NEXT-GENERATION SECURITY FOR HIGHER EDUCATION INSTITUTIONS

Higher education institutions must balance academic openness with protecting the personal information and intellectual property of staff and students. It's another balancing act to maintain continuous, high-bandwidth access to resources while blocking threats and intrusions that could damage the institution's reputation. Palo Alto Networks® meets the security needs of higher education institutions by automatically preventing cyberthreats across cloud, network and endpoint devices at network speeds, as well as keeping sensitive data safe by administering granular security policies based on users, applications and content.

Higher Education Security Challenges:

- Maintain student satisfaction with high network performance and availability
- Protect against cyberthreats growing in speed, volume and sophistication
- Prevent data breaches and the loss of sensitive information, including financial transactions, personal data, and intellectual property resulting from third-party funded research
- Support faculty by identifying and protecting vulnerable departmental servers and devices
- Manage disjointed, distributed network and endpoint security

Agile Security for Modern Higher Education Networks

Keeping pace with dynamic online environments, and known and unknown threats, is an ongoing struggle for IT teams. Palo Alto Networks helps higher education face security challenges relating to:

- **Cloud security:** Higher education is investing in modern infrastructure for interconnectivity, flexibility and ease of administration. Whether they leverage public cloud infrastructure, specialized cloud services and/or SaaS applications, they need to protect the data in transit while ensuring no threats infiltrate their networks.
- **Performance:** Many schools are consolidating their data centers while increasing virtualization within them to improve performance and productivity. Security must be flexible enough to meet the demands of swiftly changing virtualized environments and increasing demands for network bandwidth.
- **Valuable data:** Higher education institutions are a prime target for cybercriminals seeking monetary gain from the theft of cutting-edge research, intellectual property, payment data, and student and faculty information.
- **Appropriate access for all:** With students, visitors, faculty, administration, vendors, equipment managers and research partners on the network, giving the right people access to the right resources – without compromising security – is an ongoing challenge.
- **Mobile and "smart" device access:** With everything from student smartphones to campus security cameras connecting to the network, IT teams have little visibility into who is using these devices or what users are doing with them.
- **Distributed environments:** Different departments maintain servers, desktops and other network-connected equipment with varying levels of host protection. Faculty often use tablets or notebooks that need to be protected, no matter where they travel. IT must protect faculty and staff devices from clickjacking and other schemes that can take over users' systems or steal identities and login credentials.

Secure High-Performance Education Networks With a Platform Approach

The Palo Alto Networks Next-Generation Security Platform helps educational institutions all over the world deploy new technologies (including cloud, IoT, online course delivery and virtualization) without compromising security or performance. The platform offers educational institutions real-time visibility and cohesive security for the school's cloud, network, endpoint devices and content, reducing cyber risk. The Palo Alto Networks Next-Generation Security Platform is comprised of natively integrated:

- Next-generation security capabilities – including firewall, IPS, decryption, unknown threat detection, network antivirus and URL filtering – that work together to deliver application, user, and content visibility and control, along with protection against network-based cyberthreats.
- Threat intelligence that correlates, synthesizes and analyzes brand-new threats and related metadata gathered from global platform deployments. The result of this intelligence analysis is the automatic reprogramming of all The result of this intelligence is the automatic reprogramming of all devices to stop new threats in as little as five minutes after they are detected anywhere in the world. Correlation capabilities help analyze and block similar future threats even more quickly, allowing schools to stay a step ahead of cyberattacks.
- Advanced endpoint protection that stops zero-day exploits and modern malware on devices from network servers to remote laptops.

These elements share security context and work together to automatically prevent quickly changing threats from impacting students, endpoints, networks or data. This platform approach reduces silos of information and manual intervention from overburdened IT teams. Unified visibility, policies and reporting across security functions greatly simplifies management and compliance and reduces the potential for misconfigurations, outdated policies or overlooked threats.

Higher education institutions around the world use Palo Alto Networks to:

- Gain granular visibility into network usage.
- Improve their security posture with virtual network segmentation.
- Automatically prevent known threats or zero-day attacks from impacting students, staff, networks and data.
- Protect school-owned devices.
- Enable safe and secure remote access.
- Secure cloud use and SaaS applications.

Gain Granular Visibility Into Network Usage

Simple-to-manage, yet granular network segmentation is key to preventing the spread of cyberthreats while serving the diverse needs of faculty, staff, students and other valid network users. Palo Alto Networks platform deployments, whether stand-alone or virtualized, enable campuses to segment networks to reduce the chance of threats moving through the network and provide another level of access control to sensitive data or applications.

- Leverage user information from a wide range of repositories, enabling IT teams to identify users and groups, not just IP addresses.
- Grant or deny user access to network segments hosting certain applications or servers, providing another layer of security beyond usernames and passwords.

> *"Palo Alto Networks allows us to significantly increase bandwidth, deliver more services faster, and elevate security. The visibility, scalability, and dynamic threat prevention of Palo Alto Networks makes us confident that we can fully protect and support our academic mission."*
>
> – Simon Lane,
> Senior Professional Specialist,
> Enterprise Systems Development,
> University of Southampton

- Protect vulnerable systems – such as faculty computers involved in sensitive research, unpatched servers, or facilities management systems – in their own network segment, while continuously scanning for data exfiltration.
- Prevent threats from spreading in the data center using east-west segmentation in virtualized public or private environments.
- Give administrators valuable insight that can prevent security incidents with near-real-time, easily understandable reports.

Improve Security Posture With Virtual Network Segmentation

Campuses can maintain academic freedom while simultaneously reducing security risks that would affect the network and its users. The Palo Alto Networks platform offers granular visibility into users and applications, allowing higher education institutions to monitor usage, reduce risk, and maintain high availability and performance.

- Leverage user identification to create role-based permission policies, ensuring everyone has access to the network resources they need while denying access to systems they don't.
- Identify thousands of applications traversing the net-work, including applications that may pose a risk to the institution's network or reputation.
- Monitor application use by group, time of day, or other criteria, ensuring that critical applications have the bandwidth they need and IT has up-to-date information for capacity planning.

Automatically Prevent Known and Unknown Threats From Impacting Networks and Data

Protecting the network from threats, and thereby protecting users and their devices, is a competitive advantage for many institutions. Faculty and students, whether using school-owned devices or their own laptops and smartphones, may unwittingly or deliberately put the network or your organization's reputation at risk. And with 30,000 new pieces of malware created every day, higher education IT teams must constantly update security posture to be effective. Palo Alto Networks offers coordinated and automated threat prevention. Palo Alto Networks advanced malware analysis environment conducts dynamic analysis of suspicious content – even encrypted content – in a virtual environment to discover brand new threats anywhere in the world. It then triggers the creation of new protections, which are delivered to the platform's IPS in five minutes or less. Security Appliances are continuously updated with new phishing and malware sites, malicious links in emails, and command-and-control infrastructure, blocking any part of an attack. This automation vastly reduces the operational burden on IT teams, which would normally have to manually update multiple security devices across the network to block even one part of these attacks.

> *"Visibility and throughput is significantly better. Before, we trawled through logs to get information, but now we can see the biggest risks, where they're coming from, which apps are being used and more. The information and detail is fantastic."*
>
> – James Holland,
> Network and Security Services Manager,
> University of Portsmouth

Protect School-Owned Devices Inside and Outside the Firewall

Traditional antivirus is not the solution to modern endpoint security – it's the problem. IT teams must protect university- or college-owned faculty and staff devices not only from unknown cyberthreats but also from the failures of traditional antivirus solutions. Advanced endpoint protection coordinates with threat intelligence and pre-emptively blocks known and unknown malware, exploits, and zero-day threats, enabling staff to use the web safely.

Enable Safe and Secure Remote Access

Sometimes the weakest security link is the endpoint device, particularly if it is outside the campus network. The Palo Alto Networks platform extends both a VPN and granular security out to remote faculty, staff and third-party devices – computers, tablets and smartphones – no matter where they travel. Remote devices maintain the same security posture and access capabilities as inside the network perimeter.

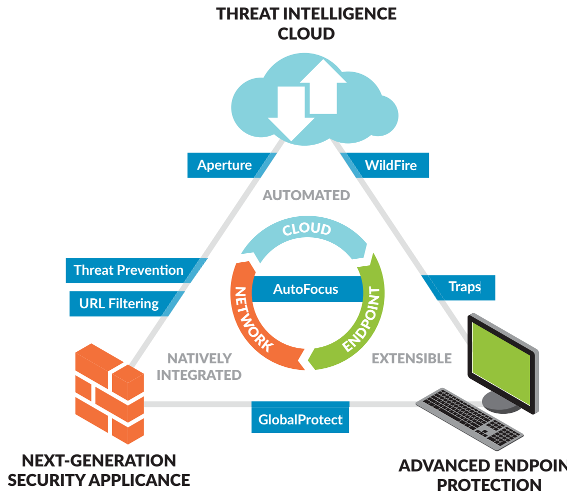
Safely Enable Cloud Use and SaaS applications

Palo Alto Networks virtualized platform deployments bring the security of the on-premises network to public and private clouds. Protect AWS® and Microsoft® Azure® environments and private clouds from advanced cyberattacks while providing application-level control between workloads, policy consistency from the network to the cloud, fast deployment, and dynamic security policy updates as workloads change.

SaaS applications are traditionally invisible to IT. Palo Alto Networks solves this problem by providing full visibility into the day-to-day activities of employees using SaaS applications, such as Microsoft Office 365®, Dropbox and more. Granular security policies help eliminate data exposure and threat risks.

Increase ROI With Palo Alto Networks Solutions for Higher Education

The biggest question for many IT teams in higher education is how to maximize user and data protection with minimal network and security resources. The Palo Alto Networks Next-Generation Security Platform natively integrates many capabilities, eliminating point products and the cost and management overhead associated with them. The platform approach centralizes policy creation and deployment and consolidates security event logging, reporting and forensics, dramatically simplifying security operations. Schools may start with one capability and add new ones to the platform over time, growing protection levels without the cost and complexity of installing and managing new network devices. Each security capability automatically correlates insights on newly emerging threats across endpoints, data centers and cloud resources, ensuring fast responses to any threat with no IT intervention required. As you add security capabilities, coordination increases, and IT teams enjoy even greater returns on investment.



Palo Alto Networks Next-Generation Security Platform

- **Next-Generation Security Appliance:** classifies all traffic – including encrypted traffic – based on applications, users and content, without sacrificing performance. Gain granular visibility into network traffic and easily create granular security policies that reduce the potential for security breaches. Appliances are available in a variety of physical sizes as well as virtualized for all popular virtualized environments, serving the smallest colleges to the largest universities.
- **WildFire™** threat analysis service dynamically analyzes suspicious content in a virtual environment to discover unknown threats. The environment gathers and correlates threat insights across thousands of platform deployments in real time. Then, it automatically creates and delivers protections, protecting higher education networks from zero-day threats in as little as five minutes after a threat has been detected anywhere in the world. WildFire is available in the cloud or on-premises.
- **Threat Prevention** includes IPS, malware protection, DNS sinkhole, and command-and-control protection, automatically protecting the network from known threats that could extract

valuable data. Threat Prevention, WildFire and URL Filtering all leverage global threat intelligence to automatically discover unknown malware and deliver protections to all platform deployments.

- **URL Filtering** continually updates new phishing and malware sites and sites associated with attacks, even blocking malicious links in emails. URL Filtering works with WildFire to recognize URLs associated with brand-new threats – including short-lived credential theft sites or sites hosting new ransomware – protecting institutions within five minutes of discovery. WildFire interrogates suspicious links in emails or the documents they contain. If a site is deemed to be phishing, URL Filtering blocks it.
- **GlobalProtect™** network security client for endpoints extends the protection of the The Palo Alto Networks platform to mobile faculty, staff and third-party contractors. GlobalProtect provides a remote access VPN, secures internet traffic, enforces acceptable use policies and security posture, and helps secure access to SaaS applications. Suspicious files and content are automatically sent to WildFire for analysis.
- **Traps™** advanced endpoint protection eliminates the need for traditional antivirus. Traps prevents cyber breaches by pre-emptively blocking known and unknown malware, exploits and zero-day threats. Using automatically updated threat intelligence gained from WildFire, Traps automatically prevents breaches, enabling staff to use the web safely.
- **AutoFocus™** contextual threat intelligence service prioritizes the most important threats and provides context around them, ensuring IT teams use their valuable time wisely.
- **Aperture™** SaaS security service delivers complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any additional hardware, software or network changes. Integration with WildFire identifies and blocks unknown malware in SaaS applications and shares malware discovered in SaaS applications.
- **Panorama™** network security management reduces administrator workload and improves security posture with a single console for viewing, configuring, creating and distributing policies, as well as generating reports.

Getting Started

Start by gaining visibility into the users, applications and content in your network. Sign up for a free **Security Lifecycle Review**. This non-disruptive process will help discover unknown applications, malware, and bandwidth usage on your network and help define top risks.

The Palo Alto Networks Next-Generation Firewall – the core of the Next-Generation Security Platform – is a **Gartner® Magic Quadrant leader** for the fifth year in a row.

For more information on how we protect higher education networks worldwide, please visit https://www.paloaltonetworks.com/solutions/industries/education/education-higher.

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

security-for-higher-education-sb-040717