Cylance® and Aruba Partner To Deliver Zero Trust at the Endpoint

Lowering Risk by Improving Endpoint Visibility and Access Control

CYLANCE

aruba
a Hewlett Packard Enterprise company

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise. Visit www.cylance.com for more information.

About Aruba

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Introduction

Cylance and Aruba have formed a technology alliance which combines AI-based endpoint prevention with enterprise-grade and seamless network access control. This approach limits risk by allowing only protected endpoints access to enterprise networks and assets. Aruba ClearPass Policy Manager integrates with CylancePROTECT® and gives customers the ability to ensure all connected assets are secure and malware free.

Value Statement

ClearPass integrates with CylancePROTECT to construct and enforce real-time access criteria. Local security information is gathered from each endpoint at the time of authentication to determine whether access should be granted. CylancePROTECT collects and returns numerous security attributes to ClearPass, which then integrates them within an enforcement policy. This ensures that endpoint devices accessing corporate assets are fully secured by Cylance and the network remains free of potentially infected endpoints. Devices are likewise secured against infection from internal systems.

Use Case

Unified Access Control and Policy Enforcement

- Challenge: Critical controls such as authentication and pass phrases do not protect internal systems and assets from authorized endpoint devices that are improperly protected or compromised.
- Solution: By combining CylancePROTECT with Aruba ClearPass, organizations can ensure their endpoint devices are fully protected and free from malware. ClearPass uses a multitude of data returned from endpoints protected by Cylance before making a policy enforcement decision. These checks can provide validation to questions like “Is CylancePROTECT installed?”, “Is the agent running?”, “Is it running an updated agent version?”, and most importantly, “What is the security state of the endpoint?”.
- Additional Benefit:
  - If a connection is attempted by an endpoint that is not managed by CylancePROTECT, a more restrictive access policy for the device can be enforced by ClearPass, limiting access to corporate assets. Overall security posture is improved when users are encouraged to install the CylancePROTECT endpoint agent for improved access to organizational resources.
  - With CylancePROTECT’s prevention-based architecture, assets that aren’t fully patched are still protected and do not pose an increased risk to an organization’s network.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20181218-1433