aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba & Microsoft Defender Advanced Threat Protection

Zero Trust Context-Aware Network Access Control

Enterprises are experiencing an unprecedented rise in the number of mobile, IoT, unmanaged, and unpatched devices that users want to connect to corporate networks. This raises security concerns since zero trust guidelines dictate that no device should be allowed network access without first validating its identity and the context in which it is being used.

Failure to heed zero trust guidelines can be costly because breaches can tarnish brand reputation and directly impact revenue. For example, the average cost of a healthcare-related data breach has grown to $3.92 million[1]. Organizations with sensitive data – such as customer databases or intellectual property – need to prevent unauthorized access to their networks before data are lost.

Aruba and Microsoft have partnered thru Microsoft's Intelligent Security Association (MISA) to protect enterprise networks from threats to mobile, IoT, unmanaged, and unpatched devices. As a MISA member, Aruba has integrated its ClearPass security platform with Microsoft security products to extend solution capabilities and share threat intelligence.

Aruba ClearPass is a policy enforcement platform that centrally enforces network access across devices used in a broad range of vertical markets. ClearPass integrates with more than 150 security solution vendors, and provides fine-grained policy enforcement based on a device's role, type, authentication method, EMM/MDM attributes, device health, traffic patterns, location, and time-of-day.

Microsoft Defender ATP is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

WHY ARUBA AND MICROSOFT

- Zero trust policy-based network and application level access control pulls user details from ClearPass Policy Manager and device-level context from Microsoft Defender ATP
- Automated enforcement denies access to untrusted devices and supports custom policies to protect different types of users and devices
- Standards-based authentication, authorization, directory resources, and certificate management services for interoperability with current work flows
- Multi-vendor solution works with your existing wireless or wired network infrastructure

- **Endpoint behavioral sensors:** Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.
- **Cloud security analytics:** Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- **Threat intelligence:** Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

[1] https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

Member of
Microsoft Intelligent Security Association
Microsoft

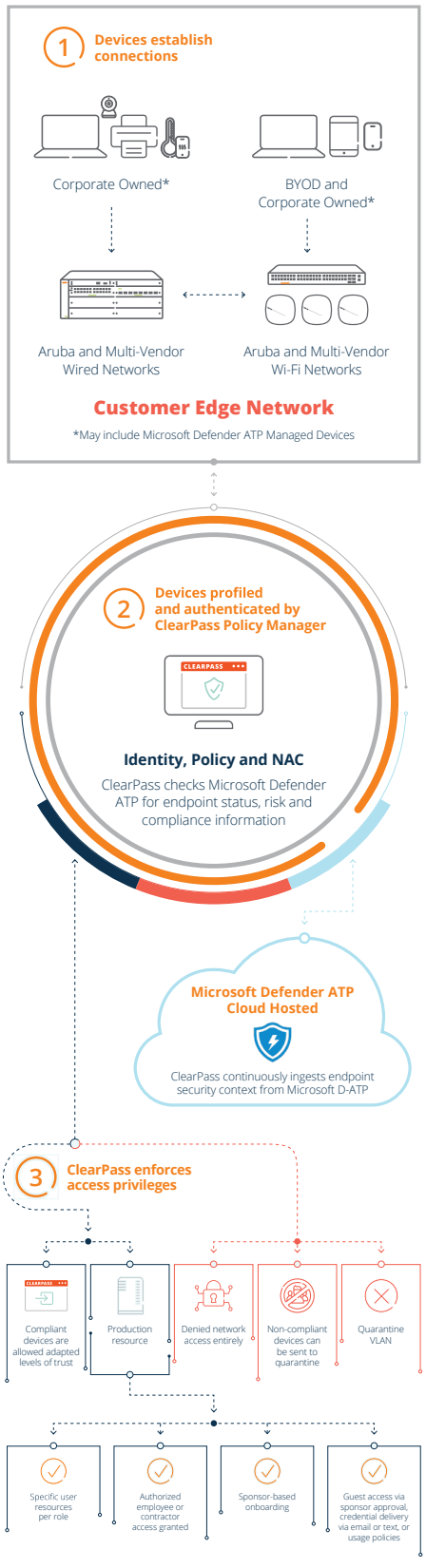
Working in concert, Aruba ClearPass and Microsoft Defender ATP coordinate security-related data with policy enforcement during network access requests, ensuring that the correct policy is applied and appropriate remediation occurs when access is denied.

HOW IT WORKS

ClearPass Policy Manager is the gatekeeper for users and devices as they attempt to connect to the network. Going beyond typical access control, ClearPass Policy Manager securely onboards devices and enforces policies restricting access only to specified resources.

ClearPass Policy Manager checks the real-time status of device information from Microsoft Defender ATP to determine if/how devices should be allowed access to the local network and ultimately what applications may or may not be accessed. When a device is authenticated, Microsoft Defender ATP Extension feeds the security policy context into the ClearPass Enforcement Policy to make real-time network access decisions.

Microsoft Defender ATP & ClearPass



Regardless of whether it's a corporate or personal device, or if falsified credentials or spoofed accounts were used, the joint solution continuously enforces posture and can remediate or quarantine devices in the event of a violation.

FEATURE	ATTRIBUTE	BENEFIT
Informed Access Control	Validate the endpoint is managed.	Ensures devices have managed security policies.
Shared Data	Microsoft Defender ATP and Aruba ClearPass Policy Manager share insights regarding known devices and users.	Integration between best-in-class IT systems, including the sharing of contextual information, is the key to a coordinated defense.
Granular Policy Enforcement	Network access can be denied, granted, or restricted. Non-compliant devices can be quarantined or sent for remediation.	Devices access only resources to which they're entitled.

SUMMARY

Within the context of MISA, and integration between ClearPass and Defender ATP, Aruba and Microsoft have enhanced zero trust network security, workflows, and analytics for mobile, IoT, unmanaged, and unpatched devices connected to corporate networks. The results enhance threat intelligence and increase cybersecurity using a multi-vendor, standards-based approach.

Contact your local sales representative to see how together, Aruba and Microsoft help customers improve their overall security posture in the fight against expensive data breaches.

For more information, please visit:

Aruba ClearPass:
https://www.arubanetworks.com/products/security/network-access-control/

MISA:
https://www.microsoft.com/en-us/security/business/intelligent-security-association

DEPEND ON MICROSOFT

Microsoft

Microsoft is the worldwide leader in software, services and solutions that enable digital transformation for the intelligent cloud and edge era. They are headquartered in Redmond, Washington.

www.microsoft.com/en-us/security/business/intelligent-security-association
Phone: 425-703-6214 15010 NE 36th Street, Microsoft Campus Building 92 Redmond, WA 98052

aruba
a Hewlett Packard Enterprise company

PSO_MicrosoftDATP_062220 a50002188enw

Contact Us Share