Brought to you by Informa Tech

Publication date:
26 Jul 2024
Author(s):
Rik Turner, Senior Principal Analyst

On the Radar: Transmit Security onboards, authenticates, and verifies identities

Summary

Catalyst

Transmit Security (Transmit) develops identity management and antifraud technology. Its platform is used in B2B and B2C use cases, the latter being commonly referred to as customer identity and access management (CIAM). Transmit also covers the B2B2C scenario, such as in consumer-to-travel agent-to-airline transactions. Underpinning all its capabilities is identity orchestration technology, which not only promotes the seamless handling of identities across onboarding, authentication, and detection and response to threats but also enables Transmit to integrate with third-party tools in each of those areas.

Omdia view

As corporate infrastructures have become more complex, incorporating cloud-based assets alongside on-premises systems, they have also become more porous and, thus more difficult to secure. While protecting infrastructure (endpoints, servers, networks, and storage devices) remains of critical importance, identity clearly has moved center stage in enterprise cybersecurity, just as data security has gained in criticality, thanks to the widespread adoption of cloud computing and the resulting data sprawl.

Managing identities is a key capability for employees, partners, contractors, and customers. However, scale and user experience are vital attributes in this last domain (the B2C scenario). Large companies have workforces in the hundreds of thousands and may interact with a similar number of partners and suppliers. By contrast, the largest banks commonly serve hundreds of millions of customers, each one of whom must

enjoy an online service experience that can guarantee their loyalty and appetite for further engagement. Meanwhile, security is an integral part of the equation, both for the end customer and the institution.

This is the world of CIAM. While several major players are already in this space, Transmit's identity orchestration capabilities, not to mention its antifraud nous, stand it in good stead to win business here.

Why put Transmit Security on your radar?

While it undoubtedly has expertise in key areas, such as customer onboarding, authentication, and fraud detection, Transmit's real crown jewels reside in its ability to orchestrate and secure the full identity lifecycle. Transmit can be brought into an account for any single facet of that lifecycle. It can also underpin it by orchestrating third-party systems in an organization's identity infrastructure. This should make it possible to streamline the creation, handling, and maintenance of identities, as well as their timely deletion when and where appropriate.

Market context

Identity management, particularly in B2C interactions, has grown increasingly complex in recent years. First, there was the move to e-commerce, with more engagement with customers online. Then came the proliferation of devices from which customers can contact an organization (e.g., a laptop, smartphone, or tablet), each requiring a different form factor for the content served to them.

The multi-channel requirement

Beyond the form factor, many areas of activity—online and mobile channels—must coexist with other channels (e.g., in financial services, think physical branches, phone banking, and even in some cases, actual letters, also known as "snail mail"). Across them all, there is the need for a consistent experience and seamless service. For example, if loan information is provided online and the customer calls the next day to find out about their application, then a bank manager should have that data on their screen during the conversation.

Antifraud

Then, there is the challenge of defending institutions and customers from fraud. As interactions have moved online, fraudsters have followed. Registering false identities and hijacking user sessions are now commonplace ways of committing fraud. As a result, a secure onboarding experience for new customers coming onto a platform and for those resetting their account because they have lost their phone or whatever is fundamental. From the perspective of the company onboarding them, it is necessary to certify that a person is who they claim to be, which is achieved through identity validation or identity proofing.

Once a person is registered, an authentication process must be performed each time they log in to the service, and it should be secure and user-friendly. Although minimal friction and maximal security may seem at odds, they must be two faces of the same platform. Customers can access more trivial operations, such as consulting their bank account. However, anything that entails a transfer of funds may mandate an escalation of authentication requirements on a sliding scale, depending on the value of the proposed transaction.

Detection and response

Finally, there is the need to defend the application from attack in real time. This implies a detection and response capability tied in with the identity repository, where anomalous behavior can be detected and remedial action is taken.

Different suppliers will frequently provide various systems that enable all the above functionality. As such, there is an opportunity to deliver an underlying platform to orchestrate the management of identities across them all. This capability has come to be known as identity orchestration in recent years, and it is Transmit's claim to fame. It underpins the vendor's entire identity security platform. It also enables it to offer a whole suite of capabilities or to work with third-party packages in any of the areas of activity outlined above.

Product/service overview

Transmit takes its technology to market as a platform, namely the Transmit Security Platform, with different modules for various use cases. These use cases are as follows:

- **Identity verification (IDV):** With customer onboarding itself an activity increasingly carried out in online channels rather than face to face, organizations must certify that the identity being presented to them to become an account holder is indeed that of the person presenting it. This entails the automated analysis of an ID document, such as a passport or driver's license, and a comparison with a selfie taken on the presenter's phone.
- **Authentication services:** This technology enables the person to log in and transact with the organization once the identity has been verified and an account created. This can be done using passkeys (Transmit is a member of the FIDO Alliance, whose technology standards underpin passkey functionality), passwordless technology, such as biometrics, email magic links, and other multi-factor authentication (MFA) forms.
- **Identity management:** This involves the ongoing management of the identities that have been created, with a single identity store serving all channels, unified user profiles, single sign-on (SSO), and role-based access control (RBAC) to maintain the security of the identity repository.
- **Identity orchestration:** This is, in essence, the glue that holds the consolidated identity stack together, enabling centralized decision-making and automating the customer journey through an organization. Identity orchestration underpins consolidation because an organization may not have every other module provided by Transmit. However, it will nonetheless need all parts of the stack to work together to optimize the customer experience and enable fraud protection and security.
- **Fraud detection and response (antifraud and scam detection):** The first four modules listed above combine to enable Transmit, beyond managing customer identities, to play in the fraud space:
  - Identities are validated on their first appearance on an organization's platform.
  - Then, check for signs of tampering or spoofing every time the customer logs back in.
  - Finally, identity management is controlled via RBAC to ensure that rogue insiders cannot alter the information or configuration related to it.

The range of Transmit's modules and platform approach enable the company to sell its technology for different individual use cases, such as secure onboarding, working with third-party tools for other parts of the stack, and orchestrating the customer journey with its identity orchestration capability. This also means there is the potential for upselling once it is in an account and demonstrating the strength of its technology. The mantra here is "Orchestrate to Consolidate."

User events drive Transmit's platform power. Transmit's focus is on CIAM rather than the business-to-employee (B2E) world of traditional identity and access management (IAM), which, on the contrary, is driven by directories. It notes that some of its competitors in CIAM, such as ForgeRock, remain directory-based, which Transmit believes is a significant drawback regarding the latency it adds to the platform. Transmit syncs with directories, but its operation is not based on them.

Company information

Background

CEO Mickey Boodaei and President Rakesh Loonkar founded Transmit in 2014. Both men were previously the co-founders of Trusteer, a security vendor specializing in financial services requirements. IBM acquired it in 2013 for an estimated $1bn. Likewise, Boodaei served as CEO and Loonkar as President.

Transmit has raised a total of $583m in two funding rounds. Most recently, it announced a $543m Series A round in July 2021, led by Insight Partners and General Atlantic, with additional investments from Cyberstarts, Geodesic, SYN Ventures, Vintage Investment Partners, and Artisanal Ventures. This was thought to be the largest Series A to date.

Current position

The Transmit Security Platform (which is being renamed "Mosaic") can be deployed in the cloud or on a customer's premises, which is important for some of the large banks the company works with.

The vendor currently has a customer base of roughly 100 organizations, including large financial institutions such as Citibank, J.P. Morgan, UBS, HSBC, major telecom operators, other large enterprises, and governments.

Transmit's competitive landscape varies by the area of activity. In antifraud, it goes up against IBM's Trusteer and other specialists. In ID proofing, there are the likes of Jumio. In CIAM, there are several vendors, including Okta (via Auth0), Ping, IBM, and Microsoft. ForgeRock was also a significant player in CIAM. Yet, now that its owner, Thoma Bravo, has merged it with Ping, a more formidable competitor may emerge.

That said, in the identity orchestration market, Ping's DaVinci platform is still relatively new and is currently more mid-market focused. ForgeRock's Trees platform was launched several years after the Transmit Security Platform, and it still does not compete at the high end of the market.

Future plans

Identity, fraud detection and prevention, and cybersecurity are converging. The threat landscape has repeatedly pointed to this convergence in recent years, with identity becoming a significant part of the attack surface and a constant barrage of attacks on IAM platforms like Okta. Furthermore, organizations

start to feel the pain of managing multiple point products to secure and manage the entire identity lifecycle of their customers, partners, and machines (which is short for software, workloads, and containers). With all this in mind, some key future areas of

Transmit's platform expansion plans include:

- **Enhanced antifraud, scam, and mule account detection:** The availability of artificial intelligence (AI)/machine learning (ML) services, such as FraudGPT and EvilGPT, adds to the complexities and pace of fraud. Traditional antifraud technology struggles to keep up with exploits such as authorized push payment (APP) fraud. Transmit aims to develop ways organizations can catch such scams without increasing operational costs or negatively impacting customers/partners.
- **Generative artificial intelligence (GenAI) for administration and security/optimization of user journey workflows**: Since attackers now use GenAI tools to help develop their attack campaigns, the sensible response is to leverage the technology to respond. Transmit Security was early among the first identity-security vendors in leveraging large language models (LLMs) built into the administrative interfaces to help administrators "short-circuit" tasks:
  - They can use natural language in a chatbox (within the Transmit Security Platform interface) to input questions/tasks such as "Please generate a report that shows me all of the failed authentication attempts….". This can help IT leaders gain insight into various identity lifecycle threats, issues, and other concerns versus without traversing multiple interfaces or generating a disparate set of reports.
  - Transmit is also developing a "Co-Pilot" for creating user journeys (recommended paths/workflows, etc.). This can help administrators quickly build user journey workflows (such as secure onboarding) and ensure they are optimized and secured. Optimization comes from the transmit security platform automatically making intelligent recommendations (similar to predictive text in common word processing platforms). Enhanced security of these workflows comes by offering embedded static application security testing (SAST) for secure code creation of journeys.
- **Service resilience**: Because of recent attacks on popular IAM vendors, incident response and the resilience of these systems are now more important than ever. Transmit Security expects that IAM infrastructure attacks will continue into the future. In response, it is investing in processes and technology for both incident response and service resilience, namely:
  - Mechanisms to ensure the service can withstand an outage beyond the typical "9s" metric.
  - An active-active failover offering, whereby the vendor can fail to another cloud. For example, if Amazon Web Services (AWS) fails, the system can actively switch to Google Cloud Platform (GCP).

Key facts

Table 1: Data sheet: Transmit Security

Product/service name	Mosaic	**Product classification**	Identity and antifraud
Version number	10.5	**Release date**	2016
Industries covered	Banking, financial services, telcos, retail, airlines, healthcare, and government	**Geographies covered**	North America; Latin America; Europe, the Middle East, and Africa (EMEA); Asia Pacific and Japan.
Relevant company sizes	Large enterprises	**Licensing options**	Cloud and on-premises based on size
URL	transmitsecurity.com	**Routes to market**	Large partners—such as PWC, Deloitte, and EY—and direct
Company headquarters	Tel Aviv, Israel and Boston, Massachusetts, US	**Number of employees**	400

Source: Omdia

Analyst comment

The identity management market is already huge, while the market for identity orchestration is still very much in its infancy—there are still no corporate budgets specifically allocated to this capability. As a result, an identity orchestration vendor must find other ways to market itself, at least for the time being. For example, it was notable that when Transmit landed its monster half-billion-dollar funding round in 2021, the company positioned itself as a vendor of passwordless authentication technology.

Transmit sees a trend for IDV, IAM, and fraud detection to converge, with orchestration as the "glue" that brings all these components together. While attackers think and attack across the identity lifecycle, where siloed products typically perform each function, a standalone IDV platform used just for onboarding, for instance, will not see attacks in other channels.

Hence, the need for orchestration. This also underpins a trend for vendors in one of the segments mentioned by Transmit to expand into the others. For instance:

- In April 2024, authentication heavyweight Entrust bought IDV vendor OnFido.
- In October 2023, passwordless authentication vendor HYPR launched its HYPR Affirm IDV product.
- In June 2021, Ping bought antifraud vendor SecuredTouch.

Transmit can cast itself today as an enabler of customer onboarding, underpinned by its IDV capability, general identity management for B2C environments, identity detection and response, and even antifraud

technology. Its identity orchestration, an incipient market about which Omdia recently published a Market Landscape report (see the **Further reading** section below), underpins all these capabilities.

Orchestration is of growing importance to large enterprises in the financial services, retail, travel, and hospitality industries, all of whom must balance the need to provide a seamless online customer experience with the security of their customers' money and their own. With customer bases often running into the tens of millions and multiple silos of identity management technology deployed to control their interactions, identity orchestration holds the promise of joined-up operations that can both satisfy the customer and keep them secure.

While it competes against heavyweights in each of its market segments, Transmit is off to a good start. It has built up a customer base that includes major brands with huge identity requirements, and its most recent funding round has given it the kind of reserves that will enable it to mount significant marketing campaigns. Transmit must now evangelize on the merits of identity orchestration, even while winning deals in the individual use cases it covers. Omdia suspects identity orchestration is a market that will coalesce over the next couple of years and sees Transmit as well-placed to be a leading player in that space.

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. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Market Landscape: Identity Orchestration (June 2024)

On the Radar: Strata offers identity orchestration across hybrid and multicloud environments (March 2024)

On the Radar: AU10TIX offers rapid ID verification with support for verifiable credentials (September 2023)

Omdia Universe: Identity-as-a-Service Solution, 2023 (June 2023) *On the Radar: Jumio aims for a role beyond ID proofing with its KYX Platform* (April 2022)

On the Radar: 1Kosmos leverages distributed identity for ID proofing and passwordless authentication (April 2022)

"ForgeRock to combine with Ping Identity" (September 2023)

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

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

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com