



ENJOY PEACE OF MIND WITH BEST IN CLASS EMAIL PROTECTION

Advanced email security for Microsoft 365



EMAIL IS STILL THE NUMBER ONE TARGET FOR CYBERCRIMINALS!

With just one single email attack, they can penetrate the entire Microsoft 365 suite along with other corporate systems and data, wreaking significant financial and reputational damage.

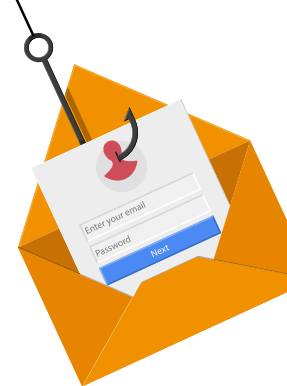
The key to protecting your Microsoft 365 environment is to adopt a layered security approach. While Microsoft 365's native security features catch most mass spam waves and known threats, they don't provide sufficient protection against advanced phishing and spear phishing attacks, as well as unknown, polymorphic malware.



NEW ATTACKS ARE NOT BLOCKED BY EOP AND ATP

Exchange Online Protection (EOP) and Advanced Threat Protection (ATP) for Microsoft 365 are reputable forms of protection against mass spam attacks, relying on traditional signature and reputation-based security tools. But they cannot identify new threats such as spear phishing attempts or Business Email Compromise (BEC) attacks due to their sophisticated nature.

Advanced Email Security for Microsoft 365 by Vade bolts itself onto EOP as a complementary layer of security. It enhances protection by using machine learning to predict patterns for new and emerging threats, while building technical profiles for individuals you regularly communicate with, identifying malicious imposters to circumvent spear phishing attacks. With Vade, you can relax knowing you're covered.



EOP & ATP PROTECTION

KNOWN SPAM

KNOWN MALWARE

KNOWN PHISHING

ADVANCED EMAIL SECURITY FOR MICROSOFT 365

UNKNOWN SPAM

UNKNOWN MALWARE

ADVANCED PHISHING

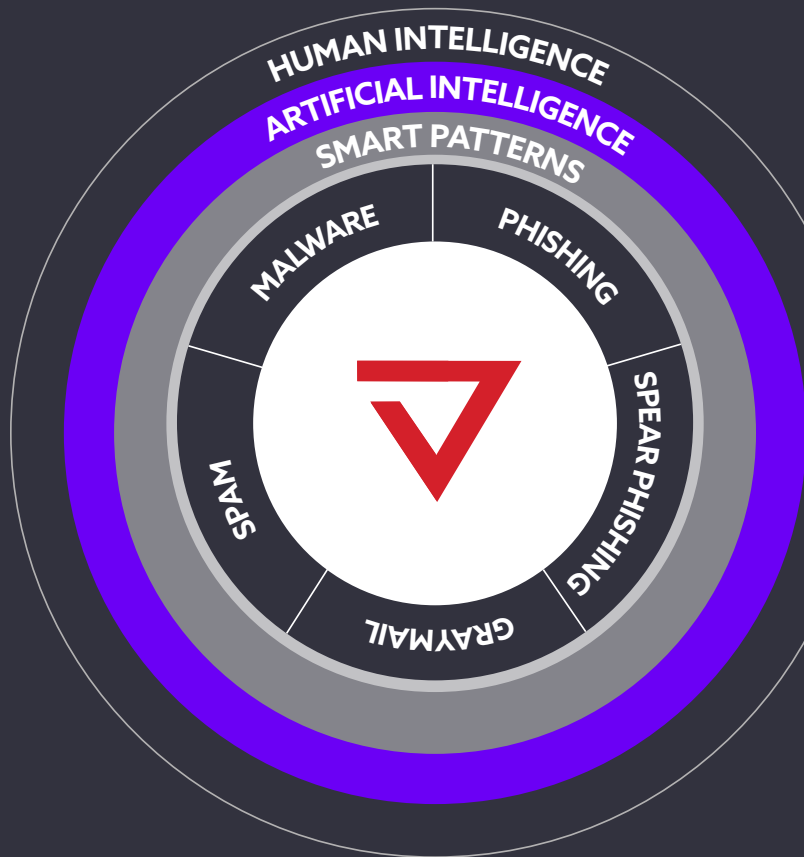
SPEAR PHISHING / BEC

POST-ATTACK REMEDIATION

WHY PROTECT MICROSOFT 365 WITH VADE SECURE?

Vade's advanced cyber security solutions help protect users from advanced cyber threats, such as phishing, spear phishing, and malware. Fed by data from more than 1 billion mailboxes, it's multi-level encryption safeguards your data and offers 360° email protection against the most complex attacks for complete peace of mind.

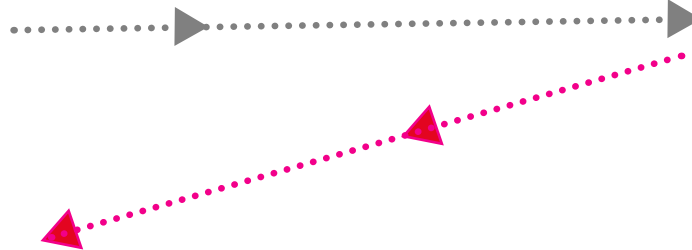
Vade is the only native email security solution that sits within Microsoft 365, you won't even notice it's there. You and your team can work remotely or in the office, safe in the knowledge Vade is working hard in the background to protect your business.



CYBER CRIMINALS NEVER SLEEP, NEITHER DOES ARTIFICIAL INTELLIGENCE

Traditional signature-based security tools are now ineffective against new and emerging zero-day threats. By using AI and machine learning algorithms, Vade identifies and predicts new threats from previous patterns, enabling their 24/7 global threat intelligence to reliably identify one-off spear phishing emails, sensitive data requests, and zero-day malware hidden in executable files, PDFs, Office documents and more.

Its 360° analysis of the origin, content and context of emails/attachments means it examines more than 30 features of email content to block both known and unknown threats before, during and after attacks. So, should the worst happen, you can be at peace knowing threats can be easily identified and deleted to prevent further infection. Vade Secure also supplements its protection with traditional spam filters, blocking 99.9% of spam, an extensive blacklist and two complementary virus scanners.

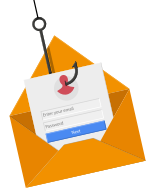


MALWARE & RANSOMWARE



Vade fights malware by analysing the email origins (IP reputation), contents (code for attachments, fingerprint, sandboxing) and the context of the threat using artificial intelligence for optimal efficiency. Zero-hour detection and resistance to multi-form malware are its key features.

PHISHING



Using heuristic technology and machine learning, Vade's search engine identifies dangerous links and associated pages to defend against phishing waves that use URL shortcuts or URL changes. Web page searches are done in real-time and at the time of the click.

SPEAR PHISHING & BEC



Vade uses Identity Match technology to detect minor technical and contextual changes of emails that make dangerous emails difficult to identify. It can discover if malware is attempting to usurp identity. Attached documents and URL links are also inspected in order to avoid malware insertions.

SPAM & GRAYMAIL



The email filter analyses and classifies message contents, priority emails and identifies other emails by their category. Users can access no-priority emails (notifications, advertising, newsletters, etc) and spam if needed, but the undesirable emails are isolated.

INSTANT DEPLOYMENT, INSTANT INTELLIGENCE, SUPERIOR PROTECTION

Advanced Email Security for Microsoft 365 by Vade is fully integrated with Microsoft's API for Microsoft 365, meaning it can be deployed in minutes with no disruption to your email flow. Running a zero-risk trial period (for around five days) in the default monitoring mode enables Vade Secure to analyse your emails without activating email defence. A full report would be supplied after the initial monitoring period, breaking down the outcome of what would have happened in active mode.

Intuitive, Efficient User Experience

- Continue using the familiar Outlook interface, no separate quarantine required
- Know you're safe with customised spear phishing warning banners and phishing detection URLs
- Focus on your important emails with automatic classification of low priority messages, as well as one-click safe unsubscribe from unwanted communications.

**DEFEND YOUR MICROSOFT 365 ENVIRONMENT AGAINST
ACTIVE ZERO-DAY THREATS WITH CUTTING-EDGE
ADVANCED EMAIL SECURITY FOR MICROSOFT 365.**



**FOR MORE INFORMATION,
CONTACT US TODAY.**

Tel: 0330 024 4222
Web: www.mcsgroup.net
Email: info@mcsgroup.net

