CLEARPASS EXCHANGE

Open third party integration for endpoint controls, policy and threat prevention

While billions of Wi-Fi enabled smartphones and tablets connect to enterprise networks, it's a major challenge to ensure security while also delivering an exceptional user experience without creating a provisioning nightmare.

That challenge is complicated by the fact that IT still relies on multiple, disparate systems like network access control (NAC), enterprise mobility management (EMM), policy management, firewalls, guest management, single sign-on solutions, helpdesk and trouble-ticketing systems.

IT needs a better way to secure the mobile enterprise. More importantly, the security products and management systems that have been deployed must be able to exchange contextual data and work together to provide increased visibility from top to bottom.

Aruba ClearPass Exchange supports a wide range of third-party IT systems, giving you the benefit of a coordinated defense where all components operate as one fully-integrated system.

MAKE BETTER-INFORMED DECISIONS

As the gatekeeper for incoming access-layer traffic, Aruba ClearPass performs profiling, authentication and authorization of users and devices. In this role, ClearPass Policy Manager collects a wealth of valuable and authoritative contextual data such as:

- The identity of users
- The current status and posture of a device
- The location of the connected user and device

This data is gathered from numerous internal and third-party systems through one-way and bidirectional communication. To simplify the sharing of context, ClearPass supports data exchange methods via APIs, Syslog messaging, and the use of an integrated respository called ClearPass Extensions.
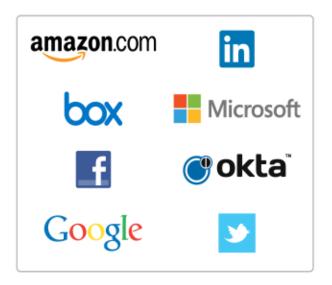
For example, using XML APIs, ClearPass can poll EMM systems for a variety of device information, including manufacturer and model, encryption status, blacklisted and whitelisted applications, and jailbroken status. When EMM systems detect policy violations, they are incorporated into ClearPass policy decision making.

SOME OF OUR TRANSACTION PARTNERS

SOME OF OUR AUTHENTICATION PARTNERS

Why share context?

After the access decision is made, the contextual data that ClearPass collects is shared with other systems to help protect your network or to deploy a new service.

ClearPass integrates with existing security, transaction or authentication systems that are on-premise or in the cloud. Customers benefit from the ability to integrate their own systems.

For example, Aruba has prepackaged an exchange of information with the Palo Alto Networks next-generation firewall to strengthen security by enforcing app-level policies more accurately. Likewise, SIEM solutions like Splunk and ArcSight can archive access connectivity data and trigger ClearPass to perform endpoint remediation actions based on unexpected endpoint activity.

ClearPass can also interact with non-network IT systems and helpdesk tools to automatically create and populate tickets with information about a specific user, device and location in the event of an authentication failure.

It's even possible to add mobility context to other IT workflows by extending network, device and user intelligence to cloud-based services such as Twilio, ServiceNow, and Nearbuy/RetailNext.

The result is improved automation, user satisfaction and less time spent on manual IT tasks. Just imagine what else you can do now that the mobility infrastructure is communicating with your security and business systems.

SOME OF OUR NOTIFICATION PARTNERS

THE POWER OF PARTNERS

In addition to custom integration, Aruba works with industry-leading partners to natively integrate ClearPass with EMM, firewalls, single sign-on, and many other systems, right out of the box.

ENTERPRISE MOBILITY MANAGEMENT

Integrating EMM with a NAC system is critical as BYOD and Internet-of-things (IoT) proliferate in the workplace. EMM systems share contextual data about devices and makes it easier to enforce network policies using attributes gathered by an EMM agent.

ClearPass offers rich bidirectional integration with multiple Tier 1 EMM vendors, including MobileIron, AirWatch by VMware, Citrix XenMobile, JAMF Software, IBM, SOTI, and SAP Afaria.

For example, EMM can tell the ClearPass server about a device's posture, its OS version, the apps running, who owns the device, whether the device is personal or corporate-owned, and other information.

This detailed contextual information enables ClearPass to determine whether to allow the device to connect to the network, what resources it is allowed to access once it connects, and actions that the device can perform while connected.

If a user fails to authenticate with the network multiple times, ClearPass can trigger an EMM system to send a notification message directly to the device and trigger the network to automatically quarantine the device or take other corrective action.

Conversely, device posture assessments performed by EMM systems for missing agents as well as blacklisted applications can trigger ClearPass access enforcement, remediation and notifications.

This built-in EMM integration ensures that ClearPass has the necessary device posture information to make the best network access decisions. Additional notifications and value-added policy events can also be triggered.

JAILBREAK DETECTION WORKFLOW

1 JAIL-BROKEN DEVICE DETECTED

2 HELPDESK NOTIFICATION AUTO GENERATED

CLEARPASS

pagerduty

3 MESSAGE TO DEVICE AUTO GENERATED