GURUCUL
PREDICTIVE SECURITY ANALYTICS

A BUSINESS CASE FOR **BEHAVIORAL ANALYTICS**

WHITE PAPER

Introduction

What is Behavioral Analytics

In a world in which web applications and websites are becoming ever more diverse and complicated, running them effectively has become equally complex. In the incredibly competitive world of the contemporary Internet, ensuring that an e-commerce business remains ahead of rivals required utilizing a series of procedures and tools.

Within this field, behavioral analytics has become particularly important, and in addition the technology has also frequently been applied to the analysis of online games and other online systems which necessitate mass participation.

Behavioral analytics can essentially be seen as a branch of business analytics. The difference between the two is really that business analytics has an extremely wide focus, while behavioral analytics is a subset with a very specific and targeted focus. Behavioral analytics enables companies to draw together two or more seemingly completely unrelated data points, and identify patterns, draw conclusions and predict trends for the future.

This phenomenon is particularly intended to take a holistic view of data, ensuring that individual data points are collated in order to explain to a business not only what, but also how and why a particular trend is occurring.

Behavioral analytics is frequently associated with Google Analytics, and it is becoming a critical way for businesses to glean value from their e-commerce platforms, along with other similar applications. Indeed, without applying behavioral analytics accurately, it is almost certain that any business will put itself at a significant commercial disadvantage.

The case for adopting behavioral analytics can be made by assessing some of the issues commercial companies on the Internet typically face. But first it is valuable to look at some of the benefits of behavioral analytics.

Benefits of **Behavioral Analytics**

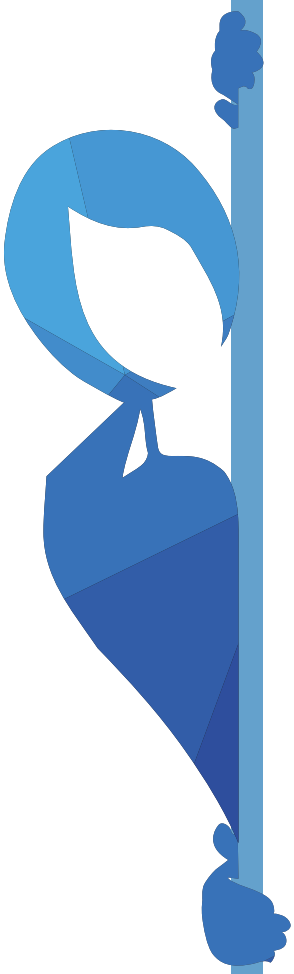
Behavioral analytics revolves around sophisticated pre-built algorithms which are able to capture and analyze human interaction and behavior in real time. This can be utilized to both assess customer behavior, and also to root architecture to match customers with the most suitable employee, for example.

Essentially, behavioral analytics systems create a huge and evolving database of information in real time, which can be tweaked according to business preferences. Behavioral analytics has particularly provided value to businesses when assessing such metrics as customer satisfaction, and when employed in its best possible form, behavioral analytics can provide insight into such critical data as future purchase likelihood.

Data acquired via behavioral analytics can be utilized in order to improve operational performance going forward, and also for such facets of business as proactively communicating with customers.

The collaboration between behavioral analytics systems and the cloud has enabled them to gather, collate and analyse even more data, as cloud computing makes immense collection and storage of data feasible. In this context, behavioral analytics can enable businesses to address problems that would otherwise be insoluble.

IP Theft



One of the issues that all companies must deal with in the contemporary era is the danger of fraud such as IP theft. Security is quite obviously a major issue for any Internet business today, and this has been highlighted by some particularly high profile breaches of security in recent months and years.

Of course, there is already a significant amount of technology available to assist you in dealing with this. But the very fact that it has become such a major issue would indicate that existing systems are not always doing the job for which they are designed.

The best way of dealing with this issue is to nip the problem in the bud before it materializes, and it is this which behavioral analytics promises to achieve. Security is a critical aspect of any business, affecting customers, clients, members and employees, and your organization as a whole. But not only does security impact upon all of these people, but sadly all must be considered a security threat.

The NSA and GCHQ revelations related to Edward Snowden have made this clear, and there have been other high profile examples of IP that in the news recently. While opinions are divided on the Snowden case, and not all insider incidents are malicious, the importance of addressing this threat must be understood by all businesses.

Considering the vast amounts of information and data that modern behavioral analytics systems are able to gather, it then becomes plausible to detect suspicious activity which is significantly inconsistent with established normal behaviour on your network. This will make the identification of fraudsters considerably easier, preventing them from completing fraudulent payments and others stealing sensitive personal information and IP.

The threat of this should not be underestimated. There have been numerous examples of hackers breaking into major retail systems, and in some cases they have been able to steal literally millions of credit card numbers. Obviously this is extremely embarrassing for any company, not to mention financially painful, thus reacting to such activity before it occurs is always the sensible option.

IP fraud is notoriously difficult to measure, but what is known is that it already takes place on a massive scale. There is a huge amount of money to be made through such fraudulent activity, and naturally this attracts very ambitious and organized criminals. According to recent estimates, IP fraud accounts for financial losses equal to $650 billion every year worldwide. Other Estimates related to small geographical areas suggest that the Arab world sees $50 billion of IP fraud a year, while the UK alone experiences the equivalent of $15 billion annually.

Thus, the importance of deploying protection against this risk which protects your company against the widest array of new and emerging threats, and identifies what other solutions miss, is of critical importance.

Brand Damage

The amount of brand damage that can be caused by IP fraud is quite exceptional. And what complicates the issue is that such activity can be tied to data breaches related to insiders. This leaves companies very vulnerable towards such major instances of fraud as credit card theft, or the exposure of sensitive personal data. Naturally when such information is lost, it can cause significant and often irreparable damage to the reputation of a company.

The extent of insider fraud which is carried out may surprise some individuals and companies, but this is a widespread phenomenon. Studies have found that the average organization has in fact been exposed to over 50 employee-related incidents of fraud each year. Privileged users are able to cause significant problems to a system, and the long-term consequences of this for a business can be extremely drastic.

It has also been reported that rogue insiders who steal data or conduct fraudulent transactions are responsible for financial loss in around three-quarters of organizations that have experienced a problem with fraud. This can amount to extremely innocuous activity such as merely accessing private customer data without authorization. Similarly frequent access can signal a breach in security, and this is where behavioral analytics can assist in assessing and identifying where behavior is inappropriate or suspicious.

Yet despite this apparent threat, organizations often fail to take significant security measures, and indeed it is not at all uncommon for extremely unhelpful procedures to be undertaken on a regular basis. For example, security experts have observed that senior executives frequently share security credentials with lower ranked members of staff, which is a fundamental security breach in itself. When such activity takes place on a widespread basis, obviously the chances of something going badly awry are magnified.

Unfortunately, although conventional technology exists to attempt to address this issue, typically it is unfortunately pretty lacking. Data loss prevention, database activity monitoring and log management can play a part in detecting suspicious activity, but surveys have indicated that they are often inadequate in terms of detecting a malicious insider determined to keep his or her actions covert.

Two more trends are making this issue increasingly difficult for organizations to deal with. Firstly, employees are using a wide variety of devices to tap into company networks in this day and age. Increasingly, businesses need their members of staff to have access to work-related information when they are outside work premises, and the types of devices being used to utilize this data continue to expand. Additionally, on-site technology such as Bring Your Own Device further muddies the waters.

Additionally, according to a study carried out by Ponemon Institute - an organization which conducts independent research on privacy, data protection and information security policy - the time taken to resolve fraud is increasing significantly. The report found that the average instance of fraud will take nearly 90 days to resolve before the root cause of the incident is determined. Increasingly, businesses must rely on highly specialized and expensive teams of forensic experts to conduct independent and highly technical investigations, and this may often be followed by internal auditing.

The need for a solution to this problem couldn't be clearer, and thankfully behavioral analytics provides this remedy.

Gurucul Behavior Analytics and Risk Analytics

Gurucul Risk Analytics (GRA) is an identity-centric behavioral risk intelligence platform that provides real-time contextual and situational awareness for user access and activity. Central to the GRA portfolio is Actionable Risk Intelligence; a flexible and sophisticated system which provides an inordinate amount of customer data via its state of the art behavior profiling algorithms.

Over a period of time, Gurucul has created an innovative platform based upon Human Behavioral Risk Intelligence metadata. The powerful software package which has been developed by Gurucul continually monitors behavior and identifies possible risk patterns. Not only does it do this in real time, but it is also able to actually project such patterns before they even occur.

The GRA suite is the ideal way to mitigate against threats which are leveraged against intellectual property. GRA expands the value of existing Security Information and Event Management logging, DLP and other security systems by continually cross-correlating source data activity with people and system access and information.

This state-of-the-art approach insures that GRA can deliver full 360° risk context that business, security and technology users can utilize to visualize and take appropriate action. The powerful and sophisticated algorithms developed by Gurucul ensure that insider threat data can be analyzed and understood extremely rapidly. And GRA's open Hadoop backend data repository is extremely scalable, and can potentially store Petabytes worth of data.

Not only is this a sophisticated system to begin with, but the GRA platform in fact utilizes self-learning algorithms which are able to create risk patterns which lead to predicted, actionable risk intelligence. In effect, the longer that you run the Gurucul system, the more effective it becomes, as it literally teaches itself as it goes along. The more data loaded into the system, the better your defense against IP fraud and insider threats.

GRA greatly enhances the risk, threat, and compliance posture of an organization by applying a unique identity-centric approach of correlating identity, activity, and access information to provide actionable data and prioritized alerts. This is the most sophisticated system for risk profiling in the entire industry, and one that is a huge boon for any business in a world characterized by a morass of insider and external cyber threats.

About Gurucul

Gurucul is dedicated to transforming the cyber security landscape using machine learning, intelligence-driven, big data security analytics. Using identity as a threat surface, Gurucul provides Actionable Risk Intelligence™ to protect against targeted attacks and under-the-radar cyber campaigns. Gurucul is able to proactively detect, prevent and deter advanced insider threats, fraud, and external threats to system accounts and devices using sophisticated self-learning, advanced behavior and anomaly detection algorithms.

Gurucul is backed by a strong advisory board comprising of fortune 500 CISOs, world renowned experts in government intelligence and cyber security. The company was founded by seasoned entrepreneurs with a proven track record of introducing industry changing enterprise security solutions. Their mission is to deliver rapid results to any organization that desires to protect its intellectual property, regulated information, and brand reputation.

GURUCUL | 5959 W. CENTURY BLVD. SUITE 1111. LOS ANGELES. CA 90045 | 213.373.4878 | INFO@GURUCUL.COM | WWW.GURUCUL.COM