ON THE
RADAR

Publication date
2 Nov 2022

Author
Rik Turner
Principal Analyst

Report: On the Radar Classification: SaaS data Security

Brought to you by Informa Tech

Brought to you by Informa Tech
OMDIA

Publication date:
02 Nov 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

On the Radar: DoControl provides SaaS data access control

Summary

Catalyst

DoControl offers a security platform for data in software-as-a-service (SaaS) applications. More specifically, it provides SaaS data access control technology.

Omdia view

The SaaS market is booming, with new corporate customers signing up and new applications coming to market apace. Security for so much SaaS usage is thus a vital requirement, and one approach to addressing it is to start with the data: find out where it resides, who can access it, and where else it can flow to. Once an organization has achieved that comprehensive view of its cloud data landscape, it can start to remediate issues, such as reining in excessive permissions/access rights and terminating data sharing that it deems unnecessary or risky. These are the kinds of actions that the DoControl platform enables.

The SaaS security market is also undergoing something of a renaissance at the moment, with multiple vendors, many of them start-ups, offering data security or access control/management to supplement or replace the old-school approaches of cloud access security brokers (CASBs) and data loss prevention (DLP). DoControl is very much in the data-centric camp, which is attracting considerable attention both from the VC community and end user organizations. This vendor's approach of building a full inventory then updating it with continuous monitoring, plus alerting on anomalies and no-code workflows for remediation, positions it to conquer a significant share of this emerging segment.

Why put DoControl on your radar?

The fact that DoControl not only inventories all SaaS data repositories but keeps its list up to date, alerts on apparent misuse and, crucially, enables remediation with no-code workflows is a powerful combination that makes a compelling argument for the vendor to be on the watchlist of any organization using SaaS apps.

Market context

The SaaS delivery model for applications has enjoyed huge success since the company that was arguably its pioneer, Salesforce, was founded, way back in 1999.

According to the most recent edition of Omdia's Cloud Services Market Size and Forecast, published in July 2022, the SaaS market had reached $139.8bn in calendar year 2021, thereby retaining its overall leadership among the delivery modes, ahead of both infrastructure- and platform-as-a-service (IaaS and PaaS). Together IaaS and PaaS now outstrip SaaS, however, which a few years ago was not the case.

One qualifying note here is that Omdia splits out a further market segment called container-as-a-service (CaaS), whose $68bn revenues in CY21 could, through a slightly different lens, be split evenly between IaaS and PaaS, which would send the IaaS number ($132bn without any CaaS component) over the SaaS total for the year.

Finally, it should also be mentioned that Omdia predicts a further huge uptick in SaaS, reaching $328bn in 2026.

Clearly much of this success can be attributed to the ease with which SaaS can be adopted, often requiring no more than a quick sign-up process and a corporate credit card. Indeed, so successful has SaaS been that it has thrown up major challenges for IT and security teams over the last decade, the first of which was a direct result of its ease of adoption: shadow IT.

The fact that line-of-business users could sign up for a new SaaS app at the drop of a hat resulted in a loss of visibility, and thus also control, on the part of IT and SecOps, an issue that led to the rise, in the mid-2010s, of CASB technology.

CASBs use either a proxy- or API-based approach, or often a combination of both, to SaaS security. They identify which SaaS apps are in use within an organization, and by whom, then enforce policies that can vary from outright blocking to forcing data encryption, limiting access to the read-only variety, and blocking actions such as copy and paste or forwarding via email etc.

For a few years CASB was the sole SaaS-focused security tool, with the focus of innovation shifting to IaaS and PaaS security (with tools names such as cloud workload protection and cloud security posture management). More recently, however, we have seen an upsurge in new approaches to SaaS security, driven by the fact that SaaS is still burgeoning, and indeed received a further fillip from the coronavirus pandemic, which supercharged digital transformation projects and drove ever more knowledge workers into working from home.

These new approaches address other types of SaaS security issues: SaaS security posture management (SSPM) tackles the problem of misconfigurations, data security posture management (DSPM), while not SaaS- or even cloud-specific, seeks to discover, classify, and protect its customers' data, wherever it resides, and cloud permissions management (CPM, which other analysts call CIEM) started looking at access rights in

IaaS and PaaS environments, but is now adding support for SaaS apps too. DoControl provides data access monitoring, orchestration, and remediation for SaaS apps.

Product/service overview

DoControl's eponymous product works via a phased process that begins with onboarding all the sanctioned SaaS applications in use within a customer's organization. This is done by creating a connection with each app through a secure OAuth flow that allows DoControl access to the necessary metadata and change logs.

DoControl then builds an inventory of all sanctioned and unsanctioned SaaS applications (via OAuth), as well as all users, external collaborators, assets, third-party domains, and so on. The inventory provides visibility and analytics, which can be used for security investigations, third-party vendors off-boarding, compliance evidence, and incident response. While the first scan of the customer's SaaS estate is a complete one, the inventory can be updated thereafter by adding the deltas as changes take place.

From this baseline of what SaaS is in use within an organization, DoControl proceeds to monitor all data access on those SaaS applications in a continuous fashion, with reporting, dashboards, and alerting. For instance, it sends an alert if it sees data sharing underway that includes private, sensitive, or confidential information. The platform operates via webhooks and can reach out via Slack or email to an individual involved in a perceived anomalous action, checking whether there is a justifiable reason for it.

If not, the customer's IT or security team can carry out remediation from within the DoControl platforms, with remedial action and policy enforcement carried out using no-code workflows that operate across all SaaS apps. Several dozen workflow templates are provided out of the box for easy deployment.

In this way, enterprises can improve their security posture, mitigate vendor risk, and ensure compliance with their data access policies.

Company information

Background

DoControl was founded in 2020 by CEO Adam Gavish, CRO Omri Weinberg, and CTO Liel Ran.

Gavish was previously product manager for Cloud Security & Privacy at Google and, before that, senior product manager for Consumer Payments at Amazon. Meanwhile Weinberg was previously general manager for the US at SafeDK (a provider of SDK management technology that was acquired by mobile marketing company AppLovin in 2019) and, before that, senior VP of Online Performance Marketing at digital marketing company Matomy. Ran's previous career includes the roles of software and cloud architect at cloud-based analytics tools vendor Amenity Analytics and tech lead at SaaS HR provider Hibob.

DoControl has raised a total of $43.35m in funding to date, most recently announcing a $30m Series B round in April 2022, led by Insight Partners and with participation from its existing investors, including StageOne Ventures, Cardumen Capital, RTP Global, and CrowdStrike's early-stage investment fund, the CrowdStrike Falcon Fund.

Current position

DoControl delivers its technology entirely as a cloud-based service in SaaS mode and its charging model, which is a per-user subscription, reflects that approach.

The number of SaaS applications with which DoControl integrates is growing almost weekly. It currently supports most of the usual suspect (i.e., those most widely used in enterprises such as Google Drive, Dropbox, OneDrive, Box, Slack, Microsoft Teams, SharePoint, GitHub, Bamboo, Okta, and Salesforce.)

DoControl also has a partnership with security vendor CrowdStrike that enables organizations using the latter's endpoint detection and response (EDR) platform to access the DoControl platform to remediate access to malicious files in connected SaaS apps, with the DoControl app being available on the CrowdStrike Store.

In terms of its market landscape, DoControl sees various types of tech vendors in competitive scenarios. There are, of course, the traditional DLP and CASB vendors, but their products don't really address the same types of issues. It also sees Nightfall AI, a cloud data protection vendor that raised $40m in a Series B round in August this year, as well as SSPM vendors like Adaptive Shield and even BetterCloud, which offers a broader SaaS management platform (SMP) that includes data security.

Key facts

Table 1: Data sheet: DoControl

Product/Service name	DoControl	**Product classification**	SaaS Data Security
Version number	V2	**Release date**	April 2021
Industries covered	All	**Geographies covered**	North America, EMEA
Relevant company sizes	Enterprise and Midsize	**Licensing options**	Per-user licensing
URL	www.docontrol.io	**Routes to market**	Direct and Channel
Company headquarters	New York, NY, USA	**Number of employees**	60+

Source: Omdia

Analyst comment

DoControl competes in a busy market, in which there are a lot of vendors offering some form of data security, either specifically for SaaS apps, or for the cloud as a whole (i.e., including IaaS and PaaS), or even for an organization's entire data, regardless of where it resides (in the cloud or on its premises). The reasons are manifold: data volumes continue to explode, cloud and SaaS adoption advance in leaps and bounds, and authorities pass ever more legislation around data privacy and protection, creating a growing need for compliance.

This particular vendor's approach is a good one, in that its technology is straightforward to adopt and starts to deliver a return on investment almost immediately. Omdia particularly likes the fact that it not only alerts on apparent anomalies but double-checks to see whether the source of the anomaly has a good explanation for it and provides IT and SecOps teams with the wherewithal to remedy the situation via no-code workflows.

DoControl is also doing all the right things in terms of partnering with leading SaaS providers to enable tighter integrations with their technology, often giving it additional routes to market through their app stores.

One of the challenges the vendor will face is, of course, the very busy nature of this market. While it may currently be circumscribed to start-ups, Omdia expects larger security vendors, as well as some of the cloud service providers (CSPs), to cast covetous eyes at this emerging segment, either developing cloud data access control technology themselves or acquiring one of the start-ups to the enter the market. And while the CSPs may restrict their offerings to their own platforms (at least, that is what one would expect from AWS, though potentially not Azure), the big security vendors will obviously want to be heterogeneous, a.k.a. multicloud in their abilities.

At that point, smaller specialist players like DoControl may find it difficult to make their voices heard over the cacophony of noise emanating from such vendors, with their deeper pockets and huge marketing machines. As such, it behooves DoControl to get out in front of any such evolution in the market landscape, establishing its brand and positioning itself as the thought leader in data access control.

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.

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