Ovum
TMT intelligence | informa

On the Radar: Entrust Datacard takes aim at authentication-as-a-service market with IntelliTrust

Mobile smart credentials bolster security while streamlining user experience

Publication Date: 07 Sep 2017 | Product code: IT0022-001079

Rik Turner

Summary

Catalyst

Entrust Datacard has rebranded and revamped its Authentication Cloud Service, renaming it IntelliTrust and endowing it with features such as mobile smart credentials to raise its profile in the market for business-to-employee (B2E), business-to-business (B2B), and business-to-consumer (B2C) identity services.

Key messages

- IntelliTrust is a software-as-a-service (SaaS) authentication offering.
- It replaces the so-called “second” factor such as a token or one-time password (OTP) with high assurance mobile, behavioral biometric and device reputation checks.
- It also supports mobile smart credentials for workstation smartcard login and physical access.
- Self-learning capabilities are being added to IntelliTrust for a more predictive stance.

Ovum view

As identity services move online and go global, cloud-based authentication is a requirement, and the IntelliTrust service is a compelling offering in this context. The intersection of payments and information security is gaining momentum. Entrust Datacard offers a combination of trusted identity and secure transaction technologies to enable this development.

Recommendations for enterprises

Why put Entrust Datacard’s IntelliTrust on your radar?

By delivering authentication from the cloud and using next-generation mobile approaches, behavioral biometrics, and device reputation as the additional factor beyond user name and password, IntelliTrust can span B2E, B2B, and B2C use cases. The fact that the service can be white-labeled makes it suitable both for enterprises themselves to rebadge it, and for managed security service providers (MSSPs) to offer it under their own logo.

Highlights

The rationale behind IntelliTrust is that authentication needs to move beyond the conventional paradigm of:

- who you are (your name)
- what you know (your password)
- what you have (a token or an OTP delivered to a mobile phone, for example).

Driving this need for change is first the fact that the B2E environment where authentication began has evolved, thanks to developments such as cloud, mobile, and virtual desktop.

Second, the requirement in B2B, which is where authentication went next, has gone from granting employees of a partner company access to applications within your environment to having them access cloud-based applications based on federated identity.

The third and most recent area to require authentication capabilities, B2C, transforms it even further, because on the one hand, the numbers of users needing to log in can go into the millions, while on the other, the amount of information stored about them is far less than for employees or business partners.

Entrust Datacard speaks of the need for its customers to develop what it calls a “digital trust framework” that covers the interaction of people, systems, and, for the Internet of Things (IoT), the many things that will soon be connected to the internet and communicating autonomously on it. For systems, it offers its Entrust Authority PKI technology, while for things, it has the ioTrust platform. IntelliTrust addresses what it perceives as the requirements for authenticating people in the B2E, B2B, and B2C scenarios.

The cloud is the logical place to meet the authentication requirements of all three areas. To overcome the inevitable end-user friction caused by tokens and OTPs, Entrust Datacard supports technologies that enable identity verification to go on in the background, checking the identity of both the user and the device. IntelliTrust also comes with “click and drag” policy definition, so that administrators can define the parameters for risk-based authentication decisions, weighting, and ranges.

On the user side, the technological approach involves pattern and behavioral analysis, enabling the system to tell whether the person seeking authentication is using the mouse or touchpad on the laptop or swiping their smartphone screen in the same way as they have in the past.

On the device side, Entrust Datacard has recently introduced device intelligence, which assesses real-time device reputation with an anti-fraud network of more than 2 billion devices. IntelliTrust also supports so-called mobile smart credentials, including smart card-based security, with encryption and certificates on a mobile phone. With this approach, organizations can ensure the integrity of the user’s device before issuing a trusted smart credential.

There is clearly the potential on the B2E side to integrate authentication for network access and for physical access to facilities. IntelliTrust supports near-field communication (NFC) technology and QR codes for when someone is at a building entrance seeking access.

Background

Entrust Datacard is the result of the December 2013 acquisition of Entrust by the then Datacard Group, a vendor of secure identification and card personalization products. Entrust was a developer of technology for securing digital identities and information and a longtime player in the authentication market. It was taken private for $124m by Thoma Bravo in July 2009. After the acquisition, the merged entity became Entrust Datacard.

Entrust was founded in 1994 when Canadian networking vendor Nortel spun off its Secure Networks division. Its technology offering spans authentication, PKI, and services around SSL certificates such as issuance, management, and discovery. Datacard, which was founded in 1969, had products in identity card issuance, specialized card printers, desktop embossers, and passport systems, as well as the supporting software.

Entrust Datacard has offered on-premises authentication server technology since the 1990s, and launched its first cloud-based version of the product, Authentication Cloud Service, in 2016.

Current position

IntelliTrust is a cloud-based platform for the delivery of authentication services. It represents the next evolution of Authentication Cloud Service (version 3.0). It has multitenancy, with users having their own secure and dedicated area within the platform with their own customer-controlled keys.

This enables channel partners and MSSPs to resell the service and let each of their business customers rebadge the service with their own logos. White-labeling is a core part of the vendor's thinking for the service.

The charging mechanisms for IntelliTrust are designed to address different use cases. There is monthly billing on a per-user basis, which is suitable for the B2E and B2B scenarios, and a per-transaction alternative, which is more suited to B2C.

As for the competitive landscape, Entrust Datacard considers primary competitors to be the more specialist 2FA players like RSA and Duo, and believes that its ability to incorporate the strongest levels of authentication and the next generation of mobile and adaptive capabilities through a single unified platform are key differentiators for its offering.

Entrust Datacard's technology roadmap for IntelliTrust sees the platform gaining more predictive capabilities in 2018, performing pattern analysis with machine learning to enable it to flag anomalies and trigger some form of step-up challenge such as a face check. To this end, it is adding a self-learning feature to the Insight Engine that forms the core of IntelliTrust. The vendor also plans to deliver its first iteration of a dashboarding capability next year, adding more intelligence in 2019.

Entrust Datacard believes that everything begins with identity, across both the physical and digital realms. Its primary market focus is on payments and information security, and these two worlds are themselves beginning to intersect. Consumers, citizens, and enterprise employees are beginning to leverage one core identity to make purchases, move money, cross borders, access e-government portals, log onto networks, and enter secure buildings.

Data sheet

Key facts

Table 1: Data sheet: Entrust Datacard

Product name	IntelliTrust (formerly Authentication Cloud Service)	**Product classification**	Authentication as a service, adaptive auth as a service, high assurance auth as a service, fraud detection
Version number	3.0	**Release date**	October 2016
Industries covered	Professional services, manufacturing, education, energy and utilities, healthcare, high tech, banking and insurance, government, hospitality, retail, media and entertainment	**Geographies covered**	All, with points of presence in NA, Europe, Japan
Relevant company sizes	All	**Licensing options**	User subscription or transaction-based
URL	www.entrustdatacard.com/intellitrust	**Routes to market**	Direct, reseller channel partners, managed service providers, SIs
Company headquarters	Minneapolis, MN, US	**Number of employees**	2,000+

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: Entrust Datacard's ioTrust provides identity and data security to the Internet of Things, IT0022-000975 (May 2017)

RSA crafts a coherent message combining GRC, fraud, identity, and threat defense, IT0022-000840 (December 2016)

On the Radar: Duo secures remote access with easy-to-use 2FA, IT0022-000860 (December 2016)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@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

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