



Security

ID Analytics for Authentication

Network-Based Identification Platform Is Based On Identity Risk

June 30, 2008

Available as a packaged client browser or an API for integration with existing online systems, ID Analytics for Authentication seeks to provide the ability to positively and automatically authenticate the person behind selected transactions. A hosted platform, the product relies both on the vendor's ID Network repository of aggregated identity information as well as components that can analyze that information and provide response actions in real-time.

The vendor states that their ID Network is a proprietary, cross-company aggregation of identity information, "...a national compilation of identity information from Fortune 100 companies" who contribute customer identity data. It includes 360 billion attributes and 2 million reported frauds, which has been extended and linked with personal identification information and online ID elements, such as IP address, device fingerprints, E-mail addresses, and locations. ID Analytics for Authentication compares the transaction and identity in question to this bed of information to generate a risk-based analysis of the individual's identity (using the vendor's ID Score-Risk technology). This risk score can, in turn, trigger further authentication action by the platform should the risk be determined to be high; and can allow (i.e., authenticate) the transaction directly if the risk is low without requiring further interaction from the end user.

The vendor states that the raw data within their repository is not sold or shared, nor is it shared across the contributing organizations.

If the risk is high, the platform turns to the vendor's Certain ID technology, which also examines the existing ID Network information and analyzes both the information pertaining to the individual in question as well as how that individual interacts with other individuals towards the goal of automatically generating challenge questions for the end user based on the aggregated information. The vendor states that these questions are based on information from the ID Network and not from public records; and as such would be very difficult to answer by potential bad guys. Customization options allow the organization to specify the number and type of questions that are asked, and the number of correct answers required for authentication. The number of correct answers can further be dynamically adjusted by the ID Score-Risk itself (i.e., riskier IDs require more correct question answers for verification).

Contact ID Analytics for further information.

product submission by EITPlanet Staff