

Verosint Launches Account Fraud Detection and Prevention Platform

Security startup 443ID, which previously focused on bringing open source intelligence (OSINT) to access management, is now refocusing its solution to tackle account fraud detection and prevention, and has changed its name to Verosint to better describe its new focus. It is launching what is technically version 2 of 443ID's IAM platform, but is effectively version 1 of Verosint's account fraud solution.

"The previous product was focused on measuring the likelihood of risk to enable risk-based access control," Mark Batchelor, co-founder and CTO of Verosint, told *SecurityWeek*. "Since release 1, we shifted our focus and product development to account fraud detection and prevention. Capabilities that we have added [to the new product] include behavioral analytics, rules engine, identity graphing, and AI/ML that automatically tags different forms of account fraud, such as promo abuse and account sharing."

According to a February 2023 report from Aite Novarica, comments, "A spate of reports from the U.K.'s House of Lords to the National Retail Federation reveal that fraud as a criminal enterprise is more pervasive and poorly addressed than most observers realize... Recent reductions in U.S. postal inspectors and ever-improving methods for broadcasting vulnerabilities have significantly increased check fraud in North America."

With account fraud increasing, Verosint is now concentrating on preventing such fraud rather than simply measuring the risk of fraud. Key to its approach is the OSINT part of the new name. "Verosint's patent-pending SignalPrint technology predicts the likelihood of fraud based on capturing and tracking data about each user, enriching that data with open source intelligence (OSINT), and analyzing relationships and patterns to determine risk – within milliseconds," claims the firm.

The system can ingest and use months of the company's client logs, including from SIEM systems, and begins to build user profiles from the first day. This data is supplemented by OSINT. "Even if a new user is registering for the first time, we will be able to match them with their OSINT footprint," Batchelor. "Based on that match, we can make risk decisions even though we've never seen them before."

SignalPrint will already most likely contain the user's IP location, accounts, email or phone number, and other OSINT-collected data, and this is used by its machine learning algorithms to form an opinion. "If we don't have any data at all, we would flag the account as high risk and invoke the appropriate security controls and workflows," he continued.

Verosint does not collect any data directly from users, and is

consequently not hampered by any privacy rules. It collects data that is already freely available on the internet (supplemented with data provided by a few business partners such as ecommerce or gaming platforms.

Nevertheless, the firm takes its own security seriously. “We take all the necessary steps to protect the data, with caching and encryption,” said Batchelor. “OSINT data is not very attractive to hackers; it’s freely available on the Internet. And we’re not building enhanced deep profiles of users. We are building SignalPrints,” he continued, “but they are really of no use to anyone but Verosint. Hackers would not be able to associate users and accounts with our data.”

As a server-side SaaS solution, Verosint can be deployed within hours. SignalPrint analyzes relationships, and flags anomalies based on patterns of behavior and other risk indicators from customer-provided or OSINT-collected data. High risk users can be challenged or blocked, while low or no risk users get frictionless access. It has out-of-the-box integration with leading access management systems and comes with additional APIs to customize risk-based responses.

“Account fraud is more prevalent, more sophisticated, and more capable of disruption and damage than ever,” said Stephen Shoaff, CEO and co-founder of Verosint. “Organizations need to proactively get ahead of fraud by blocking bad actors before they gain access.”

Verosint started life as 443ID. The Austin, Texas-based firm emerged from stealth in June 2022 with \$8 million seed funding. It was co-founded in 2021 by Stephen Shoaff (CEO) and Mark Batchelor (CTO).

Related: Spanish, US Authorities Dismantle Cybercrime Ring That Defrauded Victims of \$5.3 Million

Related: Bringing Bots and Fraud to the Boardroom

Related: Bolster Raises \$15 Million to Tackle Fakes and Frauds

Related: The Advantages of Threat Intelligence for Combating Fraud

Verosint Launches Account Fraud Detection and Prevention Platform