At-a-Glance

Enhancing Higher Education Security
with Extreme Networks and Palo Alto Networks Integration

Higher education institutions face unique security challenges in maintaining high network performance, supporting a diverse user base, and protecting sensitive data. Students and faculty have high expectations for network performance both at school and in the dorm but require security solutions that can keep them safe without impacting user experience. The integration of Extreme Networks and Palo Alto Networks Next-Generation Firewall (NGFW) provides a comprehensive solution to these challenges, delivering security, high availability, and a seamless user experience.

Higher Education Network & Security Challenges

- **Campus Experience:** Ensuring high network performance and availability to maintain student and faculty satisfaction.
- **Scalability and Performance:** Providing stable and reliable wired and wireless networks across large campuses is essential, especially with the increasing need for online learning and digital resources as well as the increase in users and devices.
- **IoT:** Campuses are embracing new devices across use cases – everything from smart lighting systems to wayfinding to connected security cameras. Every new device opens up a threat vector on the network.
- **Cyberthreat Protection:** Defending against sophisticated and rapidly evolving cyberthreats, including "slow and low' attacks that aim to move laterally across networks.
- **Data Security:** Preventing data breaches and safeguarding sensitive information, including financial transactions, personal data, and intellectual property from research.

Extreme Networks Solution

Extreme Networks offers robust and flexible networking solutions designed to meet the unique needs of higher education institutions. Key features include:

Network Segmentation and Control

- **Extreme Fabric:** Extreme Fabric is a network architecture solution designed to simplify and enhance the scalability, automation, and security of your network infrastructure. It simplifies network segmentation to prevent the spread of cyberthreats and provides detailed access control for sensitive data or applications.

  The solution automates key network functions, enabling faster deployment, easier troubleshooting, and sub-second failover, which significantly reduces downtime and enhances network performance. It is designed with security in mind, isolating network services to protect against breaches and ensuring a secure network environment.
- **ExtremeCloud IQ™ – Site Engine:** ExtremeCloud IQ - Site Engine simplifies network management by unifying the control of Extreme and third-party devices, providing end-to-end visibility, and automating daily tasks through intuitive workflows. It enhances security with integrated role-based network access control (NAC) and supports compliance needs through flexible deployment options.

  Site Engine offers Fabric-specific visualizations and configuration workflows, streamlining the management of Extreme Fabric and ensuring efficient operations

Policy and Access Management

- ExtremeControl for ExtremeCloud IQ - Site Engine: Delivers vendor-agnostic Network Access Control (NAC) to authenticate users and devices, enabling secure access based on roles and access rights.
- ExtremeControl integrates with next-generation firewall solutions and can orchestrate endpoint isolation and remediation based on alerts received. It shares contextual information such as users, IP addresses, and locations for powerful policy enforcement at perimeter firewalls.

Palo Alto Networks Next-Gen Firewalls (NGFW)

Palo Alto Networks next-generation firewalls offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort, so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection everywhere. The user, application and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Integration Benefits

The integration of Extreme Networks and Palo Alto Networks offers a comprehensive and agile security solution tailored for higher education:

Prevent the Spread of Malware:
Simple-to-manage yet granular network segmentation prevents the spread of cyberthreats while serving the diverse needs of faculty, staff, and students.

Granular Visibility:
Gain detailed visibility into network usage to identify and mitigate potential security threats.

Automated Threat Prevention:
Automatically prevent known and unknown threats from impacting students, staff, networks, and data.

Device Protection:
Protect school-owned devices and simplify BYOD and mobility.

Safe Cloud Use:
Enable secure use of cloud and SaaS applications .

Learn More

Discover how Extreme Networks helps power your innovation with secure, AI-native cloud networking, please visit Extremenetworks.com.