Vade Secure
Predictive Email Defense

OUTBOUND CALLING

⏱
90-Second Pitch

Introducing Vade Secure for Microsoft 365 to Your Clients

Hi, this is <caller name> from <partner name>. I am calling to introduce you to our newest email security offering, Vade Secure for Microsoft 365. We added this service to our portfolio in response to the rapid increase in the volume and sophistication of phishing, spear phishing, and malware attacks targeting Microsoft 365 users. We believe Vade Secure to be the best security offering available as we saw a significant improvement in threat detection during our internal test period.

Unlike other offerings that work off a known threat list, Vade Secure uses Artificial Intelligence (AI) to scan email messages, including links and attachments. Further, Vade is natively integrated with Microsoft 365, which provides several advantages over traditional email security products, including:

- **Quick and easy configuration** – you can be up and running in 5 minutes, with no MX change.
- **Minimal end user impact** – no external quarantine or daily digests for end users.
- **Protection against insider attacks** – internal email scanning, including links.
- **Auto and one-click remediation** – additional protection by removing threats found post-delivery.

Are you interested in a 7-day risk free trial?

Response: Yes

Complete the following steps with the partner:

1. Create client account in Vade Secure's Partner Portal.
2. Provision Vade Secure for Microsoft 365 with trial license.
3. Activate journaling in Microsoft Exchange.

Response: No

The trial is risk free. You can test Vade Secure for Microsoft 365 without making changes to your current email configuration because it does not require an MX record change and can run in monitoring mode. During POC, you can see what Vade filters and compare it to your current email security solution.

Note to partner: If your client is running Microsoft EOP, you can use the comparative report to quantify Vade's added value over EOP.

QUALIFICATION QUESTIONS

The following questions and responses can help to assess gaps and/or pain points with current email security solutions and quickly point out Vade's unique value in each instance:

Are you satisfied with the effectiveness of your existing email security solution?

- In contrast to fingerprint and reputation-based defenses, Vade's predictive approach leverages behavioral analysis of the email's origin, content, and context to identify unknown threats. The company's unique advantage stems from its global footprint of 600 million protected mailboxes. This unprecedented insight into the global threat landscape is used to train and refine highly accurate AI and machine learning models. As a result, Vade is able to detect more unknown threats than any other product—and typically, from the first email sent.

Are phishing emails reaching your employees even though you've got a filter in place? Are they clicking on malicious links despite receiving phishing awareness training?

- Vade Secure provides comprehensive, multi-layered phishing protection at the time of delivery and time of click. Unlike solutions that rely only on a blacklist of malicious IPs and URLs, Vade performs real-time behavioral analysis of the origin, content, and context of the email to detect dynamic phishing attacks. Machine learning models analyze 47 unique features of the email, webpage, and URL, including any redirects, URL shorteners, or other obfuscation techniques. In addition, computer vision algorithms identify common images in phishing attacks, including modified brand logos and QR codes, by analyzing the rendering instead of the code. If a threat should reach a user's inbox, Vade's engine has the ability to learn from its mistakes and automatically remove the message, resulting in an additional 2%–3.5% catch rate.

Have executives or others in your company been targeted with spear phishing/BEC attacks?

- Other solutions rely solely on authentication standards like DMARC and DKIM, which are only effective against exact domain spoofing. Vade Secure's patented Anti-Spear Phishing technology uses a combination of behavioral analysis, anomaly detection, and natural language processing to identify all forms of business email compromise, including harder-to-detect spoofing techniques like visible alias spoofing and close cousin domains. If spear phishing is suspected, a customizable warning banner is displayed within the email alerting the user.

Are you concerned about insider attacks should one of your employee's Microsoft 365 accounts be compromised?

- Because they sit outside Microsoft 365—in line with your mail flow—secure email gateways are unable to scan internal email traffic between employees. Vade Secure's native integration with Microsoft 365 enables it to scan your internal traffic to detect insider attacks, offering additional protection for your business.

Is email delivery delayed by your current email security solution?

- Because of its native integration with Microsoft 365, the user experience does not change with Vade Secure. Your employees continue working in the familiar Outlook interface, as Vade filters phishing, spam, and low-priority messages into Outlook folders, based on the policies defined. This means your users don't have to learn—and on a daily basis, manage—an external quarantine.