aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba & Symantec

Preventing the Spread of Compromised Devices

The proliferation of BYOD and IoT devices in the enterprise has challenged system administrators to ensure that devices attempting to connect to the corporate network are free from malware, protected against future infections, and compliant with corporate policies. This task is significantly more difficult in large enterprises, both because of the higher number of devices and the variety of ways to connect to corporate resources.

Compromised and infected devices are a major threat to network security because a single, compromised device can spread malware in a matter of seconds. The diversity of devices, operating systems, and physical locations makes the successful containment of a breach very challenging, especially in light of the shortage of cybersecurity expertise.

Ensuring that a device has the appropriate operating system patches, antivirus signatures, and other important detection mechanisms prior to accessing the network is good practice; however, it's insufficient to protect against zero-day exploits of devices already on the network. The best backstop is automated, real-time time protection that can immediately take action when evidence of infection or compromise is present.

Symantec builds security products to protect endpoints, Web, e-mail, data, and identity across on-premise and cloud infrastructures. Aruba and Symantec have partnered to integrate Aruba's ClearPass Policy Manager with SEPM to extend device visibility and enforce user and device policies to protect the network. Aruba ClearPass is the gatekeeper for The Symantec Endpoint Protection (SEP) provides endpoint security for protection against threats to desktop and mobile operating systems, and is managed by the Symantec Endpoint Protection Manager (SEPM).

The joint solution controls network access based on the current security posture of a device, preventing infected devices from accessing the network, making lateral connections, or infecting other devices. The automated solution features flexible network access policies and real-time enforcement at the time of authentication.

WHY ARUBA AND SYMANTEC

- Comprehensive endpoint protection across different operating systems and versions
- Isolation and containment of fixed and mobile devices with evidence of compromise
- User and device policy enforcement by Aruba ClearPass Policy Manager
- Automated analysis and policy-based enforcement prior to network access based on a device's true security posture at the time of authentication
- Aruba Validated Interoperability

HOW IT WORKS

The integrated solution is driven through ClearPass Extensions, a component of the ClearPass Exchange Integration framework that enables ClearPass micro-services that can be tailored for specific applications, in this case SEPM. A SEPM extension retrieves endpoint context and feeds it to the ClearPass Policy Manager. Contextual attributes include the device's operating system and version, anti-virus version, security patch status, and whether malware has been detected on the device.

ClearPass Policy Manager uses these contextual data to automatically make real-time policy decisions about admitting or denying access to the network, quarantining the device, restricting access to network resources, and remediating out-of-date anti-virus software and security patches. Manual intervention by analysts is not required, enabling around-the-clock detection and remediation.

Symantec

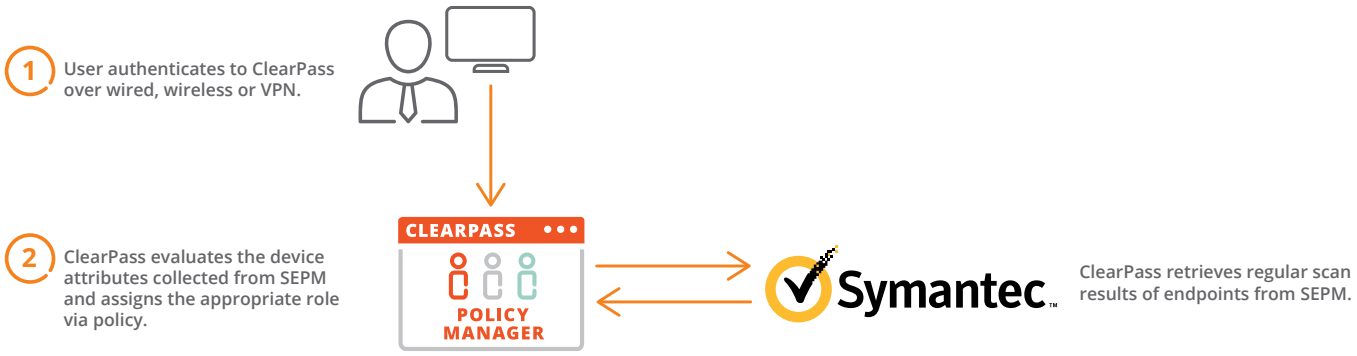

Figure 1: Aruba ClearPass Policy Manager and Symantec Joint Solution Diagram

CERTIFIED INTEROPERABILITY

This joint solution has been certified under the Aruba 360 Security Exchange technology partner program and is extremely easy to deploy. From the ClearPass Extension app store, install the micro-service application, spend 2 minutes to configure the integration, set the synchronization schedule to suit and immediately see the security context of the endpoints protected by Symantec Endpoint Manager available in the ClearPass Policy Manager Endpoint database. Using this context, ClearPass Policy Manager can ensure only endpoints in compliance with no security issues are allowed access to the corporate network.

SUMMARY

Aruba and Symantec have taken the guess work out of preventing infected and non-compliant devices from accessing an enterprise network. Contact your local sales representative to see how Aruba and Symantec deliver a comprehensive endpoint management and secure network access solution.

For more information on Aruba ClearPass, please visit: https://www.arubanetworks.com/products/security/network-access-control/

DEPEND ON SYMANTEC

Symantec helps organizations, governments and people secure their most important data with strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. They are headquartered in Mountain View, California.

www.symantec.com Phone: 650-527-8000 350 Ellis Street, Mountain View, CA 94043

PSO_Symantec_042720 a00090836enw