aruba
a Hewlett Packard
Enterprise company

SOLUTION OVERVIEW

Aruba Edge-To-Cloud Security

Enabling secure edge adoption and WAN transformation

THE NETWORK EVOLVED: EDGE AND CLOUD EXPANSION

Growth at the Edge in the form of remote workers and large numbers of new IoT devices has created unique challenges around onboarding, visibility, and security. At the same time, continued migration of applications to the cloud has changed the way we approach network planning and related security requirements, since legacy networks were not designed to accommodate a cloud-first world. While network complexity and threats continue to grow, organizations require a holistic, end-to-end approach to ensure security and compliance is addressed from the Edge, where new devices, users and branch offices reside, to the cloud, where key applications and critical data require the highest levels of protection, as well as performance and availability.

ARUBA ESP (EDGE SERVICES PLATFORM) WITH EDGE-TO-CLOUD SECURITY

Aruba ESP is the only architecture that enables organizations to implement an end-to-end network architecture composed of WLAN, switching, SD-WAN, and AI-powered automation, all with security built-in from the start. With the ICSA Labs-certified Secure SD-WAN Aruba EdgeConnect Enterprise platform, organizations can adopt the benefits of industry-leading SD-WAN capabilities, coupled with identity- and role-based traffic segmentation, enforced with a built-in next-generation firewall, and supported by IDS/IPS and other security functions. With built-in support for advanced security capabilities including Zero Trust and through a tight integration with multiple SSE (Security Service Edge) vendors, organizations can build a best-of-breed SASE architecture without compromise, increasing protection while simplifying network and security operations.

SECURITY AT THE EDGE: ZERO TRUST SEGMENTATION

With the increased adoption of IoT paired with a dramatic increase in remote users, full spectrum visibility of all users and devices connecting to the network has become an Increasingly challenging task. Without visibility, critical security controls necessary to secure the Edge are difficult to apply. Automation, AI-based machine learning, and the ability to quickly identify device types is critical. Aruba Client Insights, as well as third-party infrastructure-compatible ClearPass Device Insight, use a combination of active and passive discovery and profiling techniques to automatically detect the full spectrum of devices connected or attempting to connect to the network, including IoT devices. This allows organizations to better understand what's on their networks, automate access privileges, and monitor the behavior of each client's traffic flows to more rapidly spot attacks and take action..

ClearPass Policy Manager and Cloud Auth cloud-native NAC enable the creation of role-based access policies that allow IT and security teams to operationalize these best practices using a single role and associated access privileges that are applied anywhere on the network — wired or wireless infrastructure, in branch, at the home office or ad-hoc location, or on campus. Once profiled, devices are automatically assigned the proper access control policy and segmented from other devices via Aruba's Dynamic Segmentation capabilities.

Dynamic Segmentation establishes least-privilege access to applications and data by segmenting traffic based on identity and associated access permissions. Dynamic Segmentation offers a choice of enforcement models—centralized and distributed—that can co-exist and be flexibly adopted. Enforcement is provided by Aruba's Policy Enforcement Firewall (PEF), a full application firewall embedded in Aruba network infrastructure. Additionally, ClearPass can share identity-based telemetry with EdgeConnect SD-WAN appliances to provide granular segmentation that extends from edge to cloud.

ARUBA ESP (EDGE SERVICES PLATFORM)

Next-generation, cloud-native architecture to accelerate digital business transformation

AI & Automation
Onboarding | Provisioning | Management & Orchestration | AIOps | Analytics | Location

Edge-to-Cloud Security
Visibility | Authentication & Authorization | Dynamic Segmentation | Zero Trust | SASE

Unified Infrastructure
Wireless | Wired | SD-WAN | 5G | IoT

Figure 1: Edge-to-Cloud Security increases protection while simplifying network and security operations

UNIFIED BRANCH SECURITY AND THREAT PROTECTION

Protecting against myriad threats, such as phishing, ransomware, and denial of service (DoS) attacks, is critical within the distributed enterprise. EdgeConnect Enterprise protects the organization against these threats with next-generation firewall, intrusion detection and prevention (IDS/IPS), and DDoS detection and remediation capabilities.

The EdgeConnect SD-Branch solution can also secure branch locations using a built-in firewall, Dynamic Segmentation, and Aruba Threat Defense, including IDS/IPS. An advanced security dashboard within Aruba Central provides IT teams with network-wide visibility, multi-dimensional threat metrics, and threat intelligence data, as well as correlation and incident management. Threat events are sent to SIEM systems and ClearPass for remediation.

EdgeConnect Enterprise was the market's first complete solution to receive Secure SD-WAN Certification from ICSA Labs.

The ICSA Labs Secure SD-WAN Certification includes rigorous security-related functionality testing to validate that EdgeConnect is secure and properly enforces consistent policy for both WAN-specific functions and security functions equivalent to a standard ICSA Labs Firewall Certification. EdgeConnect Enterprise replaces outdated and difficult-to-manage physical firewalls at branch locations while delivering consistent security for all users, from any network location, from any device, and wherever applications are hosted.

CLOUD SECURITY ORCHESTRATION AND SECURE ACCESS SERVICE EDGE (SASE)

As organizations continue to migrate many of their applications to the cloud, it is critical that SD-WAN and security solutions adapt to shift. By modernizing WAN and security infrastructure, customers can gain significant 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 SSE vendors. This significantly reduces the amount of time and effort it takes to incorporate cloud-based security services into the existing network and security infrastructure. By augmenting these cloud-based security services, organizations can put security closer to their cloud-hosted infrastructure where it belongs.

ARUBA CENTRAL: THREAT INTELLIGENCE ACROSS THE INFRASTRUCTURE

Aruba Central is a powerful cloud networking solution that offers unmatched simplicity for today's networks. As the management and orchestration console for Aruba ESP, Central provides a single point of control for overseeing every aspect of wired and wireless LANs, WANs, and VPNs across campus, branch, and remote office locations. This includes an advanced security dashboard that includes IDS/IPS alerts, threat intelligence data, and correlation with incident management capabilities.

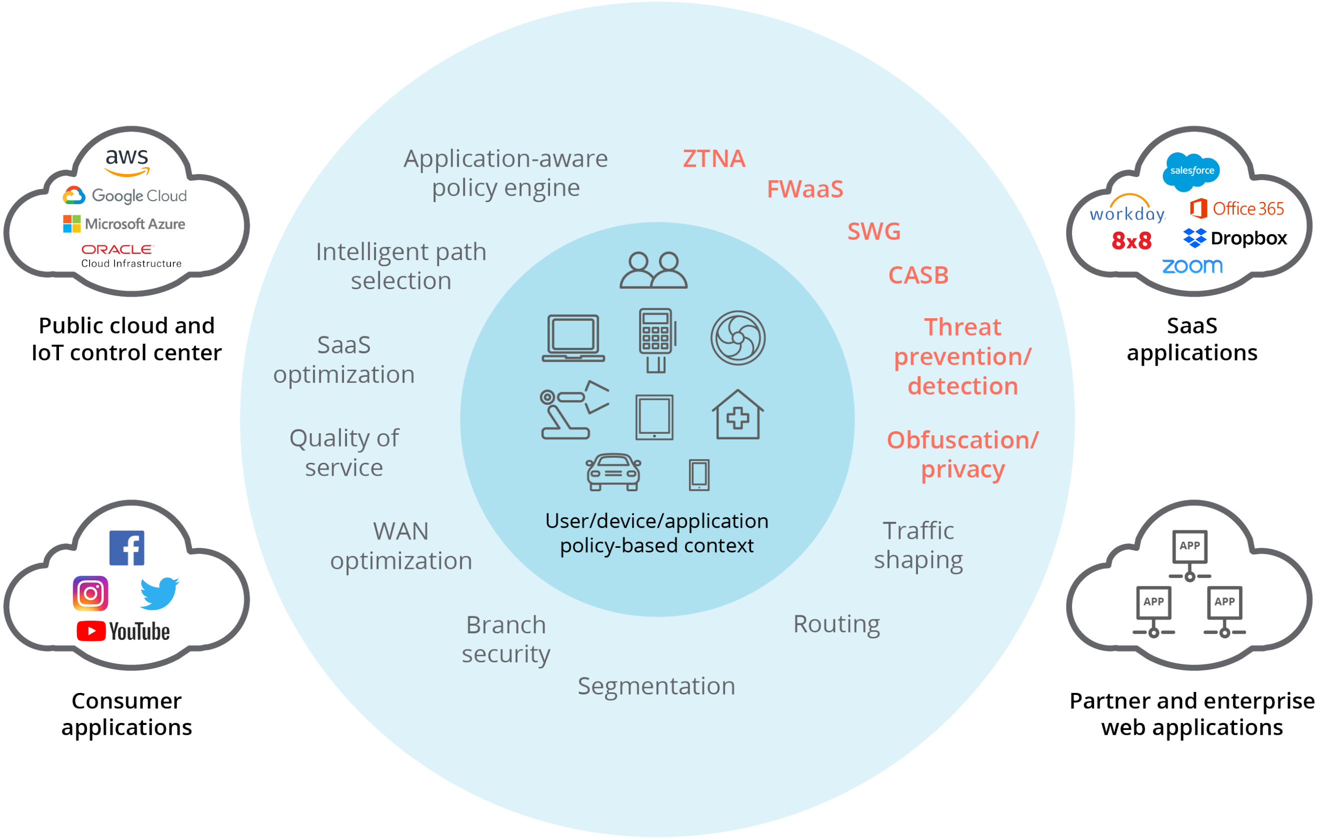

Figure 2: A secure access service edge is needed to support the enterprise's digital transformation initiatives, i.e., cloud-first strategy and workforce mobility needs. In a robust SASE architecture, comprehensive WAN capabilities need to work in conjunction with comprehensive network security functions to support digital enterprises' dynamic, secure access needs for users, devices, and applications.

ARUBA 360 SECURITY EXCHANGE: REAL-TIME THREAT TELEMETRY FOR REAL-TIME DECISIONS

Aruba's security products integrate with a wide range of third-party IT systems for best-of-breed Zero Trust and SASE frameworks without compromise. Tight integration and bidirectional communication between systems powers continuous monitoring, provides flexibility, and creates a seamless solution that is as easy to manage as a single vendor solution. With best-of-breed SASE, enterprises build a consistent security architecture that blocks the impact of cyberattacks while increasing business agility and reducing complexity.

SUMMARY

Hybrid work, digital acceleration, and IoT growth require innovative security strategies. With Aruba ESP Edge-to-Cloud security, organizations can implement an end-to-end network comprising WLAN, switching, SD-WAN, and remote access, all protected by common Zero Trust and SASE security frameworks, built-in from the start. Identity-based traffic segmentation ensures consistent security policies are applied from the access edge to the WAN edge to the cloud, while integration reduces operational complexity that can slow implementation and lead to security issues.

For more information, visit https://www.arubanetworks.com/solutions/edge-to-cloud-security/

aruba
a Hewlett Packard
Enterprise company

SO_ArubaEdgetoCloudSecurity_RVK_092822 a00112725enw.

Contact us at www.arubanetworks.com/contact