aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

ARUBA CLEARPASS POLICY MANAGER

Access visibility and security for wired and wireless

Remember when IT was the gatekeeper and ruled with a combination of strict policies and a fully-contained ecosystem? Those days are long gone. Today, IT and user-owned devices are connected inside and outside of perimeter security.

Laptops, smartphones, tablets and Internet of Things (IoT) devices are pouring into the workplace and identifying what is on the network is the first step to securing your data. Automated policy enforcement ensures that only wanted users and devices are allowed to connect, and real-time threat protection is required to secure to meet internal and external audit and compliance requirements.

And if expectations are correct, the use of IoT devices on wired and wireless networks is shifting IT's focus. Most organizations secured their wireless networks and devices, but neglected the wired ports in conference rooms, behind IP phones and in printer areas. And because IoT devices may lack security attributes and require access from external administration resources, wired access is the new risk.

As IT struggles 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. Today's access security solution must deliver profiling, policy enforcement, guest access, BYOD onboarding, and more to offer IT-offload, enhanced threat protection and an enhanced user experience.

THINK ABOUT NAC

The boundaries of ITs domain now extends beyond the four walls of an enterprise. And the goal for organizations is to provide anytime, anywhere connectivity without sacrificing security. How does IT maintain visibility and control without impacting the business and user experience? It starts with a 3-step plan.

1. **Identify** what devices are being used, how many, where they're connecting from, and which operating systems are supported – this provides the foundation. And continuous insight into changes and which devices come and go gives you the visibility required over time.
2. **Enforce** accurate 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. **Protect** resources via dynamic policy controls and real-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 blocks traffic and changes the status of a device's connection.

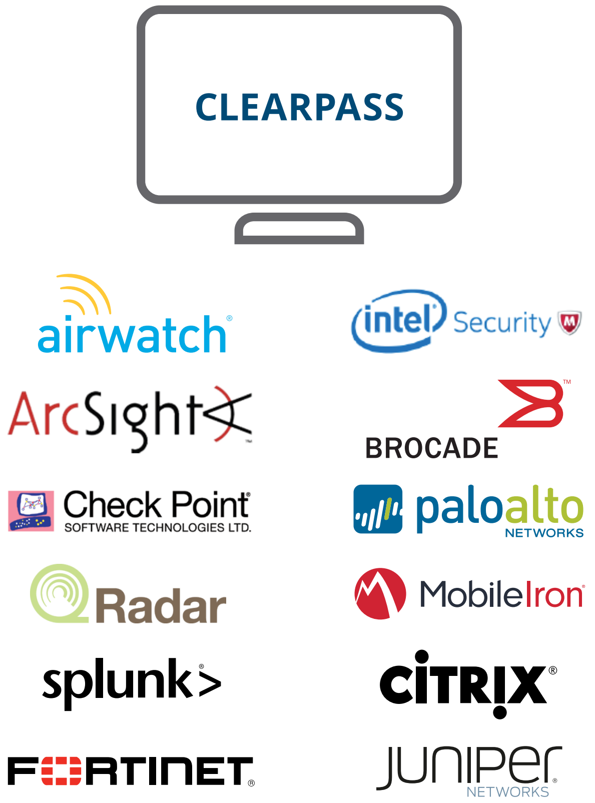
Organizations must plan for existing and unforeseen challenges. It's not realistic to rely on IT and help desk staff to manually intervene whenever a user decides to work remotely or buy a new smartphone. NAC is no longer just for performing assessments on known devices before access.

ONE PLACE TO SEE AND MANAGE ALL

The ClearPass policy and AAA solution, provides built-in device profiling, a web-based administrative interface and comprehensive reporting with real-time alerts. All contextual data collected is leveraged to ensure that users and devices are granted appropriate access privileges – regardless of access method or device ownership.

The built-in profiling engine collects real-time date that includes device categories, vendors, OS versions, and more. There's no longer a reason to guess how many devices are connected on wired and wireless networks. Granular visibility provides the data required to pass audits and determine where performance and security risks could come from.

THE POWER OF CLEARPASS EXCHANGE



The standalone ClearPass Universal Profiler provides the same profiling visibility for those organizations that may not be ready for full policy enforcement. Or, for remote areas where ClearPass may not be initially deployed.

A template-based policy enforcement lets IT build wired and wireless oriented policies that leverage user roles, device types, MDM/EMM data, certificate status, location, day-of-week, and more. Policies can easily enforce rules for employees, students, doctors, guests, executives and each of the device types that they decide to bring.

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 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. The additional security gained by using certificates is a bonus.

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

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.

Self-registration takes the task away from employees and lets guests create their own credentials. Login credentials are delivered via printed badges, SMS text, or email. Credentials can be stored in ClearPass for 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 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

ClearPass Exchange 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 that ClearPass contains allows organizations to ensure that security and visibility is provided at a device, network access, and traffic inspection and threat protection level.

Using a common-language (REST) API, syslog messaging and a built-in repository called ClearPass Extensions, automated workflows and decisions help simplify tasks and secure the enterprise – no more complex scripting languages and tedious manual configuration. And for faster integration, Extensions allow 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 prove it's really them 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 blacklist them 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 SSO 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 within the healthcare sector – doctors can easily project digital PACS images from their iPads to a larger screen anywhere within a hospital. Patient collaboration just got simpler.

ADAPTIVE FOUNDATION FOR SECURITY AND SERVICES

Providing a seamless experience for today's mobile users and the fast adoption of IoT technologies have created a host of new IT challenges. It takes planning, the right tools, and a strong foundation to secure anytime, anywhere access on wired and wireless.

ClearPass solves these challenges by delivering device identity, policy control, workflow automation, and automated threat protect from a single cohesive solution. By capturing and correlating real-time contextual data, ClearPass enables you to define policies that work in any environment – the office, on campus, or at the ball park.

The latest ClearPass enhancements also handle emerging network security challenges surrounding the adoption of IoT, stronger mobile device and app authentication, and deeper visibility into security incidents. Automated threat protection and intelligent service features ensure that each device is accurately given network access privileges with minimal hands-on IT interaction.