Intensity Analytics Awarded Key Patent for Behavioral Authentication Security Software

Proprietary algorithms identify users by their behavior
without the need for personally identifiable information

Company also announces new funding bringing total to nearly $5 million

WARRENTON, VA – September 7, 2016 - Intensity Analytics, a specialized software company with a long history of innovation in data security, announced today that the United States Patent and Trademark Office awarded it US Patent 9,430,626 titled "User Authentication Via Input of Known Text." The newly-patented IP combines advanced mathematics and machine-learning techniques to immediately recognize users by their keyboard typing patterns, while denying illegitimate users access, thus negating the value of wrongfully-obtained credentials.

This proprietary technology provides an effective solution for the 80 percent of security breaches originating from stolen credentials, and aligns with Gartner's prediction in its market guide report that over the next three years User and Entity Behavior Analytics (UEBA) will "become the preferred systems for security operations."

Escalating demands for privacy, coupled with the increasing number of security threats facing online organizations, require a different approach. Secure user authentication has become both a business risk management and legal requirement, with significant fines and damages recently levied for non-compliance. Intensity Analytics' breakthrough technology blocks access and precisely tracks security events by analyzing the keystroke behavior of individual offenders when compared to legitimate users.

"We have cracked the authentication code to prevent access by intruders," said John Rome, CEO and co-founder of Intensity Analytics. "Current security solutions in the market are incomplete, as evidenced by constant breaches resulting in substantial economic losses and legal risk to enterprises and government agencies. Our patented mathematics are based on multidimensional, geospatial algorithms which compose standard add-in software components. These can be readily deployed – quickly, inexpensively, and in a highly-scalable manner – without collecting any personally identifiable information."

While linear keystroke dynamics (based on hang/dwell/flight time subtractions) have been around in the market for decades, Intensity Analytics has successfully created a proven new method of recognizing and precisely categorizing the unique "clouds of effort" involved in keyboard patterns. By design, they complement and enhance existing security solutions without the need to "rip-and-replace" existing solutions.

The solution precisely identifies who is at the keyboard, thereby tightening security and preventing expensive breaches before they occur. The software can also run in the background, continually authenticating throughout a session rather than stopping at the point of access, eliminating the need to adopt inconvenient tokens or bespoke hardware.

Other multifactor solutions currently available face two main issues: the data cannot be revoked (e.g. employees' fingerprints cannot be changed if their record has ever been compromised), and biometric data is personably identifiable, and thus subject to HIPAA, GDPR, and other privacy regulations. Intensity Analytics' solution overcomes these problems. The data is revocable, as the reference data automatically changes when a username or password is used (since the effort profile changes with each additional input) and privacy is preserved.

Independent studies with hundreds of participants, conducted by Dr. Donald Gantz, emeritus dean of the School of Engineering at George Mason University, confirmed the unique and highly accurate capabilities of the technology and noted its ease of use, achieving these results with "little to no user training."

Rome concluded, "Our first patent is a significant milestone and we are also pleased to announce new funding, bringing our total to nearly $5 million. Our highly-experienced team of mathematicians and security experts operates extremely efficiently. We have developed a proprietary code base and framework that is relevant across numerous verticals including existing security software providers, financial services, government/defense, healthcare, e-commerce, online education, legal and others. We have earned a foundational security patent for the rapidly-growing authentication market and we expect this technology to have an outsized impact on how organizations protect themselves and their customers going forward."

About Intensity Analytics:

Founded in 2009 by a group of entrepreneurs that have been working together for decades on some of the biggest and most secure data projects in the world, Intensity Analytics develops next-generation, physical user and entity behavioral analytics ("physical UEBA") security software technology. IA goes beyond simple, first-generation keystroke dynamics solutions by analyzing the effort individuals expend while typing, and maintaining a focus on building sophisticated, new-thinking algorithms to take authentication from traditional credential verification to the point of identity recognition. Intensity Analytics' legal IP work is handled by Schwegman Lundberg & Woessner.

For more information, please visit intensityanalytics.com

Media Contact:

Alex Wellins

The Blueshirt Group

alex@blueshirtgroup.com