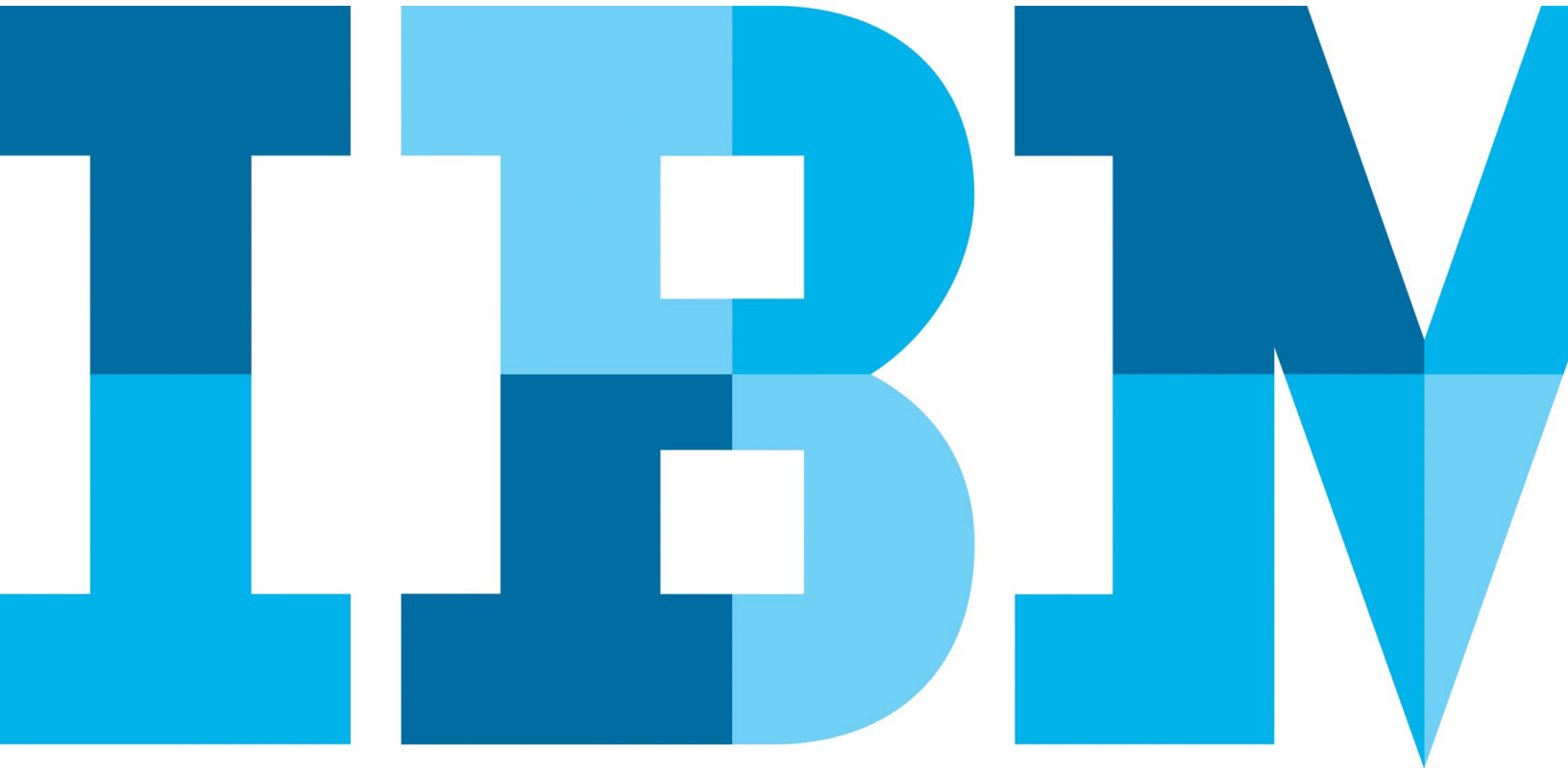
IBM Software
Thought Leadership White Paper

November 2014

Next generation criminal fraud detection

Identifying account takeover and fraudulent transactions to help stop cybercriminals



IBM

Contents

2 Introduction

2 Challenges with traditional risk engines approaches

4 A next generation criminal detection approach

8 Key benefits of evidence-based fraud detection

9 An integrated solution for comprehensive fraud prevention

11 Conclusion

11 For more information

11 About IBM Security

Introduction

In today's ever changing fraud landscape, much of the currently used statistical-based fraud detection methodology is creating significant challenges for both organizations and end users. These statistical models generate high false positive rates and provide a risk score that does not effectively distinguish between legitimate and malicious activity.

Additionally, these dated risk-based authentication solutions, working with step-up authentication, were built upon the assumption that authenticating suspicious activity will cause minimal disruption to end users, and effectively stop fraud. However, this has not been the case.

With the introduction of sophisticated threats, such as advanced phishing, pharming and malware, authentication has become less effective. Authentication methods—including out-of-band and one-time passwords—as well as security questions can be bypassed with minimal effort by fraudsters.

Consequently, more sophisticated authentication techniques have been developed. These techniques have severely impacted the customer experience and have been bypassed by advanced threats. The amount of unnecessary challenges and disruptions for end users is growing without a meaningful reduction in fraud. As fraud rises and the customer experience diminishes, there is a strong need for fraud tools that can stop fraud effectively, while actually enhancing the customer experience.

Challenges with traditional risk engine approaches

There are four main challenges with traditional risk engine approaches.

Provides inaccurate risk scores

When statistical risk-based authentication models were introduced, they were based on the assumption that fraud can be prevented using simple authentication. This assumption allowed these products to identify a relatively high percentage of transactions as risky, and perform elevated authentication for all of them. Because the authentication is simple, it is acceptable to authenticate many legitimate users. Thus, these engines are tuned to authenticate a given percent of users. For example, setting the "Risk Score" to 800 will authenticate 1.5 percent of users.

As threats have become more sophisticated and bypassing two-factor authentication has become common for cybercriminals, stopping fraud now requires more decisive action, such as putting the transaction on hold, and manually reviewing high-risk and high-value transactions. These actions impact resources who have to investigate fraud. And, they ultimately can impact the customer experience.

Most traditional risk engines use a pure statistical model for risk scoring, such as Naïve Bayesian, Decision Trees and Neural Networks. Using these types of pure statistical models for decisive fraud detection is not highly accurate for the following reasons:

- Traditional risk-based statistical scoring models heavily rely on limited and inaccurate data availability, which ultimately results in an inaccurate risk score.
  - Traditional fraud risk engines heavily rely on device ID methods for fraud detection. Complex Modes of Operation (MOs) using malware, Remote Access Tools, device spoofing, and usage of proxies can circumvent such fraud detection tools and not trigger alerts.
  - These traditional risk engines don't have visibility into critical indicators of fraud and pre-login activity, such as phishing attacks, malware infections and device spoofing, thus have no visibility to the full fraud lifecycle, and are unable to collect indicators on these threats. The traditional risk engines don't identify these threats, nor apply these inputs to the decision model, which ultimately results in an inaccurate risk score.
  - In addition, traditional risk engines utilize data received from the protected application by an API, not by integrating inside the website. This data can easily be spoofed and does not provide direct visibility to pre-login activity or user behavior in the session.
- In general, one of the key requirements for developing a successful and accurate statistical model is to train it using a representative large volume of the target population (i.e., confirmed fraud cases). The ratio between the actual fraudulent events (as low as a handful) and the total transactions (up to several millions per day) is non proportional and arbitrarily set. Due to this fact, the population used to train the models is too low and not representative, so the process of training and tuning these models tends to be inefficient. The outcome is inaccurate models that are generating high false positives and meaningless scores.
- In addition, the traditional risk scoring models are usually trained against limited historical data. Due to the low number of fraudulent transactions and the rapidly changing threat landscape, the models are trained and developed to detect specific and limited fraudulent transactional data rather than learning to generalize and protect against any MO. As a result, the statistical models are trained to detect and protect against MOs and threats that are no longer valid or are no longer the main concern for the protected financial institution.

To conclude, the statistical models are inaccurate and operate in a predictive/pattern-based mode, tuned to generate alerts for a given percent of users, and resulting in a high rate of false positives and false negatives. Once this ratio is established, changes to the model are difficult and slow, which constitutes a significant barrier to rapid and effective handling in the evolving changing fraud landscape and, thus, a new approach is necessary.

Increases investigation time and operational impact

Due to the inaccurate risk scores generated by these outdated risk engines, fraud and security administrators suffer the burden of numerous false positives and escalated authentications. Organizations need to manually investigate fraudulent events as a direct result of the many false positives and false negatives provided. This investigation is a costly, time-consuming, and resource-intensive effort for fraud teams given existing workloads. The false positives require extensive manual work, such as contacting customers, to confirm that flagged events are indeed fraudulent. Finally, extensive false positives limit the strength of action that can be taken in case of suspicion—which, in turn, allows fraud to bypass mitigation.

Negatively impacts the customer experience

Traditional risk-based authentication solutions can cause unnecessary challenges and disruptions for users, yet miss actual fraud events. Due to the inaccurate risk scores causing high false positives, customers will feel the impact, such as delays in payments, additional authentication or complicated out-of-band authentication. These actions can negatively impact the customer experience, especially in cases of time-critical business disbursements or last-minute consumer bill payments.

Sometimes, based on the risk score, banks restrict the types of transactions available to customers and set transaction limits to reduce the risk of fraud. Contrary to enhancing the customer experience, this fraud management approach can work in direct opposition to the goals of the business lines responsible for customer satisfaction, customer retention and profitability. As fraud rises and the customer experience diminishes, there is a strong need for next generation fraud detection tools that can help stop fraud and enhance the customer experience.

Increases complexity in keeping fraudster databases up to date

Risk scoring solutions heavily rely on bank fraud investigators to manually investigate fraudulent events, identify criminal devices and populate known fraudster databases. With many existing tools, this process can be a cumbersome, and time-and resource-intensive effort. As a result, many organizations find they can't keep their fraudster databases and risk scoring up to date.

A next generation criminal detection approach

IBM® Security Trusteer® Pinpoint™ Criminal Detection software uses evidence-based indicators of fraud to offer a next generation approach that helps address the challenges of traditional risk engines.

The solution combines enhanced device, geolocation, and transactional modelling with correlation of critical fraud indicators. This information is correlated using big data technologies to analyze events across time, users and activities. Phishing, malware and other high-risk indicators are correlated for evidence-based fraud detection.

By uniting the traditional risk score approach with an actionable indication of a "YES" or "NO" indication that takes into account fraud data and a deep knowledge of current MOs used by fraudsters, Trusteer Pinpoint Criminal Detection software can provide an evidence-based answer, rather than a statistical answer, on whether a transaction is fraudulent.

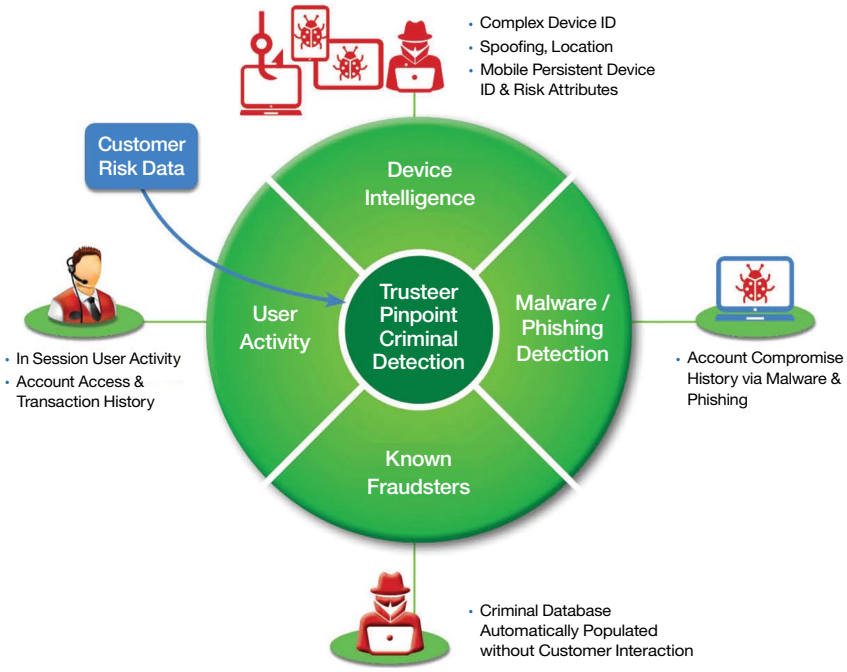


Figure 1. Trusteer Pinpoint Criminal Detection software delivers next generation criminal fraud detection.

Trusteer Pinpoint Criminal Detection software includes the following capabilities to enable evidence-based fraud detection.

Correlates device and account risk for account takeover detection

Since device fingerprint alone is often insufficient to detect account takeover, Trusteer Pinpoint Criminal Detection software correlates device risk factors with data on account malware infections and phishing incidents as they are executed to more accurately detect criminal access. For instance, access from a new device shortly after malware was detected on a different device used with the same account is an evidence-based indication of possible account takeover fraud.

Detects new, spoofed and criminal devices using complex device fingerprinting

Trusteer Pinpoint Criminal Detection software collects a variety of attributes to generate a unique "fingerprint" for each device accessing the protected web site. Criminals try to evade device fingerprinting systems by spoofing device attributes, such as the operating system, browser and IP address. Trusteer Pinpoint Criminal Detection software identifies these spoofing attempts, which are a strong indicator of fraudulent access. Criminal devices are automatically added to a global repository that is shared across organizations to help prevent account takeover.

Detects login and transaction anomalies

Trusteer Pinpoint Criminal Detection software detects login and transaction anomalies. During login, criminals often exhibit abnormal device and session characteristics, such as browser spoofing, operating system language inconsistences, time of access and geolocation variations, or proxy usage. When a transaction is submitted, Trusteer Pinpoint Criminal Detection software compares the transaction detail to the account history and considers amount, payee and other deviations in conjunction with other risk factors. Trusteer Pinpoint Criminal Detection also integrates with the organization's website, adding sensors that collect data from the front end and, thus, delivers visibility to critical information, such as pre-login activity and user behavior in the session.

Detects remote access tools

Remote access tools (RATs) provide cybercriminals with unlimited access to the legitimate customer's endpoint device and have recently become a common tool for fraudsters. Using the victim's access privileges, fraudsters can access and steal personally identifiable information and commit fraud. RATs can be used in combination with social engineering or as various parts of malware kits. RATs allow the fraudster to initiate a session and perform actions by remotely accessing the legitimate user's device, which effectively bypasses traditional fraud detection solutions that are focused on identifying access from new devices. Trusteer Pinpoint Criminal Detection offers a unique, clientless solution to detect RATs, including the most common such as Remote Desktop Protocol (RDP), VNC, Copilot, LogMeIn, WebEx, and more. Trusteer Pinpoint Criminal Detection collects this evidence and correlates it with user history and additional risk factors to identify fraudulent activity.

Identifies phishing incidents as they occur

Trusteer Pinpoint Criminal Detection software detects phishing incidents as they occur, including the site URL and compromised credentials. Organizations are notified of phishing campaigns and can initiate site takedown and URL blacklisting. Phishing incidents data is used to identify account takeover attempts, which often use phished credentials.

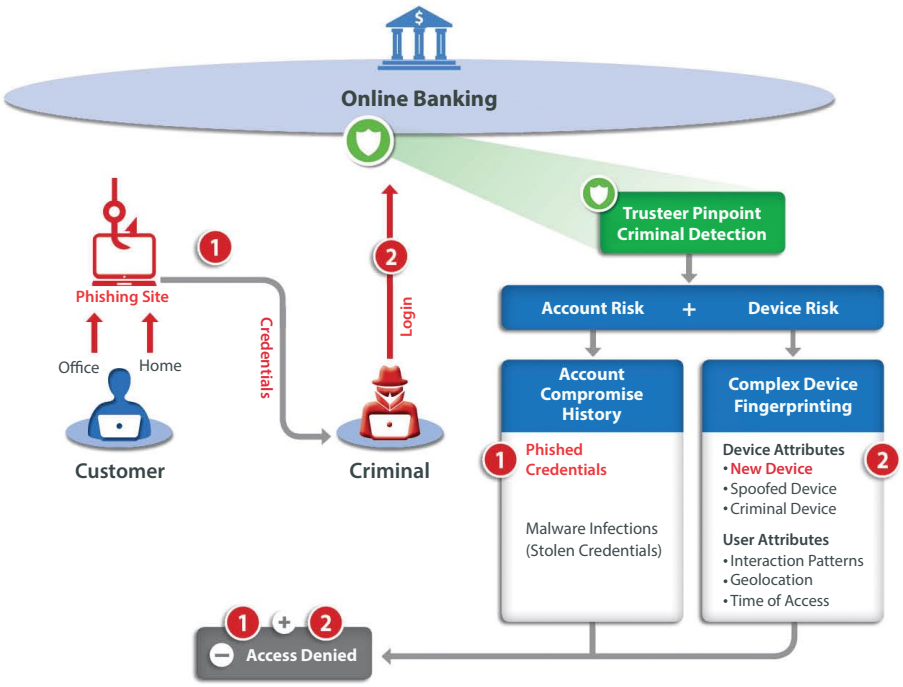


Figure 2. Example of phishing-based account takeover.

In the example shown in figure 2, a customer is a victim of a phishing attack and the customer's credentials are sent to a criminal, who uses the credentials to log into the online banking site. Trusteer Pinpoint Criminal Detection software delivers indicators of this event via phishing detection capabilities deployed on the bank website or as an IBM Security Trusteer Rapport® feed, which also detects user submission of credentials to suspected phishing sites. When the criminal logs in from his or her device, Trusteer software correlates the phishing event with the device fingerprint to detect account takeover attempts and, ultimately, takes action to stop the fraudulent transaction.

Key benefits of evidence-based fraud detection

Moving from traditional risk-based engines to an evidence-based approach enables an organization to more effectively stop fraudulent transactions—even ones with complex MOs—while enhancing the customer experience and reducing operational impact.

Reduces false positives and false negatives

With highly effective malware detection[1] and a wide-range of specific fraud risk indicators, Trusteer Pinpoint Criminal Detection software can help more accurately prevent fraudulent logins and high-risk accesses.

Improves the customer experience

Due to the low false positive rate, customers are rarely inconvenienced by blocked transactions, stepped-up authentication, and phone calls for verification, which helps improve the customer experience. Additionally, this approach helps remove unnecessary user challenges, such as challenge questions, lowering friction with customers.

Reduces operational impact

By using evidence-based fraud detection mechanisms, Trusteer Pinpoint Criminal Detection software enables fraud teams to more effectively prioritize cases and proactively respond to changing threats. Fraud investigators no longer have to wade through myriad false positives, and spend less time investigating fraud alerts and responding to customer inquiries regarding blocked or delayed transactions.

The software also helps streamline fraud prevention processes by restricting website access, stepping up authentication or using risk information in existing transaction review processes or risk engines.

The solution is updated continually based on new threats and MOs identified by the IBM Security Trusteer research team to help ensure evidence-based and actionable input to the overall risk assessment process—with minimal involvement required from fraud staff.

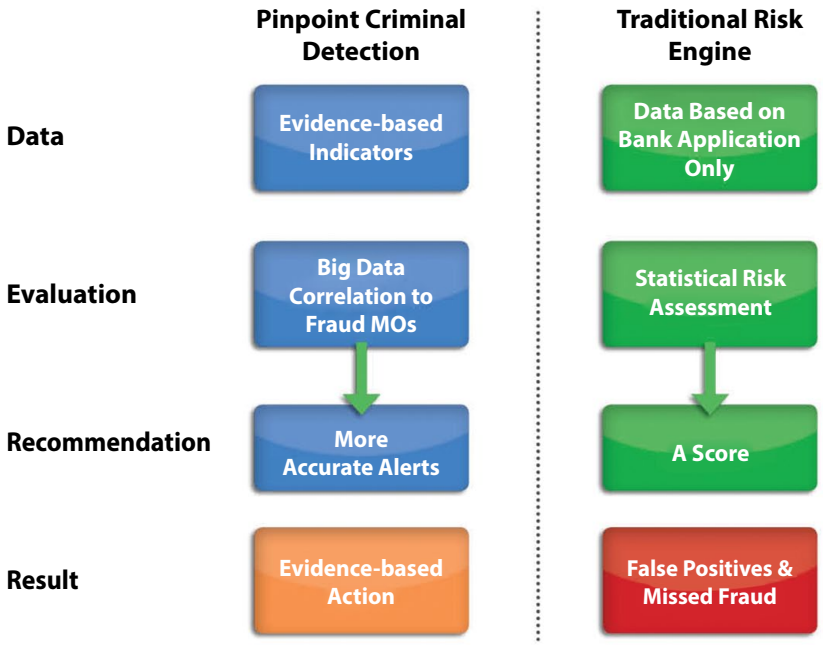


Figure 3. Trusteer Pinpoint Criminal Detection vs. Traditional Risk Engine

An integrated solution for comprehensive fraud prevention

By combining Trusteer Pinpoint Criminal Detection software with other Trusteer fraud prevention solutions, organizations can gain a comprehensive fraud prevention platform that delivers broad visibility across the threat landscape.

Shares device fingerprinting to improve detection

Trusteer Pinpoint Criminal Detection includes a unique device ID capability. It shares the unique device ID with Trusteer Rapport software, IBM Security Trusteer Mobile Browser and IBM Security Trusteer Mobile SDK, and is persistent, regardless of removal and re-installation of the Trusteer software. As a result, users who access the website through devices that have Trusteer Rapport software, Trusteer Mobile Browser and Trusteer Mobile SDK installed are associated with a persistent device ID. Pinpoint Criminal Detection uses this persistent device ID and account compromise history to detect account takeover attempts.

Provides comprehensive coverage across attack vectors

Fraudulent transactions are generated via two attack vectors: malware on the customer device and account takeover performed by criminals using stolen credentials and personal information. IBM Security Trusteer Pinpoint Malware Detection™ software detects malware infection as it occurs to help stop malware initiated transactions. Trusteer Pinpoint Criminal Detection software helps stops account takeover by detecting criminal access using correlation of device risk and account compromise history. By using these solutions together, organizations can holistically address online fraud, including malware-initiated fraudulent transactions (from the customer's device) and account takeover (from the criminal's device).

In the malware-based account takeover example shown in figure 4, if a user's device is infected with malware, the user's credentials are stolen. Trusteer Pinpoint Malware Detection software captures the malware infection indication and feeds it into Trusteer Pinpoint Criminal Detection software. When the criminal logs in, Trusteer Pinpoint software correlates the malware-on-the-account event with the device ID and session anomaly, and detects the new device. In this case, based on the account risk and new device, the transaction is denied.

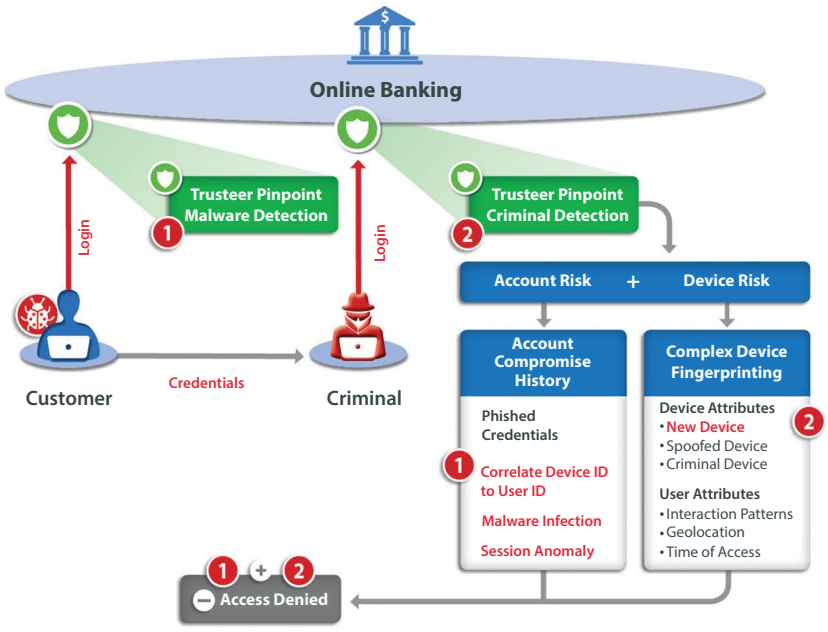


Figure 4. Example of malware-based account takeover.

Delivers in-depth security intelligence

Trusteer software provides real-time global intelligence that dynamically adapts and automatically updates protection, without customer interaction. Through the intelligence gathered from hundreds of millions of endpoints and the IBM Security Trusteer research team, Trusteer software delivers multiple layers of protection across devices and the fraud lifecycle.

Conclusion

Fraud teams are seeking a new approach to risk-based authentication solutions due to often inaccurate risk scores, and the negative impact on both operations and end users. The IBM next generation approach to fraud prevention uses evidence-based fraud indicators to help organizations more accurately and effectively detect fraudulent transactions, while improving the end user experience and reducing the operational impact. In fact, hundreds of millions of end users today benefit from the IBM Security Trusteer fraud prevention platform.

For more information

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

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2014

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.

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.

[1] Requires IBM Security Trusteer Pinpoint Malware Detection.

WGW03078-USEN-01