On the Radar: Vade targets cloud aggregators to reach business customers with its email security

OMDIA

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

1

Table of Contents :

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

2

Summary

Catalyst

Vade develops cybersecurity based on artificial intelligence (AI) technologies such as natural language processing and computer vision. The company started out by providing services to telecoms operators for them to protect their consumer email customers, and the company consolidated its position to where it is currently protecting over 1 billion mailboxes worldwide. More recently, it has begun to target business customers in the SMB segment, opting to target them via managed service providers (MSPs).

Omdia view

Email continues to be the vector of choice for many kinds of cyber exploits, from phishing campaigns to ransomware: there are estimates to suggest that as much as 90% of all breaches involve email in one way or another. Thus, email security is a must-have, and with ever more business email delivered via Microsoft 365 tools, there is clearly significant market opportunity for Vade's product. The vendor's expertise in working through partners, i.e., telcos for the consumer market and now cloud aggregators for SMBs, bodes well for its ability to carve out a share in this still expanding segment.

Why put Vade on your radar?

If you are a cloud aggregator or MSP seeking to offer security services around Microsoft 365, Vade for M365 is a compelling candidate for your consideration, given its analytics-based approach to detection, its coaching capabilities, and its plans to enable MSP-led incident response.

Market context

The single most important change in the email market over the last decade has been its migration to the cloud, with much of the infrastructure required to secure it accompanying that move. For business email, the key development was Microsoft's launch of its Office 365 service in 2011 (now Microsoft 365), though Google had of course been in market with its Gmail SaaS offering since 2004. Some firms, particularly in the SMB and cloud-native start-up segments, have standardized on Gmail, but it can safely be said that Microsoft 365 dominates the business market overall.

This in turn has created an opportunity for vendors such as Vade. Whereas in the 2000s business email was delivered mainly by on-premises Exchange servers with a secure email gateway (SEG), also on the customer's premises, providing security, cloud-based email services have changed the competitive landscape for email security. Microsoft itself is providing ever more of the basic SEG functionality, such as content filtering, URL black- and whitelists, and so on. This in turn opens up opportunities for new, cloud-based players to bring technology to market to address the more advanced forms of attack known collectively as business email compromise (BEC).

Meanwhile inspection of the traffic no longer requires rerouting through an SEG. Instead, these new platforms integrate with M365 directly via an application programming interface (API) and, given that Microsoft's email security is generally no better than "good enough", then come in as an additional layer to pick up what it has missed.

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

3

BEC typically does not entail any form of malware or a malicious URL, making detection reliant on machine learning engines analyzing the construction and behavior of an email. Clearly, this development plays to Vade's strengths.

While its first decade was spent supplying email security to telcos so that they could protect their customers, primarily in the consumer segment, Vade has now expanded to address all but the high-end enterprise segment of the business market (except in France, where it also competes in the enterprise segment), doing so via the cloud aggregators or brokers. These are firms that bring together multiple cloud services and offer them as a combined package to customers, namely managed service providers (MSPs). In essence, Vade has adopted a two-tier channel strategy for the cloud era.

The expansion into business email and cybersecurity is a logical one for Vade: while the consumer email protection market is estimated to be worth around $100 million a year, the segment it is going after with its cloud aggregator/MSP strategy is reckoned to be worth around €2.7 billion ($3.2 billion) annually.

Product/service overview

The reactive approach to email security, based on signatures and reputation, was adequate when spam was raging in the mid-2000s, because emails were static, i.e., unchanging. However, Vade believes the more predictive approach it champions has come into its own now that phishing emails have multiple variants, frequently requiring analysis of their behavior to identify ones with malicious intent. Equally, BEC exploits seek to compromise their targets without using malware or malicious URLs, making an analytical approach like Vade's vital to addressing such attacks.

Like most security companies that started life on the consumer side of the business, Vade leverages the scale and volume of its analysis of the billion-plus mailboxes it is protecting there, building what it calls its Global Network Intelligence (GNI). This is an ever-expanding database that it leverages also for business customers, modelling future attacks and providing suggested remedial actions, its aim being to enable a low-touch service for the MSPs delivering it to their business customers.

The platform also has a phishing awareness training capability Vade calls Threat Coach, which kicks in when a user has been phished. It uses real-life samples of phishing emails rather than templates, and because the content is personalized and based on the brand impersonated in the malicious email, Vade argues that users are more likely to retain the training content and avoid making the same mistake twice.

Company information

Background

Vade was founded in 2009 in the north of France with technology that had itself been in evolution since 2004. Its initial focus was on the anti-spam market, where most vendors used a combination of signatures and reputation to block unwanted traffic. Vade, by contrast, introduced technology that used behavioral analytics on both the construction and path travelled by the email, an approach that enabled a predictive stance.

Vade has security operations center (SOC) teams in Canada, France, and Japan to enable follow-the-sun operations. It remains privately held and has offices in France, the US, Canada, Japan, and Israel.

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

4

Current position

Vade's initial focus was on selling to telecoms operators. This made sense because it was a small company, but by signing up major telcos it could feed its machine learning platform with data from millions of end users. After scoring initial wins in its homeland of France (Orange Cyberdefense offers services based on its technology in seven countries), it went international in 2013 and now claims to protect over a billion mailboxes in 76 countries.

In 2019 Vade decided to focus its strategy for addressing small and midsize business customers through channel partners, such as cloud aggregators, aka cloud brokers. Among those that currently work with Vade are D&H (US), Giacom and Arrow (UK), ALSO (Germany), Resello (Netherlands), and Mindware (UAE). The kind of bundle that such firms offer is frequently a combination of Microsoft 365 for email, Vade for security, and Acronis for backup.

Deployment differs slightly from the telco to the aggregator market. While the core compute that creates Vade's intelligence is always cloud-based, for the telcos the company deploys an analytics engine on their premises to localize that intel and make it relevant to their specific customer base. By contrast, for the aggregator channel, the entire platform resides in the cloud.

Vade's licensing model is based on the number of mailboxes per end customer, with the service available on a monthly, yearly, and three-year contract basis.

Future plans

Vade is now designing an incident response capability for Vade for M365 to give MSPs an aggregated view of the attack landscape across their customer base and remediate threats centrally. It is building out from the AI-based incident response it currently offers at the end-customer level to focus on the different requirements of the MSP market.

Vade's ultimate goal here is to enable MSPs to create their own service offerings on its platform, the idea being to deliver functionality in a low-touch manner so as to facilitate them scaling their managed security business, thanks to the automation levels built into Vade.

Key facts

Table 1: Data sheet: Vade

Product/Service name	Vade for M365	Product classification	Email security
Version number	N/A - SaaS application	Release date	N/A - SaaS application
Industries covered	All (healthcare, finance, transport, retail, manufacturing…)	Geographies covered	North America, Europe, Middle East, APAC
Relevant company sizes	Midsize, SMB	Licensing options	Monthly, one-year or three-year license

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

5

URL	www.vadesecure.com	**Routes to market**	Channel partners (aggregators and MSPs)
Company headquarters	Hem (Lille), France	**Number of employees**	200

Source: Omdia

Analyst comment

With ever more companies adopting cloud-based email services, there is clearly a market opportunity for a security offering delivered in the same way. For the SMB segment, MSPs are the obvious candidates to provide such a service. Vade's decision to focus its expansion into the business market at the low end, i.e., the SMB segment, makes developing a two-tier channel strategy involving cloud aggregators and MSPs a logical move.

This approach should also reduce the amount of competition from many of the other email security vendors, which tend to focus on the enterprise end of the market and for which a channel strategy involving "generalist" MSPs, rather than the more specialist managed security service providers (MSSPs) that target the enterprise segment, is less familiar territory.

That said, one of the big beasts from the SEG world, Proofpoint, acquired Cloudmark, a provider of an email security platform for the telco market, in 2017, while the likes of Barracuda, Mimecast, and Microsoft itself clearly have ambitions in the MSP channel. Thus, one of the challenges Vade faces is gaining visibility in the market against competitors with greater brand recognition and much larger marketing budgets.

Still, given the growing awareness of threats such as phishing and ransomware, there is probably room in the market at the moment. This is particularly the case for vendors whose technology can be seen to work with, and complement, Microsoft's and is partner-friendly. These are the two criteria that will determine the success of Vade's SMB strategy.

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, Principal Analyst, Cybersecurity

askananalyst@omdia.com

On the Radar: Vade targets cloud aggregators
to reach business customers with its email
security

6

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