FORRESTER®

For: Security & Risk Professionals

Detecting Cyberthreats With Fraud-Based Advanced Analytics Technology

by Ed Ferrara, August 4, 2014 | Updated: August 6, 2014

KEY TAKEAWAYS

Customers Are In The Crosshairs, And Their Loyalty Is At Risk

Phishing and malware attacks that compromise merchant and financial services companies' networks are major sources of financial fraud. These breaches shatter consumer confidence, and as consumers are more aware of the implications of these losses, they will flee vendors that don't protect their sensitive information.

New Security Analytics Technologies Offer New Opportunities To Stop Cyberbreaches

Fraud detection is a mature technology market, with solutions employing artificial intelligence, machine learning, statistical risk scoring, big data, and data mining. The more nascent field of security analytics is now advancing with these same techniques pioneered by antifraud technology, to actively detect cyberbreaches in near real time.

Security Service Providers Will Lead The Implementation Of Security Analytics

Security analytics provides a quantum leap in cyberthreat detection, but implementation of this technology is substantially more complex. Security and risk pros will need help to get the most from these new tools, and managed security service providers will provide the necessary services to ease the implementation of this important capability.

Detecting Cyberthreats With Fraud-Based Advanced Analytics Technology

New Security Analytics Capabilities Will Replace Traditional SIEM, And Security Service Providers Will Lead The Adoption

by Ed Ferrara
with Christopher McClean, Andras Cser, Rick Holland, and Katherine Williamson

WHY READ THIS REPORT

Security and risk (S&R) professionals know that cyberattacks are often the first step in the complex dance of credit card theft and the fraud that results. Cyberattacks take many forms and affect many industries, but when cyberattacks focus on financial services, the result is serious financial loss. Starting with malware injection, followed by the exfiltration of credit card data, and then the sale of this data on the dark web, this process feeds part of a growing underground economy responsible for $11.27 billion in losses for 2012. Banks and merchants take the brunt of these losses, including breach recovery costs, regulatory fines, and the loss of customer trust and loyalty. Banks and merchants need to look at cybersecurity as an invaluable tool to protect customers against all types of fraud, stopping customer data loss and the resultant fraud. Service providers are using technology pioneered in financial fraud detection to identify cyberbreaches. This innovative application of fraud detection technology repurposed for the cybersecurity world promises to recognize cyberbreaches in near real time and, in so doing, better protect customer data. These solutions are more sophisticated and complex than prior cybersecurity detection technologies, and S&R professionals will need qualified managed security service providers to make the technology work.

Table Of Contents

Notes & Resources

Forrester interviewed six vendor companies: AlienVault, BAE Systems Applied Intelligence, Brighterion, Electronic Arts, ThreatMetrix, and Trusteer.

Related Research Documents

Market Overview: eCommerce Fraud Management Solutions, 2014
February 4, 2014

Big Data In Fraud Management: Variety Leads To Value And Improved Customer Experience
October 16, 2013

CUSTOMERS HAVE NEVER BEEN MORE AT RISK

In the past two years, customers have become increasingly aware of the threats posed by cyberthieves; most of the major newspapers globally, including The New York Times, The Washington Post, USA Today, and The Financial Times, all have written extensively about recent and highly publicized cyberbreaches. Recent credit card data breaches have led to significant financial loss on the part of merchants and banks, as well as consumers in some situations. Fraud feeds a growing underground economy responsible for losses of $11.27 billion in 2012.[1]

Because of this, customer awareness and anxiety are on the rise.[2] Customers facing cyberbreach losses are now more willing to sue, and the courts are more willing to consider these cases.[3] Customer data is clearly in the hacker's crosshairs, and customer loyalty is at risk.

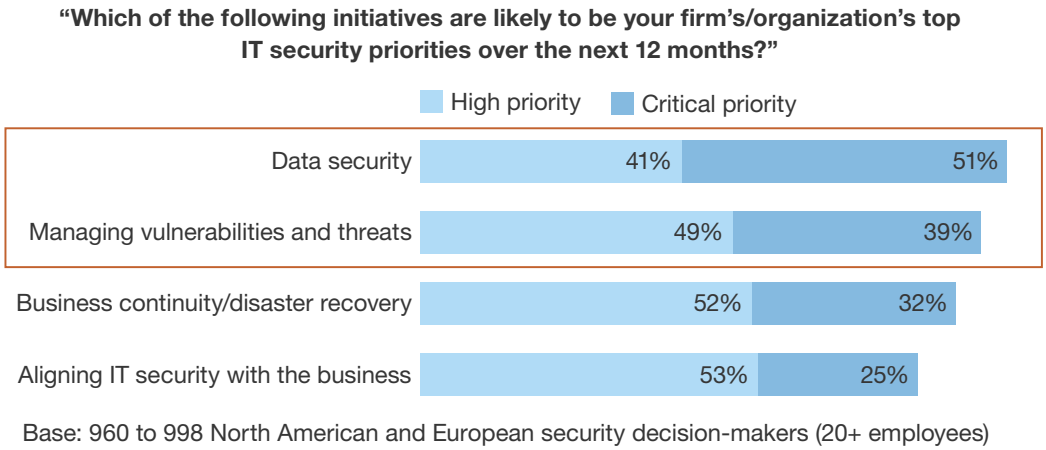
PROTECTING (CUSTOMER) DATA IS NOW THE CISO'S NO. 1 PRIORITY

Protecting data is the foundation of any security program. This is especially true in the payments industry, where total revenue loss in North America due to fraud was almost $3.5 billion.[4] The recent breaches at Target, Nieman Marcus, P.F Chang's China Bistro, and other merchants demonstrate just how vulnerable customer data can be.

In the Target breach alone, thieves stole over 40 million credit and debit card numbers, plus an additional 70 million name and address records. Target's sales fell on news of the breach and still languish. CEO Gregg Steinhafle and CIO Beth Jacob lost their jobs as a result.[5] The firm had no chief information security officer. A proxy firm, Institutional Shareholder Services, recommended that investors oust seven board members in a recent shareholder proxy vote, explaining that they failed to protect the company from last year's data breach. Board members convinced shareholders to reelect them, but the message to the board was clear — future data breaches would be their responsibility.[6]

These events clearly support security and risk professionals' recognition that protecting data, especially customer data, and managing vulnerabilities and threats are top priorities (see Figure 1).

Figure 1 Vulnerabilities And Threats



Base: 960 to 998 North American and European security decision-makers (20+ employees)

Note: Not all responses shown
Source: Forrester's Forrsights Security Survey, Q2 2013

117224 Source: Forrester Research, Inc.

SECURITY ANALYTICS EMULATES FRAUD DETECTION

One of the most important security technologies employed over the past decade to aid in the data protection mission is event correlation. Event correlation technology collects and analyzes log data to identify the telltale signs of an active hacker or malware.[7] Even with tools, this process has been time-consuming, often allowing breaches to go undetected for long periods of time. As the number of devices and applications grows for most organizations, the problem only gets worse. Security and risk professionals need a new automated approach for cyberbreach detection. Security analytics is this next-generation technology.[8]

Fraud Detection Technology Is The Envy Of Security Analysts

There are many useful strategies for protecting customer data, and each has its place in threat defense. Many in the information security industry talk about the use of big data as the solution to better threat detection. Large amounts of data are not helpful, however, unless the analytic tools exist to make sense of the information.

Financial services companies face this same issue when trying to address credit card fraud. In 2012, there were 26.2 billion credit card transactions globally, and looking for fraud in this huge amount of data requires long compute times, vast storage, and automated event correlation; fraud analysts can't do this job manually.[9] Fraud detection uses automation to automatically deny fraudulent transactions, and this similar capability — automatically stopping a potential breach while it's in progress — has been the Holy Grail of cybersecurity.[10]

Statistics, Heuristics, And Big Data Drive Fraud Detection And Security Analytics

Fraud detection technology monitors for illicit activity involving credit cards or other financial instruments, whereas security analytics technology monitors for unauthorized access to or use of information assets. The technical requirements for both capabilities are strikingly similar (see Figure 2).

In fact, many fraud detection platforms form the foundation for many of the security analytics platforms on the market today.[11] Security analytics and fraud management solutions both depend on the ability to detect patterns of anomalous behavior, which identifies suspicious transactions or potential cyberbreach activity. These systems must be able to operate autonomously, stop fraudulent or adversarial behavior, and at the same time maintain operational efficiency.[12] These capabilities come from data science, artificial intelligence research, and the expertise of fraud and cybersecurity experts.[13] The resulting techniques or technologies deliver a number of very important types of analysis:

- **Case-based reasoning uses past scenarios to detect fraud and breaches.** Case-based reasoning is similar to neural network analysis. With this approach, fraud detection systems translate financial transactions into common profiles or forms; any deviations from these common scenarios are flagged as potential fraud. Security analytics technologies aggregate data from network analysis and visibility (NAV) tools and all types of security and nonsecurity applications to create similar common profiles.[14] They then use these profiles to a standard baseline to illuminate deviations that could be malicious, be it a potential fraud or cyberbreach. For example, when analyzing fraud, a reasonable question to ask is, "Why is the customer who lives in Pennsylvania in the United States buying a refrigerator in Japan at 3 in the morning?" Similarly, a question to ask with respect to cyberbreach could be, "Why is this person whose office is in Philadelphia where it is 3 a.m. logging into a secure database?"

- **Constraint programming provides analysis validation.** The use of declarative constraints is a powerful validation method for determining the scope of fraud detection analysis. For example, a fraud analyst may program a detection tool to ignore any transaction less than $10 to limit the amount of bandwidth used on high volumes of low-risk traffic. Similarly, whitelisting and blacklisting IP addresses are examples of declarative constraints for security analytics technologies because they focus analysis on high-risk systems.

- **Data mining capabilities search various databases to identify anomalous behavior.** Fraud detection and security analytics technology performs data mining to clean, sample, cluster, and classify transactional data in search of anomalistic behavior that may indicate fraud, hacking, or both. For fraud detection, an example of data mining would be the analysis of all fraudulent, card-not-present transactions that originated from a particular part of the world that focused on specific merchandise types with purchase amounts less than $400. An example of data mining for security analytics would be poring through hundreds of thousands of spam emails to look for patterns of malware distribution.

- **Fuzzy logic uses probability to identify likely violations.** Fraud and cyberbreach detection is not always black and white, so analysis often requires probabilistic methods. Fuzzy logic systems assign a "degree of truth" to different indicators of fraud or cyberbreach. Fuzzy logic programs then cluster the information into various risk categories. The system then evaluates the clusters statistically to determine the presence of fraud or the presence of malware. For example, employees access a server that *occasionally* hosted malware in the past. However, employees must use the server for valid business purposes. The facts are inconclusive, so the system will perform additional analysis to determine if this specific server presents a threat.[15]

- **Long-term profiling builds a model for expected system and user behavior.** All merchants, cardholders, network devices, and systems have a baseline behavioral profile. Using this baseline, systems can compare current behavior against this historical baseline to determine if a fraud or hack is possible. For example, if a cardholder who normally spends several hundred dollars a month on groceries and household goods in his hometown suddenly starts spending thousands of dollars in various countries on electronics and luxury items, fraud detection systems should raise a red flag.

- **Real-time profiling evaluates and possibly intercepts adverse activity as it's happening.** Antifraud systems use real-time profiling and risk scoring to evaluate the behavior of individuals or entities such as merchants, cardholders, ATMs, network devices, and applications. Rapid real-time processing doesn't generally allow for the same level of analysis as long-term profiling, but for certain scenarios, these systems can stop a fraudulent transaction before it's completed.

- **Neural networks look for complex connections in historical data.** Neural networks interpret a vast amount of historical data looking for trends and patterns. This method mimics the way the human brain processes information by identifying complex connections; in the case of fraud detection, these systems look for links between processing elements such as the location, amount, initiator, and merchant of a credit card transaction. The systems evaluate the number and weight of the connections between the processing elements to determine if there is potential fraud. For security purposes, they may look for the presence of a long-term cyberbreach consistent with an advanced persistent threat type of attack.[16]

- **Smart agents operate in a semi-autonomous fashion.** Smart agents interact and negotiate with each other in order to make cyberbreach and fraud determinations. Often described as a form of machine learning, smart agents operate differently from algorithmic systems, where the programmer defines how the system will solve the problem: Is this fraud or a potential breach? Smart agents can automate a large portion of the fraud or cyberbreach detection process and require little human intervention. For example, smart agents focus on specific elements of a financial transaction or user-network connection, looking for specific indicators of fraud or breach. These agents use multiple models or rules, and they can construct new models and rules for fraud or breach detection with their machine learning capabilities.[17]

Figure 2 Fraud Detection And Threat Intelligence

	Fraud detection	Threat intelligence/ advanced analytics
Example attack goal	Customer account takeover, assuming control of consumer accounts for identity and financial theft	Privileged account takeover, assuming control of a system administrator's accounts or creating "backdoor" access to systems for exfiltration of data.
Example attack method	Phishing, financial malware, mobile threats	Phishing, malware, (all types — virus, Trojan BOT, etc.), web-based attacks, and mobile threats
Speed of transaction analysis	The ability to analyze a transaction and return a decision in real time (often under 200 milliseconds)	The ability to analyze a threat event and return a decision about it in real time — leading to automated control enforcement or escalation for event response
Amount of transaction data analyzed	Large amounts (petabytes) of transactional data	Large amounts (petabytes) of transactional data
Event correlation process	Context-based, adaptive, and risk-based authentication	Context-based, adaptive, and risk-based threat detection
Risk computation models	Statistical-based and rules-based analysis for fraud risk modeling	Statistical-based and rules-based risk and security event modeling
Information considered	Entity and link analytics — evaluating how phone numbers, email addresses, mobile devices, or PCs link to each other in transactions	Entity and link analytics — evaluating how phone numbers, email addresses, mobile devices, or PCs link to each other in transactions, as well as network, host, and endpoint devices
Statistical probability methods	Probabilistic models to determine the likelihood of fraud	Probabilistic models to determine the likelihood of cyberbreach

117224 Source: Forrester Research, Inc.

SERVICE PROVIDERS WILL LEAD THE ADOPTION OF SECURITY ANALYTICS

Security analytics platforms are becoming significantly more complex as they incorporate the more sophisticated capabilities of fraud detection systems. With sophistication comes the promise of better threat defense and the potential for true automated prevention of cyberattacks. In response to market advancements, many security vendors are sunsetting existing security incident and event management (SIEM) technology and replacing it with more advanced security analytics products. While these changes occur, managed security service providers (MSSPs) are not waiting for technology vendors. Many of these companies have introduced or will introduce stronger security analytics capabilities as part of their service portfolios.[18]

Because of the high level of subject matter expertise required to make full use of such capabilities, security and risk professionals should consider MSSPs as a viable option instead of trying to build their own in-house security analytics team. There are additional benefits to this approach as well: If one customer experiences an attack, an MSSP can analyze the source and method of the attack and proactively warn other customers in its portfolio.

WHAT IT MEANS

SECURITY ANALYTICS IS READY FOR DEPLOYMENT

Fraud detection science and methods provide big opportunities for security and risk professionals to address cyberthreats in a faster and more automated fashion. Techniques developed to combat fraud — including artificial intelligence, machine learning, and neural networks — are proving to be equally adept at detecting cyberbreaches and will set the standard for security event detection moving forward. Many sophisticated enterprises have already deployed security analytics. These companies are seeing significant benefit from the use of the technology; in many cases, they've been able to automate some aspects of cyberbreach detection and prevention, closing in on the Holy Grail of cybersecurity.

Challenges remain, however. Security and risk professionals not currently using security analytics should begin implementation of security analytics technology as pilot projects in their organization immediately. Complexity can be high, so security and risk professionals that lack sufficient expertise, staff, or both will need to turn to MSSPs to reduce implementation issues. As the technology matures, implementation, management, and maintenance effort should ease, but the use of a qualified service provider will still be the best approach for a successful implementation and operations for many companies.

ENDNOTES

[1] Issuers, merchants, and acquirers of credit, debit, and prepaid payment cards worldwide experienced gross fraud losses of $11.27 billion in 2012, up 14.6% over the prior year. Of that $11.27 billion, card issuers lost 63% and merchants and acquirers lost the other 37%. Card issuer fraud losses occur primarily at the point of sale because of counterfeit. Issuers bear the fraud loss when they authorize the merchant to accept the payment for a fraudulent account. Merchant and acquirer losses occur mainly on card-not-present (CNP) transactions on the Web, at call centers, or through mail order because issuers can chargeback fraudulent transactions. Fraud losses on all general purpose and private label, signature and PIN payment cards reached $5.33 billion in the US last year, up 14.5%. Issuers lost 64% or $3.41 billion and merchants lost the other 36% or $1.92 billion. Source: "Global Credit, Debit, and Prepaid Card Fraud Losses Reach $11.27 Billion in 2012 — Up 14.6% Over 2011 According to The Nilson Report," Business Wire, August 19, 2013 (http://www.businesswire.com/news/home/20130819005953/en/Global-Credit-Debit-Prepaid-Card-Fraud-Losses#.U6hTQ41dWuo).

[2] Until recently, consumers haven't been overly concerned with cybersecurity. Credit card laws and policies protect customers from theft and fraud by limiting or negating cardholder liability; similar policies protect debit cardholders. Recent incidents, including revelations of government spying and massive credit card breaches, have triggered customer calls for better security and privacy. This puts enormous attention on the CISO. Security incidents, managed well, can actually enhance customer perceptions of a company; managed poorly, they can be devastating. See the April 17, 2014, "CISOs Need To Add Customer Obsession To Their Job Description" report.

[3] In the United States it was difficult for class actions suits to proceed against breached companies, as US circuit courts have disagreed on what it takes to prove injury and class action certification. As more breaches occur, however, more consumers are affected; the tide is shifting, as courts are willing to consider inadequate data protection, and therefore negligence, as the cause for these breaches. See the October 1, 2013, "Understand The State Of Data Security And Privacy: 2013 To 2014" report.

[4] Source: "2013 Online Fraud report — Online Payment Fraud Trends, Merchant Practices, and Benchmarks," CyberSource, 2013 (http://images.demand.cybersource.com/Web/CyberSource/CyberSource_2013_Online_Fraud_Report.pdf?utm_campaign=Fraud%20Report%202013%20-%20Form%20auto-reply&utm_medium=email&utm_source=Eloqua).

[5] Source: Brian Krebs, "The Target Breach, By The Numbers," Krebs on Security, May 6, 2014 (http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/).

[6] Source: Matthew Rocco, "ISS: Target Shareholders Should Overhaul Board," Fox Business, May 28, 2014 (http://www.foxbusiness.com/industries/2014/05/28/iss-target-shareholders-should-overhaul-board/).

[7] One of the first documented examples of the use of log files to detect a hacker was Clifford Stoll's The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Clifford Stoll was a computer systems manager at the Lawrence Berkeley National Lab.in California who discovered a 75-cent accounting error in the lab's computer time billing system. This error alerted him to the presence of an unauthorized user. The unauthorized user managed to break into multiple US government computer systems and steal sensitive military and security information. Using a variety of techniques including the computer log review, Stoll was able to assist in the hacker's capture. Source: Cliff Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, September 2005.

[8] Over the past 15 years cybersecurity professionals used different acronyms to describe these systems, but each provided different and improved capabilities. There have been three generations of these tools, each providing greater event correlation and reporting capabilities. Cybersecurity professionals describe these event correlation systems using different acronyms. These include first-generation — security event management (SEM), second-generation — security information management (SIM), and a hybrid concept joining the two ideas — security information and event management (SIEM). Third-generation tools with their advanced capabilities are best described using the term Security Analytics. See the October 1, 2013, "Understand The State Of Data Security And Privacy: 2013 To 2014" report.

[9] We have covered big data in a previous report. See the October 16, 2013, "Big Data In Fraud Management: Variety Leads To Value And Improved Customer Experience" report.

[10] There have been attempts at this in the past. IDS/IPS technology, for example, has the capability to automatically stop breach activities by closing TCP ports; it was rarely used, however, because of the fear that a false positive would stop production and inconvenience customers.

[11] The following companies offer both fraud detection and security analytics solution offerings — BAE Systems Applied Intelligence, Brighterion, CSC, CGI Group, HP, SAS Institute, and SC21.

[12] We have covered autonomous and efficient systems that hamper fraud and adversarial behavior in a previous report. See the October 16, 2013, "Big Data In Fraud Management: Variety Leads To Value And Improved Customer Experience" report.

[13] Not all of the solutions or services on the market use all of the analytics capabilities, with various solutions favoring different techniques.

[14] A diverse set of tools make up network analysis and visibility (NAV). These tools provide situational awareness for networking and information security professionals. See the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[15] Fuzzy logic is most effective when used to apply numerical values to vague terms, because the fuzzy technology can numerically weight the importance of a data item with respect to its importance for fraud or breach determination. The second way fuzzy logic improves detection effectiveness is to show partial membership of data elements in traditional analysis. Detection effectiveness also increases because the fuzzy technology can address "noisy" data or outlier data. Source: Mary Jane Lenard and Pervais Alam, "Application of Fuzzy Logic to Fraud Detection," IGI Global, 2009 (http://www.irma-international.org/viewtitle/13569/).

[16] Source: Krishna M. Gopinathan, Louis S. Biafore, William M. Ferguson, Micahel A. Lazarus, Ann K. Pathria, and Allen Jost, "Fraud Detection Using Predictive Modeling," HNC Software, October 1998 (http://www.fenwick.com/fenwickdocuments/predictive_5819226.pdf).

[17] Source: Jia Wu and Jongwoo Park, "Intelligent Agents and Fraud Detection," Rutegers University - Newark (http://andromeda.rutgers.edu/~gshafer/wupart.pdf).

[18] Symantec, for example, has announced end-of-life for the Symantec SIEM, replacing it with an advanced analytics platform. HP, IBM, and RSA are quickly introducing security analytics capabilities into their ArcSight, QRadar, and enVision platforms, respectively. Many others SIEM vendors are making this shift. In the managed security services market, companies like AT&T (in partnership with IBM), BAE Systems Applied Intelligence, Dell SecureWorks, eSentire, HP, IBM (in partnership with AT&T), SilverySky, Solutionary, and Wipro have already introduced significant security analytics capability and will expand these capabilities in the next 12 to 18 months.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals