IBM Trusteer Pinpoint Detect

Leveraging cross-channel advanced analytics capabilities to better detect fraud

Highlights

- Deploy capabilities for machine learning across desktop and mobile channels with a single, comprehensive cloud-based solution
- Analyze device and account activity to reveal connections across multiple channels
- Apply security intelligence across users, sessions and devices
- Leverage advanced analytics to help financial organizations combat evolving threats while building new and better customer experiences

Financial service organizations continually seek to introduce new and innovative services to either attract new customers or improve their existing customer's digital experiences. In tandem, cybercriminals are constantly seeking new ways to circumvent existing security measures—a dilemma that can hinder the success of the bank's digital transformation efforts.

With the growing number of digital interactions and the increase of fraudsters attack techniques, being able to successfully identify legitimate users can require 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.

IBM® Trusteer Pinpoint Detect delivers adaptive, reliable, and accurate cross-channel fraud detection in one solution. It provides near-real-time recommendations regarding login attempts, suspicious session patterns, transactional anomalies, and identity validity. These are achieved by aggregating and correlating evidence-based threat intelligence, risk-based indicators, behavioral analytics and in-depth fraud information.

Leveraging these capabilities allows to accurately differentiate between legitimate users and fraudsters across multiple devices and login points helping organizations to promote customer experiences and long-term values, while helping to tackle the challenges of their digital transformation.

Protection across digital channels

Cross-channel fraud involves the use of sophisticated tools to exploit the vulnerabilities of one channel (such as a PC) to steal customer data or digital identities, and use the information it gains in another channel (such as a mobile device) to siphon funds from an associated account.

Trusteer Pinpoint Detect covers user activity conducted on any digital channel, whether accesses from a personal computer or mobile device. In doing so, the solutions can:

- Identify anomalous behavior and suspicious user patterns
- Detect device location, device spoofing attempts, and the use of remote access tools
- Monitor transactions for behavioral anomalies
- Identify malware-infected devices
- Provide actionable recommendations on whether to allow, restrict, challenge, or deny specific user activities or transactions along with detailed reasoning

Multi-channel visibility
Pinpoint Detect dynamically assesses user behavior across various channels through a layered approach including device, location, and session risk factors to deliver a proactive identity detection mechanism. It does so by correlating near-real-time data with additional sources such as malware infections and phishing incidents, information from endpoint clients, and feedback from the bank to help identify legitimate users. To further enhance the digital identity, Pinpoint Detect provides specific device-level intelligence to indicate the likelihood that the accessing device is safe to use as a second-factor authentication.

To provide an additional protection layer, the Trusteer mobile solution can integrate with Pinpoint Detect using an embedded software development kit (SDK). This component helps assess risk information from the mobile device—such as malware infections, root and jailbroken information, accurate geolocation, and Wi-Fi security status.

A cognitive approach to fraud detection

Trusteer Pinpoint Detect incorporates behavioral biometrics capabilities, using analytics and machine learning for real-time fraud detection. The behavioral biometric capabilities leverage machine learning to help understand how users interact with banking websites, creating models based on patterns of mouse movements that become increasingly more accurate over time. By building intricate digital behavioral models, the system can help to continuously authenticate online identities and more accurately differentiate between legitimate customers and fraudsters. It can also identify session and transaction anomalies and analyze device activity to determine if and when a device has been compromised or an identity has been stolen or misused.

By dynamically assessing online identities, Pinpoint Detect can balance varying security needs across locations, channels and devices without a noticeable impact on the customer experience via the following:

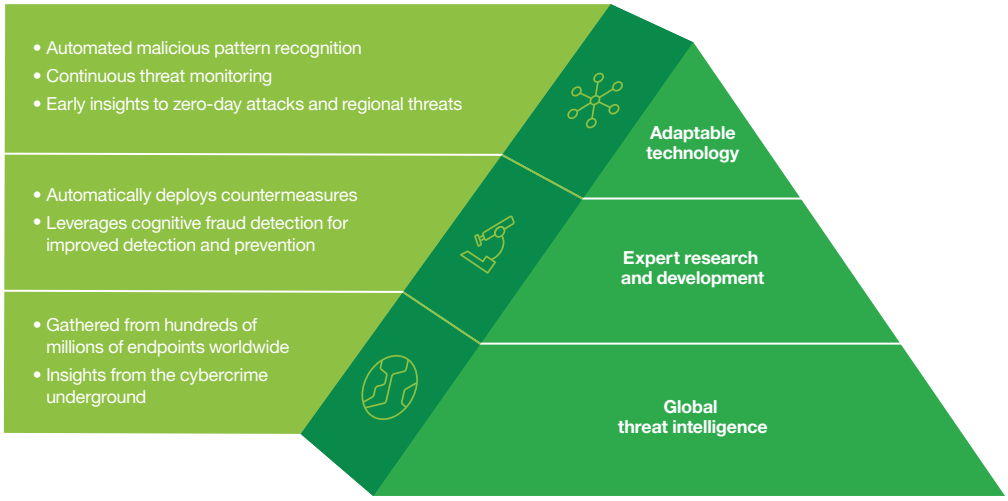
- **A seamless** assessment of the user's identity from login and across digital channels
- **Real-time** correlation of the results of behavioral biometrics analysis with multiple evidence-based fraud indicators
- **Actionable** risk recommendation that helps to maximize detection, reduce false positives and optimize strong authentication

Trusteer Pinpoint Detect provides financial institutions with an adaptable security mechanism allowing them to address the evolving threat landscape while evolving their solutions as part of their digital transformation efforts. One of the key elements lies in the organization's ability to protect itself and its customers in a constantly changing risk environment. To combat these evolving threats, Trusteer Pinpoint Detect uses advanced analytics and machine-learning capabilities to detect fraud using the following capabilities:

1. **Global threat intelligence** 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 advanced computing and machine learning, 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 has the unique capabilities to more rapidly uncover fraud, and is flexible enough so countermeasures can be deployed without bank staff support.



Global threat intelligence
With Pinpoint Detect, organizations gain access to near-real-time intelligence that tracks shifting attack tactics and malware across digital interactions with insight from multiple sources including IBM X-Force® research, underground forums, and other sources. This global threat intelligence is used by IBM security experts to help develop and deliver new protection layers and countermeasures for organizations worldwide. The continuous flow of fresh intelligence, not only helps 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.

Pinpoint Detect optimizes this unique intelligence to more effectively identify fraud and provide actionable recommendations, while helping detect and mitigate fraudulent activities.

Expert research and development
At IBM, a team of security experts scrutinizes threat intelligence as it arrives from Trusteer-protected endpoints, underground forums, and other sources. Because of IBM's global footprint, this translates 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 research and development team uses adaptive intelligence and advanced analytics to not only make sense of the data, but also learn from each interaction. This provides our security experts with insight on potential zero-day attacks and new regional trends. This unique approach provides Pinpoint Detect with fresh insight on new threat patterns, arms it with new malware logic and ultimately helps accelerate time-to-protection with new countermeasures.

Adaptable intelligence
IBM Trusteer software delivers adaptive protection layers that can be rapidly configured and updated to include the latest countermeasures. These new defenses require minimal intervention by security and have no noticeable impact to banking customers. This means that bank security personnel don't have to watch the marketplace or continuously update their criminal databases and crime logic. New product enhancements and updates, including but not limited to new protection layers, 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, advanced analytics capabilities are incorporated into Pinpoint Detect to help financial service providers detect fraud more accurately and quickly than ever before. By continuously and seamlessly learning user behavior across hundreds of millions of sessions, Pinpoint Detect analyzes current online activity to detect unusual behavior across different devices and compares 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, Pinpoint Detect provides access management systems and security analysts with a recommended action in near-real-time along with the detailed reasoning. Pinpoint Detect takes a comprehensive, layered approach to fraud detection, providing the necessary tools organizations need to welcome real users while helping stop fraudsters—all with minimal impact and without sacrificing the customer experience.

Why IBM?

The IBM Security platform provides security intelligence to help organizations holistically protect customers, data, applications and infrastructure from security threats. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development organizations.

For more information

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

IBM Corporation
IBM Security Services
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

WGS03035-USEN-02