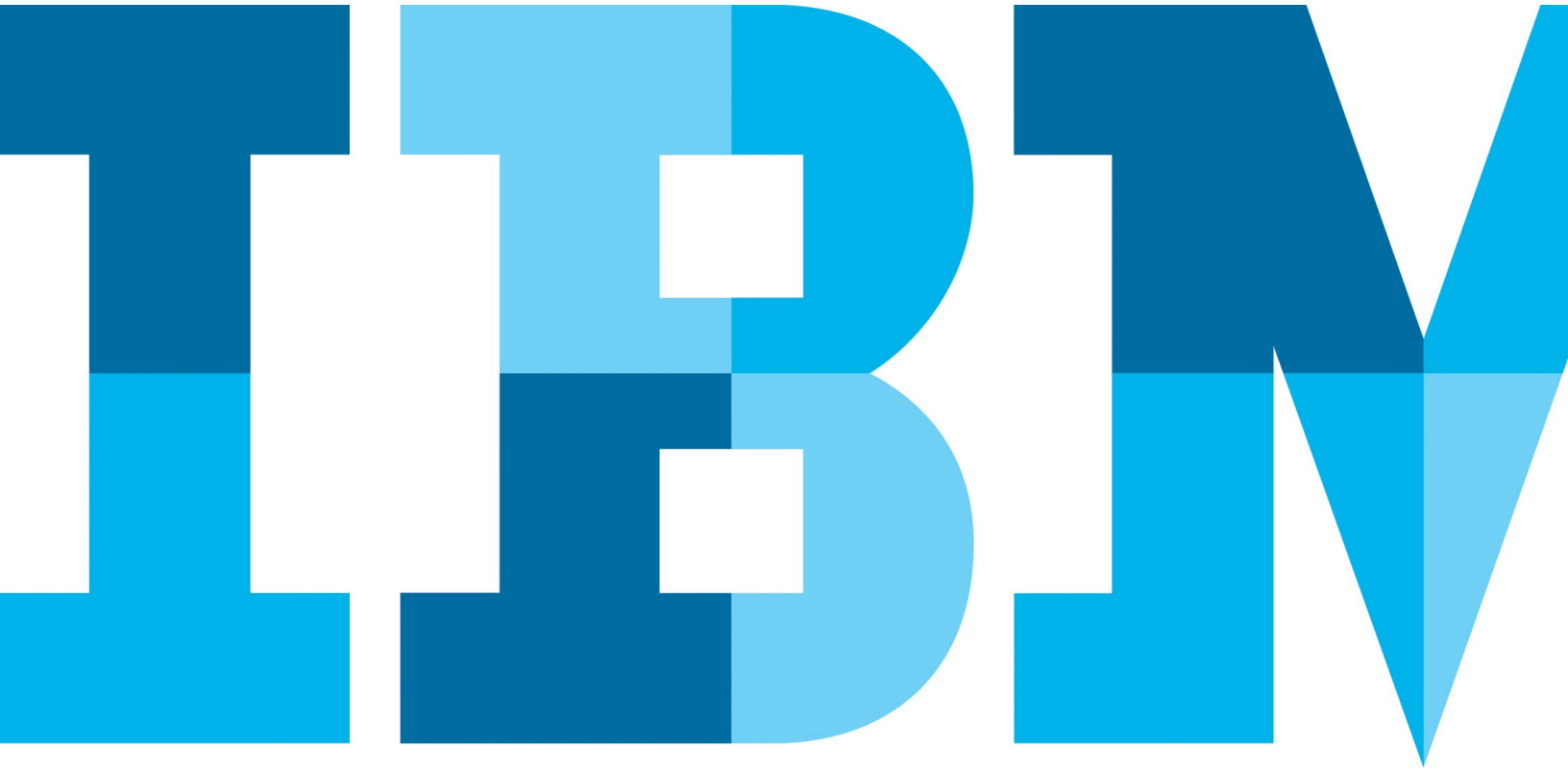
May 2017

Adapting to new threats

Policy engine delivers visibility, control and flexibility to help you rapidly build and deploy countermeasures



IBM

Contents

Introduction

In helping your organization detect, analyze and take action to prevent fraud, IBM® Trusteer Pinpoint™ Detect assesses risk and identifies recommended actions—whether to allow, authenticate, or restrict a user's activity.

The solution analyzes a wide range of data and global intelligence—drawing from insight gained from advanced analytics and patented machine learning. These advanced technologies are used to protect each application on an ongoing basis, based on the analysis of the specific threats targeting it.

But in determining what to do next, we recognize that many fraud teams seek full control over the models they use when evaluating potential risk.

Perhaps you'd like to apply new policies using additional data sources. Or maybe your fraud team has uncovered a specific attack pattern that you need to rapidly incorporate in your policies.

IBM delivers a "white box" approach to analytics, giving organizations visibility into models, control to adapt models independent of platform release cycles, and flexibility to apply new countermeasures rapidly without advanced skills.

Three important considerations when it comes to customizing policies

There are three key issues that many banks consider when it comes to customizing policies.

First, what risk indicators will you have access to? The more insight you have, the more context you have.

Second, how fast and easy is it to create, test and implement new policies? Do your fraud analysts need advanced data science skills? How long will it take to put new policies into production?

Finally, how will you manage the platform? What IT resources will you need?

IBM Trusteer Pinpoint Detect can help you address these concerns.

Policy Engine Differentiators

Rapid deployment of new policies

Hundreds of pre-calculated risk indicators

Visibility into the IBM® Trusteer® crime logic

No need for additional IT resources

Simple and intuitive interface

Extensive insight to help improve accuracy of detection

The more context fraud analysts have, the more accurate fraud detection can be, and the fewer false positives generated.

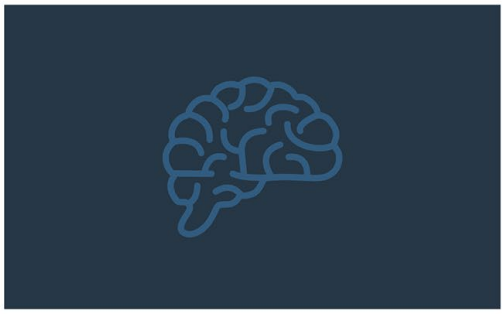
With Trusteer Pinpoint Detect, bank analysts can customize policies using comprehensive data similar to what IBM uses to detect fraud for its clients and deliver recommended courses of action. Analysts can incorporate hundreds of different data elements, including evidence-based insights such as:

- Do the end user's mouse movements match their typical mouse movement behaviors?
- Do the end user's mouse movements match known fraudster behavior?
- Is the end user using a remote access tool?
- Is the mobile device jailbroken?
- Is there malware present on the endpoint?
- Is the IP address a known fraudster address?
- Did the user input their credentials on a phishing site?

From comparing mouse movements in real-time against learned user behavior and known fraud patterns to providing in-depth behavioral indicators to delivering insight on attack patterns gathered from millions of endpoints globally, Trusteer Pinpoint Detect provides comprehensive context to help your staff rapidly develop, test and deploy new countermeasures. In fact, the platform can process hundreds of rules based on hundreds of different data elements in just milliseconds.

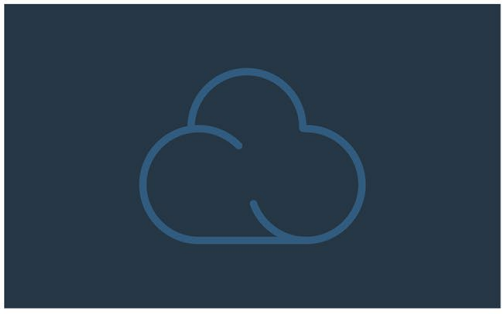
IBM® Trusteer® Pinpoint™ Detect Policy Engine

Extensive Insight
Hundreds of pre-calculated risk indicators out-of-the-box:
- device intelligence data elements
- user behavior anomalies
- advanced behavioral biometric indicators
- global intelligence on attack patterns



Machine Learning and Advanced Analytics
Predict or devise new rules
Suggest changes to tune existing rules

Easy-to-Use Technology
Fast execution time
Simple and intuitive user experience
Comprehensive built-in reports:
- champion-challenger
- rules efficacy
- management reports



Managed Service
Turnkey software-as-a-service (SaaS) platform
No additional license required
Rapid deployment without need for IT resources
Constantly updated content in response to threats and via scheduled updates
Pre-deployed policies adopted to each company's topology

Machine learning and advanced analytics to help empower fraud analysts

At IBM Trusteer®, we believe that solving our clients' challenges starts by empowering them.

Fraud analysts can use the Trusteer Pinpoint Detect pre-packaged rules or they can create their own logic using the default policy rules as a reference. The tool is simple and intuitive to use, and teams with fraud strategy experience can adjust the system at will, changing policies rapidly to help them identify and defend against emerging fraud risks.

Additionally, using advanced analytics and machine learning, the policy engine can help predict or devise new rules and suggest changes to existing rules to help minimize false positives. For example, the machine learning algorithms can identify if a new rule that an analyst is testing is causing a high false positive rate.

Comprehensive reporting and control

The Trusteer Pinpoint Detect policy engine is designed to help analysts not only quickly customize policies, but also more easily test and measure new policies.

Comprehensive built-in reports, such as champion-challenger, rules efficacy and management reports, help analysts see which policies are most effective and identify opportunities for improvement.

A rules hierarchy structure enables analysts to create a hierarchical library of rules that can be applied on multiple or individual applications so there is no need to duplicate code.

Additionally, an intuitive user experience enables analysts to deploy new rules to production in minutes so they can rapidly move from creation to test to production.

A SaaS-based approach helps simplify management

With the continued growth in cybercrime, organizations need to stay focused on stopping fraud, not managing fraud platforms.

An important element of our solution is helping simplify management and reducing the operational hassles that all too often come with technology solutions.

Using the Trusteer Pinpoint Detect software-as-a-service (SaaS) offering, fraud teams can gain all the flexibility to create or modify new rules with none of the hassles. There are no servers to purchase, or systems to manage. No IT support and related costs to plan for.

The Trusteer Pinpoint Detect policy engine is simply delivered via the cloud, in accordance with IBM data handling guidelines, so all you need to focus on is fraud prevention, not on how to maintain your fraud solution.

Conclusion

As you expand your organization's digital services, the ability to more accurately assess which user activities to allow, which to restrict, and which require more investigation will become even more important.

IBM Trusteer Pinpoint Detect offers fraud analysts the flexibility to rapidly customize, test and deploy new fraud policies.

The platform delivers the following key capabilities:

- Extensive insight into evidence-based indicators and other critical data elements to help analysts improve the accuracy of detection, along with the ability to consume additional data sources as needed
- The ability to develop rules using a simple and intuitive interface
- High performance to process hundreds of rules in milliseconds and deploy new rules rapidly
- Comprehensive reporting and administrative capabilities to help analysts better test and measure the effectiveness of new policies
- Machine learning algorithms that can help analysts devise new rules to reduce the number of false positives
- Simplified management to help organizations reduce operational costs

With Trusteer Pinpoint Detect, your organization can gain control over the models and decisions, while benefitting from IBM Trusteer's extensive experience and expertise.

For more information

To learn more about IBM Trusteer Pinpoint Detect, contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/trusteer

© Copyright IBM Corporation 2017

IBM Security Group
1 New Orchard Road
Armonk, New York 10504-1722

Produced in the United States of America
May 2017

IBM, the IBM logo, ibm.com, Trusteer, and Trusteer Pinpoint 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 cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. 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 MPLIED, 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

WGW03302-USEN-00