Vade Secure for Microsoft 365 Battlecard

Vade Secure
Predictive Email Defense

OVERVIEW

Vade Secure's email security solutions help protect users from advanced cyberthreats, such as phishing, spear phishing, and malware. Fed by data from more than 600 million mailboxes, our predictive email defense solutions leverage AI and machine learning to protect users from unknown, targeted attacks. Vade Secure for Microsoft 365 is the only native email security solution that sits inside Microsoft 365.

KEY DIFFERENTIATORS

- 10+ year history of working with the world's largest ISPs provides Vade with unparalleled access to data and helped us develop industrial-scale solutions built for speed and performance.
- Threat intelligence from 600+ million inboxes powers Vade's AI-based threat detection, allowing us to train and refine highly accurate machine learning models.
- In contrast to fingerprint and reputation defenses, Vade's predictive approach leverages behavioral analysis of the email's origin, content, and context to identify unknown threats.
- Because of its native API integration with Microsoft 365, Vade Secure for Microsoft 365 is easy to deploy (no MX changes), easy to use (no external quarantine), layers with EOP, and is invisible to hackers.

TARGET CLIENT PROFILES

At smaller companies, you might engage with business management, while larger companies might have an IT manager or director.

CLIENT PAIN POINTS

- Client and their employees are experiencing targeted email attacks, including phishing, spear phishing, and malware.
- Migrating to Microsoft 365 has led to an increase in email attacks, and clients who rely on Microsoft EOP are still seeing targeted attacks reach their inboxes.
- Client's existing email security solution, while effective at blocking known threats, is ineffective at blocking unknown threats.
- Client's employees are being bombarded with graymail, including newsletters, advertisements, etc., cluttering inboxes and affecting productivity.

CLIENT BENEFITS

- **Ease of deployment:** Vade Secure for Microsoft 365 is easy to deploy and manage, requiring no MX changes and just a few clicks to configure.
- **Best-in-class protection:** Machine learning algorithms are updated every minute with new threat intelligence, enabling a predictive approach to identifying unknown, targeted attacks.
- **Native user experience:** Users continue working within Microsoft Outlook—no external quarantine required. Phishing, spam and graymail can be classified into Outlook folders, based on the policies defined.
- **Auto and manual remediation:** Our AI engine automatically removes threats from user inboxes, without intervention from staff. Admins can also manually remediate messages with one click.
- **Continuous improvement:** By marking unwanted/malicious email as "Junk" in Microsoft Outlook, users participate in continuously improving our AI engine.

WHEN TO ENGAGE:

Engage if the client:

- Is in the process of searching for an additional layer of email security.
- Expresses dissatisfaction with their current email security solution.
- Is experiencing targeted email attacks.
- Is migrating to Microsoft 365.

FAQ

Can I install more than one filtering solution? Will Vade coexist with my incumbent?

Yes. Thanks to the native API integration with Microsoft 365, Vade Secure for Microsoft 365 can be deployed as an additional layer of security to augment EOP/ATP.

Will there be any disruption to users?

No. By starting your POC in monitoring mode, Vade can analyze your email traffic without taking action, allowing you to evaluate our efficacy without any risk.

Do I need to train my users after installing your product?

No. Vade Secure has no external quarantine and therefore requires no user training. User-facing elements (e.g. time-of-click phishing warning and spear phishing banner) are fully customizable.

Does your product support internal scanning as well?

Yes. Unlike secure email gateways, Vade Secure scans internal emails to protect from insider threats.

Can I configure policies at the threat level?

Yes. IT admins can configure specific actions to be taken when an email threat is identified, including deleting emails or moving them to the desired folders.

DISCOVERY QUESTIONS

1. What are some of the Microsoft 365 related issues your organization is facing? Too many phishing emails getting through the current filtering system?

2. Are your employees clicking on too many phishing emails? Are they unable to determine the difference between legitimate and malicious emails?

3. Have you had any instances of CEO fraud/business email compromise type of attacks?

4. Are you satisfied with Microsoft EOP/ATP's efficacy?

5. Are you concerned about employee productivity? Are your employees spending too much time cleaning up their inboxes?

RESOURCES

- Boys and Girls Club of Puerto Rico bolstered their email defenses after migrating to Microsoft 365, blocking more than 400 malicious emails in the first week.
- KVC Health Systems experiences a 15% catch rate improvement with Vade Secure for Microsoft 365.
- Vade Secure for Microsoft 365 receives 5-star product review from SC Magazine.
- SC Magazine explores the benefits of Vade Secure for Microsoft 365 with Vade Secure customer KVC Health Systems.

*Find more resources in the Vade Secure Partner Portal, including marketing, sales, and support materials.

About Vade Secure

- 5,000+ customers in 76 countries
- 95 percent renewal rate
- 8 active international patents
- 600 million mailboxes protected
- 2 billion messages filtered last year

Contact

Vade Secure Sales
US/EMEA
sales@vadesecure.com