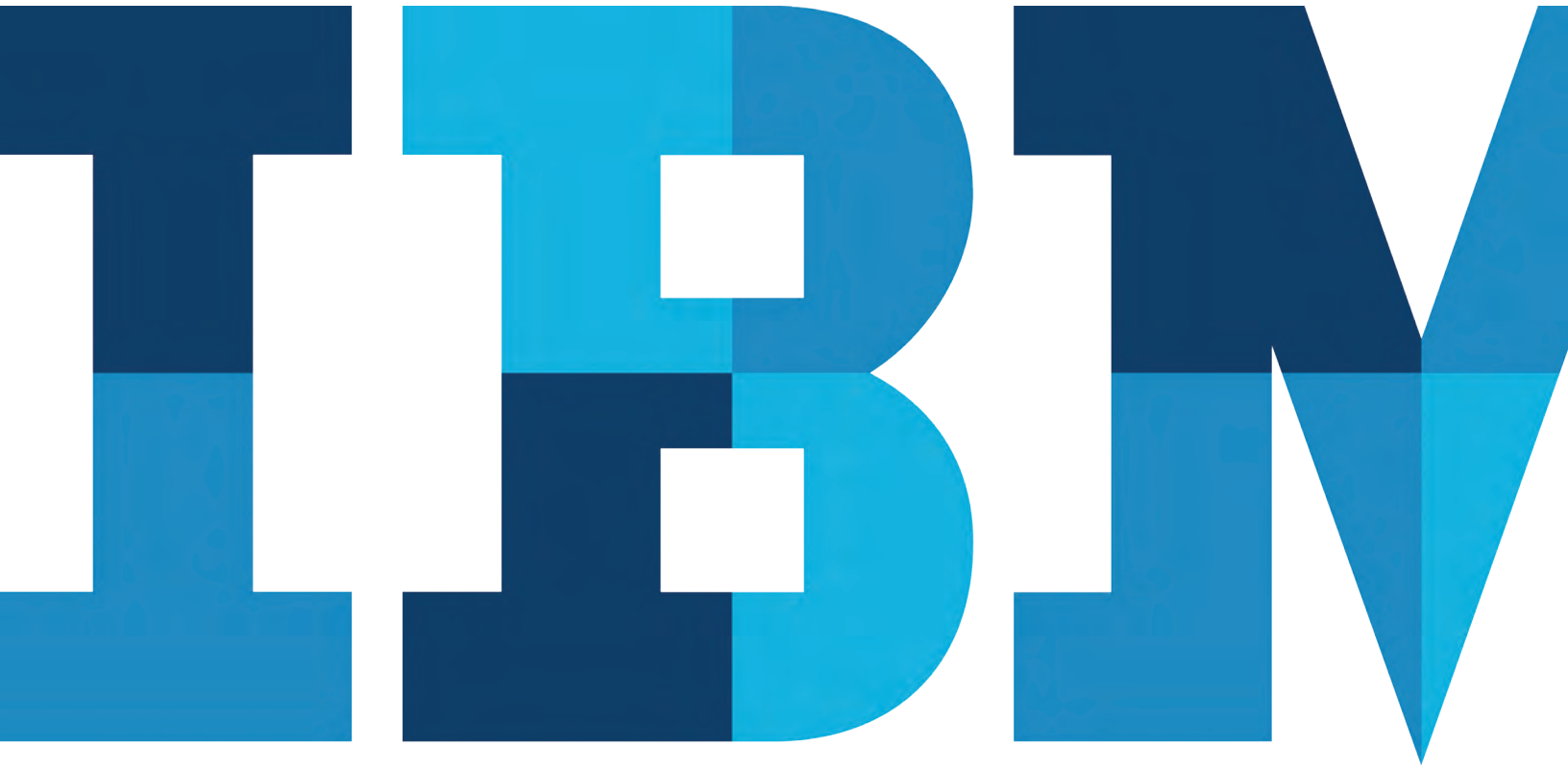
IBM Analytics
White Paper

1 + 1 = 3: The new math when countering fraud

IBM Counter Fraud Management and Trusteer team up to detect and fight new torrents of fraud attackers



IBM

What's cyber crime got to do with fraud?

Both security intrusions and fraud events are on the rise worldwide, driven in large part by the "professionalization" of cyber crime. Today, cyber criminal organizations often function much like their enterprise targets, complete with executive staffs, strategic plans and ROI targets. The extreme sophistication of today's threats is forcing executives in financial institutions and other industries to take note—and puts them under enormous pressure to institute effective countermeasures.

Once considered separate disciplines, fraud prevention and cybersecurity are merging into a single operational concern for COOs, CISOs and others in the boardroom. According to a recent study by the IBM Institute for Business Value, weak cybersecurity was a factor in more than a quarter of all fraud cases. The same research found that executive staffs conduct quarterly reviews of fraud and cybersecurity in more than 80 percent of institutions.[1] There is growing awareness among corporate leaders that cyber attacks are the key to the enterprise's front door: once intruders get inside, they can help themselves to a full range of valuable corporate assets—in other words, perpetrate fraud.

Traditional fraud defenses fall short

Neither fraud nor cyber crime are new phenomena; enterprises have been deploying countermeasures of varying levels of effectiveness for decades. The usual strategy is one of accretion of defenses over time, resulting in siloes of separate tools such as anti-money laundering (AML), fraud detection and intrusion prevention systems. While each of these countermeasures may be effective against specific attack vectors, they don't exchange intelligence and alerts with each other and therefore can't fully cover the threat space. Furthermore, modern cyber criminals are versed in the technologies behind these countermeasures, discuss them openly in online forums on the "dark" Internet and even collaborate on ways to bypass enterprise defenses at multiple levels.

In short, the traditional approach to countering cyber crime and fraud needs rethinking. An effective strategy requires both new processes and advanced tools. On the process side, collaboration among the departments that are responsible for fraud, AML, cybersecurity and even operations is an essential first step. C-level visibility is equally important to ensure both a high level of priority and the budget and other resources needed to improve the organization's counter fraud posture.

On the technology side, it's not a matter of building better tools; for the most part, today's security products are effective within their (often narrow) domains. But what if you could combine the power of multiple tools? The resulting solution would broaden the sphere of action to deliver a far higher level of protection and adapt faster than the criminals. And that's exactly the IBM approach.

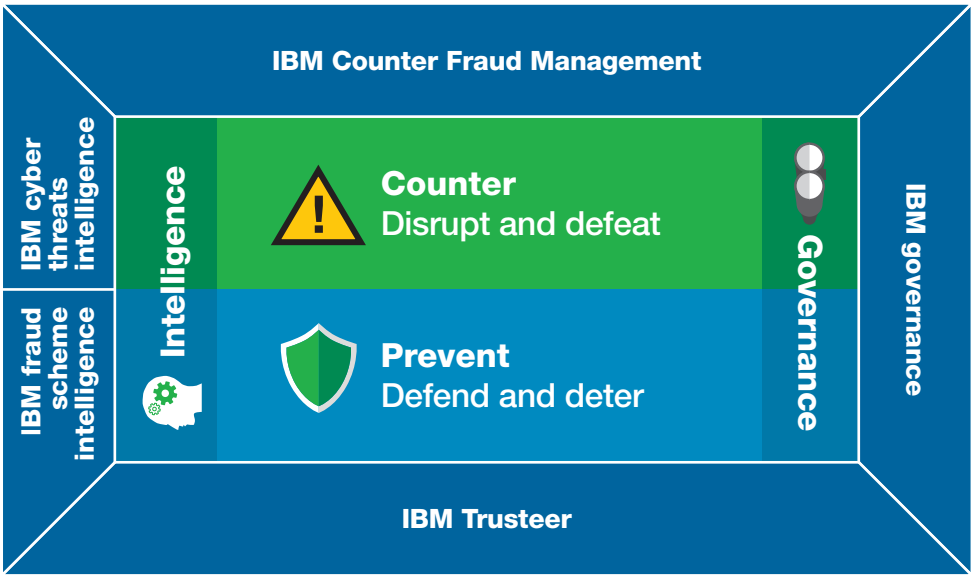


Figure 1. IBM offers a comprehensive approach to fraud detection, prevention and counter measures.

Better together: Trusteer and IBM Counter Fraud Management

To meet the needs of modern fraud fighters, IBM offers an integrated solution that both prevents and counters fraud based on proven technologies (Figure 1):

- IBM® Trusteer®, part of the IBM security portfolio, is an industry-leading online malware and fraud solution that detects and prevents most intrusion attempts from internal and external sources and foils account takeover attempts.
- IBM Counter Fraud Management provides a rich set of analysis tools that automatically detect suspicious customer behavior and unusual transactions, enabling investigators to identify fraudulent transactions.
- IBM intelligence informs prevention and counter measures from the IBM ecosystem. The solutions focus on analysis of malicious attacks experienced across the global IBM footprint, as well as the tactics and processes used by cybercriminals.
- IBM governance helps ensure all activities are aligned with the organization's counter fraud strategy and compliance mandates.

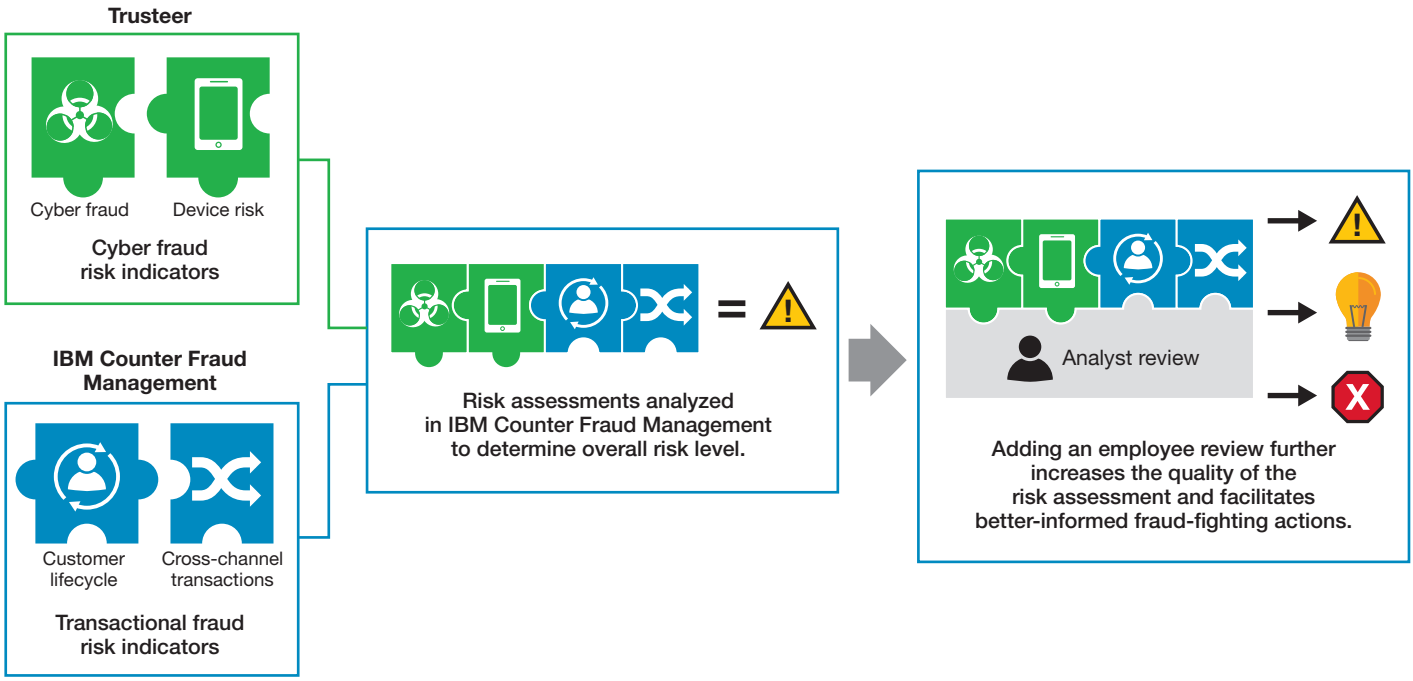


Figure 2. Trusteer and IBM Counter Fraud Management together provide analysts with a multifaceted view of the true risk, enhancing their ability to identify fraud and prevent losses.

Fraud investigators get an edge

What makes the IBM integrated solution so powerful? The power of two. Trusteer automatically feeds accurate fraud risk indicators into Counter Fraud Management's case management and analytic tools. The Counter Fraud Management models and screens use Trusteer alerts to further strengthen the accuracy of detection and investigation. Counter Fraud Management can also send confirmed fraud notices back to Trusteer to inform future decisions about that customer or device.

Connecting the cyber and transactional fraud dimensions, the IBM solution essentially "opens the aperture" to give investigators a multifaceted view of the situation. When investigators have a more complete view, they are able to identify exploits that otherwise would "fly under the radar" of individual security components. This integrated approach drives more accurate risk assessments and creates the conditions for faster and more effective decision-making, which ultimately contributes to reductions in the number and severity of fraudulent transactions (Figure 2). In effect, the combination is greater than the sum of its parts—think of it as a 1+1=3 solution.

Smarter counter fraud in action

The Trusteer–IBM Counter Fraud Management integrated offering addresses a wide range of fraud scenarios in the financial industry including account takeover and mobile fraud, each of which is discussed in the following sections.

Account takeover

Account takeover refers to the situation in which a cyber criminal poses as a genuine customer to gain access to a checking, savings or payment account to make unauthorized transactions. Trusteer and IBM Counter Fraud Management together create an effective defense by sharing intelligence to arrive at the appropriate risk assessment.

As an example, the following three events all occur within a short period of time for the same account:

- An unknown device logs in from an unusual location.
- A new payee is added through the call center.
- An international wire transaction is requested through the bank's website.

None of those activities is overly suspicious by itself—each might well be assessed individually as low or moderate risk. However, IBM's integrated approach digs deeper to determine the risk of these events in context to arrive at a more accurate risk assessment:

1. Trusteer combines traditional device IDs, geolocation and transactional modeling, and critical fraud indicators to detect the anomalous login. In some cases, this single event will generate a high-level risk assessment to block further transactions on the account.
2. IBM Counter Fraud Management analyzes all the information in context and determines that the combination of anomalies presents a high-enough risk to suspend the wire transaction and trigger an alert.

In effect, the two IBM tools working together have widened the observation space to provide fraud analysts with the information they need to create a more accurate risk assessment and initiate effective countermeasures. In addition, investigators gain powerful insights into this particular attempt and can better identify patterns to inform security rules and fraud models, and strengthen the organization's overall counter fraud posture.

Mobile fraud

Cyber criminals are nothing if not opportunistic, as illustrated by the rise of mobile fraud. Just a few years ago, mobile fraud was an insignificant footnote. Today, it represents 20 percent of the USD 6 billion cost of fraud to merchants and card issuers in the United States.[2] Here's a typical scenario that shows how IBM addresses this growing problem:

1. A cyber criminal logs into a mobile website using stolen credentials.
2. Trusteer detects the unknown device in an unusual location for this customer and issues a Moderate cyber-risk assessment.
3. At the same time, IBM Counter Fraud Management detects a number of anomalies such as profile changes, new beneficiaries and cross-channel transactions,[3] leading to a Moderate fraud risk assessment.
4. When these two Moderate assessments are combined, the risk level is elevated to High, reflecting the more serious nature of the potential threat.

The next move

Cyber criminals continue to come up with new and more potent fraud attempts, with no end in sight. As a result, enterprises must develop more sophisticated ways to thwart such attacks. Strengthening defenses requires both a new spirit of collaboration among the various disciplines—security, risk, AML and operations—and smarter, more powerful tools. The combination of Trusteer and IBM Counter Fraud Management broadens the observation space of the fraud risk landscape, enabling more effective detection and elimination of cyber threats and more accurate assessments of the risk of fraud.

For more information

To learn more about powerful counter fraud solutions from IBM, visit:

- www.smartercounterfraud.com
- www.trusteer.com
- ibm.co/bankingfraud

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Analytics
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

[1] "Winning the face-off against fraud," IBM Institute for Business Value Global Study, January 7, 2016. ibm.biz/fightingfraud

[2] Olga Kharif, "Watch Your Mobile Wallet: Fraudulent smartphone payments are becoming a pricey problem," BloombergBusiness, February 12, 2015.

[3] Cross-channel transactions occur when a consumer begins a transaction in one channel and completes it in another. A typical example is paying for an online transaction by check as opposed to an online payment method. While not all cross-channel transactions are fraudulent, they do represent a disproportionate fraction of fraud cases.

Please Recycle

ASW12364-USEN-00