aruba
a Hewlett Packard Enterprise company

AT A GLANCE

ARUBA POLICY ENFORCEMENT FIREWALL DESIGNATED CYBER CATALYST℠ BY MARSH

As networks become the catalyst for digital transformation, traditional perimeter security defenses no longer suffice. Mobile and IoT devices are being connected by employees, partners, customers and guests everywhere within an organization, driving the need for improved segmentation of traffic based on specific IT access permissions.

Standard security firewall rules and physical network configuration based on IP addresses are no longer adequate. Organizations now require edge-based protection that is dynamically enforced regardless of user role, device type or location.

Aruba has pioneered the use of a comprehensive role-based access control solution called the Policy Enforcement Firewall (PEF) that specifically helps solve this problem. This proven technology is the only user- and device-centric firewall that provides a "zero trust" boundary at the point of access and carries the Cyber Catalystsm by Marsh designation for reducing risk.

CONTAINING POTENTIAL BUSSINESS LOSSES AND IMPACT

Mobile technology and transactions over the Internet and cloud play key roles in how organizations now conduct business and reach prospective customers. Unfortunately, this adds to the attack surface. Organizations must decide on an appropriate security posture, which risks are acceptable or avoidable, and what financial liability they are willing to endure.

In addition to technology, process and people, cyber insurance has become a key pillar of cyber security, for organizations large and small. In fact, a report recently released by Verizon shared that approximately 43% of all cyber-attacks target small to medium-sized businesses (SMBs). Organizations must also contend with lawsuits associated with the release of confidential information or the costs of extortion due to ransomware.

WHAT IS THE CYBER CATALYST℠ BY MARSH PROGRAM?

As part of the Cyber Catalyst℠ program, leading cyber insurers evaluate and identify solutions they consider effective in reducing cyber risk. Participating insurers include Allianz; AXIS; AXA XL, a division of AXA; Beazley; CFC; Munich Re; Sompo International; and Zurich North America. Microsoft is a technical advisor to the program.

Cybersecurity products and services viewed as effective in reducing cyber risk will be designated as "Cyber Catalyst℠". Organizations that adopt Cyber Catalyst-designated solutions may qualify for enhanced terms and conditions on cyber insurance policies from participating insurers.

Both the Aruba Policy Enforcement Firewall and HPE server Silicon Root of Trust (SiROT) are designated Cyber Catalystsm.

ROLE-BASED CONTROL FOR ZERO TRUST PROTECTION

Traditional firewalls that leverage IP-based VLANs for control only become active after a user or device is admitted to the network, leaving a tempting opening for advanced attacks. Aruba's PEF technology uses identity, traffic attributes and other context to centrally enforce access privileges at the time of an initial connection. This is important as each second an attacker is connected to a wide-open network, they can unleash thousands of malware packets to capture user credentials, expand the malware footprint and other disruptive activities. Closing the gap between when a device connects and a policy is enforced is essential.

When using Aruba's wireless or wired infrastructure, the identity of each user or device is verified before being granted access to the network or its resources. A role is assigned and permissions are granted based on pre-defined rules. This limits what applications and data a user or device can reach or who they can communicate with. For example, a surveillance camera would only be allowed to communicate with the video server to download content.

Once an attack such as data exfiltration or ransomware is detected, PEF can automatically change the permissions associated with a user or device by updating their role and authorization privileges. Attack responses can include a range of actions from bandwidth reduction, quarantining to outright block. Attack alerts can be triggered from any of the security products in an organization's security ecosystem based on simple API integrations.

PEF is administered with either an on-premise or cloud-based management console and is bundled with Aruba networking infrastructure or via a standalone security gateway.

By enabling organizations to implement zero trust role-based access control, the Aruba Policy Enforcement Firewall has been designated "Cyber Catalystsm" based on its ability to effectively reduce risk. For more information, consult the following resources about the Cyber Catalyst program, Aruba PEF and HPE SiROT.

ADDITIONAL RESOURCES

- Aruba Policy Enforcement Firewall
- HPE Servers
- Cyber Catalyst by Marsh

Cyber Catalyst

In the Cyber Catalyst℠ program, leading cyber insurers evaluate and identify solutions they consider effective in reducing cyber risk. Participating insurers include Allianz; AXIS; AXA XL, a division of AXA; Beazley; CFC; Munich Re; Sompo International; and Zurich North America. Microsoft is a technical advisor to the program.

aruba
a Hewlett Packard Enterprise company

AAG_CyberCatalyst_090919 a50000156enw