

Building an integrated defense with HPE Security ArcSight and Aruba ClearPass

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security — Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.



Aruba's mobile-first, cloud-first approach addresses the fundamental changes in today's business environment—the move towards the digital workplace and the explosion of big data. Aruba allows IT professionals to build networks that keep up with these changes by migrating away from expensive-to-operate and proprietary infrastructures, which were originally designed for fixed network connections within the physical confines of the corporate headquarters.

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 that provide much greater end user mobility.

IT network and operations departments are 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 to address both identity and traffic behavior to mitigate cyberthreats 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.

Solution overview

Aruba ClearPass and HPE ArcSight provide a coordinated and galvanized defense, which helps to enforce industry audit and regulatory compliance requirements for any user and device that connects to wired, wireless, and VPN networks. Together, we provide full

visibility and control that leverage user profiles, device types, and suspect traffic patterns to insure that users—even those authenticated on the network—can be continuously monitored.

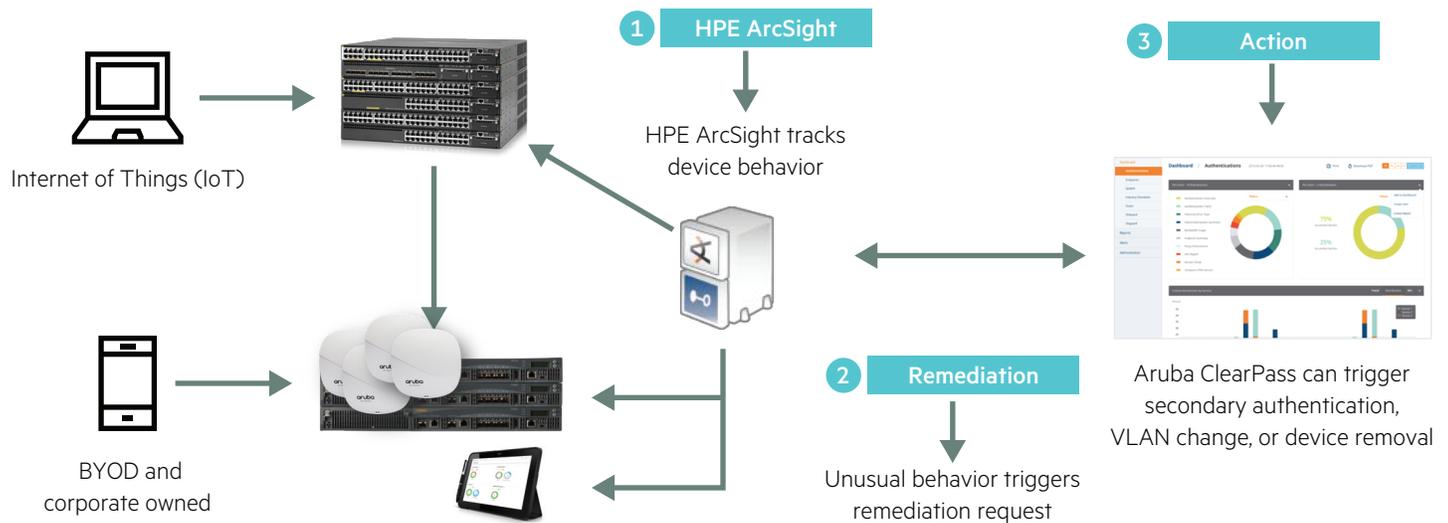
ClearPass provides context-based network policy management regardless of user, device type, or location. Aruba ClearPass includes device profiling, BYOD and guest onboarding, authorization, authentication, and accounting (AAA) services, and built-in troubleshooting tools.

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, HPE ArcSight is able to identify threats and initiate response action automatically or manually to mitigate damage.

Key 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

Solution brief



Use cases:

Suspect traffic remediation

In this use case, when users are logged into the network and HPE ArcSight Security Information and Event Management (SIEM) receives information from a firewall regarding suspicious traffic, HPE ArcSight can trigger an alert back to Aruba ClearPass to interdict the traffic and 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 log event feed to HPE ArcSight. HPE ArcSight calls out to ClearPass to track the device threat status and initiate a change in authorization thereby inducing the device to re-authenticate.

Behavior analysis for mobile and IoT

ClearPass feeds data into HPE 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 HPE 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 HPE 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 HPE 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 comprehensive set of historical data
- Create compliance reports to meet regulatory or governance requirements

Additional resources

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

For additional information on

Aruba ClearPass, visit: arubanetworks.com/products/security/network-access-control

Learn more at saas.hp.com/marketplace/arc sight



Sign up for updates

**Hewlett Packard
Enterprise**

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

4AA6-6473ENW, July 2016