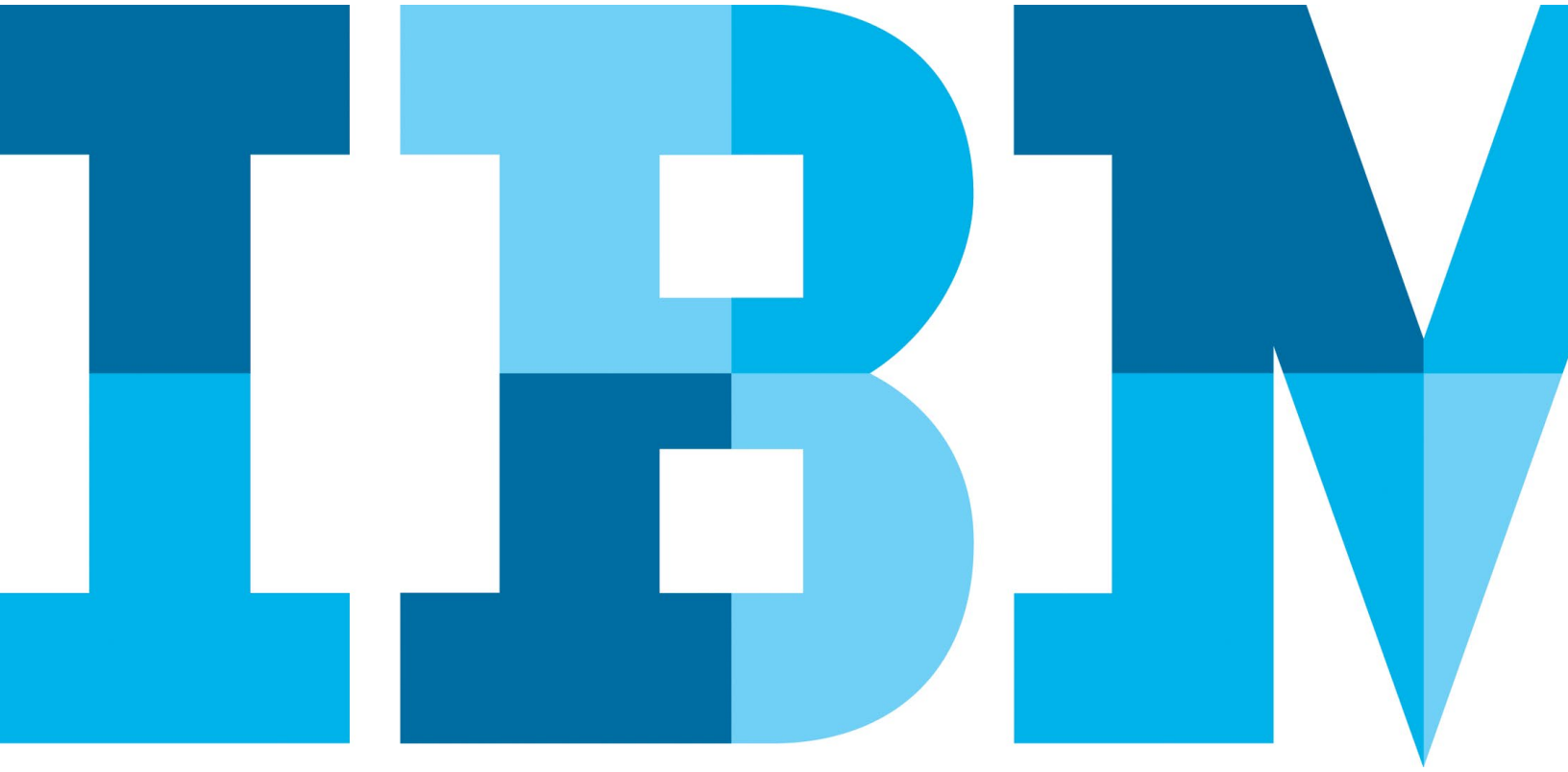
Security

Thought Leadership White Paper

October 2016

Shifting the balance of power with cognitive fraud detection



IBM

Contents

Introduction

Often in battle, there is a pivot point when the good guys gain an upper hand to overcome their adversaries. For financial service providers battling fraudsters, that pivot point has arrived with cognitive fraud detection from IBM Trusteer.

Traditional fraud protection solutions, such as complex device ID, malware detection, transaction monitoring and biometric systems, all offer some level of protection in helping financial service providers confirm that the "customer" logging into their online banking system is who they say they are.

However, their individual reach is limited and provides a slice of the data needed. As a result, security analysts are often besieged, sifting through false positives and trying to assess the implication of the data manually. It's no wonder that many security professionals feel that fraudsters are "outstripping their defenses."[1]

Cognitive fraud detection means using machine learning to understand data—both unstructured and structured—at a speed and scale like never before. It makes sense of the data and learns with each interaction, so it gets smarter every time. And because it's transparent to end users, it preserves the user experience while making it harder for fraudsters to circumvent.

By using cognitive fraud detection across different security layers, financial service providers can detect fraud more accurately and quickly than ever before as well as better preserve the user experience.

In this whitepaper, you'll learn about three key cognitive fraud detection capabilities that IBM® Trusteer® solutions deliver—behavioral biometrics, behavioral analytics and adaptive intelligence—to help battle fraud even better and give financial service providers an upper hand in the constantly evolving threat landscape. These capabilities are fully integrated and include proprietary patented cognitive technologies developed with IBM Research labs.

Gaining continuous and transparent detection with behavioral biometrics

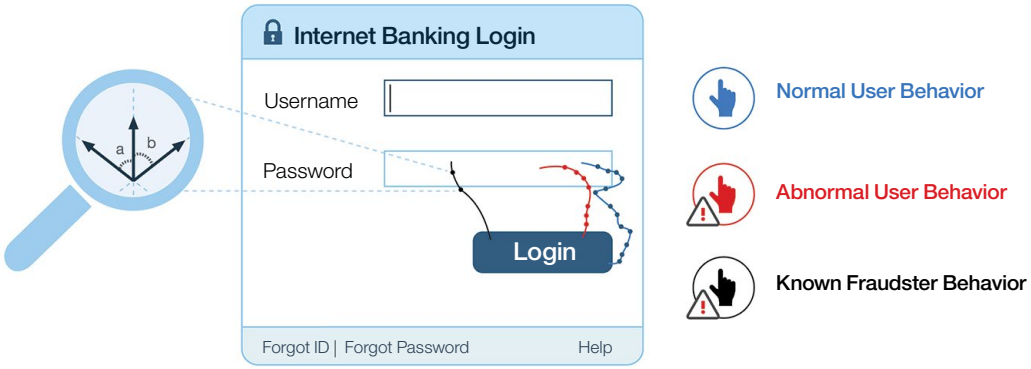
The basic goal of fraud detection is being able to uncover in real time when fraudsters impersonate legitimate users. However, to do so, one needs to be able to differentiate an account user's "normal" digital behavior from abnormal behavior.

IBM Security Trusteer Pinpoint™ Detect now incorporates behavioral biometric capabilities to provide dynamic, context-aware identity analytics that helps improve detection while preserving the user experience.

Built in conjunction with IBM Research labs, the solution's behavioral biometric capability uses machine learning to create a model based on patterns of mouse movements—from login through the entire application flow.

What angle does a user's mouse approach the login box? What direction does the user typically move the mouse? Mouse trajectory, velocity, curvature, jerk, and more are all analyzed.

The platform understands these subtle mouse movements in context and meaning, at astonishing speeds and volumes. It continuously and seamlessly learns user behavior across hundreds of millions of sessions and analyzes current online activity to detect unusual behavior across different devices, even comparing it against observed behavior of known fraudsters for even stronger evidence. If either abnormal user behavior or known fraudster behavior is detected by the platform's sophisticated algorithms, Trusteer Pinpoint Detect provides access management systems and security analysts with a recommended action in real time along with the detailed reasoning and session details so an action can be taken.



IBM Security Trusteer Pinpoint Detect incorporates cognitive fraud detection with the introduction of behavioral biometric capabilities

As a result, service providers can verify users in real time, across devices, with greater accuracy while optimizing strong authentication layers to improve user experience. The passive and seamless manner of behavioral biometric analysis also makes it much more challenging for fraudsters to circumvent, as it's hard to fight what you don't see.

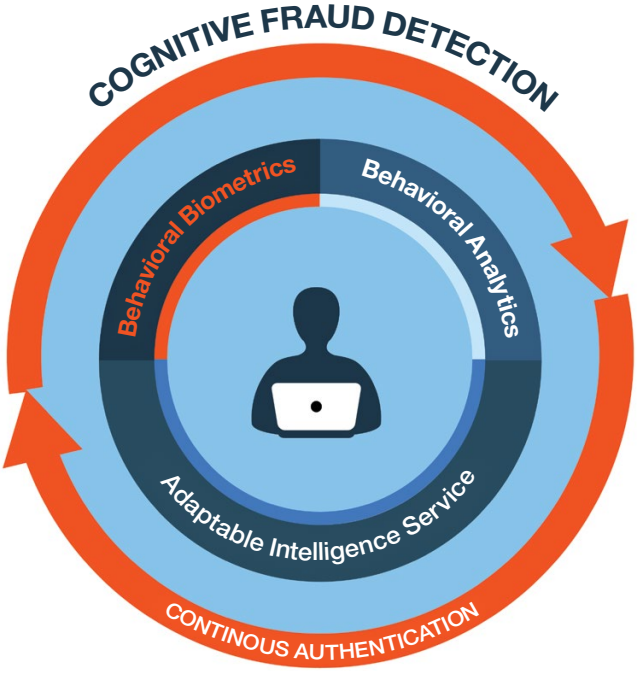
Completing the picture with behavioral analytics

While behavioral biometrics provides a strong form of user authentication verification with the lowest end user impact, there are more pieces to the puzzle.

In fraud detection, the quantity and quality of the data being analyzed is critical. More qualitative data allows for even better differentiation between fraudulent and legitimate activities.

Therefore, in addition to behavioral biometrics analyzing patterns of mouse movements, Trusteer Pinpoint Detect also analyzes many other behavioral indicators, including device activity, transactional data and geolocation data, on every access to the digital banking application, to understand user, device and session anomalies across channels.

It correlates these behavioral analytic insights with the behavioral biometric results, as well as other critical fraud indicators, such as phishing attacks, malware infections, compromised credentials, remote access Trojans (RATs) and advanced evasion methods, to help determine, with a high degree of certainty, both the nature of a threat and the potential risk.



Cognitive fraud detection from IBM Trusteer

With this rich combination of risk data and pre-integrated logic that makes sense of it all, applications can adapt their logic in real time to effectively manage risk and make context-aware decisions to allow, restrict or step up authentication during an end user's journey.

Uncovering evolving threats earlier with adaptive intelligence

Effectively fighting fraud has a lot to do with the speed of detection, investigation and countermeasure deployment. IBM's global threat intelligence network gathers threat intelligence from millions of end user endpoints along with other sources. Armed with this intelligence, IBM Trusteer threat analysts, research and investigate industry and organization-specific threats, and then adapt defenses automatically without additional effort of the financial organization.

To facilitate this work, IBM's dedicated Research and Development team now uses an adaptive intelligence system to not only detect user anomalies, but also understand and prioritize evolving threats.

Leveraging machine learning capabilities, this cognitive system synthesizes new threat patterns and defense logic by analyzing millions of digital banking sessions that flow daily to its threat network. For example, the system can rapidly cull through a full day's worth of recordings (millions of sessions)—an amount that simply couldn't be handled by humans-—to uncover and alert IBM security researchers of web injections as they appear.

Conclusion

By integrating cognitive capabilities across its fraud protection and service offerings to enable behavioral biometrics, behavioral analytics and adaptive intelligence, IBM Trusteer is helping financial service providers shift the balance of power and gain an upper hand in the battle against fraudsters.

With the ability to analyze unstructured security data at a speed and scale not possible by humans, and continuously learn from the data, IBM's cognitive fraud detection capabilities help financial service providers more accurately and transparently determine if a customer is who they say they are and detect new online banking threats as they emerge.

By providing a multilayered approach that correlates a wide range of data into a comprehensive risk assessment, IBM can help reduce the number of false positives organizations face so they can respond more quickly and efficiently.

For more information

To learn more about cognitive fraud detection, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/trusteer

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

Please Recycle

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment" IBM Center for Applied Insights, December 2014. P.5
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03061USEN

WGW03249-USEN-00