Ovum
TMT intelligence | informa

On the Radar: Averon provides Direct Autonomous Authentication

Averon delivers automated, frictionless, and secure user verification and authentication facilities

Publication Date: 21 Mar 2018 | Product code: INT003-000103

Andrew Kellett

Summary

Catalyst

The Averon Direct Autonomous Authentication (DAA) platform and service delivery engine brings together smartphone SIM technology and real-time data signaling to automatically and securely authenticate users through their devices. Its API-based technology is used to trace the origin of data packets and verify that each transaction was initiated by the user's authorized device.

Key messages

- The Averon DAA platform and service delivery engine is an automated, API-based identity verification and authentication platform.
- Averon DAA uses the same metering functionality that is provided by the major US wireless service providers to track the origin of each transaction/data packet.
- As such, DAA's identity verification and authentication solution is approved and used in the solutions offered by those same service providers.
- The automated nature of Averon's technology ensures that it is unaffected by and therefore safe from credential reuse, second-factor code intercepts, and device-based interception.

Ovum view

There are so many different forms of authentication available, and choosing the right ones to meet user and business protection requirements has become an onerous task. Many organizations continue to rely on basic username and password approaches, and even where these are allied to stronger two-factor authentication, there is too much reliance on users to maintain, update, and keep safe their credentials. Organizations looking for a secure, automated approach to user verification and authentication should consider Averon's frictionless DAA technology.

Recommendations for enterprises

Why put Averon DAA on your radar?

User and device security is a major concern for all types of organization when providing always-available online access to business systems for the mobile workforce. Existing authentication solutions that require manual input and two-factor links via SMS, app downloads, and/or email can add to rather than reduce the frustrations associated with authentication and access control. For organizations that are looking for a fully automated replacement, Averon DAA can offer a safe, fast, and frictionless alternative.

Highlights

The Averon DAA platform and service delivery engine is an automated, API-based identity verification and authentication platform. It offers real-time, frictionless authentication controls for mobile users, requiring no software installations on end-user devices, no apps to maintain, and, importantly, no manual interventions from users during the verification and authorization-of-access processes.

The Averon DAA technology, which is patent protected in the US and internationally, uses smartphone SIM technology and real-time data signaling techniques to trace and verify the origin of data packets and confirm that each transaction was initiated by an authorized user's device.

Averon works closely with the major US wireless service providers, which are both technology partners and users of its authentication technology. The key business protection benefits on offer include device identity controls that make use of the same security standards used by the carriers for metering customer data usage. This approach makes the DAA solution immune to social engineering and client-based malware attacks. The automated, real-time nature of the technology also frees it from credential reuse, second-factor code intercepts, and device-based interception.

In operational use, the Averon DAA platform manages and fulfills the following tasks:

- Each time a user initiates a transaction, the Averon customer's internet service sends a request to the DAA platform that includes a hashed representation of the user's authorized mobile device phone number.
- Averon DAA generates and returns Session ID and TrapURL information that the internet service delivers to the mobile device.
- Dependent on the requirement, JavaScript (from a website) or a RESTful API (from an app) is used to contact the Averon server using http(s) requests.
- Averon DAA extracts a hash of the mobile phone number and compares it to the hash of the number being analyzed to confirmed a pass or fail result.
- The pass or fail result is encrypted and returned to the originating customer internet service, where a positive result allows the transaction to continue.

The Averon DAA platform can function just as effectively whether mobile devices are connected to the customer organization's home carrier network or roaming on third-party networks. DAA technology can be used to replace less secure legacy authentication methods such as SMS, app downloads, and email links. Although the DAA solution is set up to provide the only user verification method needed to keep business systems safe, in some situations it can also be used as the second factor in a strong authentication process, such as when the technology is integrated and combined with biometric controls.

Background

Averon was founded in 2015 by Lea Tarnowski and Wendell Brown, and its corporate headquarters are in San Francisco, California. In March 2018, the company closed its Series A funding round after raising $13.3m, the leading contributors being Avalon Ventures and Salesforce founder and CEO Marc Benioff.

The company's senior management team consists of an experienced group of business managers, engineers, and cybersecurity experts. CEO and founder Wendell Brown is an acclaimed computer scientist, entrepreneur, and inventor, and is best known for his innovations in telecommunications and mobile security. COO, company president, and co-founder Lea Tarnowski is an accomplished investor in business mobile and consumer internet technology, and prior to Averon she held a directorship role at Northzone and was an associate at Morgan Stanley and McKinsey. Mark Klein, a Silicon Valley veteran, is the company's chief data scientist and has co-founded several successful technology start-ups. Mark Herschberg, the company's CTO, has worked in Fortune 500 organizations and start-ups, tracking cybercriminals on the dark web and developing wireless application platforms and big data tools. Aaron Mahone, the company's director of operations and finance, was formally a management consultant at KPMG and has worked in the healthcare sector.

Current position

Averon believes that the total addressable market for authentication solutions and therefore the potential market opportunity for its DAA platform currently exceeds $50bn. Its key target markets are e-commerce organizations, where the growth in cardholder not present (CNP) and transaction fraud causes huge problems, and banking and financial institutions, which are also at risk from transaction fraud as well as the inefficient access management controls currently in use.

However, these are just the tip-of-the-iceberg opportunities, as the technology can be used to solve authentication problems across most business sectors. Other target markets include healthcare, enterprise, and the government sector, where security, fraud prevention, and regulatory, compliance, and data protection issues continue to grow. Averon's potential customer is any end-user organization or managed service provider (MSP) that conducts some type of authentication through online touchpoints (websites, apps, email, and so on).

Data sheet

Key facts

Table 1: Data sheet: Averon

Product name	Direct Autonomous Authentication (DAA)	**Product classification**	Identity verification and authentication
Version number	2.3.144	**Release date**	November 2017
Industries covered	Fintech and banking, e-commerce, healthcare, government, and the smart car sector	**Geographies covered**	North America
Relevant company sizes	All sizes	**Licensing options**	Perpetual, term, and software-as-a-service (SaaS)
URL	https://www.averon.com/	**Routes to market**	Direct and through technology and channel partners
Company headquarters	San Francisco, CA, US	**Number of employees**	20

Source: Ovum

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.

Further reading

On the Radar: iovation prevents fraud and authenticates consumers with device intel, INT003-000035 (January 2018)

"It's a busy time for M&A in privileged access management," INT003-000045 (February 2018)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@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.

Copyright notice and disclaimer

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.

CONTACT US

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

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