aruba
a Hewlett Packard
Enterprise company

SOLUTION OVERVIEW

Implementing Zero Trust Best Practices

WITH ARUBA ESP AND EDGE-TO-CLOUD SECURITY

Network security challenges have evolved significantly over the years as users have become increasingly decentralized and attacks have become more sophisticated and persistent. Traditional security approaches that focused primarily on the perimeter of the network have become ineffective as stand-alone security strategies. Modern network security must accommodate an ever-changing, diverse set of users and devices, as well as much more prevalent threats targeting previously "trusted" parts of the network infrastructure.

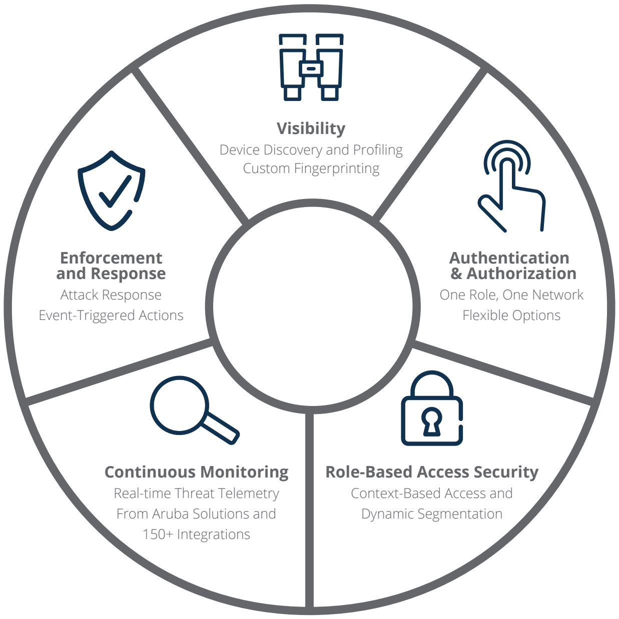
Zero Trust has emerged as an effective model to better address the changing security requirements for the modern enterprise by assuming that all users, devices, servers, and network segments are inherently insecure and potentially hostile.

Several years ago, the SASE (Secure Access Service Edge) model emerged, reflecting the importance of cloud-based workloads and extending Zero Trust to include SD-WAN and cloud-delivered security services. Zero Trust and SASE frameworks provide the blueprint for a secure network foundation that uses identity-based segmentation built in to the network to protect the organization.

With Aruba's built-in foundation for Zero Trust and SASE, Aruba ESP offers edge-to-cloud security, improving overall network security posture by applying a rigorous set of security best practices and controls to previously trusted network resources.

ARUBA ESP: CORE ZERO TRUST PRINCIPLES

Zero Trust varies significantly depending on which domain of security is being considered. Although application-level controls have been a focal point within Zero Trust, a comprehensive strategy must also encompass network security and the growing number of connected devices, including the hybrid work environment. Aruba ESP with Edge-to-Cloud Security incorporates comprehensive visibility, least-privilege access segmentation and control, as well as continuous monitoring and enforcement. Even traditional VPN solutions are enhanced by ensuring that the same controls applied to campus or branch networks, also extend to the remote location and mobile worker.



In the age of IoT, basic principles of good network security are often difficult to implement. When possible, all devices and users should be identified and properly authenticated before granting them network access. In addition to authentication, users and devices should be given the least amount of access necessary to perform their business-critical activities once they're on the network. This means authorizing which network resources and applications any given user or device can access. Finally, all communications between end users and applications should be encrypted.

THE NEED FOR COMPREHENSIVE VISIBILITY

With the increased adoption of IoT, full spectrum visibility of all devices and users on the network has become an increasingly challenging task. Without visibility, critical security controls that support a Zero Trust model are difficult to apply. Automation, AI-based machine learning, and the ability to quickly identify device types is critical.

Aruba's cloud-based network management solution Aruba Central includes AI-powered visibility and profiling with Client Insights. 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 Aruba Central or with third-party network devices, ClearPass Device Insight (CPDI) can be leveraged for ML-based identification and profiling of clients.

AUTHENTICATION & AUTHORIZATION

Once a user or device is known and profiled, the next step is to authenticate its identity each time it connects to the network. With ClearPass, organizations can deploy wired or wirelessly using standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT and headless devices that may lack support for 802.1X. For wired environments where RADIUS-based authentication cannot be deployed, ClearPass offers an alternative using SNMP-based enforcement. Multiple authentication methods can be used to concurrently support a variety of use cases including support for multifactor authentication based on log-in times, posture checks, and other context such as new user, new device, and more.

For networks managed by Aruba Central, cloud-native NAC solution Cloud Auth enables frictionless on-boarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores such as Google Workspace or Azure Active Directory to automatically assign the right level of network access.

ADOPTING IDENTITY-BASED ACCESS CONTROL FOR LEAST-PRIVILEGE ACCESS

Least-privilege access based on identity allows users and devices to access just the resources needed to perform their functions—and only for as long as they behave consistently with their role. This means applying an access control policy that only authorizes access to resources that are absolutely necessary for that device or user and dynamically adjusting access when anomalous behavior is observed or breach is suspected.

Aruba 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 Aruba Gateways (or Mobility Controllers). Aruba ClearPass Policy Manager enables the creation of role-based access policies that follow the user throughout the network and are applied uniformly across wireless, wired, and VPN connections. Enforcement is provided by Aruba's Policy Enforcement Firewall (PEF), a full application firewall embedded in Aruba network infrastructure.

Aruba Central NetConductor enables distributed Dynamic Segmentation using widely adopted protocols such as EVPN/VXLAN to produce a distributed network overlay. Central NetConductor offers cloud-native security services for global policy management and network configuration with simple business-logic interface and intuitive workflows. Global policy identifiers reflecting the role and access permission of the user or device are embedded in the packet header and interpreted inline by Aruba CX switches and gateways for policy enforcement.

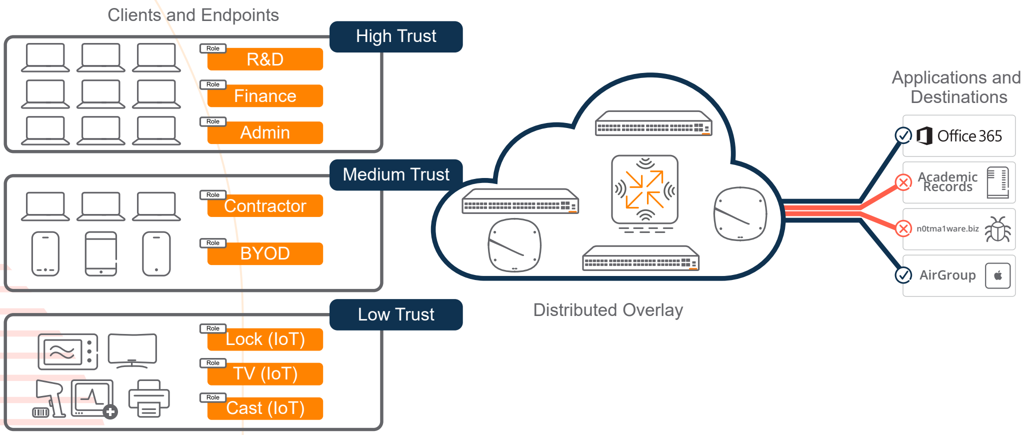


Figure 1: Dynamic Segmentation with a distributed overlay fabric

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

CONTINUOUS MONITORING AND ENFORCEMENT

With role-based access in place to enforce granular segmentation, ongoing monitoring of users and devices on the network make up another Zero Trust security best practice. This addresses risks related to insider threats, advanced malware, or persistent threats that have circumvented traditional perimeter defenses.

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. The Aruba EdgeConnect Enterprise SD-WAN platform protects the organization against these threats with next-generation firewall, intrusion detection and prevention (IDS/IPS), and DDoS detection and remediation capabilities, The market's first complete solution to receive Secure SD-WAN Certification from ICSA Labs, 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.

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.

360 Security Exchange

With over 150 integrations made up of best-of-breed security solutions that include Security Operations and Response (SOAR) tool sets, ClearPass is able to dynamically enforce access based on real-time threat telemetry coming from multiple sources. Policies can be created to make real-time access control decisions based on alerts coming from Security Information and Event Management (SIEM) tools and many other sources. ClearPass actions are fully configurable, from limiting access (e.g., Internet access only) to fully removing a device from the network for remediation.

ARUBA ESP (EDGE SERVICES PLATFORM)

To help organizations capitalize on opportunities at the Edge, Aruba developed Aruba ESP, the industry's original AI-powered platform designed to unify, automate, and secure the Edge. Edge-to-Cloud Security is a key component of Aruba ESP and, when combined with AI-powered automation and a Unified Infrastructure, enables organizations to reduce costs, simplify operations, and stay secure.

SUMMARY

Today's network environment and threat landscape require a different approach. The perimeter-centric network security of the past was not designed for today's hybrid workforce or emerging IoT devices. Aruba ESP with Edge-to-Cloud Security provides built-in support for Zero Trust and SASE security frameworks, spanning visibility, identity-based control, and enforcement to address the requirements of a decentralized, IoT-driven network infrastructure.

Learn more at arubanetworks.com/zerotrust

a Hewlett Packard
Enterprise company

SO_ZeroTrustSecurity_SK_092722 a00097694enw

Contact us at www.arubanetworks.com/contact