Ovum
TMT intelligence | informa

On the Radar: NuDetect uses behavioral biometrics to detect security violations and verify trusted users

Publication Date: 20 Oct 2017 | Product code: IT0021-000263

Adam Holtby

Summary

Catalyst

Balancing strong security with an optimal user experience continues to be a major challenge for those fighting cybercrime. The easy availability of personally identifiable information (PII) through hacking, breaches, and leaks undermines the basic user authentication and verification solutions. This has prompted the need for multifactor authentication, adding friction to the user experience. But fraudsters are increasingly using sophisticated automation and other techniques to record, replay, and impersonate these mechanisms, circumventing what was until recently thought to be highly secure authentication. Increasingly, attacks also occur after an apparently valid user authentication process, with takeovers and remote attacks that take control of an online session. Biometrics have been seen as a way to counter the authentication issue, and behavioral biometrics that passively review the actions of users throughout a session to determine if the interaction is with the actual person identified are becoming mainstream. With its NuDetect behavioral biometrics solution, NuData brings a multimodal four-layered approach to this problem to combine different biometric, behavior, and device metrics to detect and flag security violations and verify trusted good users.

Key messages

- NuDetect incorporates four integrated analysis layers (device and location analytics, passive biometrics, behavioral analytics, and real-time entity linking) in a cloud consortium.
- NuData offers access to an aggregated behavioral intelligence cloud, linking intelligence using machine learning techniques, leveraging 97 billion behavioral events analyzed in 2016.
- NuDetect provides continuous real-time fraud prevention with reduced friction.
- The solution cannot be mimicked or replicated, even when stolen credentials, identities, and "clean" devices are used.

Ovum view

Ovum has long maintained that having multiple layers of security that augment each other is a sensible approach to combating fraud and mitigating security risks, yet doing this without diminishing the user experience has always been an additional challenge. The hackers have increased their sophistication, and we are seeing more complex types of automation, such as GUI Scripts that mimic human input, as well as the manipulation of the web browser to mimic and replay what would appear to be, at face value, human input.

Behavioral biometrics tracks the way a user interacts with the system and provides a unique "signature" based on multiple measured aspects of that behavior, from the way the user swipes a screen to the devices they use and when and where they use them. Providing behavioral biometrics that rapidly identifies that the user is who he or she says they are (or a friendly known device, in the case of IoT), NuDetect can reduce the need for other forms of authentication and thereby eliminate friction for known trusted users, introducing friction intelligently to risk.

Early confirmation of identity also reduces the chances and cost of flagging up false positives. NuDetect's four-layer approach provides a solution that allows the platform to deliver deep intelligence

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

around the user's behavior in real time. It provides intelligence to both substantiate the validity of the user and identify risky or unwanted behavior.

Recommendations for enterprises

Why put NuDetect on your radar?

Customers engage NuData because of the issues arising from new account fraud, account takeover (ATO), and automated attacks, which for many e-commerce and fintech companies are on the rise. The use of a behavioral biometrics service that offers little or no friction – and potentially improves the user experience – is a key reason to look seriously at this technology. Currently, it is the larger financial and online companies that mainly use this service, but as behavioral biometrics become mainstream, Ovum expects to see more organizations adopt this type of technology. It is clearly appropriate for e-commerce, m-commerce, and digital goods businesses, as well as banking and financial institutions, credit bureaus, and online insurance, gaming, online gambling, and healthcare providers. In fact, it could be useful to any company that needs to verify customers online. It is also interesting for those involved in large-scale IoT infrastructures where the combination of session and biometric information will provide richer context around potential cyber and device-specific threats.

Highlights

NuDetect's key strength lies in its multimodal model, which merges appropriate layers of intelligence to provide a highly accurate evaluation of the risks associated with a session and reduces false positives that can result in unnecessary challenges and friction for the good user. NuDetect determines a risk score that it varies in real time using continual assessment, and challenges when appropriate to verify identity. If it sees potentially risky behavior or anomalies, it may offer more aggressive challenges so that the authentication and detection processes can be varied in real time to suit the perceived risk. The score returned can be used by other solutions and rules-based systems to prompt other actions or amend the characteristics of the session being monitored.

Device, connection, and location identification

NuData collects and analyzes hundreds of sensory inputs and data points to enhance the device ID and location data. This enhanced validation incorporates accelerometer data, magnetometer data, gyroscopic data, and users' unique settings.

Behavioral analytics

This involves continuously verifying that the user is behaving as expected. This is based on the behavior of each user's history, in terms of the way they use devices or act during sessions.

Passive (invisible) biometric verification

NuData looks at and analyzes the way groups of users – both good and bad – behave, detecting multiple elements, such as forms filled out of order or too fast to be human input, angles the device is

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

held in, and even the pressure applied when a person types. It also looks for commonality of behaviors for known risks and can highlight potential threats such as imposters and takeovers.

Real-time trust consortium

NuData connects related events together based on their behavior. It can identify fraud groups by their collective behavior. NuData analyzed 97 billion online interactions yearly in its trust consortium to build and share aggregated profiles of typical behaviors.

By combining known behaviors of risk types and groups with the rapid identification of good users based on their historic behavior, NuDetect can identify a very high percentage of risks and trigger the appropriate action. This analysis continuously informs clients of fraud risk in real time and gives them choices about what actions to take even before a transaction is completed.

NuDetect provides

- anomaly and pattern recognition and detection
- human vs. machine detection
- advanced human vs. human-like detection
- historical user profiling
- detection of malicious scripts, malware, injection
- advanced warning of account testing and harvesting
- identification of rogue aggregators mimicking trusted access.

Architecture

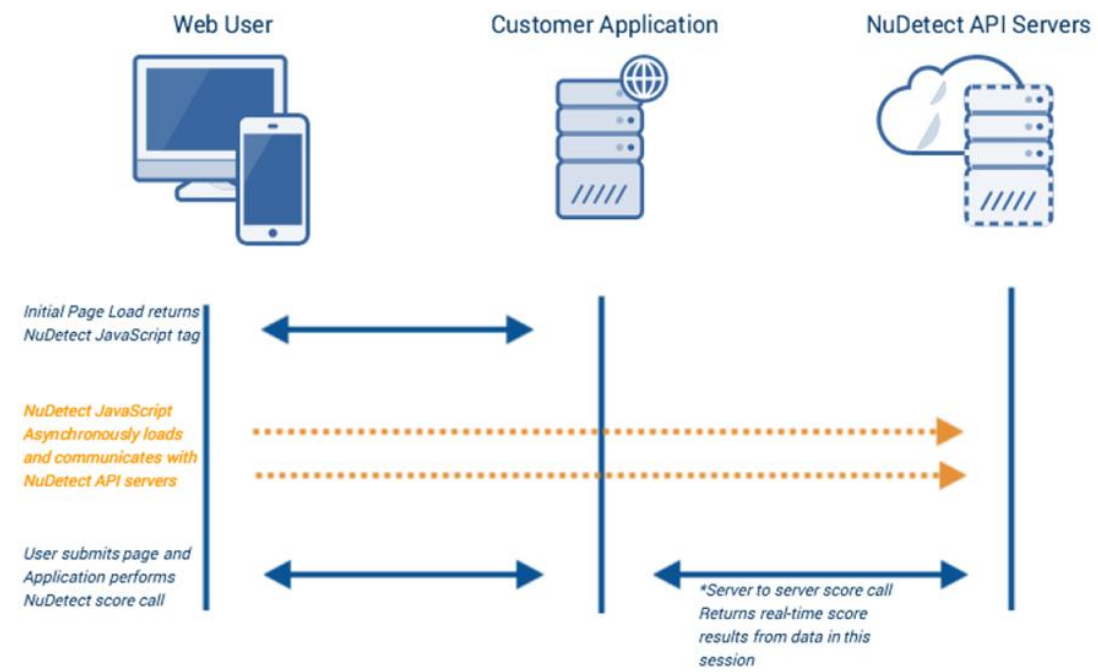
NuDetect is a SaaS, cloud-hosted, private cloud, or on-premises solution integrated using JavaScript (JS) in the web browser and a client library on the web server. Both JS and the client library collect and provide relevant data points for analysis. The JavaScript installation can be either static or dynamically applied "on the fly" and communicates to NuData, over API, using the client library. This method of integration is quick to deliver for customers, while providing easy maintenance and feature upgrades. Integration using a mobile SDK is also delivered in a similar method. Assessment scoring and information from NuData is passed back to the customer in real time, so the applications can react automatically in the appropriate fashion.

As a user interacts with the various flows within the environment, data is collected and passed to the NuDetect Machine Learning Engine in real time to be analyzed, with the result of returning scoring, threat, and behavioral intelligence that can be incorporated into a customer's risk model to enhance current capabilities.

NuDetect integrates into the customer application at specific placements, such as the login, account creation, purchase, and any other related placements. The integration points are simple: first, on page load, a NuDetect JavaScript tag is included in the Customer Application view, and second, on page submit, a server-to-server API call is made to push application data to the NuDetect platform and optionally request a real-time risk and trust score based on entities and data provided in the current session.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Figure 1: NuDetect Architecture



Source: NuData

Background

NuData Security was founded in 2008, originally with the intention of finding a better way to identify human vs. non-human interactions online, but rapidly recognized that it could offer a much more substantive solution. The company is headquartered in Vancouver, BC, Canada. NuData was privately held until April 3, 2017, when it was acquired as a wholly owned subsidiary of Mastercard. Key executives are Michel Giasson (CEO), Christopher Bailey (CTO), Jules Campeau (CRO), Curtis Sikorsky (CFO), Ryan Wilk (VP of customer success), and Robert Capps (VP of business development).

Current position

The company has 65+ employees based in its Vancouver offices, with sales representation throughout North America and Europe. NuData works with a variety of partners, including Early Warning, Accertify, Arvato, AWS, and Experian. The main technology partner is Amazon Web Services (AWS), which is used for hosting services. Current customers of the solution include two of the world's top 10 banks.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: NuData

Product name	NuDetect	**Product classification**	Financial technology, behavioral biometrics, user authentication, identity proofing, fraud/risk management
Version number	2.2	**Release date**	
Industries covered	Financial services, e-commerce, banking, retail, digital goods, gaming, online gambling, healthcare	**Geographies covered**	All
Relevant company sizes	Mainly larger companies at present	**Licensing options**	Perpetual; one-year term; one-year SaaS; transactional-based model
URL	https://nudatasecurity.com/	**Routes to market**	Direct customer engagement, regional partners
Company headquarters	Vancouver, Canada	**Number of employees**	65

Source: NuData

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Authors

Martin Gandar, Associate Senior Analyst

Adam Holtby, Research Analyst

adam.holtby@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum
TMT intelligence | informa

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo