aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

USER AND ENTITY BEHAVIOR ANALYTICS

Using machine learning to deliver a smarter security solution

IT organizations of every size are spending more money than ever to protect their network and assets due to the increasing threat landscape. According to IDC, security budgets will grow by 40% by 2020. And in addition to the growing number of threats, the typical IT security ecosystem is changing rapidly due to:

- The increase in the number and types of devices that a single user may deploy to access corporate assets
- Cloud-based applications (Box, Salesforce, etc.) that can be accessed outside the control of corporate IT
- The need to provide access to high value assets to outside entities such as partners and contractors to increase efficiency of key business processes
- "Non-traditional" IoT devices accessing the corporate network

The result is that it used to be a matter of defending the castle (the corporate network) with a moat (security products at the entrance and exits). Now it's about protecting a borderless, uncontained collection of employees, contractors and partners – all using multiple devices from anywhere, at any time – from outside and within the secure boundaries of the corporate network.

To deal with this new threat landscape, Aruba's User and Entity Behavior Analytics (UEBA) solution, Aruba IntroSpect, detects attacks by spotting small changes in behavior that are often indicative of attacks that have evaded traditional security defenses. Aruba IntroSpect integrates advanced AI-based machine learning, pinpoint visualizations and instant forensic insight into a single solution. Attacks involving malicious, compromised or negligent users, systems and devices are found and remediated before they damage the operations and reputation of the organization. With a Spark/Hadoop platform, IntroSpect uniquely integrates both behavioral-based attack detection and forensically-rich incident investigation and response at enterprise scale.

THE NEED FOR UEBA

Traditional cyber defense products were not designed to deal with the sophisticated, carefully-crafted and targeted attacks that enterprises now face. They are still needed to deal with the vast majority of "standard" threats that come in every day, but require help with the smaller number of deadly "advanced" attacks that arrive without warning and evade perimeter defenses. We call these "attacks on the inside".

By definition, attacks on the inside are "unknown bad"—they use techniques and tools that haven't been seen before. This means there are no "signatures" to match or rules to fire, which is why IntroSpect features a new class of detection analytics that utilizes machine learning—artificial intelligence technology that does not require pre-programming or setup.

Instead, IntroSpect builds baselines of normal behavior for a user, a system or any device with an IP address—known as an "entity". The baselines are built by machine learning models that operate on key data from logs, netflow and packet streams—anything that characterizes an entity's IT behaviour. These baselines are then used to detect abnormal behavior that, aggregated over time and put into context, will indicate a gestating attack.

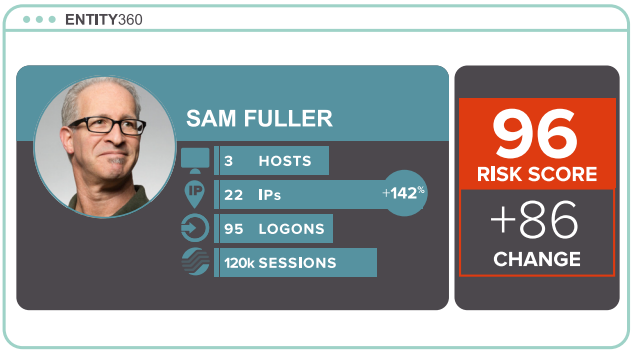

Figure 1: IntroSpect Machine Learning detects attacks before they do damage

Given this approach, Gartner dubbed the category UBA (User Behavior Analytics) and then extended this to UEBA (User and Entity Behavior Analytics) to reflect products like IntroSpect that profile not only users and systems, to anything with an IP address (i.e., IoT).

A QUICK OVERVIEW OF MACHINE LEARNING

Machine Learning is an umbrella term that encompasses techniques used to learn and make judgments without being programmed explicitly for every scenario. Unlike signature-based products, machine learning models learn from data and their results are reported as a probability. The likelihood of a decision being accurate is expressed as a percentage and can be interpreted as a measure of confidence in that conclusion.

IntroSpect has over 100 machine learning models (algorithms) in its arsenal that feature two different techniques:

1. **Supervised Machine Learning.** These models are trained in a lab with large amounts of data to find specific types of attacks. Once the model is developed it can then be used to predict an attack for any new set of inputs. For example, IntroSpect uses supervised machine learning models to spot systems that are controlled by a malicious outsider by detecting unusual url's that are typical of this situation.
2. **Unsupervised Machine Learning.** In this model type, the algorithm is "self-learning" which means there is no prior training or preparation required before it is deployed. The algorithm automatically constructs a "baseline" to detect small changes in behavior indicative of pending attacks.

   Baselines can be established for individual users, systems or devices. For example – an employee accessing a new system at an odd time of the day will be noticed, or an IoT device in a factory that has increased its network traffic usage by a factor of 5.

TYPICAL USE CASES

IntroSpect UEBA is deployed in a wide variety of industry verticals and organizations of all sizes.

- **HEALTHCARE:** The installation requires processing logs from 300,000 users that result in billions of events per day. Key use cases include monitoring high value users such as sysadmins for abnormal behavior and detecting shared credentials.
- **FINANCE:** A SIEM customer needs additional analytics support to detect email-based exfiltration and help analysts prioritize correlation alerts while accelerating incident investigation.
- **LEGAL:** A 2,000 employee law firm with 14 offices around the world lacks visibility into LAN network traffic which blocks their ability to see negligent behavior such as password sharing and abnormal cloud usage.

KEY DIFFERENTIATORS

Aruba is the only networking provider with the industry's leading UEBA solution.

1. **Continuous monitoring and attack detection.** 100+ supervised and unsupervised models that detect the widest range of attacks.
2. **Total visibility.** IntroSpect uniquely incorporates all sources of IT-relevant data into both the analytics and forensics, including packets, flows, logs, alerts, endpoint, cloud, etc.
3. **Accelerated incident investigation.** IntroSpect combines both attack detection via supervised and unsupervised machine learning with integrated forensic data in a consolidated security profile called Entity360. Entity360 is key to reducing the time and effort required to understand, diagnose and respond to an attack. Entity360 provides comprehensive and continuous risk scoring and enriched security information that analysts would otherwise spend hours or days searching for – months and years of security data down to the packet level.

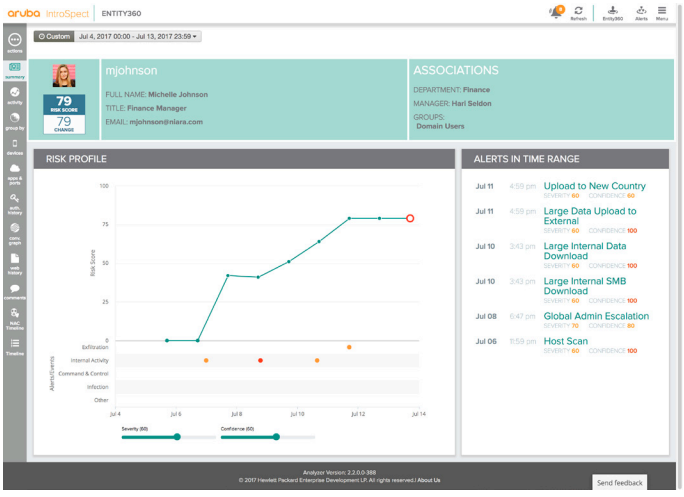

Figure 2: Consolidated forensic information in an Entity360 profile

4. **Mature enterprise-class scalability.** Support for a Big Data architecture – IntroSpect has a 3 year head start in perfecting this technology.
5. **Seamless integration.** With bi-directional integration with the major SIEM and log aggregation systems such as ArcSight, McAfee ESM, QRadar and Splunk, IntroSpect leverages both their centralized data repositories as well as returning machine learning-based alerts and forensic data to the SIEM console and workflow.
6. **Business context and policy-based attack response.** Integration with access control systems such as ClearPass provide IntroSpect with the ability to automate the response to attack alerts based on policies set by the organization. And, because IntroSpect attaches business significance to its risk scoring, policies and actions can be tuned based on the value of the assets and actors involved. In a world where it is almost impossible to block all attacks, IntroSpect is a "post-admission" security complement to the ClearPass "pre-admission" visibility and control.

ARUBA INTROSPECT PRODUCT FAMILY—STREAMLINED FOR QUICK TIME-TO-VALUE, SCALED FOR THE ENTERPRISE

The IntroSpect UEBA product family consists of Standard and Advanced Editions:

IntroSpect Standard is a streamlined, fast-start version of the full UEBA platform, perfect for Aruba networking installations. It requires as little as three data sources (Active Directory or equivalent authentication records, LDAP-based identity information and and AMON logs that are generated by Aruba wireless controllers.) to deliver attack detection focused on abnormal asset access, attempts at attack expansion such as beaconing, and indications of data exfiltration attempts.

IntroSpect Advanced provides all the attack detection, incident investigation and threat hunting capabilities that customers have come to rely on for the broadest protection available in the UEBA market. If a customer starts with IntroSpect Standard, upgrading to some or all of the Advanced Edition functionality is seamless and requires no change to the base product.

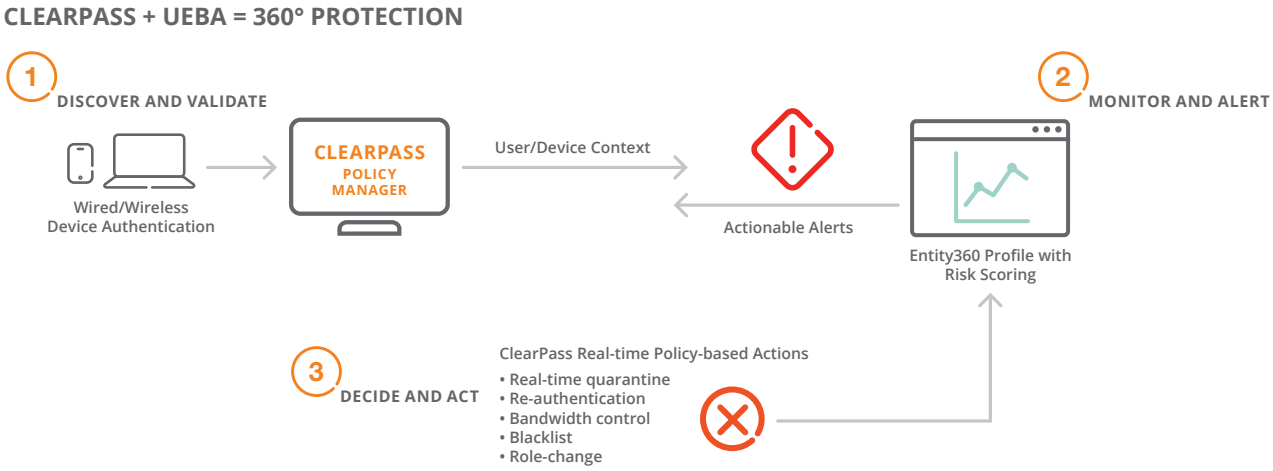

Figure 3: When IntroSpect is integrated with Aruba ClearPass, the combined solution delivers three key security innovations: advanced attack detection, accelerated investigation, and automated policy-based enforcement.

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