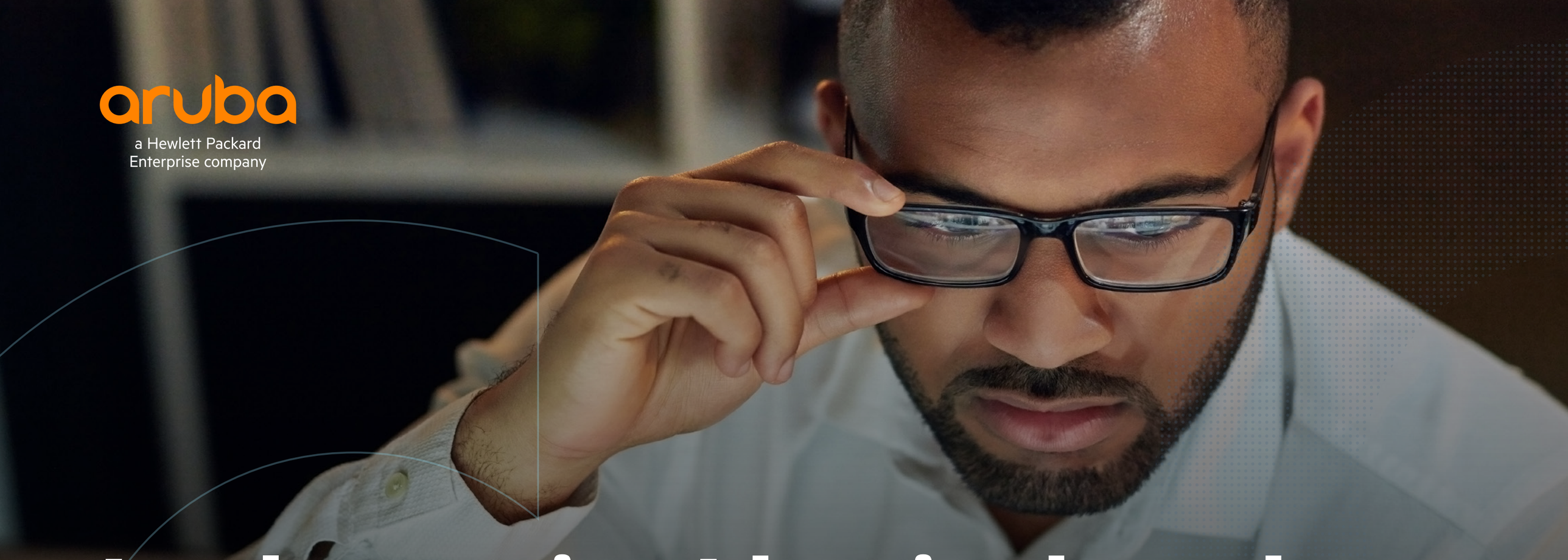
aruba
a Hewlett Packard Enterprise company



Implementing Identity-based Zero Trust and SASE Architectures

HOW TO USE NETWORK ACCESS CONTROL TO PROTECT THE ORGANIZATION

Table of contents

Why security must evolve

Network security challenges have significantly increased as workers have become more decentralized, new IoT devices have flooded the network, and attacks have become more sophisticated and persistent. Traditional security approaches focused primarily on the network perimeter have become ineffective as a primary security strategy.

Modern network security must accommodate an ever-changing, diverse set of users and devices, as well as much more potent threats targeting previously “trusted” parts of the network infrastructure.
To address this issue, two major network security initiatives were launched as a guide in planning, designing, and implementing more secure networks in support of an overall IT protection strategy. In the 2014 Federal Information Systems Management Act (FISMA), the National Institute of Standards and Technology (NIST) was impaneled to develop a set of overall security guidelines and architecture that has evolved into Zero Trust Architecture. In 2019, Gartner defined the Secure Access Service Edge (SASE) concept in recognition that IT access and corresponding security services will be available in the cloud.

Zero Trust and SASE rely on identity

A foundational principle of Zero Trust and SASE architectures is that access to IT resources should not be dictated solely by where or how a client connects. In other words, the network is inherently untrustworthy, and an "overlay" security fabric must be added based on a well-defined, identity-based architecture that segments traffic to those paths and resources that have been explicitly permitted. In addition, these architectures can cover the security "lifecycle" of an endpoint from authentication and authorization to continuous monitoring and attack response.

The objective is to authenticate the client and then continuously compare its configuration and status to a defined set of acceptable security states to ensure that it will not introduce vulnerabilities or is not participating in an attack. In this guide, you'll learn how to implement a Zero Trust and SASE architecture using identity as the foundation.

Support both frameworks by addressing 5 key security challenges

1 **Eliminate network blind spots.** The goal is to discover and profile all devices connected to the network—including IoT devices outside the purview of the network and security team.

2 **Verify identity before allowing access.** Starting with 802.1X, there are many authentication techniques to ensure that only legitimate users and devices connect to the network, including emerging solutions for IoT devices.

3 **Compare endpoint configuration to compliance baselines and remediate as needed.** This allows the security team to define and enforce configuration guidelines that reflect the application of the appropriate patches and updates.

4 **Establish least-privilege access to IT resources by segmenting traffic based on identity-based policies.** After identity and configuration compliance are confirmed, the user or device can be assigned a set of IT privileges dictated by pre-defined access policies enforced in the network infrastructure.

5 **Continuously monitor the security state of the user and device and bi-directionally communicate with other elements in the security ecosystem.** Reduce or eliminate access rights if there are signs that a network-connected user or device has been compromised.

Know what's on your network

The ability to broadly and accurately identify all wireless and wired devices connected to the network—from traditional IT-managed devices to previously undetected IoT devices such as cameras, medical equipment, sensors, and other hard-to-detect endpoints—is an essential security control.

The most effective approach uses multiple discovery methods to find and classify a wide range of device types. The most advanced solutions use machine learning to constantly evaluate contextual and behavioral information, dynamically update fingerprints, and provide recommendations for previously unseen devices.

In support of granular traffic segmentation, device discovery and profiling can be integrated with access policies for closed-loop, end-to-end access control from visibility to network infrastructure enforcement. Devices can automatically be assigned access privileges based on a given policy or quarantined in the event they are out of configuration compliance or behaving in a malicious or insecure manner.

What you can do now

- **Build a device inventory of what is connected to the network.**
- **Continuously monitor for new devices and connections.**
- **Leverage cloud-based fingerprint databases to access profiles for previously unseen devices.**

Ensure consistent authentication for assigning privileges

After a user or device is known and profiled, the next step is to authenticate its identity each time it connects to the network. Organizations can rely on secure authentication using standards-based 802.1X enforcement. MAC address authentication can also be used for IoT and headless devices lacking support for 802.1X. In addition, the Wi-Fi Alliance has recently defined a Wi-Fi CERTIFIED Easy Connect™ standard for securely onboarding certified IoT devices.

Comprehensive guest access simplifies visitor workflow processes to enable employees, receptionists, and other non-IT staff to create temporary guest accounts for secure wireless and wired access. Highly customizable, mobile friendly portals provide easy-to-use login processes that include self-registration, sponsor approval, and bulk credential creation.

What you can do now

- **Set up an authentication solution that can work with multiple protocols and interfaces with a wide variety of identity databases.**
- **Establish a guest portal to seamlessly onboard visitors.**
- **Implement 802.1X authentication for both wired and wireless connections and prioritize Wi-Fi EasyConnect-enabled devices for IoT applications.**

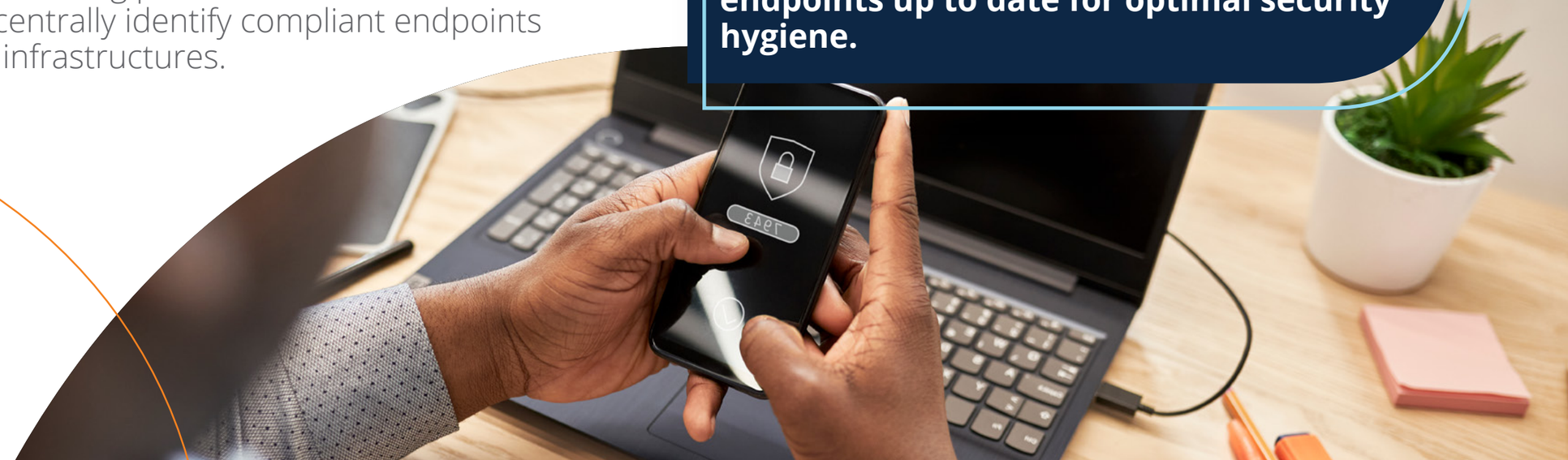
Enforce configuration compliance

Configuration compliance and security posture assessment are critical security controls that can be done by the network. During the authorization process, health assessments are performed on specific devices to ensure they adhere to IT-defined configuration standards, including patch levels, antivirus, antispyware, and firewall policies. Devices not meeting compliance standards can either be automatically remediated with a persistent agent or redirected to a captive portal for further follow-up.

Posture-based health checks are built for common environments and can eliminate vulnerabilities across a wide range of operating systems. Whether agentless or using persistent or dissolvable clients, these solutions can centrally identify compliant endpoints on wireless, wired, and VPN infrastructures.

What you can do now

- **Establish standards for configuration, version, and patch levels required for endpoints accessing the network.**
- **Subscribe to a vulnerability database to ensure that devices connected to the network have the necessary patches to deal with validated attacks.**
- **Educate your end users and IoT administrators regarding the need to keep endpoints up to date for optimal security hygiene.**



Leverage identity to dynamically segment network traffic

At the core of the NIST Zero Trust Architecture is a collaboration of two key network components:

- A Policy Engine/Administrator that defines the conditions under which a user or device can connect to the network and what access privileges they are entitled to, based on the authentication and compliance process they must go through

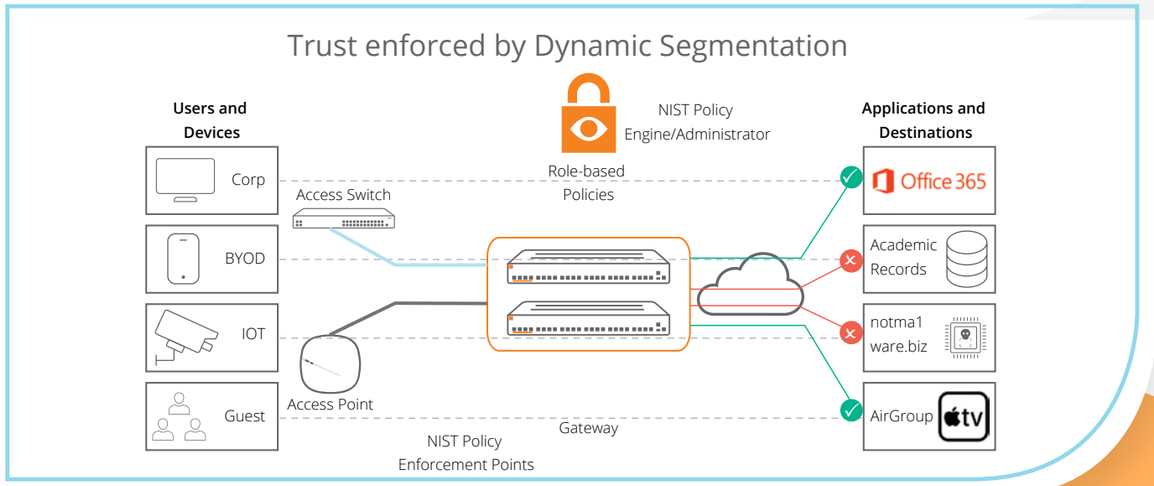
- A Policy Enforcement Point that interprets and enforces the access instructions delivered by the Policy Engine

Together they constitute real-time, or dynamic, traffic segmentation. However, this kind of control cannot be added in after the fact to a network built without consideration for how to manage and enforce identity-based access that must adjust in real time to accommodate changes in endpoint and network status.

The ability to microsegment traffic based on identity and role delivers two main benefits:

Dynamic process: Role-based policy is assigned on the fly to a wired port or wireless connection based on factors such as the access method of the client. Contextual data—like time of day, type of machine, etc.—can also be included so IT staff no longer must use static attributes to control access.

Fine-grained segmentation: This allows client traffic to be segmented based on permissions in the access policy. Microsegmentation provides enhanced security and performance benefits, given that access controls can be much more granular than hard-to-manage VLAN assignments, and they are enforced by the network infrastructure.



When VLANs are not enough: Using EVPN-VXLAN to extend network segmentation on a global scale

The proliferation of endpoints due to BYOD, workplace mobility, and IoT is driving a need for more fine-grained segmentation strategies to separate different profiles of users, devices, and traffic on a global basis—beyond what traditional VLANs can offer. Modern network switches have expanded configuration and policy enforcement choices to include industry standards such as EVPN-VXLAN for more flexibility, global scale, and third-party interoperability. EVPN-VXLAN enables businesses to connect geographically dispersed locations using Layer 2 virtual bridging, and has emerged as a popular networking framework largely due to the limitations of traditional VLAN-based networks. VXLAN encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, meaning virtual Layer 2 subnets can span underlying Layer 3 networks and extend network segmentation across physical locations.

What you can do now

- **Establish groups of users and devices that have similar access permissions to IT assets.**
- **Build access control policies that reflect the organization's security controls.**
- **Map roles to identity at time of authorization and assign an access policy based on role.**

Build deep integration with the security ecosystem

As emphasized in both the NIST Zero Trust Architecture and SASE frameworks, organizations must be able to deploy best-of-breed security solutions and ensure that their entire security ecosystem communicates and coordinates attack awareness and response.

A critical advantage of this approach is that organizations can leverage their existing security investments by seamlessly integrating solutions such as next-generation firewall (NGFW) and security information and event management (SIEM) technologies with their network access control solutions. This avoids single solution lock-in that results in costly upgrades and a single source of products. A network security framework that integrates with the broader security ecosystem provides the best elements of a unified solution with the flexibility of an open architecture.

Sharing context between each component supports end-to-end policy enforcement and visibility. This enables the access control solution to respond to changing threats for users and devices after they have authenticated to the network.

What you can do now

- **Build an overall Zero Trust and SASE-based security strategy to guide your security investments.**
- **Ensure your security solutions are open and can seamlessly integrate with your network access control.**
- **Design policies that will make the network an ally in detecting and responding to attacks.**

How Aruba can help: The Aruba Edge Services Platform delivers Zero Trust and SASE Edge-to-Cloud security solutions

The Aruba Edge Services Platform (ESP) supports Zero Trust and SASE architectures by delivering device discovery, authentication, configuration enforcement, role-based access control, built-in policy-based traffic segmentation, and continuous threat protection, all from a single solution comprising:

Aruba Central Client Insights:

Security and networking teams are constantly watching for devices that are connected to the network outside the proper controls. Client Insights uses a full range of passive and active discovery techniques along with AI fingerprinting to ensure that every device is located and profiled.

ClearPass:

ClearPass performs a wide range of Zero Trust Architecture functions. It starts with a range of authentication services to identify users and devices. Based on identity, ClearPass Policy Manager will assign a set of access permissions that are enforced by the Aruba network. ClearPass OnGuard performs advanced endpoint posture assessment and remediation to ensure security and compliance requirements are met prior to users and devices connecting to the network.

Dynamic Segmentation:

Aruba's market-leading Dynamic Segmentation solution is a critical element of the edge-to-cloud security built into Aruba ESP. It establishes least-privilege access to IT resources by segmenting traffic based on roles and associated access permissions. Dynamic Segmentation unifies role-based access and policy enforcement across wired, wireless, and WAN networks, ensuring that users and devices can communicate with destinations consistent with their role only—keeping traffic secure and separate.

Policy Enforcement Firewall (PEF):

PEF is a stateful, Layer 7 firewall that can be enabled on Aruba wireless access points, gateways, and controllers. PEF is the companion enforcement point for ClearPass policies and enforces policy-based per-user and per-device traffic segmentation for wired, wireless, and WAN connectivity.

Central NetConductor:

This suite of cloud-native network connectivity and security services enables organizations of all types and sizes to automatically configure wired, wireless, and WAN infrastructure to deliver optimal network performance while enforcing the granular access control security policies that are the foundation of Zero Trust and SASE architectures. With Central NetConductor, Dynamic Segmentation can be managed via the cloud with the ability to centrally define and enforce access policies either in a distributed or centralized fashion based on the choice of overlay.

Aruba 360 Security Exchange:

Aruba security products integrate with a wide range of third-party IT systems for end-to-end policy enforcement and visibility for mobile and IoT devices. ClearPass Policy Manager is bi-directionally integrated with over 150 third-party security and management products to provide identity-based information to the ecosystem and receive threat and attack information to inform policy decisions.

The Pentagon modernizes wired and wireless connectivity, across all classification levels, with Aruba infrastructure

The Pentagon, headquarters of the United States Department of Defense (DoD), is modernizing its classified and unclassified networks to support tens of thousands of devices daily. Aruba's ESP-based architecture will provide the Pentagon an automated networking infrastructure that eliminates manual processes like port mapping and initial switch configuration. It is also expanding its deployment of Aruba ClearPass Policy Manager for secure network access control across its networks.

Security Requirements	Zero Trust and SASE Architecture	Aruba Solution
Know what's on the network	An organization protects resources by defining what resources it has	**Aruba Client Insights**
Authenticate all users and devices	Create, store, and manage enterprise user accounts and identity records	**ClearPass Policy Manager**
Ensure con-figuration and compliance guidelines are followed	Gather information about the enterprise asset's current state and apply updates to configuration and software components	**ClearPass OnGuard**
Assign and enforce access policies in the network	All resource authentication and authorization are dynamic and strictly enforced before access is allowed via coordination between a Policy Engine and a Policy Enforcement Point	**Dynamic Segmentation enabled by:** **- ClearPass, PEF with Aruba access points and gateways** **- Central NetConductor, policy manager, and inline enforcement via Aruba switches and gateways**
5. Communicate bi-directionally with the secu-rity ecosystem and respond to attacks	Provide real-time (or near real-time) feedback on the security posture of enterprise information systems; integrate with security information and event management systems	**ClearPass Policy Manager/ Aruba 360 Security Exchange**

Summary

Networking solutions with intrinsic support for Zero Trust and SASE architectures provide a strong, built-in security foundation. Without comprehensive support for all five of the major security requirements, organizations are faced with assembling complicated, unintegrated solutions that leave gaps in their protection.

Ready to get started? Learn more at:
https://www.arubanetworks.com/connect-and-protect/

aruba
a Hewlett Packard
Enterprise company

Thank You

Contact Us

ebk_security_RM_020122 a00118824enw