domains and IP addresses every few minutes.
- **Threat Prevention** eliminates evasive threats at every stage of an attack, preventing exploits from reaching devices, disrupting command-and-control (C2) traffic, and enforcing intrusion prevention system (IPS) protection across all ports and protocols.
- **Credential theft prevention** builds upon user and content visibility by blocking the transmission of corporate login credentials to websites that exhibit phishing characteristics. It also works with URL Filtering to block access to known phishing sites.
- **Data filtering** profiles enable schools to prevent sensitive information, such as credit card and Social Security numbers, from leaving a protected network. You can configure policy to filter keywords that signal harmful or threatening content for certain applications or file types.
- **DNS Security service** applies predictive analytics, machine learning, and automation to block attacks that misuse and abuse DNS, and eliminates the need for independent tools.

Although Zero Trust should be the ultimate goal, many K-12 environments have very open internal networks, and IT may still perceive implementing such a model as a significant challenge. However, even taking a few steps toward Zero Trust can help institutions better protect critical functions and sensitive information as well as prevent the movement of ransomware or other malware through their networks.

Student and Management Information Systems

Whether in the cloud or in the data center, your HR, payroll, invoicing, student information systems (SIS), and other management systems house highly sensitive data and require the highest levels of cybersecurity. Here are some common best practices our K-12 customers use for these zones:

- Enable only certain user groups (e.g., the "administration" group) to access sensitive applications, such as your HR records, payroll, and SIS. Deny all other users, even those with proper login credentials. This stops cybercriminals from using stolen credentials to gain access to your systems. Palo Alto Networks Next-Generation Firewalls enable role-based access control (RBAC) by leveraging user groups in enterprise directories to specify what users can access. Application-specific RBAC permissions (e.g., who can pay invoices) are handled by the application.
- Block all traffic from entering the zone except that from whitelisted applications.
- Use data filtering profiles to prevent sensitive data (such as credit card or Social Security numbers) from leaving the zone. This prevents configuration errors (e.g., posting payroll information on a public-facing web portal).
- As with all zones, scan all traffic entering the zone for malware and exploits.

While they also contain sensitive information, student information systems offer community and student web portals. These web services could be assigned to a zone with a lower level of criticality. Alternatively, you could house student information systems in their own Zero Trust zone and allow web services requests to access the zone.

Depending on the systems running in the data center, you may want to further segment the data center into different zones, such as HR, payroll, and SIS.

School Wi-Fi Zones

Districts should consider Wi-Fi zones inherently unsecure. Some schools use a captive portal that allows students, staff, and guests to access Wi-Fi with their own computers or mobile devices. This BYOD network is typically logically segmented from other Wi-Fi networks. Beyond logical segmentation, a best practice is to create separate Zero Trust zones that segment BYOD from school-owned classroom devices (notebooks, smart boards, printers, etc.).

It's Easier Than Ever to Secure K-12 Environments

Palo Alto Networks now provides day-one K-12 best practice configuration templates for Palo Alto Networks Next-Generation Firewalls or Panorama™ network security management. These configuration templates reduce the need to manually configure and audit devices and help K-12 institutions meet government regulations relating to child protection and data security. Your network administrators can quickly enable:

- Safe Search
- K-12 reports
- Targeted decryption policies that reduce risk
- Network administrators to optionally block IP addresses from most countries and more

Find these templates at https://github.com/PaloAltoNetworks/K12Skillet.

Regardless, students will access the internet from these zones, for schoolwork or otherwise, and schools have a duty to protect them from threats and inappropriate content. This should be the only zone students can connect to, however, so schools can use Next-Generation Firewall capabilities to enforce internet usage policies and comply with regulatory requirements while respecting privacy.

To keep students safe from inappropriate material, IT can use the URL Filtering subscription on the Next-Generation Firewall to block entire URL categories as well as implement granular web content filtering rules that vary by user group. For example, schools may choose to:

- Entirely block certain URL categories, such as High Risk, Phishing, Copyright Infringement, Adult, Hacking, Gambling, Extremism, Command and Control, and Proxy Avoidance and Anonymizers.
- Flag certain search terms or URL categories for reporting purposes.
- Grant more web surfing freedom to older students, such as by enabling social media access but disabling the chat feature for younger students.
- Bandwidth-limit certain applications, such as streaming media or gaming apps, at all times or during school hours to ensure appropriate network performance for learning.
- To maintain privacy, schools can set policies to decrypt most traffic while leaving some categories encrypted (e.g., health and medicine, financial services).

WildFire automatically updates the URL Filtering database every few minutes with the latest websites, so URL categories are always up to date with the latest websites, including sites associated with phishing or malware.

Administration Zone

As previously discussed, schools should specifically limit which users, and perhaps devices, can access zones that house sensitive data. This helps limit the scope of compliance for regulated information, such as personally identifiable information (PII) or financial information. In this example, finance teams, student records administration, and HR staff are segmented in their own zone, along with any servers and related applications not in the data center or cloud environments. For example, schools can:

- Require valid users who travel with school-owned laptops to use remote access security (see the Securing Remote Access section).
- Deny valid users who attempt to log in to HR or finance applications from their personal devices.
- Deny valid users whose devices do not have appropriate endpoint protection installed.

Protecting Endpoints

Endpoint protection presents a number of challenges for districts and schools:

- **IT management overhead:** Continuously patching computers and servers to plug vulnerabilities takes considerable time and effort.
- **Security operations overhead:** Traditional endpoint protection products operate independently of other cybersecurity efforts, complicating operations and increasing costs.
- **Insufficient protections:** Endpoint protection may depend heavily on signatures to repel malware, and these protections may not be up to date enough to repel the very latest malware or exploits.

Palo Alto Networks endpoint protection works with Next-Generation Firewalls and enables IT teams to apply consistent policies as well as manage endpoints as part of their cybersecurity infrastructure. Rather than run as a separate process scanning for malware, Palo Alto Networks endpoint protection automatically injects itself into individual processes as they start and monitors all application activity, looking for patterns of behavior that are unusual or associated with previously documented exploits. When it identifies such behavior, the agent automatically blocks advanced attacks that would otherwise evade detection.

In addition to establishing effective policies and segmenting the endpoint zone, schools can apply exploit and malware prevention solutions to school-owned endpoints. Palo Alto Networks endpoint protection:

- Blocks exploit techniques, such as threat injection, even on unpatched systems.
- Detects and stops malware. When it discovers an unknown executable file, the agent automatically queries its local caches—and WildFire, if necessary—to assess the file's standing.
- Blocks any applications or content disallowed by policy.

Securing Cloud Environments

As schools adopt the cloud, they often add more point products to secure their new environments, dramatically increasing the complexity of their cybersecurity. Palo Alto Networks helps schools extend the same consistent security policies and prevention, including Zero Trust, to the cloud. We also provide security orchestration and ways to automate compliance across multi-cloud environments.

Public, Private, and Hybrid Clouds

Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls extend the security of the on-premises school network to public and private clouds. The VM-Series supports the same security features available with physical firewalls, safely enabling applications flowing into and across your private, public, and hybrid cloud computing environments. The virtualized platform protects a range of private and public cloud environments based on technologies from VMware, Cisco, KVM, OpenStack, Nutanix, Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud. Prevent advanced cyberattacks while providing consistent application-level control between workloads, consistent policy across network and multi-cloud cloud environments, fast deployment, and dynamic security policy updates as workloads change.

For orchestration, our security orchestration, automation, and response (SOAR) platform, Demisto®, integrates with your existing cloud security tools to coordinate and automate response processes across cloud and on-premises environments. Security teams will be able to standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response and overall cyber operations.

For schools using multi-cloud environments, Prisma™ Cloud simplifies security operations by enforcing consistent security policy as well as ensuring consistent visibility and compliance across multi-cloud environments.

Software as a Service

Data resident within enterprise-enabled SaaS applications is typically not visible to an organization, which can make SaaS apps a source of malware and a popular way to exfiltrate data. Palo Alto Networks Prisma SaaS security service connects directly to the most popular enterprise SaaS applications to provide data classification, sharing/permission visibility, and threat detection. This yields unparalleled visibility, allowing IT teams to inspect content for data risk violations and control access to shared data via a contextual policy. For example, schools can:

- Extend security policies to SaaS applications.
- Block known and unknown malware that may be coming from files in SaaS applications.
- Quickly quarantine data in the event of a policy violation, such as an attempt to exfiltrate PII to a storage application.
- Consistently protect SaaS in multi-cloud environments.

Securing Remote Access

The weakest links in security are often endpoint devices, particularly those outside the campus network. Palo Alto Networks enables you to protect mobile users and secure access to your data center and cloud environments in the same consistent manner as if users were in a school network. Prisma Access extends a secure access service edge (SASE) out to individual schools or users' computers, tablets, and smartphones, no matter where they travel. The GlobalProtect™ app protects mobile devices (including laptops, tablets, and smartphones) and supports two-factor authentication (2FA). Remote devices are subject to the same security policies and access capabilities as they would be inside the network perimeter, ensuring compliance with all security regulations and policies even if your users are remote. Suspicious files and content are automatically sent to WildFire for analysis, while students are always protected from the latest malware and malicious URLs. For example:

Migrating to Palo Alto Networks

Palo Alto Networks offers a number of tools to strengthen your network security and simplify your operations by leveraging a prevention-focused architecture with Next-Generation Firewalls and associated services.

For more information, please visit our Transformation Services page.

- Students using school-owned Chromebook® devices can access e-learning applications and safely browse the internet from anywhere.
- Third parties can securely and remotely support devices on school networks (such as smart building systems) without being able to access other devices on the network.
- Staff can use their own laptops, secured with the GlobalProtect app, to access SIS remotely and enter grades without being able to exfiltrate data.

Managing Smart Buildings and the Internet of Things

Schools are using connected internet of things (IoT) devices to enhance physical safety and improve learning outcomes. A best practice is to segment internet-connected devices, such as security cameras, smart TVs, and smart boards, in their own zone. Critical IoT devices, such as fire alarms and wireless door locks, should ideally have their own zone as well.

For more information on Zero Trust and network segmentation for IoT, read our Cybersecurity Reference Blueprint for Building Management/Automation Systems.

Securing the Future of K-12 Networks

As you continue to expand your digital environments, you must integrate cybersecurity into every aspect of your IT systems.

Harnessing Big Security Data

Modern learning environments are generating huge amounts of security data, and security operations centers (SOCs) are feeling the pressure. While a prevention-first strategy is critical, it may not stop everything. Schools should be planning how to use cybersecurity data to quickly detect and investigate incidents and automate response. With Palo Alto Networks, schools and districts can add capabilities that work with their existing security services to:

- Collect, transform, and integrate their security data.
- Use machine learning and analytics to detect and respond to attacks by harnessing endpoint, network, and cloud security data.
- Empower cyberthreat investigation, prevention, and response using threat intelligence that delivers unrivaled context.
- Manage alerts, standardize processes, and automate security actions.

For more information, visit our Cortex page.

Maintaining Compliance

K-12 institutions are subject to numerous government and industry regulations relating to child protection and data security. For example, in the US, schools that want to access E-rate federal grants available to offset the cost of internet access or internal connections must comply with the Children's Internet Protection Act (CIPA). Through granular web filtering and consistent security policy administration; the ability to monitor activity by user, application, and user logs; and comprehensive application visibility and control, the Palo Alto Networks platform helps schools address CIPA and other children's protection initiatives. Similarly, education institutions have used the Zero Trust approach and Palo Alto Networks platforms to support compliance with health regulations (such as the US-based HIPAA Security Rule) and the protection of personal information (such as PIPEDA, GDPR, or other country-specific regulations).

For more information on our product certifications and how we enable privacy, visit our Trust Center. For more information on how Palo Alto Networks helps schools exceed CIPA compliance, read our brief, Exceed CIPA Compliance with Palo Alto Networks.

V. SUMMARY

Implementing consistent security controls helps K-12 institutions protect themselves against cyberthreats as well as safeguard student and staff data. Palo Alto Networks coordinates security innovations across network, endpoint, and cloud environments, with automation to safeguard K-12 institutions against attacks and errors that threaten their data, operations, student safety, or compliance. This integrated approach also reduces costs associated with point security products and simplifies security operations.

To learn more, please visit our K-12 Education page.

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

cybersecurity-reference-blueprint-for-k-12-it-wp-011720