aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

ENHANCED NETWORK SECURITY WITH ARUBA CLEARPASS AND CYBERHOUND

The challenge of securing high capacity, transient networks, has become increasingly complex with security threats existing on both sides of the network perimeter. Wide-scale use of unmanaged devices, IoT and BYOD is resulting in infected devices connecting to the network more than ever before.

Next Generation Firewalls and Intrusion Prevention Systems are powerful tools in identifying threats, protecting networks and controlling access to data and systems, as well as blocking malicious activity. These are, however, just one element of the overall security fabric a network needs to have in place. In order to address evolving threats, network administrators require additional tools to quickly identify and automate the quarantining or removal of infected devices from the network.

Aruba ClearPass extends a network's security capabilities by utilizing CyberHound's Intrusion Prevention threat intelligence feed, to manage infected devices. With policy-based network controls, Aruba ClearPass can isolate offending devices into a quarantined network, remove devices completely or instigate technical support workflows to assist in the remediation process. All of this happens automatically, with policies set for specific actions based on the threat identified.

CyberHound IPS and ClearPass Integration benefits include:

- Hyperscale architecture for high throughput scanning of network traffic for malicious content
- Detection of Malware, Viruses, Botnets, Exploits and more
- Real-time threat intelligence feeds to Aruba ClearPass for security policy enforcement
- Automated device quarantining and removal based on threat severity levels, IPS policy rules and threat categorization
- Customizable Aruba ClearPass network policy controls
- Automated workflows to remediate infected devices

Customizable integration policy options ensures an administrator has full control so that, for example, only threats of a defined threat threshold instigate network policy controls with the lowest risk threats reported on for further investigation or monitoring.

FREQUENTLY ASKED QUESTIONS

Q: Does the CyberHound/ Clearpass Integration support more than a single ClearPass appliance?

Yes. The CyberHound service can be configured to send threat intelligence feeds to more than one Aruba ClearPass server, within the same network.

Q: Does CyberHound and Aruba ClearPass integration support user-based authentication?

Yes. CyberHound utilizes the Aruba ClearPass RADIUS accounting capabilities to create user based authentication sessions. Authentication session management is seamlessly controlled as users join and leave the network.

Q: Can Aruba ClearPass apply different actions based on an identified threat severity?

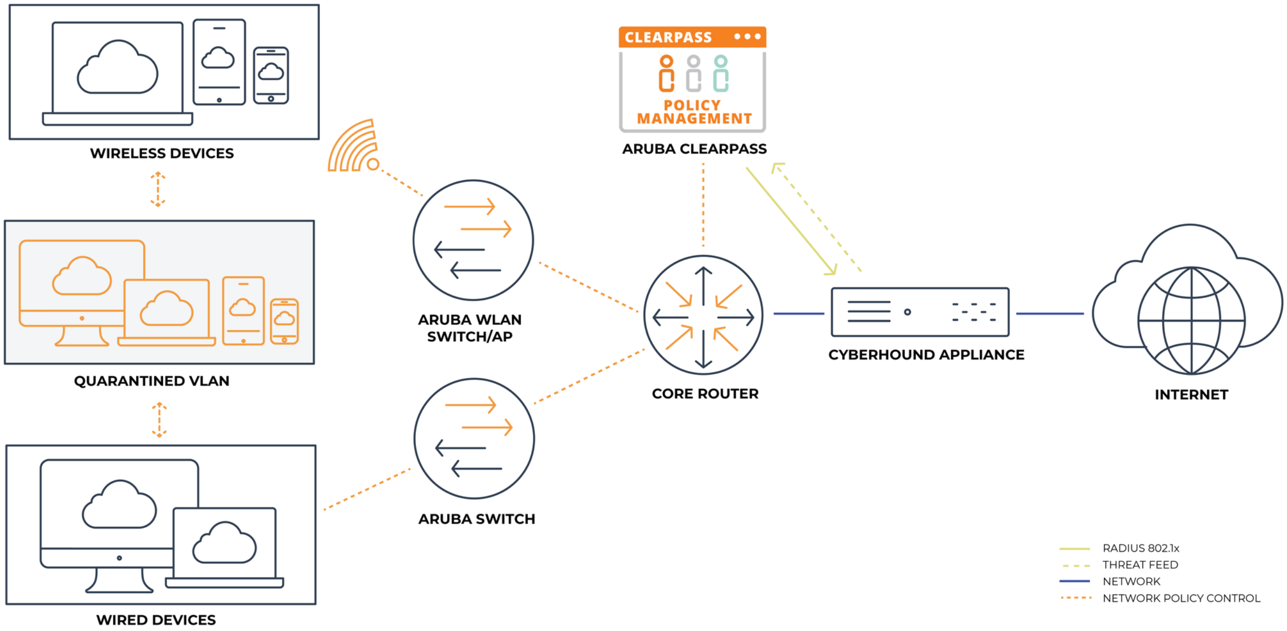
Yes. The threat intelligence feed to Aruba ClearPass can be customized to ensure that only the specified threat categories, with defined severity thresholds, will enforce a network policy change to the relevant device.

Q: What are the most common examples of the integrated solution picking up infected devices?

CyberHound IPS identifies both known, and zero day threats, using its comprehensive IPS ruleset. Malware threats such as New BabyShark and Farseer can be identified, blocked and alerted on with intelligence feeds shipped to Aruba ClearPass for proactive threat mitigation and device management.

Q: How is CyberHound's Advanced Threat Protection Service kept up to date with all the latest threats?

CyberHound IPS rulesets are updated daily via a managed consortium of rule providers from around the globe. This ensures maximum coverage and protection against the greatest number of threats.



CONTACT DETAILS

cyberhound.com
+61 7 3020 3330
team@cyberhound.com

a Hewlett Packard
Enterprise company