HPE aruba networking

Edge-to-cloud security in higher education

HPE GreenLake

Every individual, organization and industry—including higher education—can be the target of cyberattacks. Educause listed "Increasing need for data security and protection against threats to personal privacy" as the top trend in IT issues in higher education in 2023[1]. 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 an educational institution.

Broad attack surface

University network infrastructures are complex and driven primarily by the need for always-on, anytime and anywhere access—all in support of student learning and their university experience. With 21 years of delivering secure, high performance networks to higher education institutions, HPE Aruba Networking 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 higher 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 HPE Aruba Networking 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
- Continuously monitor for change and take action when compromise is suspected

[1] educause.edu/ecar/research-publications/higher-education-trend-watch/2023

The 2022 Verizon Data Breach Investigations report determined that 74 percent of all breaches include the human element through error, privilege misuse, social engineering, or use of stolen credentials.[2]

The education/research sector was the number one most attacked industry globally, seeing a 43% increase in 2022 compared to 2021, with an average of 2,314 attacks per organisation every week.[3]

Cyberattack incidents in education include[4]:

- **Phishing**
- **Ransomware**
- **Distributed denial-of-service attacks**
- **Video conferencing disruptions**

HPE Aruba Networking secure solutions for higher education

Secure infrastructure

For 21 years, HPE Aruba Networking has delivered high-performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by HPE Aruba Networking experts and delivers a range of security and ease-of-use features.
- Secure boot delivers anti-tampering features for access points.
- Military-grade encryption ensures traffic is secure.

HPE Aruba Networking Edge Service Platform (ESP) is the only architecture to implement an end-toend network architecture composed of WLAN, switching, SD-WAN, AIOps—all with security built-in from the start.

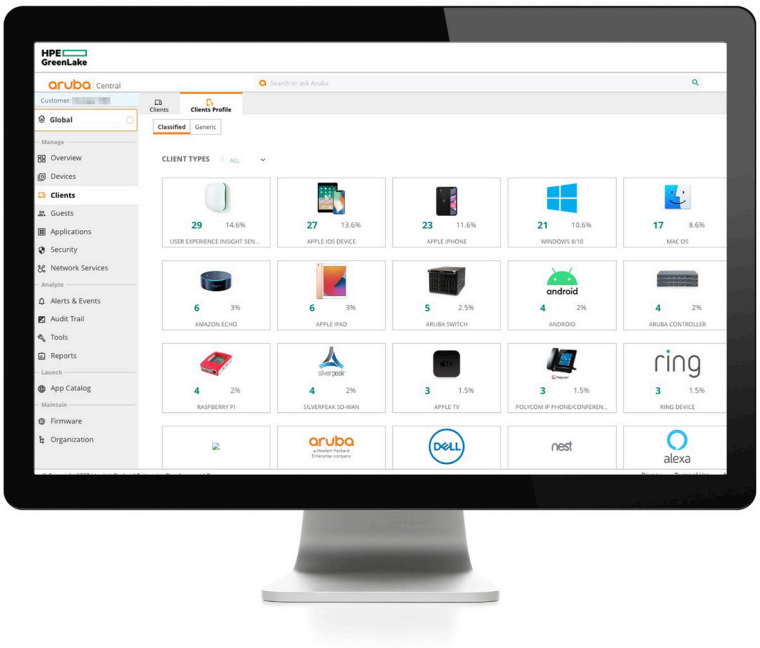
Automate and simplify global security operations

HPE Aruba Networking Central NetConductor is the next-generation solution for increasingly complex networks, enabling educational institutions of all types and sizes to automatically configure LAN, WLAN, and WAN infrastructure to deliver optimal network performance while enforcing granular security policies that are the foundation of Zero Trust and SASE architectures.

[2] verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

[3] blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

[4] gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done



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. Within HPE Aruba Networking Central NetConductor, Client Insights leverages native infrastructure telemetry from access points, switches, and gateways, as well as clients, without requiring installation of physical collectors or agents. ML-based classification models are used to automatically fingerprint and identify with up to 99% accuracy a wide variety of endpoints connecting to the network, including a diverse set of IoT devices across the entire wired and wireless infrastructure. For environments not managed by cloud-based HPE Aruba Networking Central or with third-party network devices, ClearPass Device Insight (CPDI) can be leveraged for ML-based identification and profiling of clients.

Zero trust access to the network

HPE Aruba Networking ClearPass network access control delivers comprehensive 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 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 HPE Aruba Networking EdgeConnect SD-WAN to provide granular segmentation throughout the distributed organization.

For higher education organizations that use HPE Aruba Networking Central, Central NetConductor provides the flexibility to use HPE Aruba Networking Central Cloud Authentication and Policy, the first built-in, cloud-native NAC and identity management solution, or ClearPass. Each build on our history of delivering simple-to-use employee, guest and IoT network protection across distributed networks.

The use of Cloud Auth also enables IT organizations to use MPSK to streamline the onboarding of student devices. For enhanced endpoint visibility, Client Insights performs AI-powered endpoint profiling and provides the ability to “tag” groups of endpoint clients for segmentation per location, SSID, port, or other attributes. This allows universities to eliminate manual steps currently being used, further streamlining device onboarding for students, faculty, and staff.

Precise control and Dynamic Segmentation

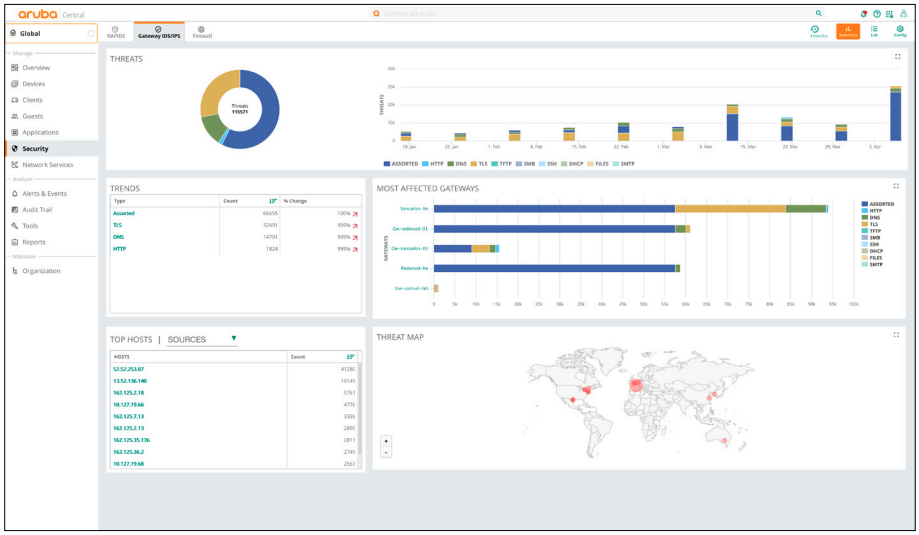
Dynamic Segmentation establishes least-privilege access to applications and data by segmenting traffic based on identity and associated access permissions. Dynamic Segmentation supports two enforcement models—centralized and distributed—allowing IT to use one or both models based on the needs of the environment. With centralized Dynamic Segmentation, traffic is kept secure and separate with the use of GRE tunnels between access points and HPE Aruba Networking gateways (or mobility controllers) with HPE Aruba Networking Policy Enforcement Firewall (PEF), a full application firewall embedded in HPE Aruba Networking network infrastructure. With distributed Dynamic Segmentation, enabled by HPE Aruba Networking Central NetConductor cloud-native network security services, global policy identifiers reflecting the role and access permission of the user or device are embedded in the packet header and interpreted inline by CX switches and gateways for policy enforcement.

Unified branch security and threat protection

With students, faculty and 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. HPE Aruba Networking solutions defend against myriad threats, including phishing, denial of service (DoS), and increasingly widespread ransomware attacks. Supported HPE Aruba Networking EdgeConnect SD-Branch gateways perform identity-based intrusion detection and prevention (IDS/IPS), working together with Aruba Central, ClearPass, and Policy Enforcement Firewall. Identity-based IDS/IPS performs signature- and pattern-based traffic inspection on both the branch LAN (east-west) traffic as well as the SD-WAN (north-south) traffic flowing through the gateway to deliver embedded branch network security.

Security management dashboard

An advanced security dashboard within HPE Aruba Networking Central provides IT teams with network-wide visibility, multidimensional 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 HPE Aruba Networking ClearPass for remediation.



WAN, cloud security orchestration, and Secure Access Service Edge (SASE)

Hybrid educational models and 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. By combining the advanced capabilities of HPE Aruba Networking EdgeConnect SD-WAN, SD-Branch, and Microbranch solutions with the cloud-delivered, Zero Trust security services of an SSE (Security Service Edge), universities can build a flexible SASE architecture to ensure stable, secure access to applications while converging network and security functions.

HPE Aruba Networking SSE empowers organizations to unify secure access across campus, satellite campus, and remote locations. The platform delivers authenticated user access to private applications at the network edge (Zero Trust Network Access—ZTNA), a secure web gateway (SWG) to safeguard user access to the Internet, and a cloud access security broker (CASB) that enforces policies to protect sensitive data, as well as data loss prevention (DLP) capabilities. When deployed with the EdgeConnect portfolio, universities gain the operational benefits of a unified, single-vendor SASE solution.

Next steps for a healthier security posture

With advanced access controls and network security, and interoperability with over 150 multi-vendor network and security solutions, HPE Aruba Networking provides the visibility you need and the confidence you want that your security policies are dynamically enforced to support a strong security posture.

To learn more

arubanetworks.com/zerotrust

arubanetworks.com/sase

arubanetworks.com/solutions/highereducation/

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

All third-party marks are property of their respective owners.

AAG_SecurityInHigherEd_CT_100423 a00089536enw