SOLUTION OVERVIEW

BUILDING AN INTEGRATED DEFENSE WITH ARUBA CLEARPASS AND HPE ARCSIGHT

Rapid detection and response to security threats in mobile and IoT environments

Today's mobile workforce and the adoption of bring your own device (BYOD) has changed how we connect to enterprise networks and access our digital information. The profile of an end user has changed dramatically, from being tethered to the desktop computer to now accessing the network from multiple devices, anytime and anywhere.

IT is now responsible for greater complexity when onboarding not just employees, but contractors, partners, and customers onto the same network infrastructure, while working to keep their traffic separate and private. This complexity requires network policies that address both identity and traffic behavior to mitigate cyber threats that can start from inside the perimeter of the enterprise.

The seamless integration offered by Aruba ClearPass and HPE ArcSight provides secure access and authorization, policy enforcement, and real-time correlation of network security events. Therefore, when anomalous behavior is detected there are multiple remediation alternatives.

A COORDINATED DEFENSE

ClearPass and ArcSight provide a coordinated defense for any user and device that connects to wired, wireless, and VPN networks. Together, they give IT full visibility and control by levaraging user profiles, device types, and suspect traffic patterns to ensure that users—even those authenticated on the network—can be continuously monitored.

ClearPass provides context-based network policy management regardless of user, device type, or location. ClearPass includes device profiling, BYOD and guest onboarding, authorization, authentication, and accounting (AAA) services, and built-in troubleshooting tools.

HPE ArcSight Enterprise Security Management (ESM) offers consolidated data archiving and parsing of data, with analysis and real-time correlation to detect anomalous behavior and potential threats. Combining information on network connections from ClearPass and other network security devices, ArcSight is able to identify threats and initiate response action automatically or manually to mitigate damage.

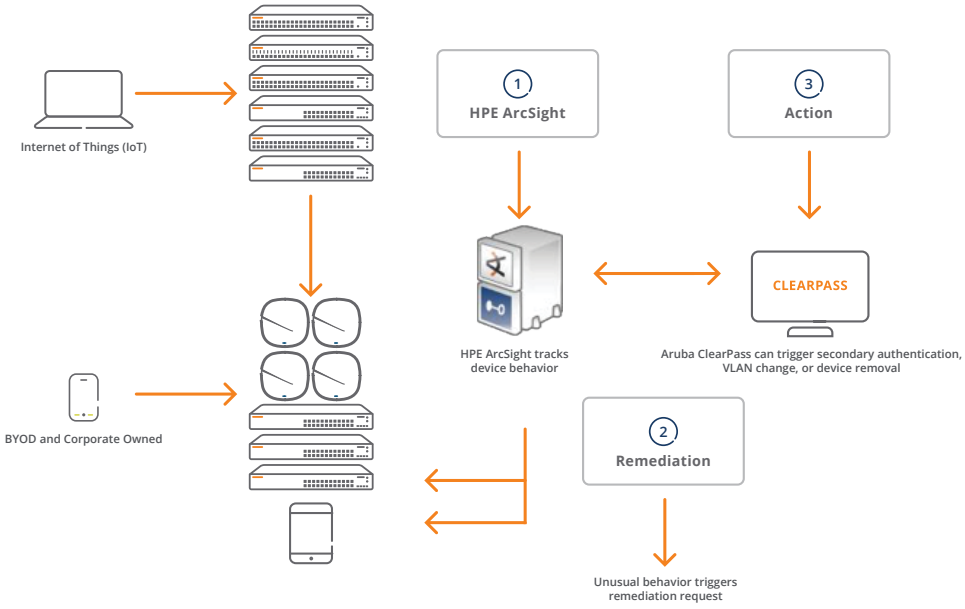

figure 1.0_090216_clearpassarcsight-soa

Benefits:

- Per session authentication and authorization for all user and device types before granting network access
- Centralized storage of all log event data for compliance, analytics, and reporting
- Real-time correlation and advanced analytics to detect suspicious network and device activity
- Real-time remediation of device and network connections that exhibit anomalous behavior
- Policies and services enforced on any type of network

SUSPECT TRAFFIC REMEDIATION

When users are logged in to the network and HPE ArcSight Security Information and Event Management (SIEM) receives information from a firewall regarding suspicious traffic, ArcSight triggers an alert back to ClearPass to enforce a device policy requiring reauthentication, quarantining, or other policy-driven actions.

- ClearPass authenticates users as devices are brought on to the network verifying access and policy mandates.
- A firewall or other network security device detects suspicious traffic and sends this information as part of a log event feed to ArcSight—ArcSight then calls out to ClearPass to track the device threat status and initiates a change in authorization, forcing the device to re-authenticate.

BEHAVIOR ANALYSIS FOR MOBILE AND IOT

ClearPass feeds data into ArcSight ESM that—combined with other contextual data—allows monitoring of behavior for Internet of Things (IoT), corporate, or BYOD devices. If unusual behavior is detected, a trigger is fired from ArcSight to perform a remediation request via ClearPass.

- HPE ArcSight ESM correlates device traffic with other security events to identify anomalous device behavior based on deviation from baseline or as a result of an investigation.
- Remediation is triggered by ArcSight and can include secondary authentication, VLAN change, or device removal.

COMPLIANCE AND DATA ARCHIVE

ClearPass generates event logs covering user, device, and system activities. This information is captured and stored in the central ArcSight platform.

This consolidated view and centralized store is valuable for analytics and compliance reporting use cases.

- Create a central point for policy and analysis
- Search and report using a comprehensive set of historical data
- Create compliance reports to meet regulatory or governance requirements

CONCLUSION

BYOD and IoT have put more pressure on IT, increasing the complexity of network security. This complexity requires network policies that address both identity and traffic behavior to mitigate cyber threats that can start from inside the perimeter of the enterprise. The seamless integration of Aruba ClearPass and HPE ArcSight provides secure access and authorization, policy enforcement, and real-time correlation of network security events. That means that IT can take advantage of mobility and IoT, while keeping the network secure—all without spending additional dollars.

For more information about Aruba ClearPass, visit: http://www.arubanetworks.com/products/security/network-access-control/

For more information about HPE ArcSight, visit: http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/index.html

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com