SOLUTION BRIEF

vade

Anti-Malware /Ransomware Solution

Behavioral-based analysis and detection of unknown malware

WHY – Sophisticated malware can adapt its behavior according to the environment it detects, allowing it to lie dormant, change its code, and even morph into new structures. Email — the no. 1 method for malware delivery — is under attack..

SOLUTION – Vade's Anti-Malware/Ransomware Solution goes beyond traditional malware detection with a heuristic approach that analyzes behaviors in addition to code, identifying anomalies and suspicious behaviors that traditional filters miss.

Behavioral-based anti-malware technologies

Vade's behavioral approach to malware/ransomware detection draws on threat intelligence and user feedback from our 1 billion protected mailboxes globally. Our behavioral engine detects malicious behaviors and obfuscation techniques in emails, documents, shared files, and webpages—blocking malware and ransomware without sandboxing and the resulting latency to end users.

Heuristics-based Behavioral Analysis — Examines emails, webpages, and attachments based on heuristic rules developed by Vade R&D. New heuristic rules are constantly created and used to fine-tune the filter based on the latest threats.

Real-time Attachment Parsing — Parses Office documents (Word, Excel, PowerPoint), PDFs, and ZIP files to detect malicious behaviors, including executable files, suspicious code, malicious macros, and URLs.

Hosted-file Analysis — Analyzes URLs in files from third-party hosts, such as OneDrive, SharePoint, Google, and WeTransfer, to detect malicious URLs hidden in shared attachments.

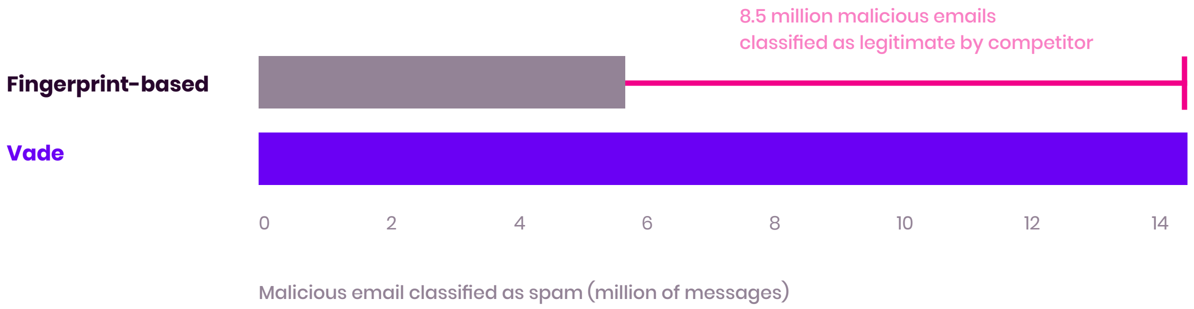
Machine Learning — Analyzes emails and attachments to identify suspicious behaviors common to malware and ransomware attacks, a behavioral approach to filtering that often identifies malware without examining the file itself.

Beyond fingerprinting

Known malware code is easily recognizable to email filters that use fingerprinting to detect malicious emails. In response, hackers have developed sophisticated filter-bypassing techniques to evade detection, including:

- ✓ **Code Obfuscation** — Manipulating code in files and macros to either render the code incomprehensible or conceal the true purpose of the code.
- ✓ **Excess "Noise"** — Adding non-essential and otherwise useless code to files and macros, altering the "fingerprint" of a known threat and confusing a filter. Excess noise can include millions of bytes of useless data designed to exhaust a sandbox.
- ✓ **Environmental Awareness** — Creating anti-analysis capabilities that initiate an environmental scan before execution. Environmentally aware malware is designed to execute only in certain environments, detecting sandboxes and remaining dormant for the duration of the analysis.

Anti-malware solutions that rely on fingerprinting and traditional methods of threat detection consistently fail to detect new and emerging malware techniques . **Vade's behavioral-based detection consistently outperforms competitive solutions that use fingerprinting technology.**



- ✓ **Instant Analysis/No sandboxing or quarantine** — Vade's anti-malware and ransomware solution examines emails and attachments in real-time, delivering an instant verdict with no delay in email delivery. Heuristic analysis allows the filter engine to examine the behaviors that could otherwise be concealed by a virus in a sandbox.
- ✓ **Continuous Feedback Loop** — Vade's 1 billion protected mailboxes provide continual threat intelligence to our SOC, resulting in an industry-high malware catch rate and low false-positive rate. More than 10,000 heuristic rules are consistently updated to reflect the latest threat data captured by Vade and from user reports.

About Vade

- 1 billion mailboxes protected
- 100 billion emails analyzed / day
- 1,400+ partners
- 95% renewal rate
- 15 active international patents

Learn more

www.vadesecure.com

@vadesecure

Contact sales

US / EMEA

sales@vadesecure.com