Security
Banking

Solution Brief

IBM Security Trusteer Fraud Protection Suite

IBM solutions help detect, enforce, investigate and remediate fraud fast and efficiently

Highlights

- Help detect fraud while helping significantly reduce false positives using the evidence-based fraud detection capabilities of IBM® Security Trusteer® Pinpoint™ Detect
- Enable rapid enforcement based on actual risk using the threat-aware authentication capabilities of IBM Security Access Manager[1]
- Streamline investigations and threat analysis using the advanced case management and reporting capabilities of IBM Counter Fraud Management[1]
- Quickly remove existing financial malware from infected endpoints using the powerful remediation capabilities of IBM Security Trusteer Rapport® for Mitigation

Organizations can purchase Trusteer Pinpoint Detect to address specific fraud detection challenges, and then add enforcement, investigation and remediation layers as needed using its built-in integrations. These integrations can help facilitate the sharing of information across the fraud management lifecycle and can reduce both upfront and ongoing management costs.

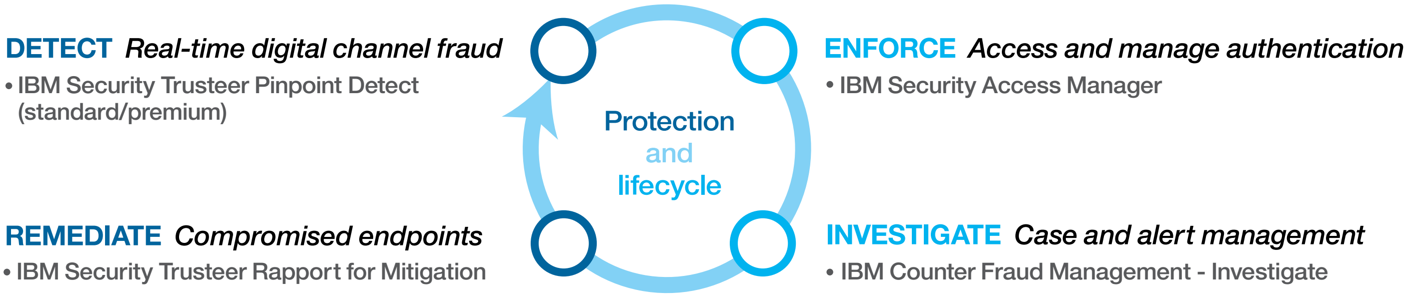
IBM Security Trusteer Fraud Protection Suite delivers more accurate fraud detection as well as simplified integration with IBM enforcement, investigation and remediation solutions. As a result, you can gain greater visibility and adaptability across the fraud management lifecycle.

- The suite offers highly effective intelligence- and evidence- based fraud detection with fewer false positives.
- It can help you reduce customer friction with enforcement based on an end user's actual risk, rather than statistical risk, through integration with IBM Security Access Manager.
- It can help you improve operational efficiency, reducing the time and cost of investigations, case management and remediation through integration with IBM Counter Fraud Management.
- It can help you remove existing financial malware from infected customer endpoints.
- It can help you decrease operational costs with simplified integration across the fraud management lifecycle.

And, finally, it can deliver increased protection with the ability to rapidly and automatically adapt to emerging threats based on extensive security intelligence.

The holistic Trusteer architecture provides a flow of data and intelligence between various layers and products. The tables describe products and capabilities provided by the Trusteer suite as well as other IBM products.

<table>
<tr><th>Offering</th><th>Key capabilities</th></tr>
<tr><td><b>IBM Security Trusteer Fraud Protection Suite:</b> Offers a simplified approach to fraud management to help your organization more accurately identify and prevent fraud—all while helping to lower costs and improve the end-user experience.</td><td>At the heart of Trusteer Pinpoint Detect is an engine that correlates a wide range of critical fraud indicators—including phishing attacks, malware infections, compromised credentials and advanced evasion methods—with enhanced device, geolocation and transactional modeling to help more accurately identify fraudulent transactions.
• Evidence-based fraud detection using Trusteer Pinpoint Detect can help uncover fraud while helping significantly reduce false positives.</td></tr>
<tr><td>Organizations can purchase Trusteer Pinpoint Detect to address specific fraud detection challenges. They can then add enforcement, investigation and remediation layers as needed using the built-in integrations. The integrations can help facilitate the sharing of information across the fraud management lifecycle.</td><td>You can receive authentication, enforcement of internal procedures and security policy management by integrating IBM Security Access Manager.* IBM Security Access Manager enables you to create and enforce threat-aware access policies across channels, based on actual risk to your organization.
• Threat-aware authentication using IBM Security Access Manager enables rapid enforcement based on actual risk.</td></tr>
<tr><td colspan="2">By integrating IBM Counter Fraud Management,* you can leverage case management, reporting, and alert management to help prevent and intercept attempted fraud, while building evidence against past fraudulent activity and improper payments. It includes advanced analytics and investigative analysis.
• Advanced case management and reporting through IBM Counter Fraud Management streamlines investigations and threat analysis.</td></tr>
<tr><td colspan="2">By integrating Trusteer Rapport for Mitigation, your organization can quickly and easily help end users clean their malware-infected machines. Once malware is suspected on an end user's computer, bank staff simply provide the end user with a link to download the malware removal tool, which can quickly be installed with one click. Once installed, the solution immediately goes to work, helping both detect and remove existing financial malware.
• Powerful remediation using Trusteer Rapport for Mitigation helps quickly remove existing financial malware from infected endpoints.</td></tr>
</table>



DETECT *Real-time digital channel fraud*
- IBM Security Trusteer Pinpoint Detect (standard/premium)

ENFORCE *Access and manage authentication*
- IBM Security Access Manager

REMEDIATE *Compromised endpoints*
- IBM Security Trusteer Rapport for Mitigation

INVESTIGATE *Case and alert management*
- IBM Counter Fraud Management - Investigate

IBM Security Trusteer Fraud Protection Suite provides a SaaS-based cross-channel solution with full visibility into the entire fraud lifecycle.

Offering	Key capabilities
IBM Security Trusteer Pinpoint Detect: Integrates the capabilities of IBM Security Trusteer Pinpoint Criminal Detection and IBM Security Trusteer Pinpoint Malware Detection™ into a single cloud-based offering. These combined capabilities are now offered as a single, fully integrated solution, greatly simplifying deployment and ongoing updates.	• Visibility throughout the fraud lifecycle correlates critical fraud indicators, including phishing attacks, malware infections, compromised credentials and advanced evasion methods. • Continuous intelligence across the threat landscape is gathered from 270 million endpoints. • Greater agility helps organizations rapidly adapt to the changing environment.
IBM Security Trusteer Pinpoint Malware Detection*: Provides clientless fraud-prevention engine designed to accurately detect malware-infected end-user computers when they go to a bank's website or access the financial institution's protected web applications.	• Transparently detects malware-infected devices or attempts by malware to commit web fraud. • Alerts the fraud team of high-risk devices so they can take protective action. • Leverages Trusteer Rapport for Mitigation to remove existing financial malware from end-user machines.
IBM Security Access Manager: Enables authentication, enforcement, and security policy management.	• Allows organizations to create and enforce threat-aware access policies across channels based on actual risk to the organization. • Combines integrated authentication with highly accurate detection to deliver powerful enforcement that can help you stop fraud based on actual risk, rather than statistical risk.
IBM Counter Fraud Management – Investigate: Provides advanced case management and reporting capabilities to streamline investigations and threat analysis.	• Provides case management, reporting and alert management that helps help financial institutions prevent and intercept attempted fraud, while building evidence against past fraudulent activity and improper payments using capabilities including advanced analytics and investigative analysis. • Integrated authentication, combined with highly accurate detection help lower false positives and speed determination of actual fraud.
IBM Security Trusteer Rapport: Provides client-based endpoint protection to protect against financial malware and phishing attacks by allowing investigation, remediation, blocking and removal of man-in-the-browser (MitB) malware infections from infected PC and Mac devices.	• Helps prevent and remove infection by live and inactive MitB malware from infected devices. • Helps protect browsing sessions, even if active malware is present. • Detects phishing sites and specific compromised account credentials and payment card data. • Notifies fraud teams of malware infections and removals to enable user re-credentialing and help eliminate future threats.
IBM Security Trusteer Rapport for Remediation: Extends the ability of Trusteer Rapport to investigate, remediate, block and remove MitB malware infections from infected end-user devices.	• Helps protect devices operated by bank customers, employees or business partners by preventing and removing infections by live or inactive MitB malware. • Remediates and protects compromised and infected endpoints from future threats.
IBM Security Trusteer Mobile: Helps protect native mobile applications through device risk factor analysis and the use of a persistent mobile device ID. To help further improve detection on the mobile channel, IBM Security Trusteer mobile solutions can seamlessly integrate with Trusteer Pinpoint Detect via an embedded SDK. This component collects granular risk information from the mobile device, such as malware infections, rooted and jailbroken information, accurate geolocation, and Wi-Fi security status.	• Detects mobile-based risk factors including: – Jailbroken/rooted devices – Malware infections – Installation of applications from untrustworthy sources – Unsecured Wi-Fi connections – Outdated operating systems – Geographic locations • Generates a persistent device ID based on hardware and software attributes that is resilient to application reinstallation.

Why IBM?

IBM expertise and continued success at helping clients prevent fraud is based on deep roots in global fraud intelligence and malware research. IBM performs global and financial institution-specific continuous risk assessment by analyzing proprietary intelligence data gathered from more than 270 million endpoints worldwide. This information is then used to ensure that Trusteer solutions provide sustainable fraud prevention solutions for clients. IBM continuously updates its solutions based on new threats and methods identified by the Trusteer security team.

For more information

To learn more about IBM Security Trusteer solutions, please contact your IBM representative or IBM Business Partner, or see: **ibm.com**/security/trusteer

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

IBM, the IBM logo, ibm.com, Trusteer, and Trusteer Rapport 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

Trusteer, Trusteer Pinpoint, and Trusteer Pinpoint Malware Detection are trademarks or registered trademarks of Trusteer, an IBM Company.

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 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.

[*] Also available separately

[1] Also available separately

Please Recycle