MARSH

Cyber Catalyst by Marsh
Cyber Technology Evaluation Program

aruba
a Hewlett Packard Enterprise company

Aruba Policy Enforcement Firewall — Cyber Catalyst Designation

The Aruba Policy Enforcement Firewall has been designated a 2019 Cyber Catalyst cybersecurity solution. It reduces the impact of attacks inside an organization that coopt legitimate credentials. The Aruba Policy Enforcement Firewall is a key component of an organization's "Zero Trust" architecture and ensures that no user or device can initiate network access without proper authentication and authorization.

The Aruba Policy Enforcement Firewall delivers two unique security protections. One, it uses identity and roles to enforce Zero Trust at the point of access. It fills a critical gap left by traditional firewalls that use Virtual Local Area Networks (VLAN) configuration for control and which become active only after a user or device reaches deep into the network.

Second, the Aruba Policy Enforcement Firewall eliminates configuration mistakes common with VLAN sprawl that leave networks unprotected, reducing the time and resources required to control IT access. Once a role is assigned, permissions associated with that role follow the user. If the security status changes, the assigned role is automatically altered to reduce or eliminate access, without any network reconfiguration. This shrinks the time between attack detection and response.

Aruba Policy Enforcement Firewall addresses risk in three ways: first, if a user or device has a narrow set of access permissions, it ensures that an attacker's permissions will be equally narrow. Second, it relies on roles that are independent of network topology, eliminating the need for VLAN and the associated risk. Third, it can respond to an attack alert from any security product and automatically change the role associated with that user and device—e.g. a quarantine or block. Gestating attacks such as data exfiltration are shut down before they do damage.

Aruba positions the Policy Enforcement Firewall as suitable for large Fortune 500 enterprises and government entities as well as small- and mid-sized businesses. The Aruba Policy Enforcement Firewall works with both wired and wireless network infrastructure, and can be placed wherever network access is occurring.

**Product information provided by Aruba, a Hewlett Packard Enterprise company.*

MARSH & McLENNAN COMPANIES

Why Aruba Policy Enforcement Firewall is a Cyber Catalyst-Designated Solution

Cyber Catalyst participating insurers rated Aruba Policy Enforcement Firewall highest on the criteria of cyber risk reduction, efficiency, and performance.

In their evaluation, the insurers characterized Aruba Policy Enforcement Firewall as:

- "Very powerful zero-trust boundary, used in tandem with HPE's Silicon Root of Trust. Ground-up security with an effective perimeter using only two tools."
- "Unique ability to eliminate security gap left by traditional firewalls. Valuable capability to put segmentation between user device and network, adding an additional layer of protection."
- "Addresses a unique issue prevalent to all companies: what to do when a bad actor gets past the firewall."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst-designated products or services in accordance with certain "implementation principles" that have been developed by the insurers with vendors of Cyber Catalyst-designated solutions.

The implementation principle for the Aruba Policy Enforcement Firewall is:

- The organization's firmware and software is up to date.

Evaluation Process

Applications for evaluation of cybersecurity solutions were accepted from March 26 through May 5, 2019. More than 150 cybersecurity offerings, spanning a broad range of categories from hardware to messaging security to IoT security, were submitted for evaluation. Cyber Catalyst participating insurers evaluated eligible solutions along six criteria:

1. *Reduction of cyber risk.*
2. *Key performance metrics.*
3. *Viability.*
4. *Efficiency.*
5. *Flexibility.*
6. *Differentiating features.*

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight participating insurers, which voted independently. Neither Microsoft — which served as technical advisor — nor Marsh participated in Cyber Catalyst℠ designation decisions.

The next Cyber Catalyst program is expected to open in 2020.

For more information on the Cyber Catalyst 2019 designated solutions or the program, visit the Cyber Catalyst pages at www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit marsh.com, or contact your Marsh representative.

For more information on the Aruba Policy Enforcement Firewall, visit https://www.arubanetworks.com/en-au/products/security/policy-enforcement-firewall/.

2019 CYBER CATALYST DESIGNATED SOLUTIONS

In the inaugural Cyber Catalyst program, 17 cybersecurity products and services have been designated as Cyber Catalyst solutions. More information about all the 2019 Cyber Catalyst-designated cybersecurity solutions is at www.marsh.com/cybercatalyst.