infoblox® | aruba a Hewlett Packard Enterprise company

JOINT SOLUTION BRIEF

INFOBLOX DDI AND ARUBA CLEARPASS

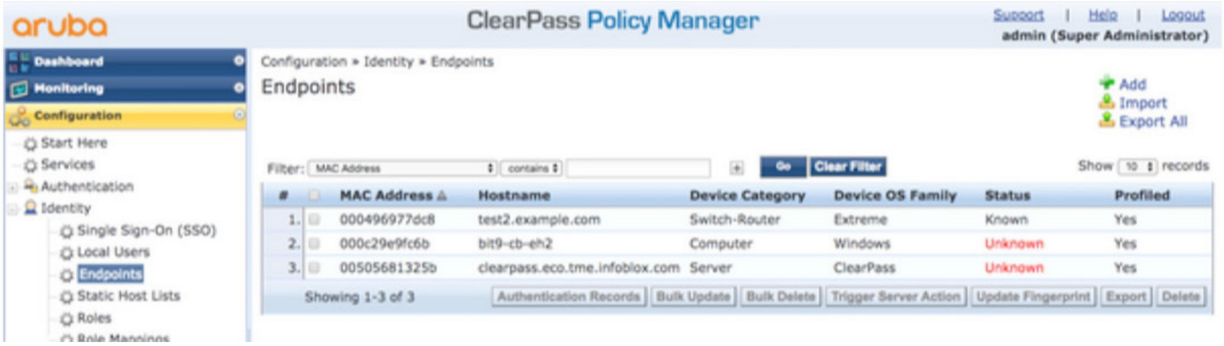
Improve SecOps efficiency and reduce time to containment

SUMMARY

Enterprise networks today contain numerous network and security devices. These devices generate their own incidents but don't always share information. The results: (1) lack of interoperability and inability to share data about ongoing events in networks and (2) security tools working in silos with no context. If customers can see all the devices in a single place, they can eliminate silos and respond quickly to security and network changes.

A 2017 Enterprise Strategy Group (ESG) research report, "Security Operations Challenges, Priorities and Strategies,"1 says keeping up with the volume of security alerts and the lack of integration between security tools are the two biggest challenges to security operations. According to the ESG report, the top security operations priorities are investing in technologies to automate security operations, detect threats and create security operations by integrating multiple tools. To improve collaboration between cybersecurity and IT operations teams, organizations are investing in automated incident responses to handle increasing security alerts, prioritize alerts and respond to incidents faster.

Infoblox supplies tight integration between network and security, with the industry's most extensive threat intelligence and API integrations. Infoblox and Aruba ClearPass have joined forces to help organizations improve their security and reduce time to containment, providing improved efficiency for security operations. Together, they enable customers to be confident their network and security are tightly integrated and built on a rock-solid foundation for better efficiency. To allow network and security administrators to automatically share information about assets and DNS security events, Infoblox, the market leader in DNS, DHCP and IPAM (DDI), has integrated with Aruba ClearPass Policy Manager. Infoblox sends information on new devices along with IP addresses and indicators of compromise (IoCs) to Aruba; then Aruba ClearPass uses this information to block or monitor infected endpoints based on security policy. As Figure 1 shows, customers can see information on devices discovered by Infoblox in Aruba ClearPass Policy Manager.



admin (Super Administrator)

Configuration » Identity » Endpoints

Endpoints

Filter: MAC Address contains

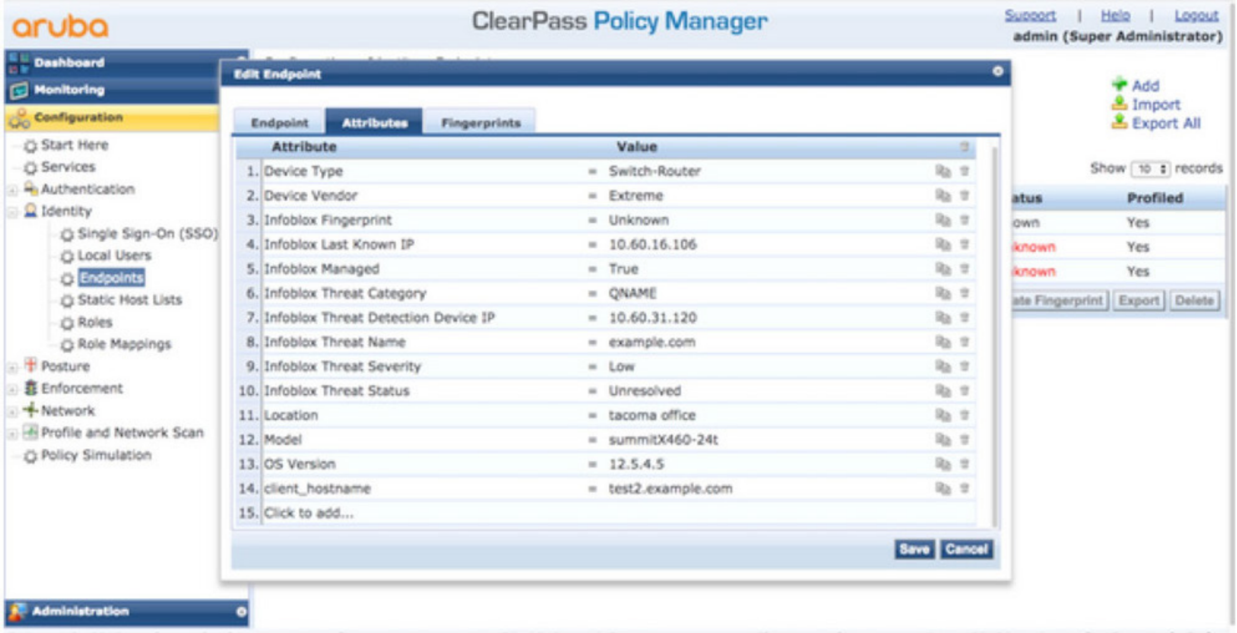
Show 10 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	000496977dc8	test2.example.com	Switch-Router	Extreme	Known	Yes
2.	000c29e9fc6b	bit9-cb-eh2	Computer	Windows	Unknown	Yes
3.	00505681325b	clearpass.eco.tme.infoblox.com	Server	ClearPass	Unknown	Yes

Showing 1-3 of 3

Figure 1: The Aruba ClearPass interface showing devices discovered by Infoblox

A click on the device shows information, such as IP address, hostname, device type and model and location (see Figure 2). The ClearPass Policy Manager then can fingerprint the device and assign a specific role and access permissions that correspond to IT control policies.



	Attribute		Value
1.	Device Type	=	Switch-Router
2.	Device Vendor	=	Extreme
3.	Infoblox Fingerprint	=	Unknown
4.	Infoblox Last Known IP	=	10.60.16.106
5.	Infoblox Managed	=	True
6.	Infoblox Threat Category	=	QNAME
7.	Infoblox Threat Detection Device IP	=	10.60.31.120
8.	Infoblox Threat Name	=	example.com
9.	Infoblox Threat Severity	=	Low
10.	Infoblox Threat Status	=	Unresolved
11.	Location	=	tacoma office
12.	Model	=	summitX460-24t
13.	OS Version	=	12.5.4.5
14.	client_hostname	=	test2.example.com
15.	Click to add...		

Figure 2: Easy access to additional attributes with ClearPass

UNIQUE BENEFITS OF INFOBLOX

Infoblox is leading the way with Secure Cloud-Managed Network Services. Our solutions bring increased security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management.

The Combined Solutions

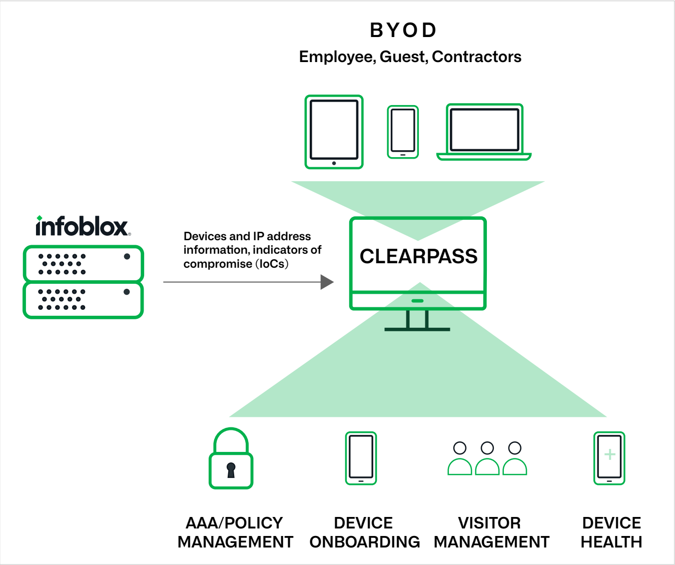

BYOD
Employee, Guest, Contractors
infoblox
Devices and IP address information, indicators of compromise (IoCs)
CLEARPASS
AAA/POLICY MANAGEMENT
DEVICE ONBOARDING
VISITOR MANAGEMENT
DEVICE HEALTH

Figure 3: With outbound notifications, Infoblox communicates with ClearPass about compromised devices

As Figure 3 shows, Infoblox sends new end hosts and information about compromised devices to Aruba ClearPass using Outbound Notifications. Aruba ClearPass can use that information and IoCs to obtain the appropriate context to prioritize threats and take action, containing problems faster.

This integration furnishes centralized visibility into new devices and infected hosts, plus context for prioritizing threats; it also eliminates silos and speeds responses to network and security events.

Aruba ClearPass (minimum code version 6.6.0) supports this integration. However, recommended versions are 6.7.x and higher. For this integration, Infoblox supports Outbound API. Additionally, the Infoblox community website supports the integration.

CONCLUSION

From the Internet of things (IoT) to an always-on mobile workforce, organizations face increasingly complex IT infrastructures that are more exposed to attacks than ever before. By combining Infoblox's DNS security and network visibility with ClearPass's control of access to the network, organizations can automate their network discovery, profiling and attack response.

Single-pane-of-glass visibility, control and response:

Threats from malicious insiders and IoT-based attacks continue to grow, bypassing perimeter security defenses. Infoblox and Aruba ClearPass integration automates a wide range of adaptive attack responses, including re-authentication, bandwidth throttling, quarantine and blocking.

Certified secure—the best defense for wired and wireless connections:

Malware has become increasingly intelligent, using DNS in over 90 percent of its campaigns. With inline protection on Infoblox DNS and policy-driven actions on Aruba ClearPass, organizations gain far better protection from DNS attacks, DNS-based data exfiltration and DNS tunneling.

Identifying what's on multi-vendor wired and wireless networks:

Infoblox automatically populates an Aruba ClearPass endpoints list with Mac addresses, revealing every network asset with unmatched clarity, context and insight. In addition to Mac address authentication, ClearPass authenticates users and devices through a wide variety of mechanisms to maintain the highest level of visibility and control.

About Aruba, a Hewlett Packard Enterprise company:

Aruba is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT and cybersecurity solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

Reference

1. https://www.siemplify.co/blog/research-backing-security-orchestration-automation-incident-response/

Other Infoblox-Aruba Integrations

1. This integration allows ClearPass to send username and MAC address mapping information to Infoblox's MAC Address Filters. https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/1861/1/ClearPass
2. This integration authenticates a device on Aruba ClearPass; then, based on data received from Infoblox through an enforcement profile, it puts the device on a chosen network. https://github.com/aruba/clearpass-exchange-snippets/tree/master/ipam/infoblox-authz

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20231031v1