AT A GLANCE

ARUBA 360 SECURE FABRIC

Network Powered Security

Not long ago, enterprise security teams could easily identify the perimeter they were protecting. IT operations would maintain tight control over computing and network resources, such as systems, apps and data their employees could access and use. Today, a number of technology disruptions – mobile, BYOD, virtualization, cloud, big data, and IoT – have rendered a perimeter-based security approach insufficient.

Legacy security technologies were designed for yesterday's threats and environments, not today's highly sophisticated and targeted attacks. A fresh approach whereby user and device risk is constantly assessed with the help of advanced technology is essential to deal with the increasingly dangerous and fast-changing threat landscape.

ARUBA 360 SECURE FABRIC

As a market leader for networking, Aruba saw the need for a modern approach to designing enterprise security that leverages the power of the network and a full range of advanced analytics including AI-based machine learning. The Aruba 360 Secure Fabric is an enterprise security framework that gives security and IT teams an integrated way to gain visibility, control and advanced threat defense.

Aruba starts with an analytics-ready secure infrastructure. Extensive protection is embedded in the foundation of all Aruba indoor and outdoor wireless access points (APs), switches, gateways and controllers to secure the physical network infrastructure and the traffic that flows through it.

The Aruba security portfolio includes:

- Aruba Policy Enforcement Firewall
- Aruba ClearPass Policy Manager (network access control)
- Aruba ClearPass Device Insight (advanced visibility of all devices connected to the network)
- Aruba IntroSpect UEBA and NTA (integrated User and Entity Behavior Analytics and Network Traffic Analysis).

With the Aruba 360 Secure Fabric, security teams can now develop a seamless path that includes user and device discovery and access control, to analytics-driven attack detection and response, based on policies set by the organization.

Additionally, the Aruba 360 Secure Fabric is as an open, multi-vendor platform that works with an ecosystem of Aruba 360 Security Exchange partners to enable organizations to leverage their existing third-party solutions to better protect their investments.

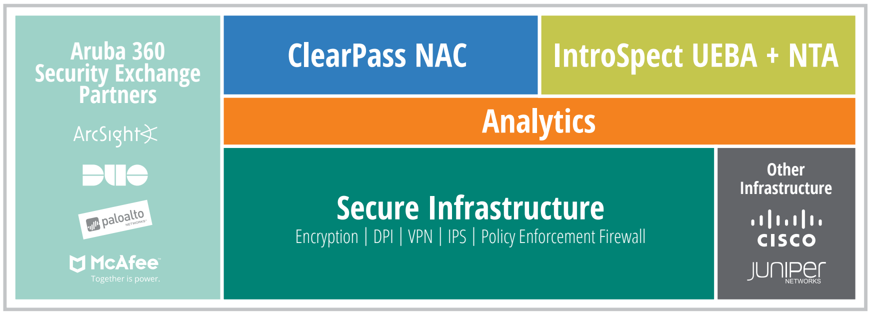

Figure 1: The Aruba 360 Secure Fabric provides an integrated security framework for IT and security teams to gain back visibility and control of their network, as well as threat detection, investigation, and response centered around analytics.

ARUBA SECURE NETWORK INFRASTRUCTURE

For over 15 years, Aruba has been at the forefront of delivering high-performance, extremely reliable and secure network access – from the campus and branch to the core to the data center. As a security provider, Aruba has consistently introduced ground-breaking innovations in the areas of encryption, physical hardening, remote access, and embedded firewalls to ensure that user, system and device traffic can be trusted. Chief Information Security Officers (CISOs) have come to rely on the security "head start" that the Aruba secure infrastructure provides.

Aruba Secure Infrastructure includes secure boot, military grade encryption, deep packet inspection, VPN, IPS and policy enforcement firewalls.

Each second an attacker is connected to the network can mean unleashing thousands of malware packets. Traditional firewalls that leverage IP-based VLANs for control become active only after a user or device reaches deep into the network which results in a security gap.

The Aruba Policy Enforcement Firewall (PEF) is a stateful, application-aware access control system that eliminates this gap. PEF runs on either a Mobility Controller or Instant Access Point and puts a firewall between a user or device and the network at time of initial access. Working in conjunction with Dynamic Segmentation, PEF makes Aruba networking more secure by uniquely enforcing IT access policies based on a user or device identity and roles (privileges) associated with that identity.

PEF is the only firewall that uses identity and roles to enforce Zero Trust at the point of access.

EXPANDED VISIBILITY AND CONTROL

The expanding IT attack surface and a constantly evolving network means organizations not only need a secure network foundation, but also additional visibility and control. The ClearPass family of products allow the enterprise to gain better device visibility and manage an entire set of access control use cases that includes wired, wireless, guest and BYOD connectivity, to policy-based remediation and attack response.

VISIBILITY
Know what's on your network
CONTROL
Authenticate and authorize all the "things"
RESPONSE
Security tool coordination through ClearPass Exchange

Figure 2: ClearPass goes beyond visibility and extends control for devices and users connecting to your network.

With the growing number and variety of devices connecting to networks, Aruba ClearPass Device Insight delivers valuable visibility and profiling to address security and compliance risks associated with unidentified and unmanaged devices connected to the network. This includes emerging Internet of Things (IoT) devices that are often deployed within a customer's environment without first considering the potential security implications. Aruba ClearPass Policy Manager then delivers the actionable control and response needed to address who and what can access internal and external resources.

The Policy Enforcement Firewall is a self-contained access control function that also integrates with Aruba's ClearPass Policy Manager. ClearPass provides a complete NAC solution that includes streamlined authentication and policy definition services that are delivered to PEF for enforcement.

ARUBA DYNAMIC SEGMENTATION

Combining Aruba Secure Infrastructure (embedded into Aruba Mobility Controllers, gateways, access points, and switches) plus Aruba ClearPass Policy Manager, IT can deliver a network edge that's smart enough to securely connect all types of devices and users. Dynamic Segmentation simplifies IT network operations and improves security by enforcing unified policies across the wired and wireless networks. This ensures that appropriate access and security policies are seamlessly distributed, automatically applied, and independently enforced (through the embedded Aruba Policy Enforcement Firewall or PEF) for all users and devices without any additional moves, adds, or changes. For more information, visit www.arubanetworks.com/dynamicsegmentation.

ADVANCED THREAT DETECTION AND RESPONSE

Aruba IntroSpect integrated UEBA and NTA detects attacks by identifying small changes in behavior that often are indicative of stealthy threats. Today's attacks can be comprised of many smaller actions that occur over long periods of time. By involving compromised users and hosts, cyber criminals can evade traditional defenses using legitimate credentials to access corporate resources – making attacks difficult to detect. Phishing scams, social engineering and malware infections are just a few of the popular techniques by which these attackers acquire employee corporate credentials.

Uniquely, IntroSpect assesses the entire infrastructure for threats by ingesting a wide range of sources – from network packets and flows to IT logs and alerts. IntroSpect uses machine learning based intelligence and automates the detection of these attacks by giving security and network operations visibility throughout the kill chain. Supervised and unsupervised machine learning models deliver actionable intelligence to proactively respond to these advanced cyberattacks with the enterprise scale to protect millions of users and devices and secure vast amounts of distributed data. IntroSpect can also work with existing infrastructure solutions or ClearPass to take a range of either manual or automated actions in response to an attack.

Both ClearPass and IntroSpect serve as Aruba security solutions and can be applied individually or in tandem to any network. While overlaying Aruba's Secure Infrastructure, ClearPass and IntroSpect provide unmatched analytics-driven protection against today's challenging threat landscape.

ARUBA 360 SECURITY EXCHANGE: OPEN, MULTI-VENDOR, CLOSED LOOP PROTECTION

A critical advantage of the Aruba 360 Secure Fabric is an open, multi-vendor integration of the Aruba security solutions with more than 140 partners in the 360 Security Exchange Program. Customers can leverage their existing security investments by seamlessly integrating Exchange sourced products with Aruba solutions. Unlike other infrastructure providers that lock customers into costly upgrades and a single source of products, the Aruba 360 Secure Fabric provides the best elements of a unified solution with the flexibility of an open architecture.

Check Point SOFTWARE TECHNOLOGIES LTD.
airwatch
Infoblox CONTROL YOUR NETWORK
Envoy
Carbon Black.
paloalto NETWORKS
MobileIron
DUO
servicenow
Radar Log Manager
McAfee Together is power.
splunk>

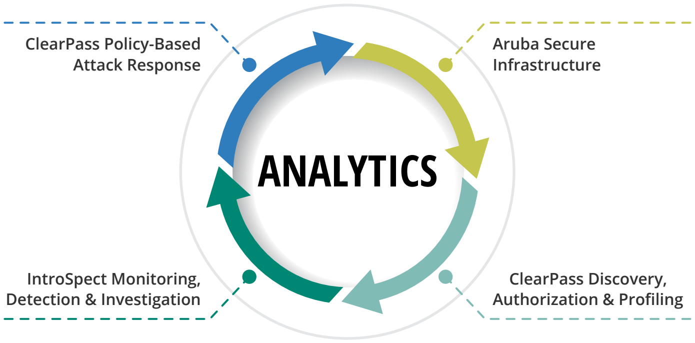
ClearPass Policy-Based Attack Response
Aruba Secure Infrastructure
ANALYTICS
IntroSpect Monitoring, Detection & Investigation
ClearPass Discovery, Authorization & Profiling

Figure 3: Analytics-driven security

SUMMARY

The Aruba 360 Secure Fabric delivers state-of-the-art network, visibility, access and advanced threat defenses designed to integrate easily into existing multi-vendor environments and the Aruba security ecosystem. Aruba's network-powered defenses employ robust AI-based machine learning, advanced analytics and a deep understanding of the network to detect, prioritize, investigate and stop threats quickly. Security and networking teams can now be more confident that they have a strong security posture with visibility and control into who and what is on their network – and what they are doing while connected to network resources – at all times. That's what it means to be "Aruba Secure".

aruba
a Hewlett Packard Enterprise company

Contact Us Share