aruba
a Hewlett Packard Enterprise company

AT A GLANCE

EDGE TO CLOUD SECURITY IN HIGHER EDUCATION

Every individual, organization and industry including higher education can be a cyberattack target. Educause, the largest community of IT leaders and professionals in higher education, listed "information security strategy" as the #1 most urgent issue to address for the last four years[1]. While general and industry specific cybersecurity reports can give us insight into threat trends and what threat vectors to pay most attention to, threats can come from anywhere anytime. Let's look at ways to stop cybercriminals as early as possible ideally before they gain access and definitely before they do any real damage to a university[2].

BROAD ATTACK SURFACE

University network infrastructures are complex and are driven primarily by the need for always-on, anytime and anywhere access – all in support of student learning and their university experience. With 15+ years of delivering secure, high performance networks to higher education institutions, Aruba understands the unique cybersecurity challenges associated with more open to the public yet secure networks, tech savvy students, students and faculty connecting a wide range of personal devices and unsecured IoT devices, the need for collaboration, technology enabled learning, securing research, institutional and student IP that is increasingly a target of cybercriminals, and more. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although education institutions are increasing investments in cybersecurity, recent breach statistics suggest there are opportunities for improvement to stay ahead of threats. The way we approach security requirements and compliance has to be addressed from the Edge, where new devices, users, and critical data reside.

Let's investigate how modern security solutions from Aruba can help education institutions better:

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices

The 2019 Verizon Data Breach Investigations Report determined that human errors accounted for 35% of data breaches in the education sector.[3]

- IBM Security

Alarmingly, out of 17 industries in the U.S., Education comes last in terms of total cybersecurity. This should be a cause for serious concern for the education industry as a whole.

Cyberattack incidents include:

- Phishing attacks and network breaches resulting in the disclosure of personal data
- Ransomware attacks
- Denial-of-service attacks
- Other cyber incidents resulting in school disruptions and unauthorized disclosures

- 2018 Education Cybersecurity Report[4]

[1] Educause 2019 Top 10 IT Issues

[2] Wired: The worst cybersecurity breaches of 2018 so far

[3] 2019 Verizon Data Breach Investigations Report

[4] 2018 Education Cybersecurity Report

ARUBA SECURE SOLUTIONS FOR HIGHER EDUCATION

Secure Infrastructure

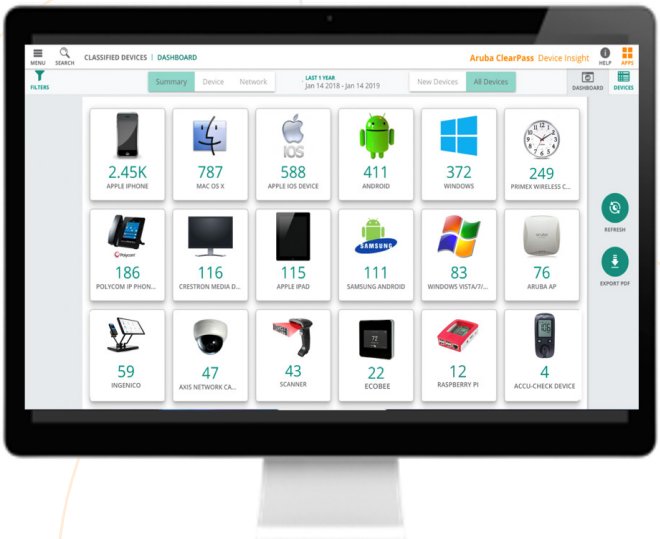
For 20 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based on user, role, application, device and location.

Aruba ESP, is the only architecture to implement an end-to-end network architecture composed of WLAN, switching, SD-WAN, AIOps, all with security built-in from the start.

Know What is on the Network

Today, many IoT devices are built on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is critical to apply the appropriate security controls necessary to secure the Edge.



Zero Trust Access to the Network

Aruba ClearPass Policy Manager provides network access control delivering discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network. Additionally, ClearPass now shares identity-based telemetry with Aruba EdgeConnect SD-WAN appliances to provide even more granular segmentation.

Precise Control and Dynamic Segmentation

ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for.

Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass Policy Manager to deliver a network edge that securely isolates and separates user and device traffic across wired and wireless networks.

Unified Branch Security and Threat Protection

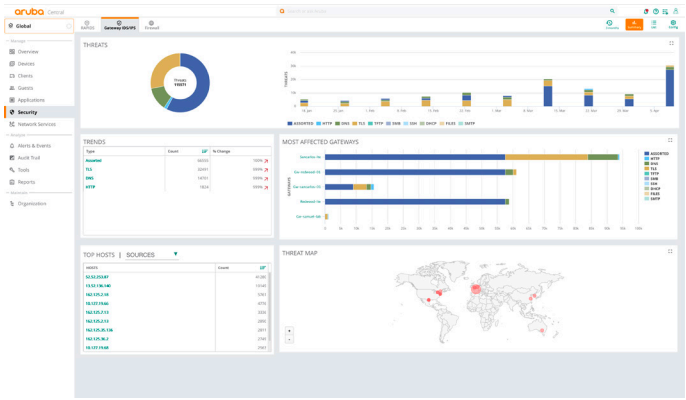
With students, staff, administrators and visitors coming in and out of environments and student personal academic records being high-value to criminals, higher education organizations are at high risk and need advanced threat detection capabilities. Aruba solutions defend against a myriad of threats, including phishing, denial of service (DoS), and increasingly widespread ransomware attacks. Supported Aruba SD-WAN gateways perform identity-based intrusion detection and prevention (IDS/IPS), working together with Aruba Central, ClearPass Policy Manager, and the Policy Enforcement Firewall. Identity-based IDS/IPS performs signature- and patternbased traffic inspection on both the branch office LAN (east-west) traffic as well as the SD-WAN (north-south) traffic flowing through the gateway to deliver embedded branch network security.

WAN, Cloud Security Orchestration, and Secure Access Service Edge (SASE)

Distributed locations require security solutions that can can be adopted across the WAN. Additionally, as higher education organizations migrate many of their applications to the cloud, it is critical that SD-WAN and security solutions adapt, providing advantages both on the networking and the security side. The Aruba EdgeConnect solution provides best-of-breed SD-WAN capabilities combined with seamless orchestration with best-of-breed cloud security vendors. This significantly reduces the amount it takes to incorporate cloud-based security services into the existing network and security infrastructure and puts security closer to their cloud-hosted infrastructure where it belongs.

Security Management Dashboard

An advanced security dashboard within Aruba Central provides IT teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, as well as correlation and incident management. Insights include threats over time, threat trends, threat metrics by category, type, and severity, and impacted users and services. Threat events are sent to SIEM systems and ClearPass for remediation



NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and network security, and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

TO LEARN MORE

https://www.arubanetworks.com/products/security/

https://www.arubanetworks.com/solutions/higher-education/

a Hewlett Packard Enterprise company

AAG_EdgeToCloudSecurityInHigherEducation_RVK_111721 a00089536enw

Contact us at www.arubanetworks.com/contact