patternex

Predicting and Stopping Account Takeover Fraud

A PatternEx Solution Guide

patternex

Problem

Every major breach fundamentally comes down to criminals obtaining legitimate credentials. Using valid ID's and passwords, crooks easily bypass existing security measures. This kind of activity is called an "account takeover," or "ATO."

Consider these recent events:

- Anthem was victimized in 2015 by a sophisticated attack that stole social security numbers, names, street addresses, emails and other personal information from over 80 million customer records. The hackers obtained valid login credentials of at least five Anthem employees.
- A recent eBay breach was the result of a stolen valid login from an employee. The fraudster roamed the internal network of eBay for 229 days before being discovered.
- Many celebrities stored personal photos in Apple's iCloud. Criminals were able to guess the ID/PW credentials, then took over their accounts and exfiltrated personal photographs.

ATO attacks hit eCommerce and SaaS sites daily...Existing solutions can't stop these kinds of attacks because they admit anyone with valid credentials.

There are several ways hackers can obtain valid ID/Password combinations. They can use techniques such as Spear-Phishing, Watering Holes, or simply purchase a list of ID/passwords on the black market.

ATO attacks hit eCommerce and SaaS sites on a daily basis. "Account takeover (ATO) fraud has also steadily risen, and is holding its ground in terms of fraud losses at $5 billion per year for the second year in a row." (Lexis Nexis "True Cost of Fraud Report 2014:") Existing solutions can't stop these kinds of attacks because current solutions admit anyone with valid credentials. To stop Account Take Overs, we need a new way to identify a hacker versus a legitimate user, and we need to identify them before they commit a crime.

Exacerbating this problem is the rollout of EMV, **the open-standard for smart card payments and acceptance devices** in the United States. EMV chips will undoubtedly cut down on fraud tied to stolen credit cards, but they will also likely push more fraud online, where the physical card is not required to make a purchase.

"Several Financial Institution Executives expected to see fraud shifting to Card-Not-Present (CNP) channels… Executives also expected to see increases in ATO and new account fraud, which could include compromised online accounts with merchants." - Lexis Nexis True Cost of Fraud, 2014

Industry Analyst Brian Krebs agrees, saying, "Fraud doesn't go away, it just goes somewhere else, and that somewhere else is always online. The thieves can still steal the card number and expiration data, which still can be used online. So that's generally what will happen. We'll see a pretty big uptick in card-not-present fraud."

Current Solutions Are Fundamentally Lacking In Key Areas

Currently, there are two kinds of InfoSec technology solutions: those that are 'analyst-driven' and those that are machine learning-driven. The former are legacy products with significant limitations while the latter are an interesting emerging set that merit consideration and evaluation.

Approach	UnSupervised Learning (No Labels)	Supervised Learning (Static labels)	Active Learning (Dynamic labels)
Real-time (learning continuously)	Anomaly Detection for UBA		$(AI)^2$: Active Learning + Analyst Intuition
Batch (Learn offline)	Anomaly Detectors	Offline Fraud models	

Analyst-Driven Solutions

Analyst-driven solutions include such products as network firewalls, Fraud Detection/ Prevention systems, SIEM's, and Intrusion Detection and Prevention Systems (IDPS). They're based on allowing analysts to create rules that allow or deny access to a user. And while these are a necessary component to your security posture, they are not sufficient.

Rules-based approaches have a high rate of undetected attacks. A rule, by definition, is something that reacts to a new attack; it prevents historical attacks from happening again. Rules-based solutions can't "see"—much less prevent—new and emerging attacks.

A second problem is the delay inherent to analyst-driven solutions. Once the attack is discovered, a human must create, test, and validate the rules that prevent the attack from happening again—in the meantime your company remains exposed.

Finally, rules are detectable and solvable. While rules remain static, cyber-criminals are constantly adapting their behavior, testing the rule until they find a way to circumvent it, starting the detection/delay/resolution process all over.

Anomaly-Driven Solutions

The new class of emerging solutions based on Machine Learning hold promise, but fall short in critical areas. These "anomaly detection" products discard static rules in favor of statistical models that determine when certain events are outliers. While these solutions tend to do better in the detection of new attacks, they suffer from high levels of false positives while still containing some important vulnerabilities.

The major failing of these anomaly detection products is not in their capability but in their approach. While they can execute complex statistical analyses to identify anomalous events, the results they generate lack context. Not all outliers are malicious. Generating alerts tied to anomalies means you generate many false positives.

The major failing of Anomaly Detection products is not in their capability but in their approach. Generating alerts tied to anomalies means you generate many false positives.

The impact of too many false positives is severe: analyst's become fatigued from seeing too many alerts, analysts begin to distrust the system that generates false alarms, and eventually the analysts abandon the system.

Time to solution is also an issue. Anomaly detection (AD) products require a "baseline" of behavior upon which they can identify outliers. To do so, AD solutions require 90 days of data to form the baseline. Malicious behaviors in the baseline data may not appear as outliers to the ML solution, leading to blind spots in your defenses.

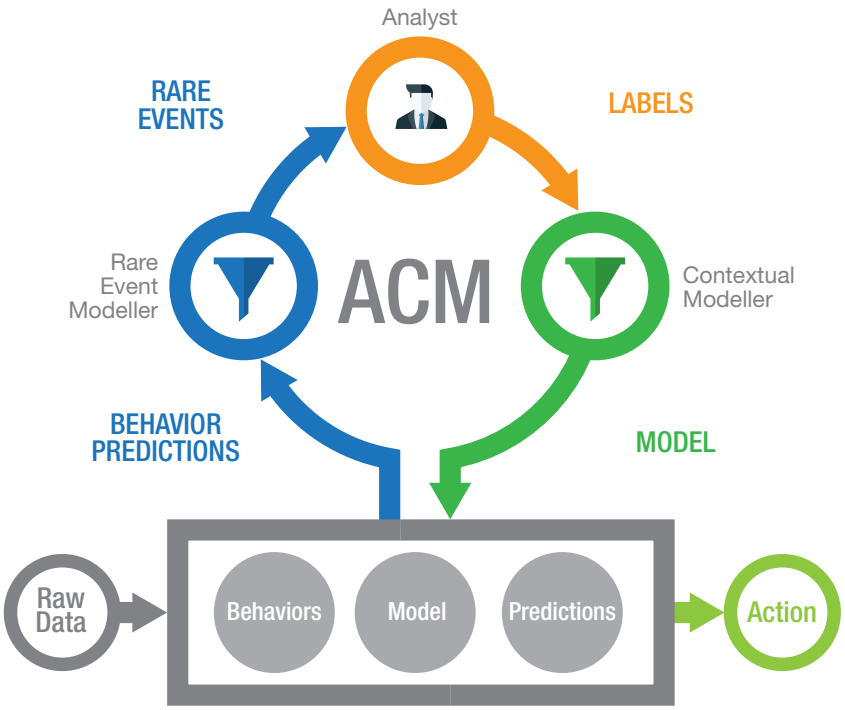
The PatternEx Solution

The PatternEx Platform helps companies *predict when fraud is about to happen with previously unachievable precision*. Simply put, PatternEx identifies the criminals and allows companies to stop them—before they act.

To appreciate how this solution works, it is important to realize that every user activity online is logged somewhere. The IT infrastructure keeps track of hundreds of user behavior characteristics and stores that information in logs. Load balancers, firewalls, web servers, email servers—they all keep track of ingress traffic and egress traffic. Based on this data, a user's behavior patterns can be identified. The PatternEx platform uses this information to identify malicious use and intent.

The PatternEx solution ingests all of the IT infrastructure logs and runs them through our patent-pending proprietary algorithms to identify likely ATO candidates. Suspicious events are sent to an analyst who provides feedback to the system, which learns from that input to enhance future accuracy.

PatternEx combines the aptitude of humans with the capabilities of machines to assess behaviors and accurately predict when a theft is about to happen. Human analysts are good at understanding context and nuance. Machines are good at computing complex relationships. Combining both greatly reduces false positives and creates extreme precision in ATO detection.



How Does It Work?

Even with valid credentials, an ATO attacker behaves differently than a legitimate user. An ATO attacker will penetrate a site with stolen credentials and then move quickly. Perhaps they buy e-gift certificates and email them to an address they control. Perhaps they buy high-demand, high-ticket items and ship them to a warehouse they control. Or they may go the user directory and steal sensitive information.

Legitimate users don't behave this way. For example, legitimate user takes more time than a criminal. They browse a bit. They click on some reviews. They tend to linger on certain interesting web pages before adding a product to the shopping cart.

Active Contextual Modeling combines the best capabilities of artificial intelligence, big data analysis, and human intuition into an end-to-end AI platform for detecting breach and fraud.

Introducing The World's First Threat Prediction Platform

The PatternEx platform combines big data infrastructure with security expertise and artificial algorithms into a proprietary solution that can predict, in real-time, when you are under attack from a botnet. The result is the industry's first Threat Prediction Platform.

The PatternEx solution is an end-to-end threat detection platform. Our patented Active Contextual Modeling™ technology combines the latest in Artificial Intelligence with the intuitive and deductive capabilities of human analysts. By applying user behavior and applying AI models, enterprises can now quickly and accurately detect malicious user intent. If malicious intent is confirmed, the system automatically takes action, in real-time, to challenge/delay/block the user. It can detect both historical and emerging threats for both fraud and breach.

Active Contextual Modeling

Active Contextual Modeling is our proprietary process that yields remarkable alert precision in real-time from any data source. It combines the best capabilities of artificial intelligence, big data analysis, and human intuition into an end-to-end AI platform for detecting breach and fraud.

Computers are excellent at processing enormous amounts of data and finding relationships in that data across many dimensions. And Big Data Infrastructure enables companies to process more data than ever before. But, no matter how powerful or accurate these systems are, they lack the human capability to understand context, see the big picture, and create “eureka” moment of powerful insight. Combining these three strengths into one seamless system delivers precise, real-time alerts when bots have penetrated your system and are executing commands of the CNC server.

Deployment Options

The PatternEx solution is available as a software package, as a service, in your private cloud, or on premise. Your requirements are basic: stream log data into PatternEx, review the real-time user behaviors, and provide feedback.

Benefits

By augmenting your InfoSec team with the PatternEx platform, you can:

- Gain visibility into previously invisible cyber attacks
- Receive real-time alerts enabling you to take immediate preventative action
- Reduce the risk of brand damage
- Reduce the risk of data exfiltration

The reduction in fraud expense using the PatternEx solution goes directly to the bottom line

- The stolen goods cost is lowered
- The forensics costs are lowered
- The remediation costs are lowered

The reduction in breach expense goes directly to the bottom line

- End user remediation costs are lowered
- A given company will not require as large a team to review alerts
- A company will not suffer the brand damage associated with data breach

Conclusion

Account Take Overs are a pervasive crime today, costing businesses $5B each year. They are particularly difficult for current solutions to prevent because the hacker has legitimate credentials. The only way to catch the bad guys is to look at their behavior. That behavior is captured in the Petabytes of logs generated by IT infrastructure and can now be processed thanks to inexpensive and elastic computing power.

Current behavior solutions are rule-based. These solutions, at best, can offer only 2% to 3% precision rate in detecting malicious behavior. PatternEx takes a different approach. By combining human and machine strengths, PatternEx achieves a 90+% precision rate at detecting Account Take Overs and can predict these events before they happen.

How To Contact Us

For more information or to request a demo, send your email to sales@patternex.com or info@patternex.com.

PatternEx is an Artificial Intelligence security company that has developed a Threat Prediction Platform to identify malicious user intent. The PatternEx solution enables security analysts to detect and prevent cyber attacks in real time, at scale

patternex

PatternEx
4620 Fortran Dr., Suite 202
San Jose, CA 95134

www.patternex.com