WHITE PAPER

aruba
a Hewlett Packard Enterprise company

ARUBA 360 SECURE FABRIC

A User-centric Approach to Network Security

March 2018

Table of Contents

Introduction

This document describes security vulnerabilities in modern networks and how organizations can address these using the Aruba 360 Secure Fabric, an enterprise security framework that gives security and IT teams a way to gain visibility and control. This framework allows them to detect internal network attacks with machine-learned intelligence and proactively respond to advanced cyberattacks across any infrastructure.

This document is intended for network business decision makers, chief information security officers, and other security leaders.

CHALLENGES

From the Internet of Things (IoT) to an always-on, BYOD, and mobile workforce, organizations encounter an increasingly complex IT infrastructure that is increasingly exposed to cyberattacks. Mobile, cloud, and IoT have redefined network security and presented new challenges and vulnerabilities to the network.

Vanishing Perimeter Network

A major challenge is a vanishing network perimeter. IT no longer controls what connects to the network or from where users access data. Workers connect to the corporate network by using their personal devices (BYOD), and the rise of software-as-a-service has led to users expecting to be able to access applications and data from any device, from anywhere. The physical perimeter of the network no longer protects inside from outside. After these devices connect to a network that uses a perimeter-based security model, they could become a threat. With a vanishing perimeter, traditional perimeter-based security systems are insufficient.

Configuring policy at the physical port or VLAN has led to a proliferation of IP subnets and VLANs at the edge of the network. Managing separate VLANs in order to enforce network privileges based on traffic types is complex and cumbersome. Access control lists (ACLs) on VLAN interfaces are difficult to maintain and keep consistent across a large deployment. Often a change to one policy leads to cascading changes to several other policies because of unforeseen interaction. Policies for mobile devices require leveraging user-roles, applications, and other contextual data in order to automatically direct users to appropriate network segments.

Merging of IT and OT Networks

According to Kevin Ashton, who coined the term “the Internet of Things,” 57% of companies have deployed IoT, and 84% of them have already experienced security breaches. One of the causes of the breaches is that these operational technology (OT) devices don’t support traditional security capabilities such as anti-malware. IoT devices can be difficult to secure due to their lack of built-in functionality.

In the past, it was common to build multiple isolated networks for IoT devices. With more devices in use, many organizations connect them to a single network with IT devices. If these devices become a threat, IT network will be compromised.

Rogue Devices and Users

With some organizations focusing on perimeter security to protect from external network attacks and the lack the emphases on control of the switch ports internally, rogue devices and users often go undetected on networks for weeks or months. There is also a risk that visitors plug directly into an open Ethernet port, or disconnect devices such as phones or printers to gain access, creating problems on the network. These rogue users or devices can cause issues by infecting other devices with malicious software. Infected devices may be used to exfiltrate data or launch denial-of-service attacks internally or against other networks. Another example of how rogue devices can cause problems is through ransomware attacks. *Ransomware* is specialized malware that is designed to block access to a user's device or database server until a sum of money is paid.

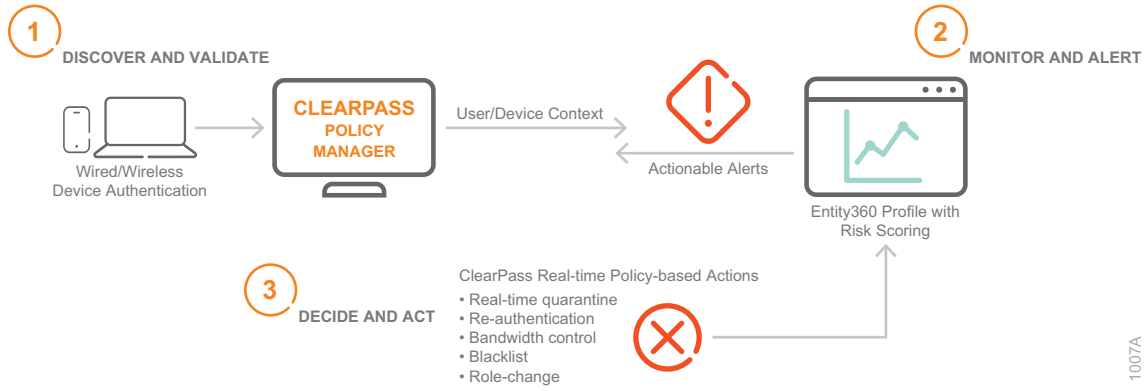
Disparate Security Systems

IT faces a challenge when implementing network security and policy. Network security devices have disparate management systems that do not communicate with each other and do not give IT security analysts easy access to a bigger picture of what is going across the network. This lack of integration causes inconsistent security and access policies leading to unpredictable results and a false sense of security.

THE ARUBA 360 SECURE FABRIC APPROACH

Many enterprise security architectures do not integrate well with each other, are based on older technology, follow models that focus on the perimeter, and attempt to close off the network to threats by relying heavily on static policy. With growing enterprise mobility, BYOD, cloud, and IoT making security more challenging for security analysts, Aruba 360 Secure Fabric offers a security framework that extends beyond traditional network security to address today's problems.

Figure 1 *Security 360 in action, discover, alert, and act*



User-Centered Model

Aruba's approach is to move away from a physical model, where policy is tied to ports or VLAN interfaces, to a user- and device-centric model, where the policy follows the user regardless of how they connect to the network. With this approach, there is no need to pre-configure VLANs, ACLs, and QoS on individual ports. When a user or device connects to the wired network, the policy is downloaded to the network access layer and moves with the user. For wireless devices, users are assigned a role when they authenticate and the policy is downloaded to their wireless controller.

Simplified Segmentation

By removing the need to statically assign VLANs and ACLs to ports or to configure multiple SSIDs to enforce security, which is not scalable, leads to poor RF performance and is confusing for users, network segmentation is greatly simplified. Network security policies are automatically assigned based on user or device role from a central location, so policy is consistent with no chance of some devices having old configurations or human-introduced errors causing inconsistent policy. The network identifies, authenticates, and grants trust based on the user or device role.

Adaptive Trust

Aruba's approach differs from traditional network access layer security by using an Adaptive Trust model. On a typical network with access layer device authentication such as 802.1X, all devices must authenticate to gain access to the network; after they are authenticated, they are assigned a role and permissions to control what network resources they can access. However, after they are on the network, their access stays the same until the next time they log in. Aruba's security solution continues to monitor the activity of the user or device after they connect to the network. If behavior changes, the policy for the device can be changed, redirecting their traffic for inspection by an enhanced security device or, in more extreme cases, quarantined or removed from the network.

The Adaptive Trust model works by tying user, device, and network behavior together. The entity, which could be a user or headless device, is monitored by the network security system using advanced machine learning to detect behavioral anomalies. If an anomaly is detected, the security system takes appropriate action and, with the help of a security analyst, can determine whether the anomaly is malicious and take appropriate action. Because the security analyst assists in the machine learning process, autonomous machine learning improves.

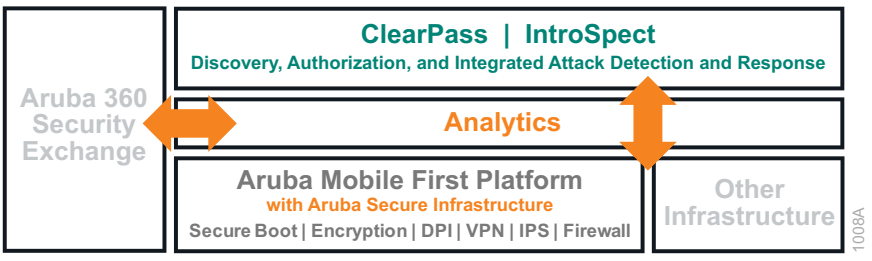
As the centralized orchestration point for policy and behavior, Aruba's security solution integrates with wide range of third-party systems to collect a wealth of valuable and authoritative contextual data, such as the user's identity, the status of a device, or the location of the connected user and device. To simplify the sharing of the context, Aruba supports many data exchange methods such as APIs, syslog, and vendor-specific integration. With a wide range of contextual information from third-party systems and the network—and whether it's mobile, BYOD, cloud, or IoT devices—Aruba truly offers 360 degrees of protection.

Solution Components

Aruba 360 Secure Fabric is an integrated security framework that incorporates the following components:

- Aruba Secure Core—Aruba mobile first infrastructure
- Aruba ClearPass
- Aruba IntroSpect
- Aruba 360 Exchange Program

Figure 2 *Aruba 360 Secure Fabric components*



ARUBA SECURE INFRASTRUCTURE—ARUBA MOBILE-FIRST PLATFORM

The foundational element of Aruba's 360 Secure Fabric, Aruba Secure Infrastructure, is composed of the wired and wireless switching infrastructure with imbedded security.

Securing the Infrastructure

Aruba ensures that network devices and their software have not been altered or compromised and prevents network device impersonation using Trusted Platform Module (TPM) security hardware. TPM is a standards-based, dedicated hardware chip designed to secure hardware devices by securely storing encryption keys and certificates used to authenticate the access points (APs), mobility controllers, Aruba switches, and the Aruba software running on them.

Aruba RFProtect prevents denial-of-service and man-in-the-middle attacks and mitigates over-the-air security threats. By continuously scanning the radio frequency (RF) and monitoring airwave activities, RFProtect provides RF spectrum visibility and guards against unauthorized Wi-Fi clients and ad hoc networks. It provides integrated wireless security and RF spectrum analysis by allowing APs to service WLAN clients while monitoring the airwaves for interference sources and rogue devices. Aruba APs may also be turned into dedicated airwaves monitors to focus on detecting and containing unauthorized APs and devices.

Securing User Data

The Aruba Policy Enforcement Firewall (PEF) enforces application layer security and prioritization based on user role, device type, application, location, and more. Aruba PEF runs on the mobility controller and provides full stateful firewall functionality at the user level controlling what they can do and enforcing policy between user groups. Deep packet inspection (DPI) capabilities allow the firewall to distinguish between business and personal applications, optimize and prioritize multicast network services such as video and apply policy, differentiate between applications running over the same port like HTTP, and even look at traffic patterns for encrypted traffic to fingerprint and identify those applications. Policies can rate limit traffic at a user, group, and application level to make sure no one is monopolizing available bandwidth and ensuring business applications have priority. Beyond permitting, dropping, and prioritizing traffic locally, the firewall can also tag traffic with appropriate QoS levels so service levels are maintained across the network.

To secure traffic across the network, Aruba supports military-grade encryption from the client to the mobility controller. Wired users can be tunneled to the mobility controller and policy enforced, just like for wireless clients, enabling services such as wired guest access and policy can be dynamically loaded on the access switch to filter traffic and protect users on the wired network.

With policies based on identities, devices, and locations, the needs of different groups of users or devices can be satisfied with a single wireless and wired network configuration. Traffic flows simply adapt to the mobility state of the mobile user and device.

ARUBA CLEARPASS

ClearPass is the centralized location to define your security policy. It pulls in relevant context from multiple sources within an organization, leverages that context to determine the appropriate policy, and then coordinates that policy across multiple enforcement mechanisms. ClearPass integrates with a range of third-party products and solutions to improve user experience and increase security.

With a suite of modules, ClearPass provides a range of options for securing all the different types of users and devices that will access the network:

- ClearPass Policy Manager (CPPM)—Provides user-role and device based network access control for employees, contractors, and guests across multivendor wired, wireless, and VPN networks. CPPM is the core and foundation of the ClearPass product suite. It supports multiple authentication/authorization sources, single sign-on for users, advanced reporting, device profiling, basic onboarding, and guest portal services. After the user or device is identified, CPPM can pass user-role or download policy to the network access device to which the client connects, ensuring the proper policy is applied. User context can be shared with third-party systems further enhancing the security of the network.

- ClearPass Onboard—Allows organizations to automate the network and security configurations of personally-owned devices for BYOD access to the network. Unconfigured and unauthorized personally owned devices belonging to authorized Employees, contractors, and partners will be automatically detected and sent through a self-service automated configuration portal. Unique user and device certificates can be generated so users experience seamless network access after the initial device onboarding. IT can create flexible user workflows and automate policy management in order to minimize the operational requirements associated with BYOD.

- ClearPass OnGuard—Performs advanced endpoint posture assessments on leading computer operating systems, ensuring compliance with endpoint security policy before devices are allowed to connect. Advanced network access control in ClearPass OnGuard ensures that devices accessing the network are running the proper software (such as anti-virus/anti-malware), are patched and up-to-date, and comply with other security policy (such as firewall-enabled and disk-encryption enabled). ClearPass OnGuard supports persistent and dissolvable agents, so both company assets and BYOD devices can be supported. If a client isn't compliant, ClearPass OnGuard allows the user to self-remediate through automatic or guided remediation options without IT involvement in most cases.

- ClearPass Guest (bundled in CPPM version 6.7 onward)—Enables customers, contractors, and other visitors to gain secure guest access to wireless and wired networks. ClearPass Guest creates a rich experience for guests that is easy to manage and administer, allowing automated or supervised guest access and differentiated policies for each type of guest. ClearPass Guest features full-featured enterprise workflows that allow for full audit trails to answer who/what/when/where/why/how visitors and their devices access the network, without IT interaction.

ARUBA INTROSPECT

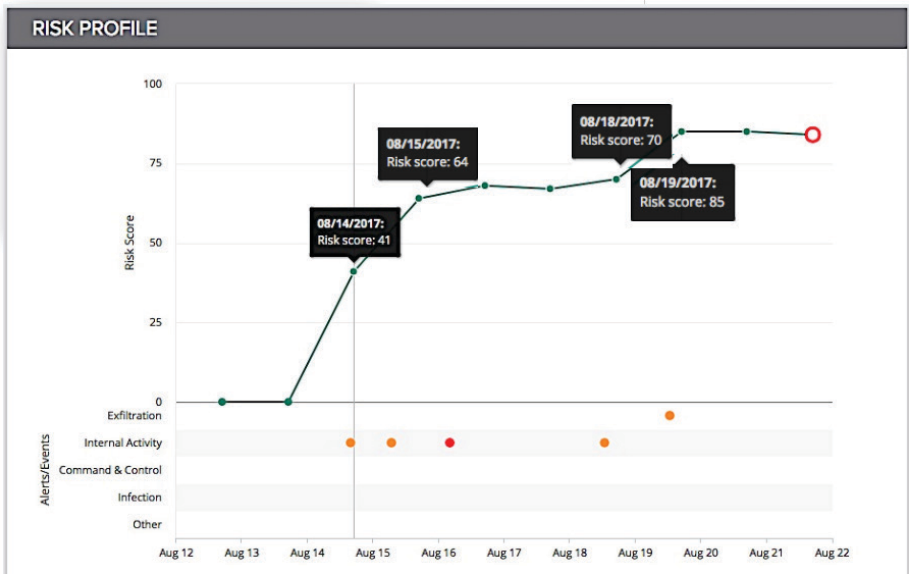
Aruba IntroSpect is an artificial intelligence–based machine learning, User and Entity Behavior Analytics (UEBA) solution that detects changes in a user's or device's behavior and alerts IT security operations. These anomalies in behavior often indicate inside attacks have bypassed perimeter defenses. By deploying IntroSpect, Security Operations Center (SOC) analyst are armed with insights into malicious, rogue, or negligent users and devices. IntroSpect is designed to find the successful infiltration and stop it before damage is done.

The specific machine-learning technology used for behavioral anomaly detection is known as *unsupervised machine-learning*. This means that a set of algorithms "self learns" user or device behavior without the need for rules or any sort of configuration from security analysts.

Unsupervised machine-learning finds anomalous behavior by sifting thought large amounts of log and network data using over 100 learning models, a task for which people are not well suited, looking for patterns that are out of the ordinary. Another kind of learning, *supervised machine-learning*, involves the administrator, who determines if the behavior is malicious.

Supervised machine-learning models add precision and depth to the unsupervised models by separating the malicious from the merely anomalous. Along with third party alerts from security information and event management (SIEM), firewalls, etc., the results of all of the IntroSpect models are combined into an Entity Risk Score. The Risk Score is continuously updated from all these sources. IntroSpect uses advanced algorithms that takes into account the type of alert, the timeframe, role in the attack, etc. to calculate the score, as described in Use Case 2 below. Based on the score, IntroSpect can take a number of actions, including alerting an analyst and putting users in quarantine using API integration with Aruba ClearPass.

Figure 3 *Risk score*



By prioritizing alerts, accelerating the incident investigation, and managing threat detection activities, IntroSpect can use analytics as a "force multiplier" for security analysts. IntroSpect enables the network security organization to efficiently prioritize and inspect the flood of alerts, with a complete forensic record.

One of the benefits of IntroSpect is the creation of the Entity360 profile. It acts as a security database for users and devices. With one click, all of the security-relevant activity for that entity across any timeframe can be displayed on a dashboard to the security analyst, along with the historical and current risk score for that entity. Summaries for device and IP address history, authentication, web access, and applications use are also available because the data is gathered from a number of network and security infrastructure devices. IntroSpect's big data platform has the compute and storage requirements needed to maintain an individual Entity360 profile for hundreds of thousands of entities.

ARUBA 360 SECURITY EXCHANGE PROGRAM

A central piece of the Aruba Mobile First framework is the open, multi-vendor integration with hundreds of partners. Differentiated from other network infrastructure providers that favor vendor lock-in, Aruba provides the best elements of a unified solution with the flexibility of an open architecture. By seamlessly integrating partners with Aruba solutions, customers can protect existing investments and leverage new features and functionality on existing networks to solve their security problems.

Third-party firewalls, MDM, EMM, SIEM, and many other systems are currently integrated leveraging Aruba's RESTful APIs, syslog messaging, and Aruba's Extensions repository in order to deliver end-to-end policy enforcement and visibility. Aruba 360 Security Exchange partners have developed security and operations features that integrate with Aruba ClearPass Network Access Control and IntroSpect User and Entity Behavior Analytics solutions.

By leveraging components of the solution that are not part of the Aruba portfolio, Aruba's solutions can be used, individually or together, for wired and wireless LAN, WAN, and remote access. Customers using Aruba's open solutions can leverage industry leading solutions to innovate at their own pace rather than being locked to a single vendor's pace of innovation.

Integration and Use Cases

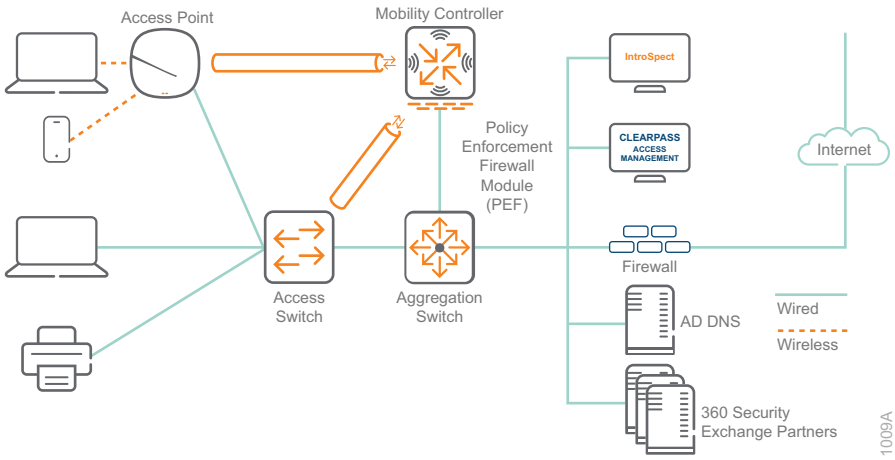
As enterprise networks shift from a fixed, static wired network to open dynamic environments, the traditional security model, with fixed endpoints and static security policies needs to evolve. Security controls should adapt to the dynamic environment of users and devices, as well as to security risks that come from anywhere. With Aruba Adaptive Trust framework, contextual information, such as user role, device type, device ownership and location, is shared across different network security endpoints in order to remove any possible security holes.

One security hole is the inside attack, where the attacker uses legitimate credentials to access the network or connects infected devices to the network. These inside attacks, which compromise users and hosts, are extremely difficult to identify because the assailants have evaded traditional perimeter-based or user/device-based security.

To have complete 360-degree protection and close this security hole, Aruba 360 Secure Fabric leverages Aruba IntroSpect and an Adaptive Trust model to:

- Secure the network by monitoring for behavioral changes (for both users and devices) in order to determine if the anomalies are malicious.
- Take steps to eliminate the threat before the network is compromised.

Figure 4 *Aruba 360 Secure Fabric network diagram*

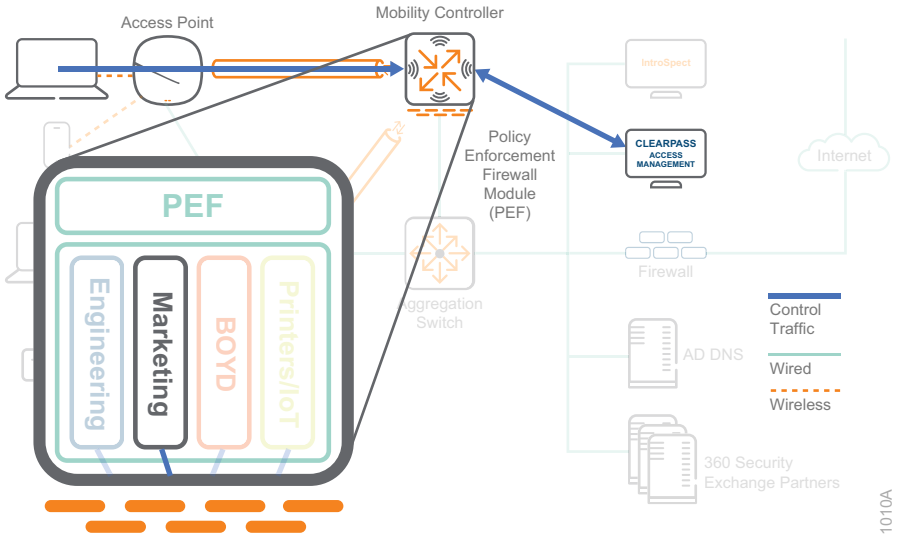


USE CASE 1: DIFFERENTIATED ACCESS BASED ON USER AND DEVICE

A company has a marketing manager named Michelle on staff. Each morning, Michelle logs in to the network, sometimes from home and sometimes from the office, from her laptop and her mobile phone. Then she spends her morning in meetings. After lunch, she accesses corporate databases to create reports.

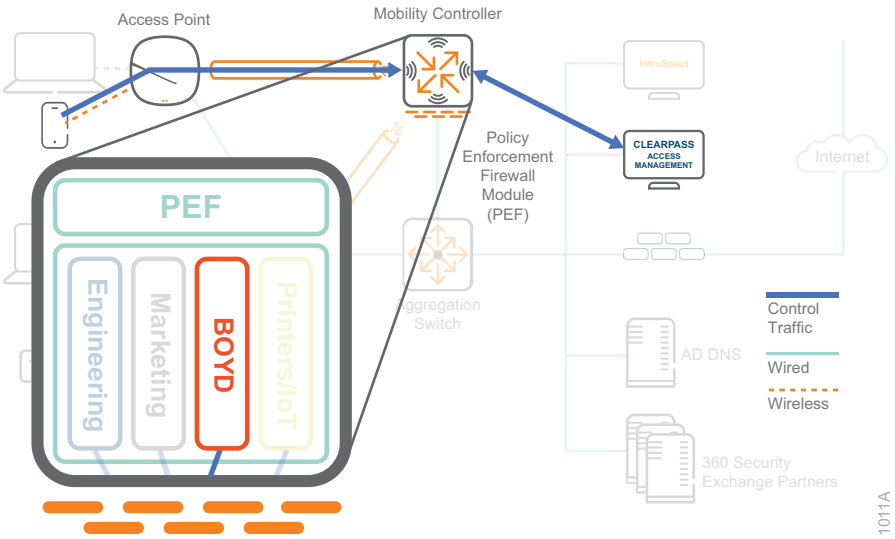
When Michelle logs onto the network with her corporate laptop using wireless, ClearPass captures contextual information about the connection such as user ID, device type, device ownership, and location. Based on the contextual information, ClearPass instructs the mobility controller to add her to the role "Marketing." The Aruba Policy Enforcement Firewall (PEF) in the mobility controller enforces an appropriate policy based on her user role.

Figure 5 *ClearPass instructs PEF to secure Michelle's traffic with the marketing firewall policy*



Michelle also accesses the organization's network with her mobile phone. When she connects to the wireless network with her phone, even though she is using the same credentials she used when she connected with her laptop, ClearPass sees that she has connected with a personal device and instructs the mobility controller to put her phone in the role "BYOD," and the firewall enforces the associated BYOD policy.

Figure 6 *ClearPass instructs PEF to secure Michelle's traffic with the BYOD firewall policy*



For Michelle's access policy, because she is in the Marketing group, she can access normal corporate database and other devices such as printers. However, she doesn't have access to engineering materials such as designs or source code. For her BYOD phone, the organization's policy allows access to only the Internet and corporate email. The firewall stops Michelle if she tries to access any engineering materials or, when she is using her phone, prevents access to corporate documents.

Figure 7 *Allowing Michelle access to printers, Internet, and the marketing database*

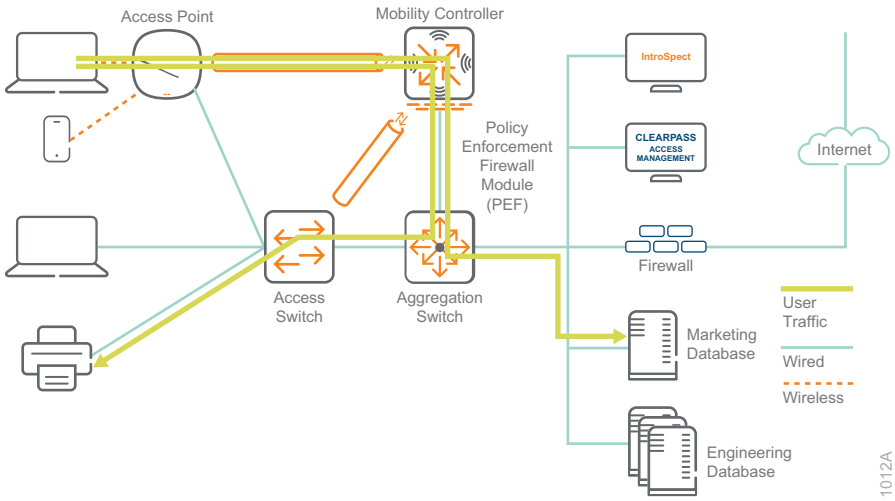
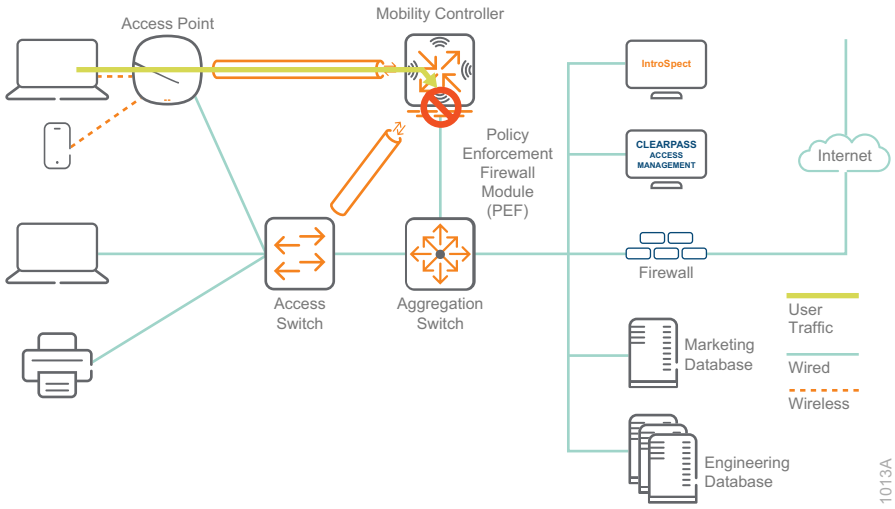


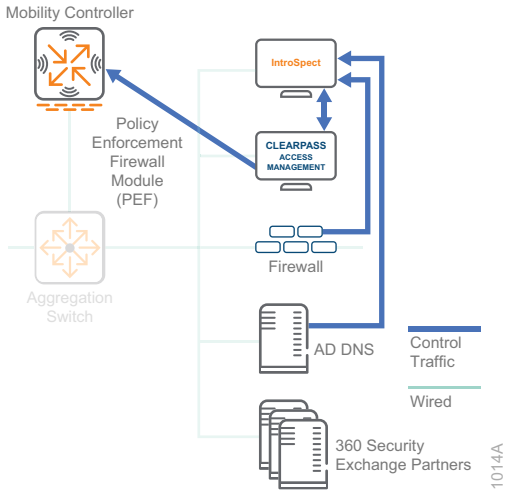
Figure 8 *PEF blocking Michelle's traffic to the engineering database*



The policy can follow the user and device regardless of location. If Michelle connects to the organization's network at another site, the same policy can be enforced.

USE CASE 2: MALWARE ATTACK DETECTION

Figure 9 *Aruba 360 Secure Fabric malware attack detection*

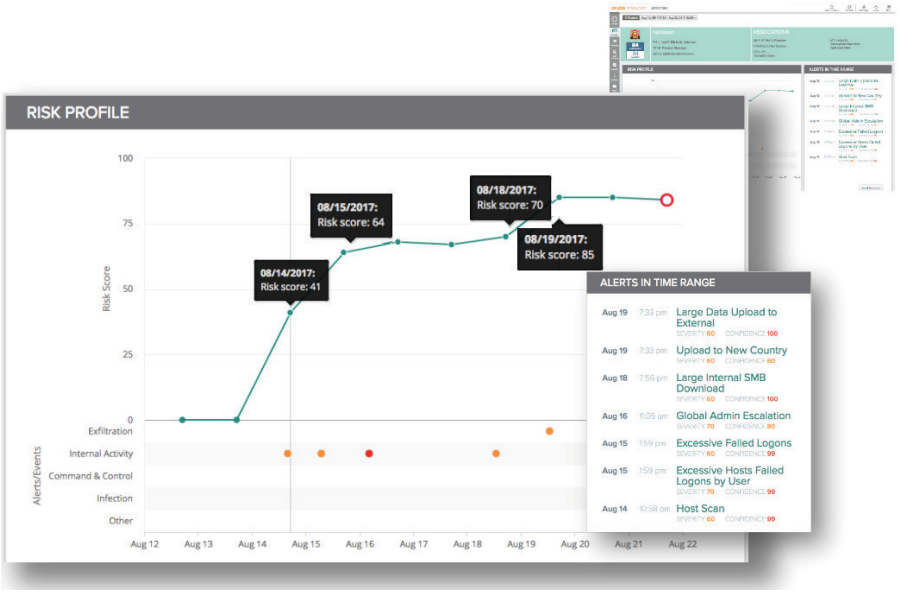


On August 14th, 2017, Michelle logged on to the network and accessed an unusual number of servers within the company. Then the following day, she tried to log in to twenty-seven different servers that she would normally not access. A few days later, she downloaded an extraordinary amount of data from five different servers, followed by a large upload the following day to a system in a foreign country that the company doesn't have business.

When Michelle accessed these servers, her access was somewhat normal, based on her role. However, her activities are anomalous. Fortunately, Aruba IntroSpect was able to detect these anomalies as the result of the integration with the Aruba Mobility Controller and Aruba ClearPass, as well as third-party logs from firewall, SIEM, AD, and DNS.

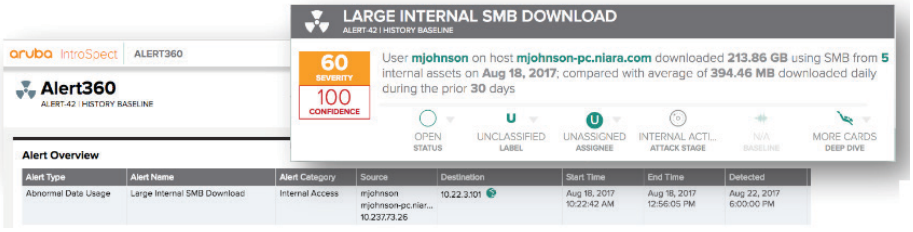
The figure below shows Aruba IntroSpect and an overview of anomalous activity for Michelle within that time period. On August 14th, Michelle attempted to access multiple servers. The activity was captured and her Risk Score went from 0 to 41 based on new activity. The next anomalous activity for Michelle was when she tried to logon to 27 servers on August 15, 2017 and increased her risk score to 64.

Figure 10 *Tracking Michelle's risk score*



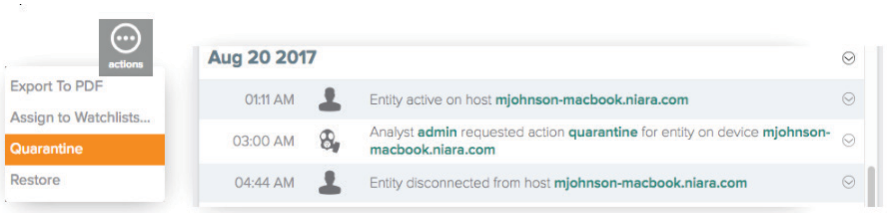
Michelle's activities got even more suspicious on August 18, 2017, when she downloaded a large amount of data (213.86GB) compared to users in her peer-group (394.46MB download average). Then the following day, Michelle uploaded the data to a new country.

Figure 11 *Alert about suspicious activity on Michelle's account*



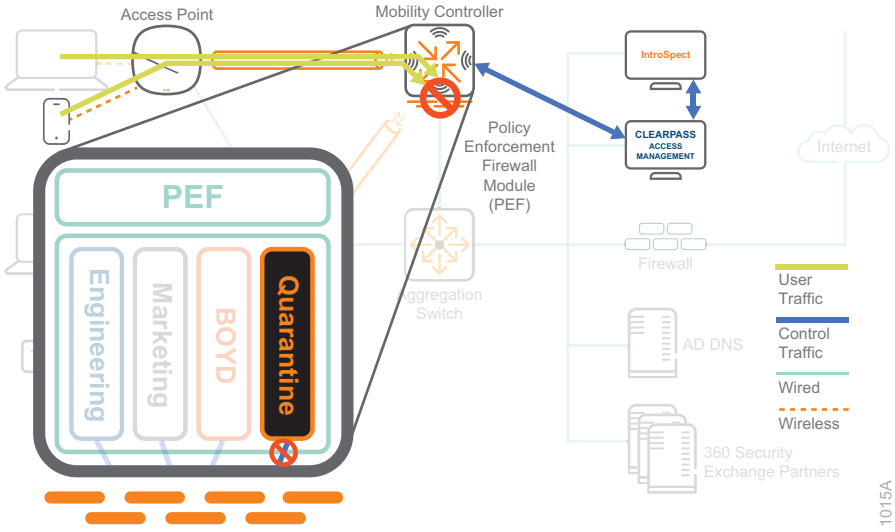
Because Michelle's score has risen to an 85, there's a good chance that her system has been compromised, perhaps with malware giving access to an external attacker. The security analyst, who has been receiving notifications about her activities, opens an investigation and decides to put her account in a quarantine state.

Figure 12 *Quarantining Michelle's account*



With Michelle's account in a quarantine status, her system has very limited access to the network. That is the result of security analyst using IntroSpect to instruct ClearPass to put her account into the role "Quarantine," where "Quarantine" was predefined policy restricting access to the network. From here there are a number of options, a case can be automatically opened with IT, Michelle can be redirected to a captive portal, letting her know that something is wrong and to contact support regarding the case that is already created. IT security can review the case and determine if there has been a breach and if further action needs to be taken. If the behavior turns out to be normal, the analyst can quickly move Michelle back to her normal role.

Figure 13 *Michelle's account in quarantine profile*

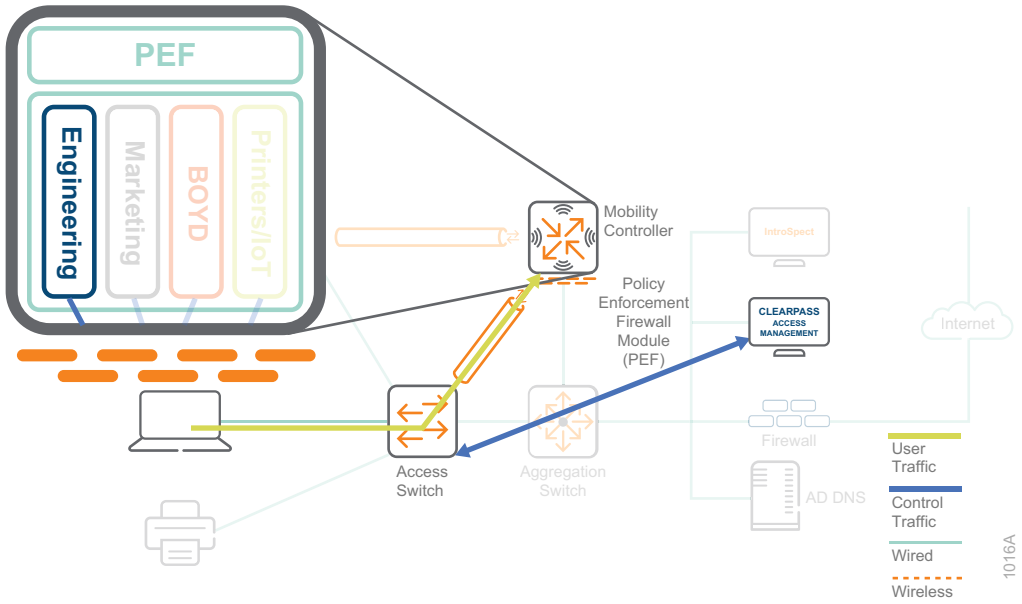


USE CASE 3: GUEST, BYOD, OR CONTRACTOR WIRED CONNECTION

Bob Smith, an engineer on contract for the organization, often works in the lab. Because of the nature of the work, Bob prefers to use a wired connection to log in to the network while in the lab. When Bob connects to a wired port on the lab access switch, he is authenticated and ClearPass collects contextual information about the connection such as user ID, device type, device ownership, and location.

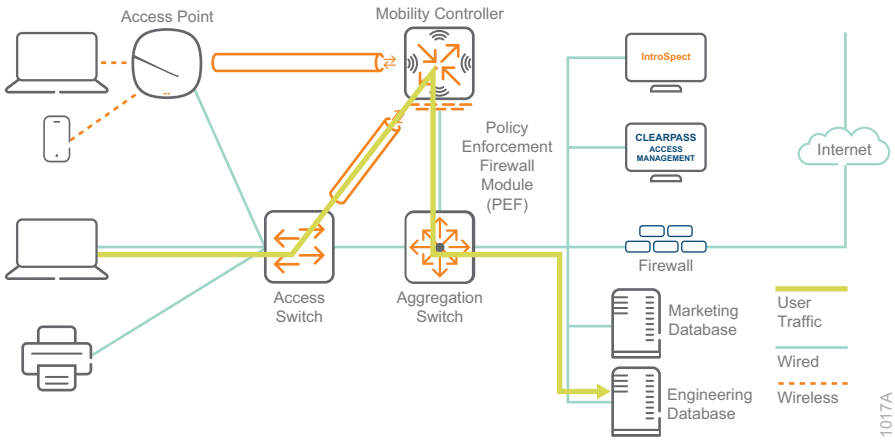
Based on the contextual information, ClearPass instructs the lab access switch to tunnel all of Bob's traffic to the mobility controller. The organization has a policy that prevents non-company owned devices from accessing the wired network directly, using the Aruba tunnel node feature allows devices that for whatever reason cannot use the wireless network to connect to the wired network, and the access switch can act like a "wired AP" tunneling the device to the mobility controller. The access switch signals to the mobility controller that Bob is being tunneled and passes the policy information from ClearPass so that the appropriate firewall policy is enforced. In this case Bob, is assigned to the role "Engineering" created for contract engineers. Now all of Bob's traffic passes through the PEF Engineering policy.

Figure 14 *PEF securing Bob's traffic with the Engineering firewall policy*



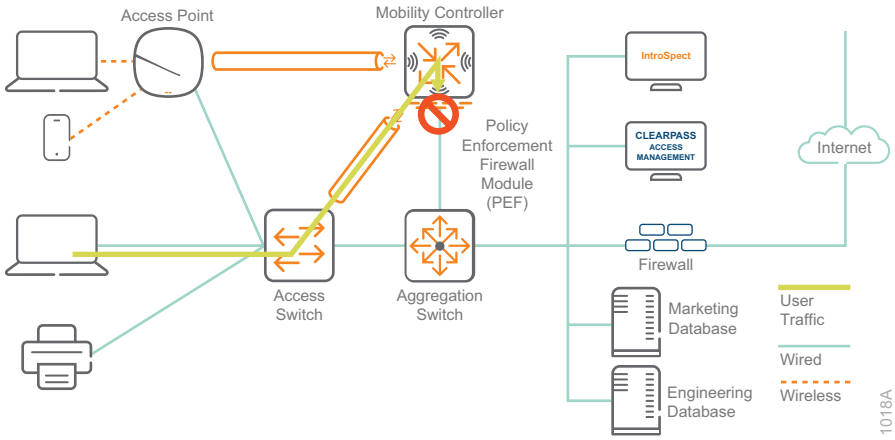
The policy follows the user, regardless of the location or connection type. Therefore, when Bob connects to the network via wireless outside of the lab or logs in at another site, ClearPass instructs the network to enforce the same policy.

Figure 15 *Allowing Bob access to only printers, Internet, and engineering database*



Because Bob is a contract engineer, he needs access to the engineering database, local printers, and the Internet to do his job. However, he doesn't have access to other resources not needed to perform his job, such as the marketing database.

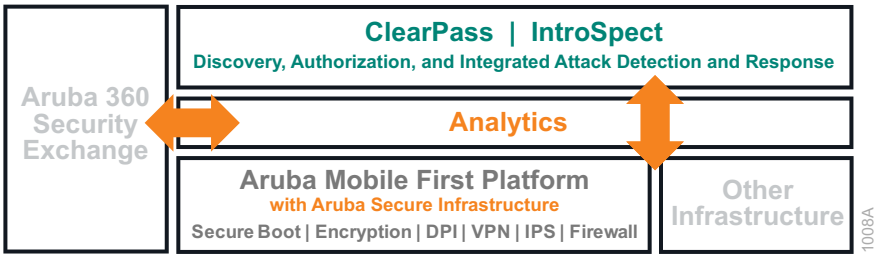
Figure 16 *PEF blocking Bob's traffic to the marketing database*



SUMMARY

Aruba's 360 Secure Fabric is an integrated security framework that encompasses Aruba's Mobile First Infrastructure with Aruba Secure Core features, Network Access Control with ClearPass, and User and Entity Behavior Analytics with IntroSpect—along with 3rd party security and network infrastructure integration through the 360 Security Exchange Program. Centered around analytics, the Aruba 360 Secure Fabric provides protection with IntroSpect by ingesting network and security data, detecting anomalies, and enabling the infrastructure to respond. The combination delivers a complete 360 degree pre- and post-admission discovery, validation, detection, and response solution.

Figure 17 *Aruba 360 Secure Fabric components*



At the foundation of the Aruba 360 Secure Fabric is the Aruba Mobile First Platform, which is composed of Aruba's Wi-Fi APs, switches, and controllers. Building upon this foundation, ClearPass provides access control integrated with IntroSpect, a machine learning–based detection tool. Along with data and policies provided by 3rd party security and network infrastructure, the Aruba 360 Secure Fabric provides 360 degrees of analytics-driven attack detection and response from the edge to the core to the cloud.

You can use the feedback form to send suggestions and comments about this white paper.

aruba
a Hewlett Packard Enterprise company

B-000170A-1 03/18