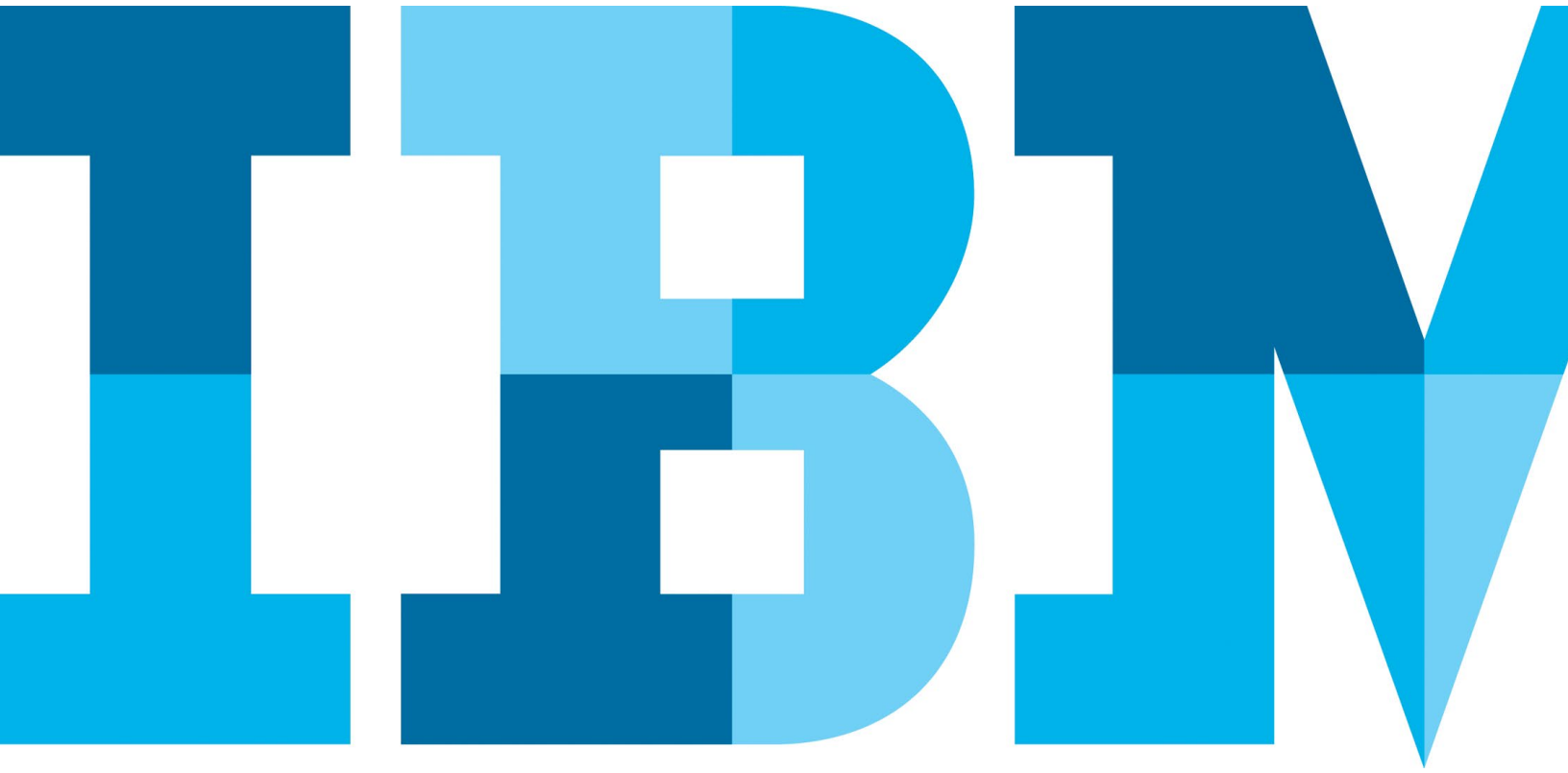
Security
White Paper

February 2017

Cognitive fraud detection fuels adaptable intelligence



IBM

Contents

2 Introduction

2 A cognitive approach for a continually evolving landscape

3 Global threat intelligence helps uncover new threats

4 Expert research and development turns intelligence into actionable insight

4 Adaptable technology helps deliver seamless customer experiences

5 Conclusion

5 For more information

Introduction

As financial organizations launch new digital services and work to deliver better customer experiences, cybercriminals are finding new ways to circumvent security measures—an issue that can ultimately impact the success of digital transformations.

In fact, malware tactics have evolved to incorporate a wide range of capabilities that enable cybercriminals to bypass static endpoint protection systems, initiate authenticated online banking sessions, and illicitly transfer money—often without either the customer's or the bank's knowledge.

Not only has malware become more sophisticated, but so have cybercriminal networks. Nowadays, underground forums operate much like legitimate online marketplaces. Vendors sell their "products"—from malware coding and engineering services, to ready-to-use malware toolkits, all the way to comprehensive Fraud-as-a-Service (FaaS) solutions.[1]

The outcome of this evolution is the emergence of hundreds of new malware configurations on a daily basis. As a result, organizations need to protect themselves and their customers against a growing number of threats and an increasing number of attacks—all while delivering stellar customer experiences.

Because of the growing number of legitimate digital sessions and the variety of new malware configurations that are released daily, identifying malicious sessions that are hijacked by malware often requires a substantial amount of manual analysis and intervention. The amount of manual investigation required has become so significant it has become nearly impossible for security teams to keep up.

Being able to tackle this challenge requires cognitive capabilities, such as machine learning and graph analysis, that can classify large amounts of unstructured data from millions of sessions and activities, identifying the risky ones, and flagging those that require further manual analysis.

In this whitepaper, you'll learn how IBM® Trusteer® uses cognitive fraud detection capabilities with proprietary threat intelligence to deliver adaptive intelligence that helps financial organizations combat today's evolving threats while building new and better customer experiences.

A cognitive approach for a continually evolving landscape

Overall, a sustainable fraud protection system that addresses the evolving threat landscape and helps banks confirm user digital identities requires three fundamental features:

1. Global threat intelligence, infused with cognitive fraud detection, that helps uncover new threats anywhere in the world as they begin to unfold, and includes immediate visibility and context across all digital channels.

2. Expert research and development, fueled by cognitive computing, that can rapidly make sense of new threats and marketplace changes, immediately assessing which threats are most damaging, and rapidly building and deploying relevant countermeasures as needed.

3. Adaptable technology that makes use of cognitive fraud detection capabilities to more rapidly uncover fraud, and is flexible enough so countermeasures can be deployed without bank staff support.

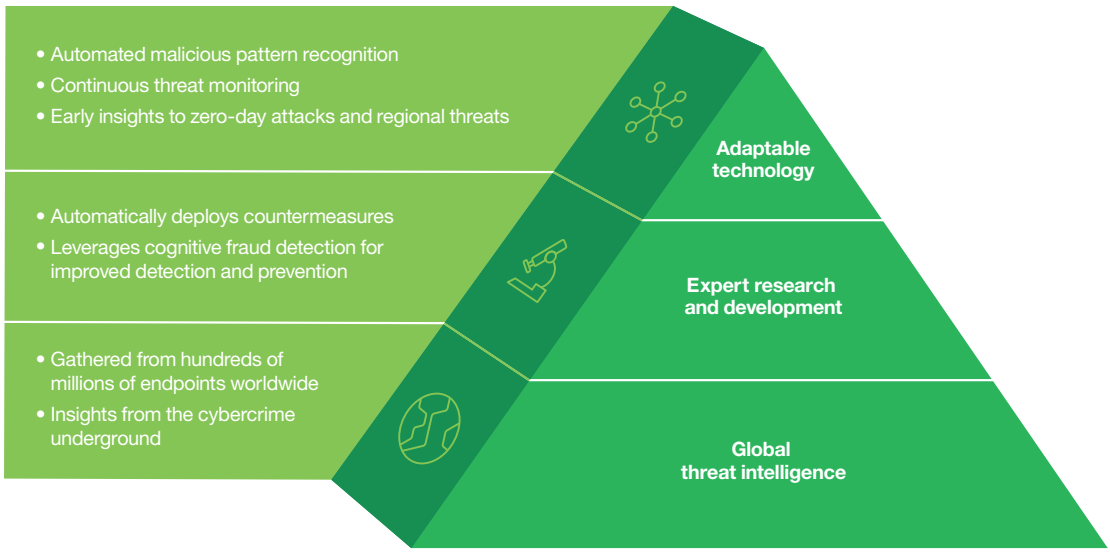
Important considerations when examining solutions include the provider's global footprint and operational track record to demonstrate that it can effectively **detect** changes in the threat landscape, **analyze** them, **build** and **deploy** the relevant countermeasures, and sustain the effectiveness of its security controls over time—all with minimal impact to the organization and its customers.

Global threat intelligence helps uncover new threats

Malware and attack techniques are continuously evolving and being able to detect zero-day threats demands cognitive intelligence gathering.

With IBM Trusteer solutions, organizations gain access to a near-real-time intelligence network that tracks shifting attack tactics and malware across myriad digital interactions and devices to provide insight from IBM X-Force® research, underground forums, and other sources.

This global threat intelligence serves as the foundation for IBM Trusteer automated threat protection capabilities and is used by IBM Security experts to help develop and deliver new protections for organizations like yours. The continuous flow of fresh intelligence, infused with a cognitive fraud detection capability, not only helps researchers uncover potential new threats, but also helps boost fraud detection, while tracking threats and hot spots as they migrate from region to region, and country to country.



Expert research and development turns intelligence into actionable insight

How is this threat intelligence turned into actionable insight that can help stop fraud before it's committed?

At IBM, a research and development (R&D) team of security experts scrutinizes the threat intelligence as it arrives from Trusteer-protected endpoints, underground forums, and other sources. As a result of IBM's global footprint, this can translate into millions of suspected events to be analyzed, something that cannot be done manually in a timely fashion.

To facilitate this work, IBM's dedicated R&D team uses an adaptive intelligence system that leverages cognitive fraud detection capabilities. This system helps to not only detect user anomalies, but also understand and prioritize new and evolving threats, flagging suspicious events that should be further reviewed by experts.

This automated malicious pattern recognition tool uses machine learning and graph analysis to analyze the millions of digital banking sessions that flow daily to IBM's threat network, at a speed and scale like never before, classifying and synthesizing new threat patterns and defense logic.

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 new web injections as they appear.

Because cognitive systems not only make sense of the data, but also learn with each interaction, they get smarter every time, providing IBM Security experts early insight to help detect zero-data attacks, understand regional trends and help accelerate time-to-protection.

As new threats are discovered, the team rapidly develops countermeasures. It's a 24x7 operation dedicated to helping keep companies ahead of the latest threats. Because the R&D team applies a rapid-release-cycle development methodology, it can deploy new defenses in hours or days, rather than weeks.

Adaptable technology helps deliver seamless customer experiences

Once new protections are created, how are they made available? Traditionally, incorporating the necessary updates to already deployed software can take IT personnel considerable time—time your staff doesn't always have.

IBM Trusteer software delivers adaptive protection layers that can be rapidly configured and updated by IBM R&D staff. New countermeasures are deployed back into Trusteer solutions without any intervention by security staff and without noticeable impact to banking customers.

Bank security personnel don't have to watch the marketplace. They don't have to update their criminal databases. They don't have to request product enhancements. New protections are delivered via a software-as-a-service (SaaS) model, and applied to the relevant Trusteer solution accordingly.

To further enhance detection and prevention capabilities, IBM Trusteer is also incorporating cognitive fraud detection capabilities within its products to help financial service providers detect fraud more accurately and quickly than ever before.

For example, machine learning capabilities built into IBM Trusteer Pinpoint™ Detect can help service providers verify users are who they claim to be in near-real time, across devices. The platform understands subtle mouse movements in context and meaning, at astonishing speeds and volumes, as users log into online banking sites.

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, 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 near-real time along with the detailed reasoning.

Conclusion

Launching new digital banking services creates new business opportunities, but also opens financial institutions to new risk. Getting ahead requires the most relevant threat intelligence and adaptability. The more threat intelligence you have, the more effective you can be. The more dynamic your security solutions, the faster you can block new threats.

An adaptable, intelligence-driven fraud detection and prevention strategy can help deliver a more efficient solution.

IBM's global threat intelligence network, infused with a cognitive fraud detection capability, continually tracks shifting attack tactics and malware as they appear.

Expert research and development, fueled by cognitive computing capabilities, turns this intelligence into actionable insight to help organizations stop fraud before it's committed. By leveraging machine learning, Trusteer systems can analyze new and unknown fraud patterns, prioritize on the most pressing risks, and respond with greater confidence and at greater speeds.

Finally, adaptive protection layers and cognitive fraud detection capabilities built into Trusteer solutions can help financial service providers quickly uncover and protect against fraud.

Through the use of cognitive fraud detection capabilities with proprietary threat intelligence, IBM Trusteer delivers the adaptive intelligence you need to help assess each user's identity throughout the entire digital journey. By doing so, you'll be better able to protect your customers while delivering new digital services and stellar customer experiences.

For more information

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

© Copyright IBM Corporation 2017

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

IBM, the IBM logo, ibm.com, Trusteer, Trusteer Pinpoint, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.

Please Recycle

[1] Richard Starnes, "The Dark Net's Fraud as a Service (FaaS)," CSO from IDG, Feb. 2, 2016. Retrieved from: http://www.csoonline.com/article/3028122/security/the-dark-net-s-fraud-as-a-service-faas.html

WGW03104-USEN-01