The Future of Fraud Prevention; User Behavior

Issue 2
2 The Future of Fraud; an Introduction from Christopher Bailey, CTO NuData Security Inc.
3 A Word of Caution About User Behavior Analytics
4 From the Gartner Files: Best Practices and Success Stories for User Behavior Analytics
11 About NuData Security
The Future of Fraud: an Introduction from Christopher Bailey, CTO NuData Security Inc.

User Behavior Analytics is the future of fraud prevention. It answers the fundamental question, “is this person really who they say they are?”

A technology once valued only by early adopters has entered the mainstream with some of the largest companies in the world using this technology to secure their websites from fraud, brand attacks, account takeovers and bad behavior from their user communities: leveraging the unparalleled accuracy, scalability and speed that Behavioral Analytics provides.

Our team of developers, engineers and data scientists work with a single goal of creating a product that predicts fraud and malicious behavior earlier, faster and more accurately than any other solution in the world.

We have ground-rules to ensure NuDetect:

• has zero impact on, and is completely invisible to the end user;
• respects the users’ Personally Identifying Information, or PII; and,
• can’t be mimicked, impersonated or spoofed.

We discovered the best way to prevent fraud and match those criteria is by leveraging User Behavioral Analytics (UBA).

Observable biometric behaviors are invisible, don’t require the storage of any PII, and take in more data points (from typing speed, angle the device is held, all the way to geo-location) than ever before. Our complex behavior model distinguishes the customers from the bad actors.

In this research paper, Gartner analyst Avivah Litan recommends that User Behavior Analytics is the answer to detect fraud and rapidly detect bad actors based on behavior. On page 9, Avihah offers up NuData Security’s verified success in using UBA to detect and stop mass attacks, including use cases from two of our clients.

It’s these continual positive testimonies that give us confidence that our innovations of today will become the standards of tomorrow.

Christopher Bailey

Contact NuData Security for further information:
bizdev@nudatasecurity.com
+1 (604) 800-3711
A Word of Caution About User Behavior Analytics

When an emerging technology receives mainstream fanfare, it can often be seen as a silver bullet solution. We all know that the marketing spin is not what makes a solution powerful. The same is true for the evolution of User Behavior Analytics (UBA) – there is more to it than meets the eye. While yesterday’s security concepts used rules and signatures to prevent “bad” occurrences, today, we need to look under the hood of User Behavior Analytics to detect the ever-increasing sophistication of attacks.

We cannot inherently trust the user or their information. Credit card numbers, usernames, passwords, and even the device they are using, should be assumed false.

While the pool of information we can’t trust continues to increase, we need to combat that distrust with information we can trust — observed behaviors. One system might flag a transaction as suspicious, but without a holistic view of the users’ relationships, it could seem innocuous. What if we could see that the account was linked? Collectively, suspicious transactions may be deemed high-risk, even if they appear normal when viewed in isolation. Imagine the power of having a holistic view – not just for a customer relationship, but spanning a network of potentially related profiles.

Nudata Security network records hundreds of individual elements of behavior that combine to build a holistic profile to offer better accuracy and added protection: 18 billion unique profiles last year, equivalent to about 35,000 profiles per minute.

NuDetect has Entity Linking capabilities that understand, in real-time, which of those thousands of behaviors to trust, revealing the true intention of the user.

The ability to detect your trusted good user and preventing fraud should be paramount in an organization’s effort to predict and prevent fraud online, and to protect your business from brand damage and financial loss caused by fraudulent or malicious acts.

So, take a close look. If a UBA solution does not have the ability to link entities in real-time, it is simply an advanced rules engine. Not a fraud prevention revolution.

Source: NuData Security

“Massive automated account takeover attacks have become much more sophisticated and have escalated substantially.”


There are various companies boasting User Behavioral Analytics solutions that only identify single actors. There is a real differentiating factor that separates the wheat from the chaff – Entity Linking.

Entity Linking is the real-time determination of relationships based on emergent behavior patterns, and making accurate decisions based on those patterns.

As fraudsters find their strategies getting blocked, they evolve their tactics, creating an ever-escalating game of cat-and-mouse. This might mean hiding their location in a more sophisticated way, or slowing their attack velocity to pass under the radar, putting institutions at risk. Avivah states that they choose to be “low and slow and distributed,” (Page 8) and to their credit, hackers often avoid detection in this way.

Entity linking sees through these comprehensive methods to mask behavior that often go unnoticed by velocity rules and data-scientists.

“...We rely on NuData to protect us from fraudulent activity but we see as much value from the trust NuDetect establishes between us and our user community.”

A Global Technology Company

“Gartner, Best Practices and Success Stories for User Behavior Analytics, Avivah Litan, 4 March 2015.”
Best Practices and Success Stories for User Behavior Analytics by Avivah Litan

Large enterprises are using user behavior analytics to detect breaches before significant damage occurs. Companies are also using UBA to prioritize alerts, as well as to reduce the volume of alerts and the time it takes to investigate them. Here, we help security managers navigate the UBA space.

Key Challenges
- “Bad guys” are evading most enterprise controls that rely on perimeter-focused security monitoring, identity access controls and various types of threat protection.
- Enterprise security teams are inundated with alerts, in some cases millions a day, which are not prioritized so that important ones indicating breaches are buried within the lot.
- Most legacy security applications used to investigate alerts are cumbersome and time-consuming to use.
- Enterprises don’t have good security controls over, or visibility into, their employees’ use of SaaS applications from third-party providers.

Recommendations
Security managers should:
- Use UBA to rapidly detect bad actors and behavior, prioritize security alerts, reduce alert volume, and streamline alert investigations.
- Use UBA to strengthen security for SaaS-based applications by detecting unauthorized access and users. UBA for SaaS is provided by cloud access security brokers.
- Use UBA to detect automated user account takeover and user account creation attacks against enterprise assets, which are especially prevalent among large consumer brands and their Web-facing applications.
- Operationalize UBA results by feeding their alerts into an existing broad-scope security monitoring system (such as SIEM) or other alert management console used by the enterprise to manage security events.
- Utilize existing infrastructure (such as SIEM and network data capture) for UBA event collection, as appropriate.

Strategic Planning Assumption
By 2018, at least 25% of self-discovered enterprise breaches will be found using user behavior analytics (UBA).

Introduction
All types of attacks are continuing to penetrate organizational defenses, highlighting the fact that most enterprise security is based on yesterday’s security concepts that use rules and signatures to prevent “bad” occurrences. What’s needed is rapid detection and response, enabled in part through behavioral analytics. Gartner has spoken with several companies that have successfully deployed UBA to:
- Find bad actors via rapid detection of attacks and other infractions without disrupting the business
- Improve alert management by reducing the number of alerts and prioritizing the ones that remain
- Improve alert investigations by reducing the time and number of staff required to investigate those alerts (since the underlying data for the correlated alerts is typically readily available)

UBA has three main components — data analytics, data integration, and data presentation and visualization as defined below. A UBA vendor’s data analytic capabilities are more critical to success than its data integration abilities are, since superior analytics are harder to replicate, and UBA can typically be made to integrate with all types of data sources.

See Figure 1 for an overview of UBA’s benefits.

Data Analytics
UBA solutions should be able to:
- Correlate and group user and other entity actions and behaviors
• Profile users, peer groups and other system entities (see Note 1)

• Detect anomalies using statistical models and/or rules to compare incoming transactions with profiles

Data Integration
UBA solutions should be able to integrate any type of structured data and optionally also nonstructured information. Sample structured data sources include:

• Logs from existing logging applications, such as security information and event management (SIEM)

• Native log collection from a limited number of event sources

• Network flow data and/or packet capture (PCAP) data

Data Presentation and Visualization
This represents the ability of the UBA solution to display data analytic results in a manner useful to the enterprise IT and business user so that patterns and trends in security infractions are readily apparent and can be acted on.

Figure 2 describes UBA.

UBA vendors are differentiated by:

• The source applications they are monitoring, whether they are on-premises or cloud-based software as a service (SaaS)

• The method in which they obtain the source data, as described above

• The type of analytics they use, whether they are packaged analytics, user-driven (through various data mining tools) or vendor-written

• The service delivery method used by the UBA solution, whether it is on-premises or a cloud-based service

FIGURE 1  Three Benefits of UBA
Alert management improvement
• Reduces number of alerts
• Prioritizes important alerts

Investigation efficiency
• Reduces time to investigate alerts
• Reduces number of staff needed

Find the bad guys
• Rapidly detects attacks or infractions
• Doesn’t interrupt the business

FIGURE 2  What Is User Behavior Analytics?
Correlations and Grouping
• User: Entity resolution
• Other entities: Application, device, IP address

Profile
• Users, peer groups
• Other entities

Anomaly Detection
• Statistical models
• What you know you don’t know; what you don’t know you don’t know

Any type, any source
Logs, existing SIEM, etc.
Network data (PCAP)

Source: Gartner (March 2015)
Figure 3 is an overview of UBA technology (also see Note 2).

**Analysis**

**Use UBA to Rapidly Detect Bad Actors and Behavior, Prioritize Security Alerts, Reduce Alert Volume, and Streamline Alert Investigations**

UBA is successfully deployed for three main purposes: finding the “bad guys,” improving alert management and streamlining alert investigations.

At the outset, your enterprise must identify the data sources for UBA, whether they are existing logs, data warehouses, data lakes or network flow data. Many enterprises are focused on narrowing down and prioritizing alerts from data loss prevention (DLP) systems, while others start with alerts and data found in SIEM applications. Still others have an identity and access management focus and use UBA to monitor the use of the access rights (entitlements) they have already assigned throughout their enterprise.

An enterprise should start small – or with a couple of essential data sources, such as one activity source (such as Windows logs) and one user context source (such as Active Directory) – and then expand to include more information to correlate. This is the strategy where Gartner has seen the most success. For example, several enterprises Gartner has spoken with have started by integrating DLP or SIEM, Active Directory, and Web proxy data to yield quick results. Over time, some of these enterprises have then found it useful to integrate information from other monitoring systems, such as advanced threat management (to correlate those alerts) and HR files (to understand an employee’s status with the company). It’s important to be selective about the information fed into UBA so as not to generate too much unnecessary “noise” in the system.

Once user, peer group, and other profiles and baselines are established in the UBA application (which can usually be done with historical data to get a running start), incoming transactions are then compared with them using statistical models and/or rules, and anomalies are detected. Not all anomalies discovered will be malicious behavior, and often administrative “mistakes” in environments and misuse of privileged accounts will be unearthed. The less tuning required and the more “out of the box” a vendor’s analytics run, the better.

Importantly, enterprises should operationalize UBA results by feeding UBA alerts into an existing alert management console (for example, belonging to a broad-scope security monitoring system or SIEM) used by the enterprise to manage security events.

See the Case Studies section for success stories in achieving these objectives.
Use UBA to Strengthen Security for SaaS-Based Applications by Detecting Unauthorized Access and Users

SaaS adoption is moving at a rapid pace. Most enterprises are moving existing applications, such as office productivity, sales and marketing, to SaaS. But along with this transition comes many uncertainties over the security of SaaS processes, applications and data. UBA for SaaS applications is provided by some cloud access security brokers (CASBs) and other niche “UBA only” providers. It can be used to monitor enterprise use of SaaS applications by applying behavioral analytics to SaaS application access and user activity (see Note 3).

One method to accomplish this is to proxy all enterprise traffic to SaaS applications through a CASB that applies UBA to the traffic streams. Other methods that CASBs and other UBA vendors use for gathering SaaS application data before analytics are applied include: using APIs made available by the SaaS providers to access their applications; and deploying agents to endpoints and servers to gather information on access and use of (both on-premises in the case of UBA-only vendors and) SaaS applications.

UBA is giving enterprises much-needed visibility into their employee use of SaaS applications so that they can learn if that access is being misused, abused or compromised. The analytics work the same way UBA works for on-premises applications and should be considered an essential component of securing use of cloud applications.

See the Case Studies section for examples of results in this area.

Use UBA to Detect Automated User Account Takeover and User Account Creation Attacks Against Enterprise Assets

Since late 2014, some Gartner clients have experienced a significant rise in automated attacks, whereby hackers use “bot armies” to run through stolen and subsequently purchased user credentials at various consumer service websites, knowing that a few percentage of them will probably work. According to a Gartner survey several years ago, more than two-thirds of consumers reuse their passwords across sites whenever they can, and Gartner believes this is still the situation.²

This automated criminal cycling through user IDs (generally email addresses) and passwords at various websites, such as online banking or credit card portals, is nothing new. We’ve heard about this from our clients for at least three years now. But these massive automated account takeover attacks have become much more sophisticated and have escalated substantially, according to our clients, with big pickups in such traffic during and right after the 2014 holiday season. Some report that such scripted attacks against large online sites doubled in the first two months of 2015.

The hackers are after anything and everything that has resale or monetary value – usually via resale on popular auction sites – including:

- Credit card or other bank account information stored in digital wallets at online retailers used to make checkouts much faster (so you don’t have to re-enter all of it)
- Digital currencies used for online games that attackers steal or purchase anew with stolen credit cards
- Digital content, such as electronic images
- Travel rewards, such as frequent flyer miles or hotel loyalty points
- Limited editions of high-fashion goods, where fraudsters or other types of scalpers buy them up in seconds or minutes, usually with stolen credit cards, and sell them at up to 450% markups on auction sites
- Stored value accounts at major brands representing favorite food and drink establishments or retailers

These massive account takeover or account creation attacks (hackers often have to create new accounts to get their jobs done or launder the stolen goods or currency through) are undetected by conventional fraud detection techniques that the hackers have learned to avert (see Note 4 for notable trends in automated attacks). Using large bot armies, they often throttle down the speed of their attacks while decentralizing the originating endpoints attacking the site so that they remain under the radar of their victims.
For example, the attackers will have one endpoint across thousands in the bot army try one account credential once or twice in one hour, and this will be repeated by different unique bot endpoints over the course of days or weeks. In this way, traditional fraud detection measures, such as device fingerprinting or velocity checks, will fail to detect the attacks. In other cases, the criminals are going through affiliate networks using popular cloud-based infrastructure services so that the originating IP addresses are indeed legitimate and won’t be suspected or blocked.

Captcha, the traditional solution used for stopping automated attacks, aren’t effective anymore. Readily accessible captcha bypass services will solve as many as 1,000 captchas for $1.39 with 90% accuracy. These outsourced services used by criminals are typically staffed with low-cost workers located in Asia.

UBA as a Solution

UBA can detect most of the automated account takeover and account creation attack activity we see today (see Note 5).

For this use case, UBA is implemented as a cloud-based analytic and fraud detection service that combines the first three layers of Gartner’s five-layer fraud detection framework – endpoint centric, navigation centric and user/account centric – with metadata on devices and IP addresses across millions or billions of transactions at various websites (the more data points, the better). It profiles and segments the population of endpoints and sessions into peer groups and is able to detect anomalous access patterns based on this segmentation, even when the access patterns are “low and slow and distributed” so that they look “normal.”

See the Case Study section for success stories in using UBA to detect mass automated attacks that were designed to elude mainstream fraud detection measures, such as velocity and IP address checking.

Case Study

Below are three live examples of how UBA helped enterprises: reduce the alert volume by consolidating alerts by users; and detect attackers who were about to wreak extensive damage:

- A large national cable network provider was getting half a million alerts a day from its security systems, and they were not prioritized properly. The firm’s staff noticed that an alert was not always a high priority just because a vendor said it was. It was only by looking across different siloed systems (for example SIEM, Web proxy data and advanced threat protection) and correlating their alerts that the firm could figure out which ones were truly high priorities. They used Bay Dynamics UBA software, and after six months, the cable network provider ended up with less than 800 alerts a day, of which the top five or 10 were clearly marked and prioritized.

- A large national grocery chain was concerned it would be the next target of a large-scale data breach against its distributed credit card payment systems. It contracted with Exabeam, a UBA vendor, and believes it stopped what could have been a large-scale attack in its tracks. Exabeam’s UBA software detected a breach of the grocery chain’s network by a remote machine that took over an employee account accessing its VPN and circumvented the grocery chain’s two-factor authentication of employees that was set up to strengthen access controls.

- A large retailer put all its security monitoring and other types of machine data (such as system resource usage) into Splunk and then used a UBA product from Silver Tail Systems (now owned by RSA, the Security Division of EMC) to detect attacks against its Web-based applications. The retailer was able to detect and stop fraudulent attacks against its sweepstakes game and e-commerce sales.
UBA can protect enterprise use of SaaS applications, as seen by customers of Adallom. For example, Adallom detected these security violations:

- An enterprise user accessing an Office 365 cloud service was actually a malware process originating from the underground Tor network.
- Enterprise users accessing Google Apps were actually hackers who also managed to compromise the two-factor authentication process that employees had to use to access the application.

Here are some success stories where customers of NuData Security’s UBA services were able to detect and subsequently stop mass automated attacks:

- A major travel booking company was attacked whereby hackers came through an affiliate network on Amazon Web Services so that the booking company could not block its IP address. The travel company experienced 5,000 login attempts per day using stolen credentials that were successfully blocked using UBA.
- Fraudsters bought gift cards for in-game currencies at a popular gaming site with 2,115 stolen credit cards. They created 563 new user accounts for the attack to buy and store the stolen currency, and they spread the endpoints used to conduct the attack across 501 different IP addresses to hide from geolocation and velocity sensors. However, UBA detected their activity, and they were stopped and thus unable to resell the gift cards on auction sites, as they had planned.

Evidence

1 According to a June 2014 study conducted by North Bridge Venture Partners in conjunction with Gigaom Research and 72 participating organizations, SaaS adoption has more than quintupled from 13% adoption in 2011 to 74% in 2014. For more information on this study, see “Industry’s Largest Cloud Computing Survey Reveals 5x Adoption of SaaS.”

2 Gartner conducts thousands of user inquiries a year on account takeover and account creation fraud. Since late 2014, these inquiries have revealed an uptick in automated attacks that take over existing accounts or create new ones. The victim enterprises also validate the fact that most consumers reuse passwords often across various websites.

3 Laz Demetrious, who at that time was the chief information security officer of a large retailer e-commerce operation, led this project, which yielded hard savings in time and money in 2012 and 2013.

Note 1

Profiling

Profiling users or other entities essentially means building up a history of the user or entity (such as a peer group or application) by monitoring each relevant action taken and then summarizing those actions so that the profile system knows what constitutes normal or typical behavior for that user or entity. Profiling is also referred to as “baselining,” which is the same activity of creating a baseline for a user or other entity, which represents its normal or typical behavior.

Note 2

Categories of UBA Technology

Note that these UBA technology categories are logically grouped into the four categories presented above, which is different from the way UBA was categorized in “Market Guide for User Behavior Analytics,” published in August 2014. Also, UBA for SaaS, a subset of CASB, was inadvertently omitted in the August Market Guide.

Note 3

UBA as a Function of Cloud Access Security Brokerage

CASBs help secure enterprise use of cloud-based applications. In the case of SaaS, UBA is one method of how CASBs can help secure use of the applications. Other methods include authentication, access controls and malware detection, among others. See “Emerging Technology Analysis: Cloud Access Security Brokers.”
Note 4  
**UBA for Human (Nonautomated) Attacks**

UBA is also successfully used to detect human (nonautomated) attacks that create new user accounts or take over existing ones. See the discussion on Layer 3 (user-centric fraud detection techniques) as outlined in “Market Guide for Online Fraud Detection” and “The Five Layers of Fraud Prevention and Using Them to Beat Malware.”

Note 5  
**Notable Trends in Automated Attacks**

In summary, here are some of the most notable trends in automated attacks:

- Use of widely distributed scripted attacks that emulate full device characteristics; that is, a full Web session with a modern browser, making it harder to detect using traditional device identification techniques.

- Circumvention of velocity checking by spreading account attacks over many IP addresses and accounts. The average online retail attack will use an IP address only 2.25 times now before moving on to the next IP address. Likewise with accounts, a single account is rarely used for more than two purchases.

- Matching the geolocation of an IP address to the location of a credit card billing address on credit card purchases, eluding common fraud detection techniques.

- Rising use of cloud-hosted solutions to launch account takeover attacks in order to evade IP address checks used to detect fraud.

- Account takeover growing as the preferred method for taking over payment instruments, as opposed to credit card cycling for fraudulent purchases. This trend will no doubt continue as more e-commerce players offer consumers digital wallets for storing their payment instruments, making it easier and faster to check out.

Source: Gartner Research, G00270142, Avivah Litan, 4 March 2015
About NuData Security:

NuData Security uses behavioral analysis to prevent fraud online, protecting businesses from brand damage and financial loss caused by fraudulent or malicious attacks.

NuData Security monitors behavior continuously: across every page, and every visit. Fraud is a chain of events, so, by analyzing every visit NuDetect sees the beginnings of fraud the moment it starts - before the transaction.

Businesses achieve improved customer trust by keeping their online brand safe. Reduced costs are realized by lowering reliance on expensive and inefficient security controls such as manual reviews and remediation. The NuDetect platform also allows firms to accept more transactions, with a greater confidence that they will not result in fraud. Operating passively, there is no impact to the user experience.

Head office:
999 Canada Place - Suite 550,
Vancouver, British Columbia,
V6C 3T4 Canada

Phone: +1 (604) 800-3711

Email: bizdev@nudatasecurity.com

Website: www.nudatasecurity.com

LinkedIn: www.linkedin.com/company/nudata-security

The Future of Fraud Prevention: User Behavior is published by NuData Security. Editorial content supplied by NuData Security is independent of Gartner analysis. All Gartner research is used with Gartner’s permission, and was originally published as part of Gartner’s syndicated research service available to all entitled Gartner clients. © 2015 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner’s endorsement of NuData Security’s products and/or strategies. Reproduction or distribution of this publication in any form without Gartner’s prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner’s Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity” on its website. http://www.gartner.com/technology/about/ombudsmen/omb_guide2.jsp.