aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

# Aruba Clearpass Network Access Control

## FLEXIBLE AND ROBUST ROLE-BASED POLICIES FOR IMPLEMENTING ZERO TRUST SECURITY IN ENTERPRISES

The accelerated adoption of IoT devices and hybrid work initiatives has increased network complexity and operational inefficiencies, while adding unique visibility and security challenges.

Identifying who and what connects to the network is the first step to securing your enterprise. Control through the automated application of wired and wireless policy enforcement ensures that only authorized and authenticated users and devices are allowed to connect to your network. At the same time, real-time attack response and threat protection is required to secure and meet internal and external audit and compliance requirements.

The use of IoT devices on wired and wireless networks is shifting IT's focus. Many organizations secure their wireless networks and devices, but may have neglected the wired ports in conference rooms, behind IP phones and in printer areas. Wired devices – like sensors, security cameras and medical devices – force IT to think about securing the millions of wired ports that could be wide open to security threats. Because these devices may lack security attributes and require access from external administrative resources, apps or service providers, wired access now poses new risks.

As IT valiantly fights the battle to maintain control, they need the right set of tools to quickly program the underlying infrastructure and control network access for any IoT and mobile device – known and unknown. One of the foundational principles of a Zero Trust Security framework is that the network is inherently untrustworthy and access to IT resources should not be dictated solely by where or how a client connects. A Zero Trust framework should manage the security lifecycle of an endpoint from identification, authentication and authorization to continuous monitoring and attack response. Today's network access security solutions must must factor in the Zero Trust Framework to enhance threat protection and provide an improved user experience.

## HYBRID WORK AND IoT ARE CHANGING HOW WE THINK ABOUT ACCESS CONTROL

Hybrid workplace initiatives, IoT, and edge computing are dissolving the traditional IT perimeter. The goal for organizations is to provide anytime, anywhere connectivity without sacrificing security and maintaining visibility and control without impacting user experience. It starts with identifying everything connecting to the network, authenticating and authorizing them, and enforcing robust policy across network.

1. **Identify** what clients are being used, how many, where they're connecting from, and which operating systems are supported – this provides the foundation of visibility. For many purpose-built IoT devices, such as those found in a hospital or manufacturing plant, understanding the actual behaviour of the device is the only way to accurately identify them. Continuous insight into the enterprise-wide device landscape and potential device security corruption, as well as, which elements come and go gives you the visibility required over time , to secure network endpoints.

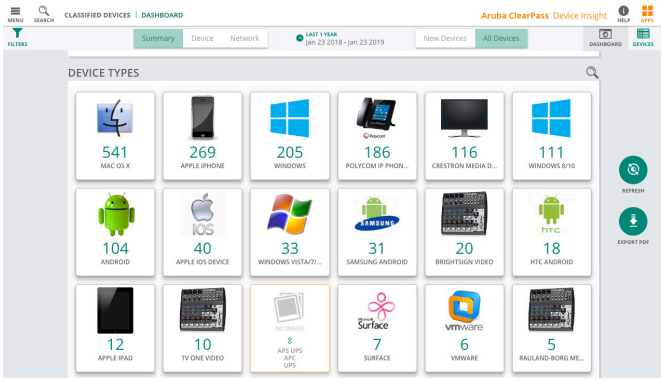
2. **Authenticate and authorize** the devices connecting to the network, applying Zero Trust best practices related to "least access". Define and apply access control policies that provide proper user and device access, regardless of user, device type or location; this provides an expected user experience. Organizations must adapt to today's evolving devices and their use – whether the device is a smartphone or surveillance camera.
3. **Enforce** automated response via dynamic policy controls and real-time threat remediation that extends to third-party systems. This is the last piece of the puzzle. Being prepared for unusual network behavior at 3 AM requires a unified approach that can block traffic and change the status of a device's connection.

Organizations must plan for existing and unforeseen challenges. With their existing operational burden, it's not realistic to rely on IT and help desk staff to manually intervene whenever a user decides to work remotely or buy a new smartphone. Network access control is no longer just for performing assessments on known devices before access. It is a critical enabler to dynamically protect the network whenever new or existing devices are on-boarded, relocated or request new services.

## FULL-SPECTRUM VISIBILITY ACROSS THE NETWORK

Security starts with visibility of all devices – you can't secure what you can't see. Aruba offers a choice of cloud-based and on-premises solutions for client visibility and profiling. Client Insights is an AI-powered, cloud-based client identification and profiling solution that comes with Aruba Central, not requiring the installation of additional collectors or host agents. ClearPass Device Insight is an on-premise device discovery and profiling solution that also works with third-party infrastructure.

Both Client Insights and ClearPass Device Insight greatly enhances core discovery and profiling capabilities to identify the wide range of IoT devices in many environments. This is accomplished through a combination of Deep Packet Inspection (DPI), advanced machine learning, and crowdsourcing device fingerprints. Learn more here.




True security only occurs when there is overarching visibility and control – ensuring that only authenticated or authorized devices connect to the network. This stems from a multi-vendor, wired and wireless per device policy.

## ROLE-BASED ACCESS AND POLICY ENFORCEMENT

Template-based policy enforcement lets IT build wired and wireless policies that leverage intelligent context elements: user roles, device types, MDM/EMM data, certificate status, location, day-of-week, and more. No matter how devices connect, Aruba Dynamic Segmentation automatically enforces consistent policies across the wired or wireless network – based on establishing least privilege access to IT resources by segmenting traffic based on identity and associated access permissions. This is a fundamental concept of a Zero Trust framework where trust is based on roles and policies, and not on where and how a user or endpoint clients such as IoT devices connect. Dynamic Segmentation unifies role-based access and policy enforcement across wired, wireless, and WAN networks with centralized policy definition and a choice of enforcement models - Centralized or Distributed - based on the overall network architecture.

### Robust network policy with ClearPass Policy Manager

ClearPass Policy Manager (CPPM) provides authentication, authorization and centralized policy definitions that follow the user throughout the network and are applied uniformly across wireless, wired and VPN connections. If the user changes to an unknown device, or is on an unsecured network, the policy will automatically change authorization privileges.

ClearPass supports standards-based 802.1X enforcement and other techniques for secure authentication. It integrates with a wide variety of authentication solutions enabling the use of multi-factor authentication and the ability to force re-authentication at key points throughout the network.

ClearPass has been recognized by coveted cyber catalyst, signaling that leading insurers believe Aruba ClearPass can help reduce cyber risk, and strongly merits consideration by organizations who seek solutions that yield meaningful improvements in cyber risk outcomes

### Automate network configuration and policy enforcement with Aruba Central NetConductor

Aruba Central NetConductor is a next-generation solution designed to automate and accelerate the deployment, management, and protection of complex, globally distributed enterprise networks.

For networks managed by Aruba Central, NetConductor offers cloud-native security services that enable globally centralized policy management and network configuration with simple business-logic interface and workflows. NetConductor uses a distributed EVPN/VXLAN network overlay to facilitate inline policy enforcement.

ClearPass complements Aruba Central NetConductor by providing AAA (Authentication, Authorization and Audit) services, enabling both RADIUS and non-RADIUS approaches for ensuring entities are properly identified and assigned a role that defines their access privileges.

### Wired is now the new threat

ClearPass OnConnect is a built-in feature that enables organizations to lock down those thousands of wired ports using non-AAA enforcement. No device configuration is needed and one command line entry in the switch is all it takes. Standard AAA/802.1X methods are also supported for wired and wireless. This allows for consistent policy enforcement and an end-to-end approach that siloed AAA, NAC, and policy solutions can't deliver.

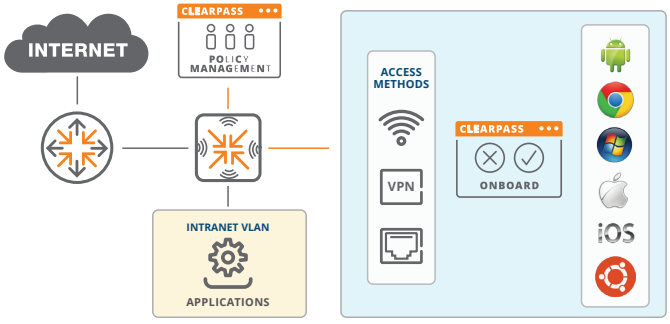
The ability to utilize multiple identity stores within one policy service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers, and internal databases sets ClearPass apart from legacy solutions.

### Device provisioning without IT involvement

Managing the onboarding of personal devices for BYOD deployments can put a strain on IT and help desk resources, and can create security concerns.

ClearPass Onboard lets users safely configure devices for use on secure networks all on their own. Device specific certificates even eliminate the need for users to repeatedly enter login credentials throughout the day. That convenience alone is a win for simplified security. The additional security gained by using certificates is an operational bonus.

Using ClearPass Onboard, the IT team defines who can onboard devices, the type of devices they can onboard, and how many devices per person. A built-in certificate authority lets IT support personal devices more quickly as an internal PKI, and subsequent IT resources are not required.




### Guest access that's simple and fast

**Automate device provisioning for secure BYOD with ClearPass Onboard**

BYOD isn't just about employee devices. It's about any visitor whose device requires network access – wired or wireless. IT requires a simple model that pushes the device to a branded portal, automates the provisioning of access credentials, and also provides security features that keep enterprise traffic separate.

ClearPass Guest makes it easy and efficient for employees, receptionists, event coordinators, and other non-IT staff to create temporary network access accounts for any number of guests per day. MAC caching also ensures that guests can easily connect throughout the day without repeatedly entering credentials on the guest portal.

Guest self-registration takes the task away from employees and lets visitors create their own credentials. Login credentials are delivered via printed badges, SMS text or email. Credentials can be stored in ClearPass for pre-determined set amounts of time and can be set to expire automatically after a specific number of hours or days.

### When device health determines access

During the authorization process, it may be necessary to perform health assessments on specific devices to ensure that they adhere to corporate anti-virus, anti-spyware and firewall policies. Automation motivates users to perform an anti-virus scan before connecting to the enterprise network.

ClearPass OnGuard features built-in capabilities that perform posture-based health checks to eliminate vulnerabilities across a wide range of computer operating systems and versions. Whether agentless, or using persistent or dissolvable clients, ClearPass can centrally identify compliant endpoints on wireless, wired and VPN infrastructures.

Examples of advanced health checks that provide extra security:

- Handling of peer-to-peer applications, services, and registry keys
- Determination of whether USB storage devices or virtual machine instances are allowed
- Managing the use of bridged network interfaces and disk encryption

### Getting more from third-party solutions

The final element of a secure infrastructure is response. The ability to respond to attack event data presented by other security vendors. Aruba 360 Security Exchange, our "Best of Breed" ecosystem, lets you automate security threat remediation or enhance a service using popular third-party solutions like firewalls, MDM/EMM, MFA, visitor registration and SIEM tools. Leveraging the context intelligence included in ClearPass allows organizations to ensure that security and visibility is provided at a device, network access, traffic inspection and threat protection level.

## THE POWER OF ARUBA SECURITY EXCHANGE


Using a common-language (REST) API, syslog messaging and a built-in repository called ClearPass Exchange, automated workflows and decisions help simplify tasks and secure the enterprise – no more complex scripting languages and tedious manual configuration. And for faster integration, ClearPass Extensions allows partners to upload an extension, for real time delivery of new services to joint customers.

With ClearPass Exchange, networks can automatically take action:

- MDM/EMM data like jailbreak status of a device can determine if it can connect to a network
- Firewalls can accurately enforce policies based on user, group and specific device attributes and leverage ClearPass to remediate a device exhibiting poor behavior
- SIEM tools can be set-up to store authentication data for all connected devices
- Users can be asked to use multi-factor authentication to verify their identity when connecting to networks and resources

Network events can also prompt firewalls, SIEM and other tools to inform ClearPass to take action on a device by triggering actions in a bidirectional manner. For example, if a user fails network authentication multiple times, ClearPass can trigger a notification message directly to the device or denylist the device from accessing the network.

### Securely access work apps from anywhere

Logging in to work apps throughout the day needs to be fast and effortless. ClearPass supports Single Sign-On and the ClearPass Auto Sign-On capability for that reason. Instead of a single sign-on, which requires everyone to login once to apps, Auto Sign-On uses a valid network login to automatically provide users with access to enterprise mobile apps. Users only need their network login or a valid certificate on their devices.

ClearPass can also be used as your identity provider (IdP) or service provider (SP) where Single Sign-On is used.

### Bonjour, DLNA and UPnP services

Projectors, TVs, printers and other media appliances that use DLNA/UPnP or Apple AirPlay and AirPrint, can be shared between users across your Aruba Wi-Fi infrastructure. ClearPass makes finding these devices and sharing between them simple.

For example, a teacher who wants to display a presentation from a tablet will only see an available display in their classroom. They will not see devices on the other side of the campus. They can also use the portal to choose who else can use the display – this keeps students from taking over the display.

Another example is in healthcare – doctors can easily project digital images, x-rays and MRI's from their iPads to a larger screen anywhere within a hospital. Patient collaboration just got simpler. User and location context is both a security and enablement tool.

## CLEARPASS DELIVERS BOTH PROTECTION AND EFFICIENCY FOR ARUBA SD-BRANCH

With dozens, hundreds or even thousands of individual branch locations to set up, secure and maintain, security and efficiency are both required for success. Because ClearPass centrally establishes role-based access control that follows a user or device across any type of network connection, labor-intensive VLAN and ACL setup and sprawl is eliminated. Within minutes, organizations can set standard permissions for typical branch users such as customers, associates and managers, as well as devices which include point-of-sale systems, building controls and peripherals. Once the policies are defined, ClearPass automatically pushes them to every location and dynamically adapts access based on device and user status.

Through embedded next generation firewalls, deep packet inspection and content filtering, Aruba branch gateways interpret and apply the permissions assigned to each role without requiring manual changes to the network. Unlike other branch solutions, ClearPass works with the Aruba branch gateway to define and enforce policies up to and including the application layer – access control that is not available with simple VLAN segmentation. In addition, ClearPass operates not just with Aruba, but with over 140 security and IT solutions, including cloud-based security solutions from ZScaler, Palo Alto Networks and Checkpoint, thus ensuring an optimized security strategy.

## DETECTING THREATS BEFORE THEY CAN DO DAMAGE

New threats now evolve from inside the organization – attacks involving malicious, compromised or negligent users, systems and devices. Organizations can no longer look at security in the same way. Machine learning and behavior analysis are the next steps to solving the dual crisis of better resourced threat actors and undervalued security operations. User and Entity Behavior Analytics, or UEBA plugs the gap between device visibility and control, and the secondary threat of malicious behavior.

Aruba's IntroSpect UEBA spots small changes in behavior – when put into context over a period of time – that are indicative of attacks that have evaded traditional security defenses. Attacks involving compromised users and hosts are notoriously difficult to detect because cyber criminals can evade perimeter defenses by using legitimate credentials to access corporate resources. Phishing scams, social engineering and malware are just a few of the popular techniques by which these criminals acquire employee corporate credentials. IntroSpect automates the detection of these attacks with analytics-driven visibility. Advanced techniques, including supervised and unsupervised machine learning, are applied to data from the network and security infrastructure.

Aruba ClearPass NAC plays a key role in enabling the implementation of Zero Trust Network Access. With the expanding cyber-attack surface, secure NAC is increasingly important to prevent malicious attacks and causing damage to the enterprise. The uses cases are several – control device connectivity, simplify BYOD, secure guest access – but the answer remains consistent. Over 10000 customers in 100 countries have secured their network and their business with Aruba ClearPass for better visibility, control, and response.



SO_ClearPass_SK_031822 a00054160enw

Contact us at www.arubanetworks.com/contact