aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

# ENDPOINT SECURITY WITH ARUBA CLEARPASS AND INTROSPECT

## CURRENT SECURITY CHALLENGES

Today's targeted attacks are designed to stay "under the radar" by moving in small, but deliberate steps over long periods of time — often with legitimate credentials from a compromised user, system or device.

Safeguarding against cyber threats now requires a multi-layered security strategy that includes the ability to detect and combat threats that have evaded traditional rule and signature-based solutions, while using legitimate credentials of compromised employees, contractors, partners or IoT devices. According to the Verizon 2016 Data Breach Investigation Report:

- Over 60% of confirmed data breaches involved weak, default or stolen passwords
- 70% of all insider and privilege misuse breaches took months or years to discover

Security teams usually deal with these types of attacks using manual, time-consuming investigation methods with reactive and delayed remediation processes that are often not effective. The goal is to leverage granular access control and visibility – combined with automated attack detection – for a more proactive and timely security approach:

- Visibility into all connected and connecting devices, multi-vendor, wired and wireless
- Control to ensure only authenticated or authorized devices access the enterprise
- Attack Response using ClearPass's own brokerage system and exchange partners to deliver security to known and unknown attack vectors

## AUTOMATED ATTACK DETECTION AND ACCELERATED REMEDIATION

From sensors-to systems-to users, attacks on the inside require a new strategy. Fortunately, innovative security solutions using machine learning-based analytics and big data platforms can now provide enterprises with a new dimension of protection that traditional security products lack.

## HIGH LEVEL BENEFITS

Whether it is a rogue partner or IoT botnets, Aruba ClearPass and IntroSpect deliver a potent antidote to attacks on the inside, no matter where they originate.

- Precision profiling and visibility based on real-time user and device context
- Support for any device type, including IoT
- Machine learning-based attack detection not available in traditional security defenses
- Scalable, comprehensive decision support for faster investigation and remediation
- Automated and accurate enforcement regardless of time, location or device owner
- Built-in, no cost seamless integration between solutions

Aruba IntroSpect, an industry leading User and Entity Behavior Analytics (UEBA) solution uses supervised and unsupervised machine learning to automatically baseline user and device behavior while actively looking for anomalous activity that may indicate a threat. When IntroSpect's UEBA is integrated with Aruba ClearPass, the combined solution delivers three key security innovations: advanced attack detection, accelerated investigation, and proactive, policy-based enforcement.

Now, compromised or malicious users, or systems participating in attacks or IoT devices conscripted into a latent botnet army can be discovered and remediated before damage is done to an organization's infrastructure, assets or reputation.

## ARUBA INTROSPECT AND CLEARPASS FOR 360 DEGREE PROTECTION

IntroSpect detects compromised users' systems or devices by using supervised and unsupervised machine learning models to see telltale changes in typical IT access and usage. When these subtle signals are aggregated and put into context over time, the presence of an upcoming attack is confirmed and alerted. Through tightly integrated bi-directional communication, IntroSpect then triggers ClearPass to perform a change of authorization for the entity in question.

Once the threat is under control, an analyst can then turn to IntroSpect's big data-based incident investigation system where the entire IT history of the entity under scrutiny—down to the packet level—is available in seconds, so that decision making and remediation is cut from hours and days to minutes.

## DETECT, RESPOND, INVESTIGATE, THEN REMEDIATE

### CLEARPASS + INTROSPECT = 360° PROTECTION

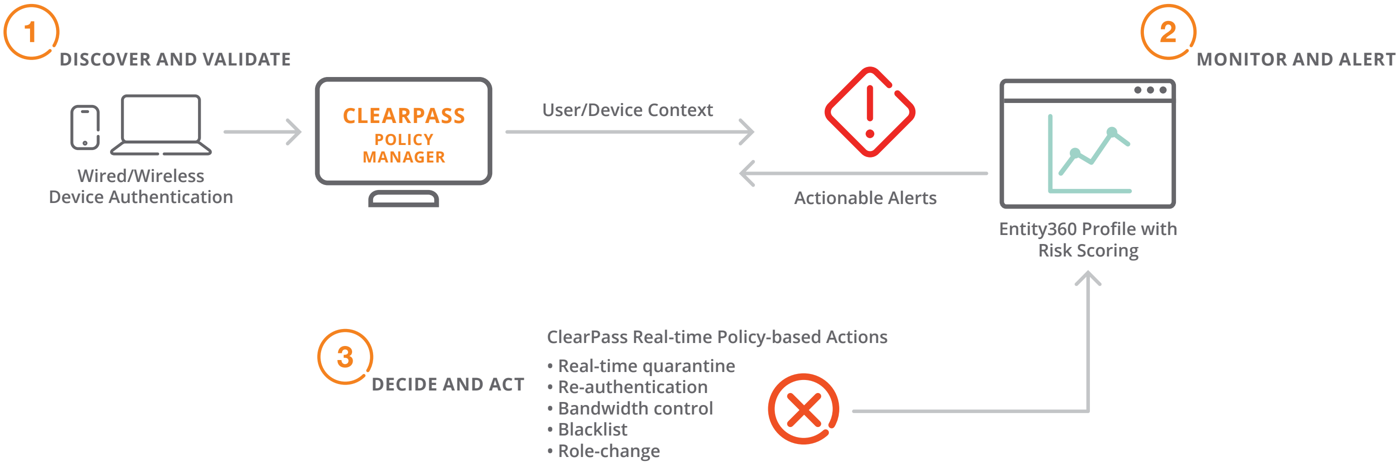

**Figure 1: When IntroSpect's UEBA is integrated with Aruba ClearPass, the combined solution delivers three key security innovations: advanced attack detection, accelerated investigation, and automated policy-based enforcement.**

## PRIORITIZE SECURITY RISKS

Laptops behaving badly? IoT devices on the rampage? Today's threats require an intelligent threat management workflow that integrates detection, response, real-time investigation and comprehensive remediation. To accomplish this advanced level of insider attack management, ClearPass provides IntroSpect with profiling information about each device that logs into the network including user or device role, connection time, location, and what the entity is allowed to access.

With detailed visibility, IntroSpect can then baseline and analyze a device's traffic based on expected characteristics. For example, if IntroSpect detects that a device associated with a "Guest" is exhibiting anamalous behaviors, IntroSpect can trigger a policy-based security response that ClearPass can then enforce, which can include quarantining an entity or blacklisting it.

As part of IntroSpect's investigation workflow, an analyst can easily see changes in the amount of data transferred, addresses visited, duty cycle, and time or location for which an anomaly is recognized. The ability to leverage profiling, granular access rules and differentiated levels of enforcement ensures the appropriate remediation of a compromised entity.

a Hewlett Packard
Enterprise company

Contact Us    Share