Brought to you by Informa Tech

Publication date:
23 Oct 2023
Author(s):
Rik Turner, Senior Principal Analyst

On the Radar: Nudge Security offers SaaS security with patented discovery and collaborative governance

Summary

Catalyst

Nudge Security is a developer of security technology for software-as-a-service (SaaS) applications. After employing a patented approach to SaaS app discovery, it works with corporate employees, encouraging them to adopt secure and compliant SaaS usage policies, rather than seeking to impose company diktats upon them.

Omdia view

SaaS was already a huge market, even before the COVID-19 coronavirus pandemic forced millions of knowledge workers into working from home. The pandemic merely turbocharged the adoption curve, as well as compounding the problems of IT and security teams seeking to track and control SaaS usage within an organization, imposing governance and enforcing security policies.

Nudge's approach to the challenge of securing SaaS usage within an organization and ensuring ongoing compliance combines a methodology for discovering app usage based on email analysis with an approach to enforcement that engages with employees rather than imposing corporate policy on them.

The attraction of this collaborative stance is evident, particularly in the era of widespread working from anywhere. It looks especially well suited to organizations that already have a culture of trust in their workforce and personal responsibility for individual employees.

Why put Nudge on your radar?

Nudge's first differentiator is clearly its approach to discovering SaaS apps, which inspects employees' email inboxes for signs of interaction with SaaS providers. Its second is the way it seeks to affect security policy and compliance, working with the end users in an organization rather than dictating to them.

Market context

SaaS security, like SaaS itself, is an evolving and expanding market. Worth in excess of a quarter of a trillion dollars in 2023 and, according to Omdia's forecast, set to top the half-trillion mark by the end of this decade, SaaS currently accounts for almost 50% of the total market for cloud computing services—48% this year to be exact, which is larger than the infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) markets combined.

SaaS achieved this commanding position as the leading delivery mode for the cloud primarily due to its ease of adoption. Lines of business can and do sign up and start using SaaS platforms without the blessing, or even the knowledge, of their IT or security teams. Research by Nudge itself suggests that as many as 60 new SaaS assets are adopted every day in the average enterprise with 1,000 employees. An asset could be a new application, a new user account within an existing application, an OAuth grant connecting two SaaS applications, or even resources created, such as a new registered domain. Thus, an initial problem for those charged with controlling where corporate data resides and how it is used is simply visibility into what SaaS applications are in use in the organization.

"Shadow IT," as it has become known, is a direct consequence of the success of SaaS. The first technology to emerge to address this problem, by discovering employees' SaaS usage and restoring visibility for IT, was the cloud access security broker (CASB) platform. After that, CASBs evolved to include control capabilities, such as the ability to force encryption of data uploaded into a SaaS app or to impose read-only access. Multiple CASB startups came to market around the middle of the 2010s, with a buying frenzy in the latter years of the decade as larger security players snapped up the specialists to add the technology to their broader portfolios.

In more recent times, a need was perceived for another technology to address a different type of SaaS security challenge. As SaaS usage became even more widespread within organizations, awareness grew that the misconfiguration of how each app is accessed can lead to serious security issues. And because each SaaS application has its own terminology to describe its configurations, it is difficult even for experienced security professionals to know the implications of a setting. Moreover, even applications that are configured securely at the time of adoption will tend to drift as users adjust settings to improve functionality.

Thus the next SaaS security technology, arising in the last couple of years, is part of the proactive wave of platforms that seek to find and remediate problems before any attack takes place: SaaS security posture management (SSPM). This is technology to which a customer grants read-only access to their SaaS estate, at which point it surveys it for misconfigurations, excessive access rights, and so on, alerting the customer's IT or security team and suggesting remedial actions.

However, SaaS security requirements have now expanded beyond the capabilities of both CASB and SSPM platforms, with a need to be able to address the following issues:

- So-called SaaS-to-SaaS communications, whereby, unbeknown to their IT or security team, a user integrates third-party apps into the core SaaS stack to improve app functionality. Furthermore, since the most common method of integration between apps is through an OAuth grant, which requires no technical skill on the part of the end user to enable, the potential for proliferation of this problem is huge. Essentially, the app pops up a convenient window with a big button and all the user has to do is click "OK."
- There is also the problem of users logging in from compromised devices carrying malware that can be exploited to purloin access credentials and tokens.
- Finally, there is the need for identity detection and response (IDR, also known as identity threat detection and response, or ITDR), which is the ability to detect and block identity-based attacks, whether from a rogue insider or an external attacker using compromised credentials.

Product/service overview

The Nudge Security platform, or simply Nudge, performs three key functions:

- Discovery: CASBs are network-centric proxies that see all the attempts to log into SaaS apps as they traverse them but will often struggle to discover SaaS apps that are being used by remote workers, since they are not on the corporate network. Meanwhile, SSPM platforms tend to start from a list of the SaaS applications that are known to be in use, accessing them via API so as to discover employees' activity within them. Nudge takes a different tack, discovering apps that are in use in off-network scenarios, and even from employees' personal (i.e., non-corporate) devices. Nudge does this by hooking into an organization's corporate email account (Microsoft 365 or Google Workspace) and using read-only API access to look for evidence of SaaS activity. Primarily, it searches for machine-generated emails of the "no-reply@acme.com" type that SaaS applications send whenever a user creates an account, changes security settings, requests a password reset, and so on. It can also identify and inventory OAuth grants in ways that enable customers to visualize app-to-app relationships across their SaaS footprint. Of course, an employee could also use a personal webmail address to create an account in an SaaS app, and Nudge would not see that because it does not access non-work email accounts (Nudge calls this scenario a "shadow root user"). Nudge does, however, provide evidence of a shadow root user whenever the user starts to invite other colleagues to collaborate in the application.
- Inventory: Again, this feature is also part of what SSPMs promise, but Nudge considers a key differentiation here to be the level of usage and resulting risk insights it provides with the list of applications. These include information about adoption trends—who is using SaaS apps most often, who has the most privileged access, and which third- and fourth-party applications are the most frequently breached at any given moment. Nudge says it typically takes just over an hour to build an SaaS asset inventory for a new customer, which will include all SaaS assets ever created by any employee as far back as the organization's email history goes, even assets for former employees that may have been overlooked during offboarding. Thereafter it monitors the estate for any changes.

- Orchestration: This is where the reason for the vendor's name becomes self-evident. It enables an engineer in a customer's IT department to nudge an employee (e.g., the business or account owner) to make a change in their SaaS usage—for example, switching to an approved alternative app, turning on multi-factor authentication (MFA), or removing abandoned accounts that can still access the app in question. These nudges can be sent via email or Slack.

While discovery describes a key technical differentiator of the Nudge platform—that is, its patented method for SaaS app discovery—it is orchestration that encapsulates the essence of the vendor's approach to SaaS security. Nudge's philosophical stance here is to involve the employees in the SaaS security and governance activities of its corporate customers. Indeed, it argues that to exclude them would simply lead to more circumvention of the rules: it has carried out surveys to show that 67% of corporate users say they find workarounds to access any blocks their employers put on the SaaS apps they want to use.

Company information

Background

Nudge was founded in 2021 by CEO Russ Spitler and CTO Jaime Blasco. Spitler was previously an assistant vice-president (AVP) of product at AT&T for nearly two years, having joined the telecoms heavyweight with its 2018 acquisition of AlienVault, where he had been for six years, ending up as senior VP of product. Blasco was also previously an AVP at AT&T, responsible for product development, and before that had spent 13 years at AlienVault, his final post there being that of VP and chief scientist. While at AlienVault and AT&T Cybersecurity, Blasco and Spitler built and operated what is believed to be the world's largest collaborative community for open threat intelligence sharing, the Open Threat Exchange, which has over 210,000 participants today.

In April 2022, Nudge raised a $7m seed round from Ballistic Ventures, a venture capital firm that focuses on early stage security startups and whose general partners include Barmak Meftah and Roger Thornton, former president and CTO, respectively, of AT&T Cybersecurity. In July 2023, Nudge was granted a patent by the United States Patent and Trademark Office for its SaaS app discovery technology, which is based on email analysis powered by machine learning (ML).

Current position

Nudge has just over 50 enterprises as paying customers for its product after its first year in operation. Nudge's charging mechanism is to offer a 14-day free trial, after which companies can sign up to one of three packages:

- Starter, which costs $299 a month and covers up to 100 users/accounts
- Growth, which charges $3 per user, per month, for 101–3,000 users/accounts
- Enterprise, for customers with over 3,000 users/accounts, where it charges per user and offers volume discounts as the number rises

Nudge is currently focused on the North American and European markets, with a customer base that spans multiple verticals. It considers the sweet spot for its technology to be companies with between 500 and 5,000 employees in a highly distributed environment. It sells its platform into IT and security teams.

As for its competitive landscape, Nudge comes up against a range of vendor types. There are the SaaS management platforms such as BetterCloud, Zluri, and Torii HQ, but they all start from a license management perspective, and so typically rely on mining expense claims or integrating with networking monitoring technologies for app discovery. As such they are not security focused.

Then there are the SSPMs, but because they rely on APIs into the different SaaS apps, the rate at which they can add new integrations is slower: for example, Nudge believes that no SSPM platform exceeds 200 integrations with SaaS apps. Also, they are largely rules-based, whereas Nudge uses ML and human intelligence for SaaS security and governance.

Other vendors in the general area include Grip Security and Push Security, both of which are focused on the discovery aspect of SaaS security, with Grip starting by inspecting the identities and credentials in a customer's environment, while Push calls itself an identity security company and uses a browser plug-in to achieve its goals. In either case, their coverage is only partially what Nudge does.

Key facts

Table 1: Data sheet: Nudge Security

Product/service name	Nudge Security	**Product classification**	SaaS security and governance
Version number	N/A	**Release date**	October 2022
Industries covered	Tech, finance, healthcare, retail, manufacturing	**Geographies covered**	North America and Europe
Relevant company sizes	500–5,000 employees	**Licensing options**	Annual SaaS subscription $299 flat monthly fee up to 100 active users; then $3 monthly fee up to 3,000 active users; then enterprise license agreement (ELA)pricing. ("Active users" refers to Microsoft 365 or Google Workspace active user accounts)
URL	www.nudgesecurity.com	**Routes to market**	Direct: product-led, sales-led Channel
Company headquarters	Fully remote	**Number of employees**	19 FTE

Source: Omdia

Analyst comment

With tens of thousands of business-to-business (B2B) SaaS vendors on the market today, each with its own nuanced administrative controls, it is no longer a reasonable expectation for any one organization or IT team to have all the expertise. In this scenario, Nudge aims to serve as an authority, helping organizations navigate the business context of each SaaS service to ensure compliance with their own IT and security policies. As it allies in this process, it seeks to enlist those within an organization who have the best understanding of the business context for a SaaS application: the individual business units and employees adopting, using, and administering the service.

Nudge's two key differentiators are its approaches to the discovery and enforcement required for SaaS security and compliance. Omdia applauds the company on both counts.

Regarding its use of email analysis to uncover SaaS app usage among an organization's workforce, Omdia was particularly impressed by Nudge's readiness to point out and address what might be considered a shortcoming, namely the fact that it cannot and does not inspect employees' private webmail accounts. Clearly this constitutes a loophole through which a rogue employee could still establish an account with a SaaS provider and not be discovered by his or her IT department.

Nudge points out that it would still be able to detect whenever that employee invites other colleagues to collaborate in the application, going on to argue that if there is "a ring of employees trying to keep their work covert by sharing personal email addresses," the company has a different type of problem altogether; in other words, there is some sort of conspiracy underway.

As for Nudge's approach to achieving secure and compliant SaaS usage by encouraging employees to take personal responsibility for it, clearly that is not suited to all organizations. Enterprises that adopt a top-down strategy of dictating policy, and harnessing technology to enforce that, are unlikely to find Nudge's way to their liking, although they might still find value in its SaaS discovery capabilities. On the other hand, those companies that actively promote employee engagement with policy setting and implementation should find it very much to their taste.

It is interesting, in this context, that Nudge has appeared just as the zero trust mantra is at its height. That approach to enterprise security preaches the abandonment of a "trust, but verify" stance in favor of "never trust, always verify, and continually monitor," and while we see the clear benefits, not to say justification, for it, Omdia has nonetheless referred to it on occasion as institutionalized paranoia.

Organizations adopting the Nudge approach to SaaS governance will need to put extra effort into trusting their workforce, while at the same time making sure they monitor their environment for the first signs that anything has gone awry.

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

"Blockchain is good for more than just Bitcoin" (September 2019)

Blockchain Technology and Adoption Trends (December 2019)

"CenturyLink goes 'colorless' and takes on the edge cloud" (February 2020)

Service Provider Routers & Switches Market Tracker – Q4 2019 (February 2020)

Li You, "Tech-savvy Hangzhou tries out new 'City Brain'," *China Daily* (retrieved June 17, 2021)

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