aruba
a Hewlett Packard
Enterprise company

AT A GLANCE

EDGE-TO-CLOUD SECURITY IN HOSPITALITY

The hospitality industry has seen an increasing number of brazen cyberattacks in the past few years. Recently, a massive cyberattack at an international chain compromised personal information of nearly 400 million guests[1] including birthdates, passport and credit card information. These stolen details can become highly lucrative as they provide the necessary foundation to launch identity theft scams, phishing attempts, and a variety of financial and other cyberattacks at individuals and organizations.

BROAD ATTACK SURFACE

When addressing IT strategies, hospitality organizations globally are faced with new security and connectivity challenges. Millions of new connected devices are being added to the network every day and guests expect to use their devices to access a variety of services, from check-in to check-out and everything in between. The explosion of these unpredictable device types renders manual device profiling techniques inadequate and makes automation a key requirement for securing users and devices. To add to the complexity, many IoT devices are often connected to disparate overlay networks that typically support only one type of connectivity, such as Wi-Fi, Bluetooth or Zigbee. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although the hospitality industry is 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 hospitality vendors 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

Hotels are not known for being obvious cyberattack targets as hackers prefer financial or retail institutions, but the user data held by many hotels make them much more valuable. Known hacks have utilized electronic door locks, POS systems, Wi-Fi, and in one reported case, even a connected aquarium to hijack a casino's internal networks in search of corporate data[2].

Cyberattack incidents include:

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

ARUBA SECURE SOLUTIONS FOR HOSPITALITY

Secure Infrastructure

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

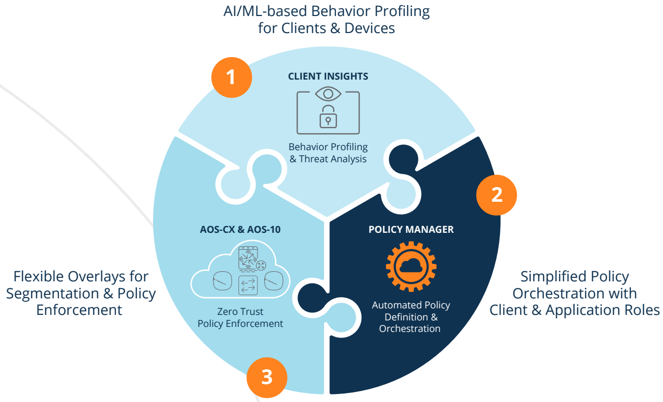
- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall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

[1] Hotel News Now, Timeline: The growing number of hotel data breaches
[2] The Hotel Hackers Are Hiding in the Remote Control Curtains

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.

Automate and Simplify Global Security Operations

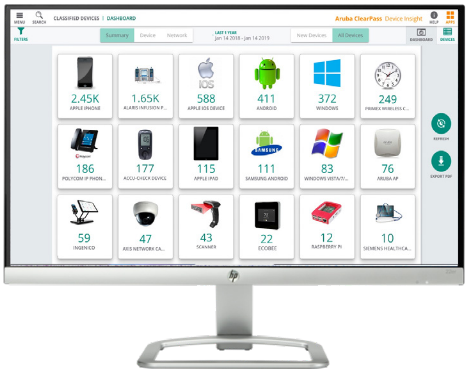
Aruba Central NetConductor is the next-generation solution for increasingly complex networks, enabling organizations of all types and sizes to automatically configure LAN, WLAN, and WAN infrastructure to deliver optimal network performance while enforcing granular access control security policies that are the foundation of Zero Trust and SASE architectures. Central NetConductor comprises services delivered by Aruba Central, the platform that is the foundation of the Aruba Edge Services Platform (ESP).


AI/ML-based Behavior Profiling for Clients & Devices
1
CLIENT INSIGHTS
Behavior Profiling & Threat Analysis
2
POLICY MANAGER
Automated Policy Definition & Orchestration
Simplified Policy Orchestration with Client & Application Roles
AOS-CX & AOS-10
Zero Trust Policy Enforcement
3
Flexible Overlays for Segmentation & Policy Enforcement

Know What is on the Network

Today, many IoT devices are built on standard hardware platforms which 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 applying the appropriate security controls necessary to secure the Edge.

Central NetConductor utilizes artificial intelligence to automatically detect network performance and reliability issues while identifying opportunities for optimization based on local and peer-based best practices.



Zero Trust Access to the Network

Aruba ClearPass NAC 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.

For hospitality organizations, that use Aruba Central, Central NetConductor provides customers the flexibility to pick their NAC solution of choice, whether that is ClearPass, our market-leading on-premises Network Access Control (NAC) solution, or Cloud Auth, the first integrated and cloud-native NAC and identity management solution, which builds on ClearPass NAC market leadership and streamlines the protection of distributed enterprise networks by working seamlessly across wired, wireless, and WAN connections.

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 network.

If using Aruba Central NetConductor, hospitality organizations can extend the capabilities of Aruba's market-leading Dynamic Segmentation across multiple network overlays, making it easier to adopt comprehensive Zero Trust and SASE security.

Unified Branch Security and Threat Protection

For hospitality companies, ensuring the security of guest data and payments is a must. 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 pattern-based 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 be adopted across the WAN. Additionally, as hospitality 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

Aruba Central as well as Central NetConductor provide 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 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.

LEARN MORE

https://www.arubanetworks.com/solutions/hospitality/

https://www.arubanetworks.com/products/network-management-operations/central/netconductor/

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

a Hewlett Packard
Enterprise company

AAG_SecurityInHospitality_RVK_060322 a00090830enw

Contact us at www.arubanetworks.com/contact