Enterprise Security Platform for Higher Education Institutions

HIGHER EDUCATION CHALLENGES:

- Protect student, faculty, alumni and staff personal data
- Protect academic research
- Protect financial data and transactions on the campus
- Preclude dangerous or bandwidth-heavy application use, where applicable
- Prevent copyright infringement and other potential student illegal activities using school network
- Protecting unpatched commercial-off-the shelf (COTS) systems from known cyber-threats and reducing downtime due to cyber-incidents or patching
- Managing disjointed, distributed network and endpoint security

ANTICIPATING DEMANDS FOR THE MODERN HIGHER ED NETWORK

IT teams who run networks for colleges and universities are being pressured to increase the schools' ability to acquire and serve faculty and students by providing unrestricted, high bandwidth access and services to anyone on or around campus. In many cases, this requires re-architecting networks and data centers to anticipate known and unknown threats, varied user types, unknown devices and new applications. Secure sensitive information of students, faculty, alumni and staff as well as academic research and financial transactions. Enable cloud, social media and peer-to-peer usage. Manage and enforce policies on devices, regardless of who owns them.

In all cases, IT teams are juggling more than security. They have to anticipate and build networks that scale to meet their current and future needs. They also need to prove they can deliver services to their stakeholders without increasing cost or risk. They must have the ability to segment, build policies for, and get reporting based on users, their behaviors, facilities/locations, URLs, applications and devices, traffic types and volume while balancing academic freedom. Some of the new initiatives they must support include:

- **Wi-Fi deployments:** IT organizations must provide Wi-Fi density and coverage to adequately accommodate three or more devices per person, and extend it to a broader user base than just their faculty and students who all have high expectations for network availability (especially if they are paying for it) — yet they must have the ability to enforce network policies regardless of user, device, location.
- **BYOD (Bring Your Own Device):** Students often have two or more devices, each with a minimum of 25 personal applications running on them. IT teams need to support the BYOD initiative from a cost-reduction perspective without adding to their administration burden of protecting the traffic, the data, and ensuring that all devices are suitably secure and authorized for use in the network.
- **Facebook or other Social Media initiatives:** IT teams must support online engagement initiatives which offload manual, face-to-face processes, drive efficiencies in how schools connect with students and faculty, and allow them to be more modern in communication activities. As IT deploys networks to support online recruiting, application and registration processes, book and merchandise sales, event broadcasting, etc., they will need the ability to detect unknown malware.
- **New applications or services:** Online course delivery, use of wearable technology, drones or virtual reality classrooms require IT teams to design specialized networks (for high availability, commerce, etc.). Yet, in many cases, they lack real-time threat intelligence about new software vulnerabilities, bad IP addresses, suspect URLs, malicious files and emerging malware tactics.

paloalto networks

- **Labs and research environments:** Many students and faculty work on research, patentable discoveries or inventions, which puts a burden on the associated infrastructure, particularly since collaboration and innovation drives the use of emerging and sometimes custom-built applications. IT teams must prevent theft of intellectual property from the outside or inside and data leakage, while still allowing researchers freedom.
- **Data Center consolidation and/or virtualization:** IT teams have to simplify and enforce network segmentation within the data center, and between the data center and the various networks it supports, yet they need to plan for a diverse set of scalability and security requirements, across campuses, users, and use cases.

THE PALO ALTO NETWORKS® NEXT-GENERATION SECURITY PLATFORM

To address these challenges and effectively secure Higher 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 platform realizes this vision of comprehensive security by integrating the power of three core elements:

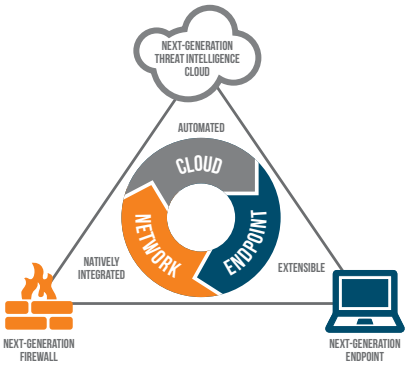

Figure 1: Palo Alto Networks Next-Generation Enterprise Security Platform

- The **next-generation firewall**[1] 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 higher education-appropriate policies that reduce the attack footprint. It further secures the allowed traffic by natively blocking known threats such as exploits, 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 to support mobile initiatives.
- The **advanced endpoint prevention**, Traps, ensures that the point of entry for most advanced 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 HIGHER EDUCATION BENEFITS FROM PLATFORM SECURITY

Palo Alto Networks Enterprise Security Platform helps Higher Education 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

- Unify security policy and enforcement capabilities across Internet edge, data center, mobile devices and endpoints.
- Detect, analyze and prevent threats across both known and unknown threats from one consolidated platform that supports key network security functions including IPS/IDS, mobile device management, URL filtering, anti-malware, anti-virus and threat intelligence.
- Increase return on security investments with the ability to correlate threat insights across security functions all within the same platform.
- Handle complex modern data center network scenarios, including advanced packet-forwarding decisions.

Detect modern threats

- Protect Higher Ed from network intrusions — we provide the team with the tools to detect zero-day events and create protections to prevent future attacks with that and other malware.
- Improve threat and overall network visibility through rich, granular reporting that highlights usage patterns and potential security gaps — and do so with reduced product footprint and therefore costs and complexity… so that even IT teams who don't have dedicated security resources can act quickly and efficiently with their knowledge.

Enable BYOD and other specific use cases

- Allow mobile computing, data center virtualization, or software defined networks with comprehensive threat prevention capabilities that offer complete identification and blocking of known and unknown malware and zero-day threats, irrespective of the vector utilized.

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

- We secure labs, research departments, and other classes who are creating the most valued assets by providing IT the ability to customize data center access — for cross-department and external collaboration, data center consolidation, virtualization, hybrid cloud and overall cloud projects.

Secure user, application and Internet access

- Give access to the variety of users that need access, with customizable security permissions and access privileges. We provide the ability to enforce policies and comply with regulations — giving more control over the applications, content and users on the network.
- 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 application visibility and URL filtering.

RESPOND TO THE NETWORK DEMANDS WITHOUT INCREASING RISK

Take action today and find out what protocols, applications and risks exist in your higher Education network. The Palo Alto Networks Enteprise Security Platform provides the scalability and performance needed to address the most diverse and complex Higher Education network demands with the security and visibility required. 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**. 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