UEBA USE CASE

PROTECT HIGH-VALUE ASSETS FROM INTERNAL SECURITY RISKS

EXECUTIVE SUMMARY

Behavior analytics can automate the detection of security threats from compromised users, negligent employees, and malicious insiders. These types of internal threats are often hard to identify with traditional security approaches, such as firewall protection, which are designed to thwart "known bad" attacks with identifiable signatures. However, organizations often face a greater risk from internal threats, or "unknown bad" activity, such as an employee who shares his login credentials with a co-worker or an IT admin who gradually downloads and sells customer information on the black market.

Aruba IntroSpect's User and Entity Behavior Analytics (UEBA) helps organizations quickly detect and resolve these threats by providing analytics-driven visibility across the entire network and multiple types of data. Our platform builds unique, Entity360 risk profiles for users and hosts by applying behavioral analytics techniques on data sources that indicate anomalous end-user activity. We offer the only solution that combines supervised and unsupervised machine learning with layered forensics that enables complete incident investigation and insider threat detection without relying on rules, configuration, and signatures.

OVERVIEW

Although external threats from organized criminal networks pose a serious threat to high-value assets such as source code, product designs, customer data, and financial records, threats from internal sources are on the rise as well. For instance, a study conducted by Intel found that among companies that experienced a data breach, internal actors were responsible for 43% of data loss. Half of those instances were determined to be accidental and the other half intentional.[1]

Internal threats come from three primary sources: compromised users and hosts, negligent employees, and malicious insiders. Protecting high-value assets from these types of internal risks is notoriously difficult because legitimate credentials are often used to access corporate resources, thereby evading existing perimeter defenses. In many cases, a legitimate user's credentials have been stolen by malicious agents whose activity can remain undetected because traditional security approaches lack the ability to deeply analyze and report anomalous behavior. Instead, they monitor for external, "known bad" threats with identifiable signatures that can be blocked from accessing network resources. But the "unknown bad," such as users with compromised credentials or disgruntled employees looking to harm the company, are more difficult to detect with traditional security approaches. Many of these technologies generate alerts for any detected anomaly, which can overwhelm security analysts and make it difficult to sift through the noise to focus on threats that matter. As a result, enterprise security teams need solutions that can provide more automated analytics and contextual visibility into the internal threat landscape.

ARUBA INTROSPECT FOR HIGH-VALUE ASSET PROTECTION

User and entity behavior analytics help analysts detect and investigate potential threats to high-value assets posed by compromised users, negligent employees, or malicious insiders. Aruba IntroSpect offers a unique solution that investigates how users interact with these assets over time, which provides historical context and generates insights by applying machine learning-based analytics across multiple data sources.

[1] http://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

DETECT ANOMALOUS ACTIVITY

IntroSpect uses diverse data sources, including packets, flows, logs, files, third-party alerts, and threat feeds to observe how users engage with sensitive corporate information. It then applies machine learning on a variety of data sources across multiple scenarios, such as authentication requests, remote access, internal access to high-value servers, cloud applications, and Internet activity. Using this detailed contextual analysis, organizations can see a complete picture of every user and host and quickly address unusual activity or compliance violations.

IntroSpect provides risk scores for every employee to help IT quantify the threat potential to corporate data security.

Aruba IntroSpect helps organizations create risk profiles for each user by analyzing information such as:

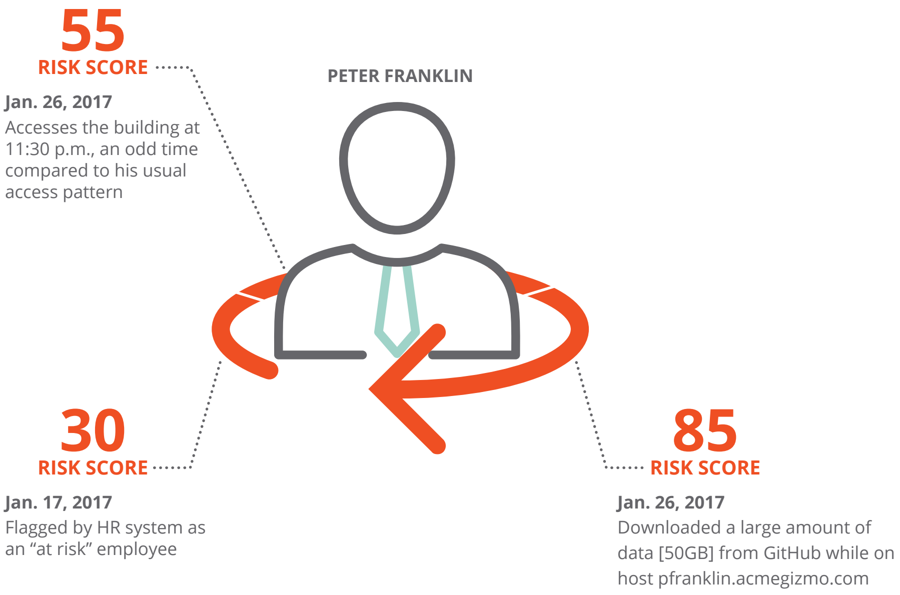
- **Unusual access behavior:** Reviews access patterns such as day and time, duration of login, and quantity and type of data accessed to help flag users who may be abusing their privileges to download high-value assets.
- **Data exfiltration:** Determines if an employee is using cloud services or external sites to exfiltrate sensitive company information to unauthorized apps or web sites.
- **Business context:** Ties into HR systems or analyst input around at-risk employees or high value assets.
- **DLP Alerts:** Incorporates DLP alerts to inform the user's risk profile.

PUT UNUSUAL BEHAVIOR IN CONTEXT

Detecting anomalous activity is the first step to stopping a potential security breach. Before acting on that information, however, security analysts need to put red flags in context. For example, an employee who downloaded a large amount of corporate data on Saturday at 2:00 a.m. may have simply been preparing for an important client presentation on Monday morning. IntroSpect can help analysts see the context around anomalies to determine if they represent legitimate employee behavior or potentially threatening activity.

Another example would be a user who over a period of four months, uploaded 1GB of sensitive information to Dropbox. To investigate this further, the security analyst may need to review months of log information, know every asset the user accessed and identify any other data that may be at risk for exfiltration. Sometimes systems cannot always detect insider activity, so analysts may need to manually view the reports to investigate the incident further.

Since IntroSpect correlates all the data and behavior patterns associated with a user or host, analysts can move from behavioral alert to detailed investigation in a matter of minutes. Analysts can also initiate detailed queries such as "Show me all the internal activity for user 'mjohnson' where she downloaded more than 10MB over the last 6 months." The analyst can then drill down into each of the entries and see complete details for each instance.



PETER FRANKLIN

55
RISK SCORE

Jan. 26, 2017
Accesses the building at 11:30 p.m., an odd time compared to his usual access pattern

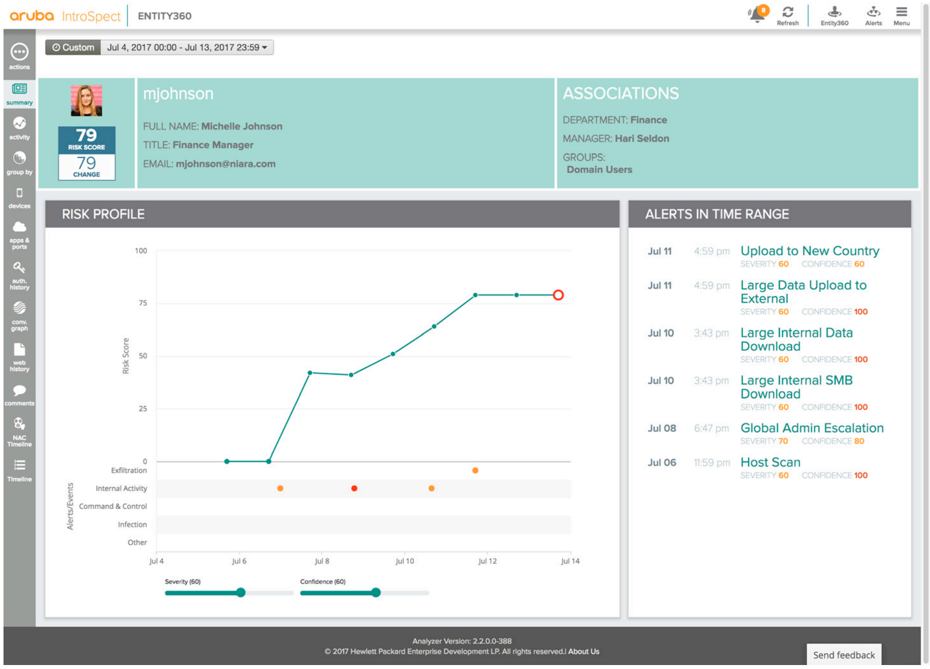
30
RISK SCORE

Jan. 17, 2017
Flagged by HR system as an "at risk" employee

85
RISK SCORE

Jan. 26, 2017
Downloaded a large amount of data [50GB] from GitHub while on host pfranklin.acmegizmo.com

Figure 1: IntroSpect provides risk scores for every employee to help IT quantify the threat potential to corporate data security.



Custom Jul 4, 2017 00:00 - Jul 13, 2017 23:59

79
RISK SCORE
79
CHANGE

mjohnson

FULL NAME: Michelle Johnson
TITLE: Finance Manager
EMAIL: mjohnson@niara.com

ASSOCIATIONS

DEPARTMENT: Finance
MANAGER: Hari Seldon
GROUPS:
Domain Users

ALERTS IN TIME RANGE

Jul 11 4:59 pm Upload to New Country
SEVERITY 60 CONFIDENCE 60

Jul 11 4:59 pm Large Data Upload to External
SEVERITY 60 CONFIDENCE 100

Jul 10 3:43 pm Large Internal Data Download
SEVERITY 60 CONFIDENCE 100

Jul 10 3:43 pm Large Internal SMB Download
SEVERITY 60 CONFIDENCE 100

Jul 08 6:47 pm Global Admin Escalation
SEVERITY 70 CONFIDENCE 80

Jul 06 11:59 pm Host Scan
SEVERITY 60 CONFIDENCE 100

Analyzer Version: 2.2.0.0-388
© 2017 Hewlett Packard Enterprise Development LP. All rights reserved.| About Us

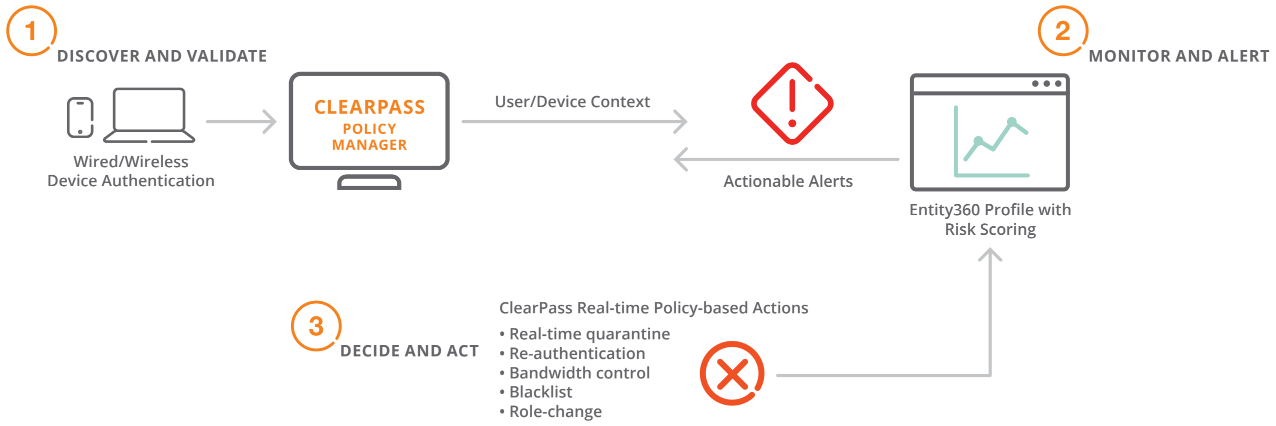
Figure 2: IntroSpect correlates user or device with a comprehensive view of their security-relevant activity to provide a complete profile of potentially compromised, negligent, or malicious entities.

THE INTROSPECT SECURITY ADVANTAGE

IntroSpect's comprehensive behavioral analytics can detect potential insider threats faster and with much greater accuracy than traditional security approaches. Only IntroSpect's unique combination of multi-dimensional analytics, diverse data sources, and integrated forensics can deliver rapid, actionable results to protect critical enterprise data. IntroSpect fully integrates with leading security and infrastructure solutions to offer flexible on-premises and hybrid/cloud deployment options. And with the integration of IntroSpect with Aruba ClearPass, the precision alerts that IntroSpect provides mean that ClearPass can respond with pre-determined policy-based actions – thus cutting off the threat before it can do damage.

The deep integration between IntroSpect and ClearPass ensures that attacks are detected and stopped before this do damage.

CLEARPASS + UEBA = 360° PROTECTION



ClearPass Real-time Policy-based Actions

- Real-time quarantine
- Re-authentication
- Bandwidth control
- Blacklist
- Role-change

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

As a result, IntroSpect enables enterprise organizations to:

- **Build detailed entity risk profiles:** Apply supervised and unsupervised machine learning tools that go well beyond statistical techniques.
- **Get complete visibility into the threat landscape:** Evaluate a broad range of data sources and logs from Active Directory, firewall and network traffic, VPN, DNS, DLP, HR systems, and more.
- **Improve threat detection capabilities:** Quickly root out abnormal activity from both compromised users and malicious insiders.
- **Reduce time from problem detection to resolution:** Combine behavorial analytics with contextual forensics to ensure anomalies don't escalate to serious security breaches.
- **Leverage existing security investments:** Quickly plug into the IT infrastructure to start analyzing data gathered from multiple tools and applications. That data is then integrated into existing IT workflows to provide seamless visibility across the entire infrastructure.

To learn how IntroSpect can help you secure access to your high-value assets and corporate data, visit us at www.arubanetworks.com/introspect.

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.