aruba
a Hewlett Packard
Enterprise company

EXECUTIVE BRIEF

ARUBA 360 SECURE FABRIC

360° of analytics-driven active cyber protection and secure access

Not long ago, enterprise security teams could identify the perimeter they were protecting and work with IT operations to gain full control of the resources their employees could access and use, from networks to systems to applications to data. Today, there's no shortage of technology disruptions – mobile, BYOD, virtualization, cloud, big data, and IoT have now taken hold of the enterprise and rendered a perimeter-based security approach insufficient. The problem is compounded by an era of IT disaggregation and highly organized and targeted attacks. Ensuring the security of the organization is not only mission-critical, it's now become exponentially more difficult. Clearly a modern approach is required to deal with today's fast-changing threat landscape.

According to Gartner, User and Entity Behavior Analytics (UEBA) is an innovative category of security technology for identifying and mitigating advanced threats. "For at least the past two years, Gartner has witnessed many new vendors with advanced analytics appear in several security market segments. One area that has spurred a lot of innovation is UEBA, which enables broad-scope security analytics, much like security information and event management (SIEM) enables broad scope security monitoring. UEBA provides analytics around user behavior, but also around other entities such as endpoints, networks and applications. The correlation of the analyses across various entities makes the analytics' results more accurate and threat detection more effective, just as it does with SIEM."[1]

THE ARUBA 360 SECURE FABRIC

Most security solutions on the market today are a myriad of security technologies designed for yesterday's perimeter-based, closed and static environments. These disparate security technologies can address only one of many types of today's threats and vulnerabilities. This requires IT and security operations to create a patchwork security solution that stitches together firewalls to IPS to access control to anti-malware to analytics.

Driven by the demands of enterprise mobility, BYOD, cloud and IoT, Aruba saw the need for a different design approach to connecting and securing networks. Aruba is now changing the paradigm with the Aruba 360 Secure Fabric, an enterprise security framework that gives security and IT teams an integrated way to gain back visibility and control. It allows you to detect gestating attacks with machine-learned intelligence, and proactively respond to these advanced cyberattacks across any infrastructure – with the enterprise scale to protect millions of users and devices and secure vast amounts of distributed data.

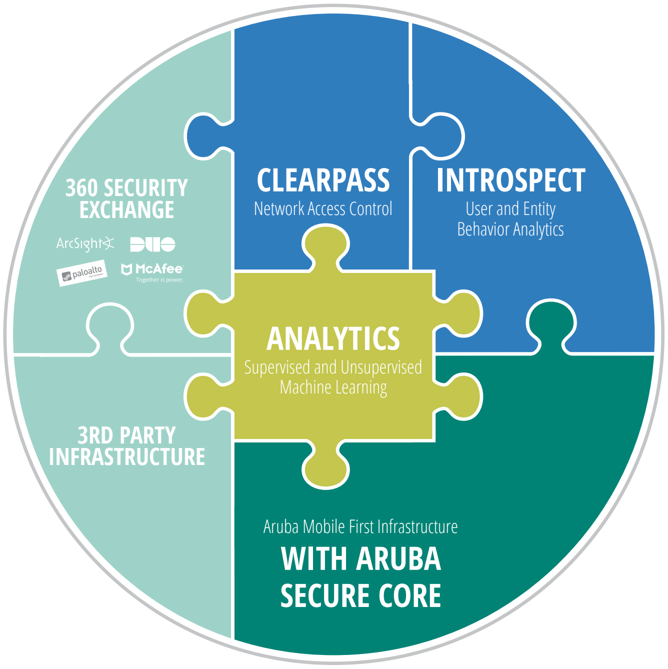


Figure 1: The Aruba 360 Secure Fabric provides an integrated security framework for IT and security teams to gain back visibility and control of their network, centered around analytics.

There are 3 elements to this fabric:

- Aruba Security Software: Proactive network access control and policy management, and industry-leading UEBA for any network
- Aruba Secure Core: Analytics-ready network infrastructure with embedded security
- A best-in-class security ecosystem

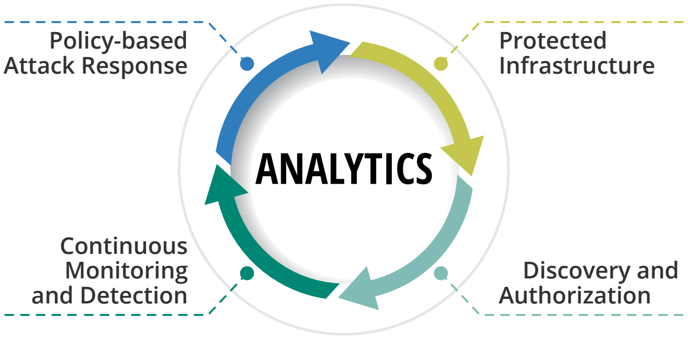

Policy-based Attack Response
Protected Infrastructure
ANALYTICS
Continuous Monitoring and Detection
Discovery and Authorization

Figure 2: The new security imperative

Starting with core security capabilities embedded in the foundation of all of Aruba's Wi-Fi access points (APs), switches, routers, and controllers, Aruba builds on this foundation by integrating IntroSpect machine learning-based attack detection with access control systems like Aruba ClearPass in an open, multi-vendor platform. With the Aruba 360 Secure Fabric, security teams can now develop a seamless path from user and device discovery and access, to analytics-driven attack detection and response – based on policies set by the organization.

A COMPREHENSIVE WAY TO GAIN VISIBILITY AND CONTROL OF YOUR NETWORKS, USERS AND DEVICES

IT disaggregation means organizations not only need a secure network foundation, but also visibility and control of the users and devices connected to the network. ClearPass allows the enterprise to cover the entire set of access control use cases from wired to wireless, guest, BYOD onboarding and policy-based remediation and attack response.

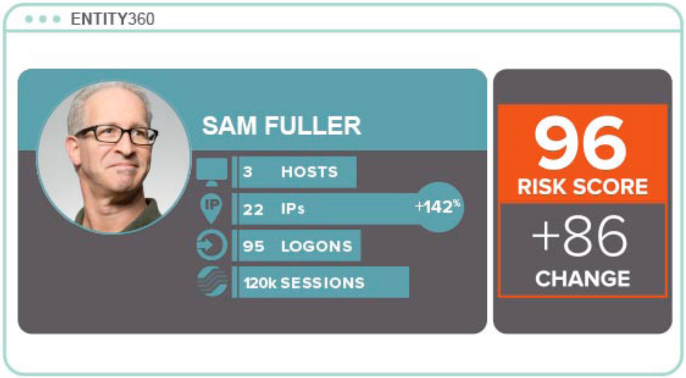
VISIBILITY
Know what's on your network
CONTROL
Authenticate and authorize all the "things"
RESPONSE
Security tool coordination through ClearPass Exchange

Figure 3: ClearPass provides not only visibility, but also extended control for devices and users connecting to your network.

Going a step further, in February 2017 Aruba added machine-learning-based attack detection capabilities by acquiring Niara. This addition leverages ClearPass' visibility into network access as well as the ability to take a range of either manual or automated actions in response to an attack.

Aruba IntroSpect's User and Entity Behavior Analytics (UEBA) detects attacks by spotting small changes in behavior that often are indicative of exploits that have evaded traditional security monitoring and analytics. Today's attacks can be comprised of many smaller actions that occur over long periods of time. These types of attacks are also notoriously difficult to detect because they can involve compromised users and hosts where cyber criminals have evaded perimeter defenses using legitimate credentials to access corporate resources. Phishing scams, social engineering and malware are just a few of the popular techniques by which these criminals acquire employee corporate credentials. IntroSpect uses machine-learned intelligence and automates the detection of these attacks by giving security and network operations early visibility. Supervised and unsupervised machine learning models process large amounts of data in order to establish a baseline of typical IT activity for a user, device or system. Deviations from these baselines are often the first indication that an attack is underway.

Both ClearPass and Introspect serve as Aruba's security software solution and can be applied individually or in tandem to any network across campus, distributed enterprise, cloud, and IoT edge environments. While overlaying Aruba's Secure Core, ClearPass and Introspect provide unmatched analytics-driven protection against today's changing threat landscape.


ENTITY360

SAM FULLER

3 HOSTS
22 IPs +142%
95 LOGONS
120k SESSIONS

96
RISK SCORE
+86
CHANGE

Figure 4: Detect threats before they can do damage with IntroSpect User and Entity Behavior Analytics.

ARUBA SECURE CORE: SECURE, TRUSTED NETWORK INFRASTRUCTURE

For more than 15 years, Aruba has been at the forefront of delivering a high performance, highly reliable and secure wired and wireless networks – starting with wireless access points and controllers, and expanding into access and core switching. 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) around the world have come to rely on the security "head start" that the Aruba secure infrastructure provides.

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 100 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 their 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

QRadar Log Manager | McAfee Together is power. | splunk>

SUMMARY

By working in conjunction with an open, multi-vendor partner ecosystem, the Aruba Secure Core in the Aruba Mobile First Infrastructure, combined with the ClearPass visibility and control and IntroSpect's advanced attack detection, the Aruba 360 Secure Fabric provides 360° of analytics-driven attack detection and response from the edge to the core to the cloud – that's what it means to be "Aruba Secure."

[1] Gartner Foundational Research Report, Refreshed 9 August 2017, The Fast Evolving State of Security Analytics

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com