Vade

AI-BASED EMAIL THREAT DETECTION & RESPONSE

vade

A1 - Vade

September 20th

Your Vade preferred contacts

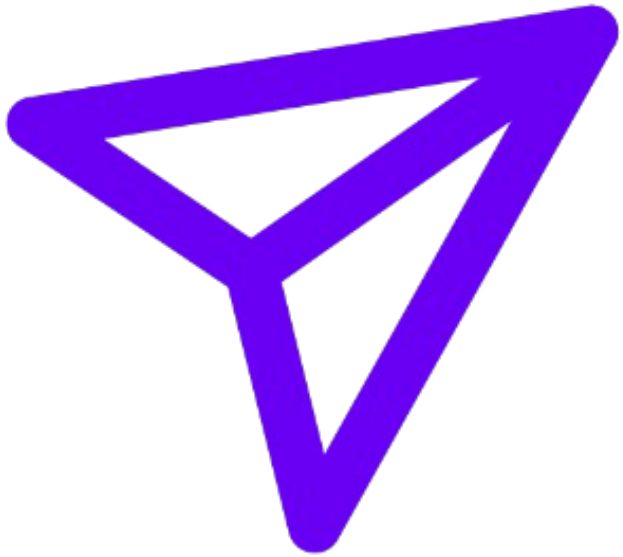
Stefano Grisari
EMEA Channel Manager
Stefano.grisari@vadesecure.com
+33 7 63 99 45 19

Monica Naida
Inside Sales EMEA
Monica.naida@vadesecure.com
+33 3 66 89 00 82

Romain Favraud
Channel Sales Engineer
Romain.favraud@vadesecure.com
+33 1 84 88 96 01

91%

of cyber-crimes
start with a simple email



+ 350%

Increase
in phishing attacks in 2020

2/3

Breaches are
financially motivated

Threat environment

Threats' evolution: from spams to hyper-dynamic attacks

Spam

Viagra and dating ads

Annoying, time-consuming but low security risk.

Basic attacks

Unclaimed heritage scam, macro-based virus

First attacks that can cause harm to corporate systems. Relatively crude, and easy to block with IP reputation and fingerprinting.

Evolved attacks

Ransomware, massive Phishing campaigns

Attacks coming from clean sender, and with basic countermeasures against fingerprinting.

Hyper-dynamic attacks

BEC – Targeted Phishing – Polymorphic malware

Low volume, short wave, targeted attacks.
They come from clean senders, target specific individuals or departments (Finance, HR) and use advanced countermeasures against fingerprinting and sandboxing.

CUSTOMERS / SERVICE PROVIDERS / SOLUTIONS PROVIDERS: ALL ARE AT RISK

UOB employee allegedly fell prey to scam & leaked personal information of 1,166 customers

The matter is currently under investigation.

Matthias Ang | May 08, 2021, 12:16 PM

AMERICAN FAMILY INSURANCE®

A letter signed by Chris Szafranski, Privacy Director, explains what happened:

> We believe unauthorized parties may have used an automated bot process to obtain your driver's license number by entering personal information (such as your name and address) they acquired from unknown sources into the American Family quoting platform.
>
> We are notifying you because you may have been affected by this incident. If you did not request an insurance quote using the American Family quoting platform between February 6, 2021 and March 19, 2021, the unauthorized parties may have requested a quote in your name and may have obtained your driver's license number. If, however, you did request a quote from the American Family quoting platform between February 6, 2021 and March 19, 2021, you are not impacted by this incident.

CYBER-ATTACKS REACH UNPRECEDENTED LEVELS IN THE MIDDLE EAST

Over 10 million Distributed Denial of Service (DDoS) cyber-attacks were recorded globally in 2020, including a 183% increase in the UAE alone, while ransomware attacks are on the rise, with the government, private, oil and gas, telecom and healthcare sectors particularly affected, according to the State of the Market Report 2021 by Help AG, the cybersecurity arm of Etisalat Digital.

How to survive the rising tide of ransomware attacks in the Middle East

Remote work and increasingly sophisticated hacking tools are contributing to increase in ransomware attacks. Here's how to protect your enterprise.

vadesecure.com

Anson experiences cyberattack; county services including phone, email affected

May 11, 2021 | Daily Journal | News, Top Stories | 0

Government services impacted

Liz O□Connell Staff Writer

Anson Record file photo

The Anson County Government Center in downtown Wadesboro.

Crime & Courts

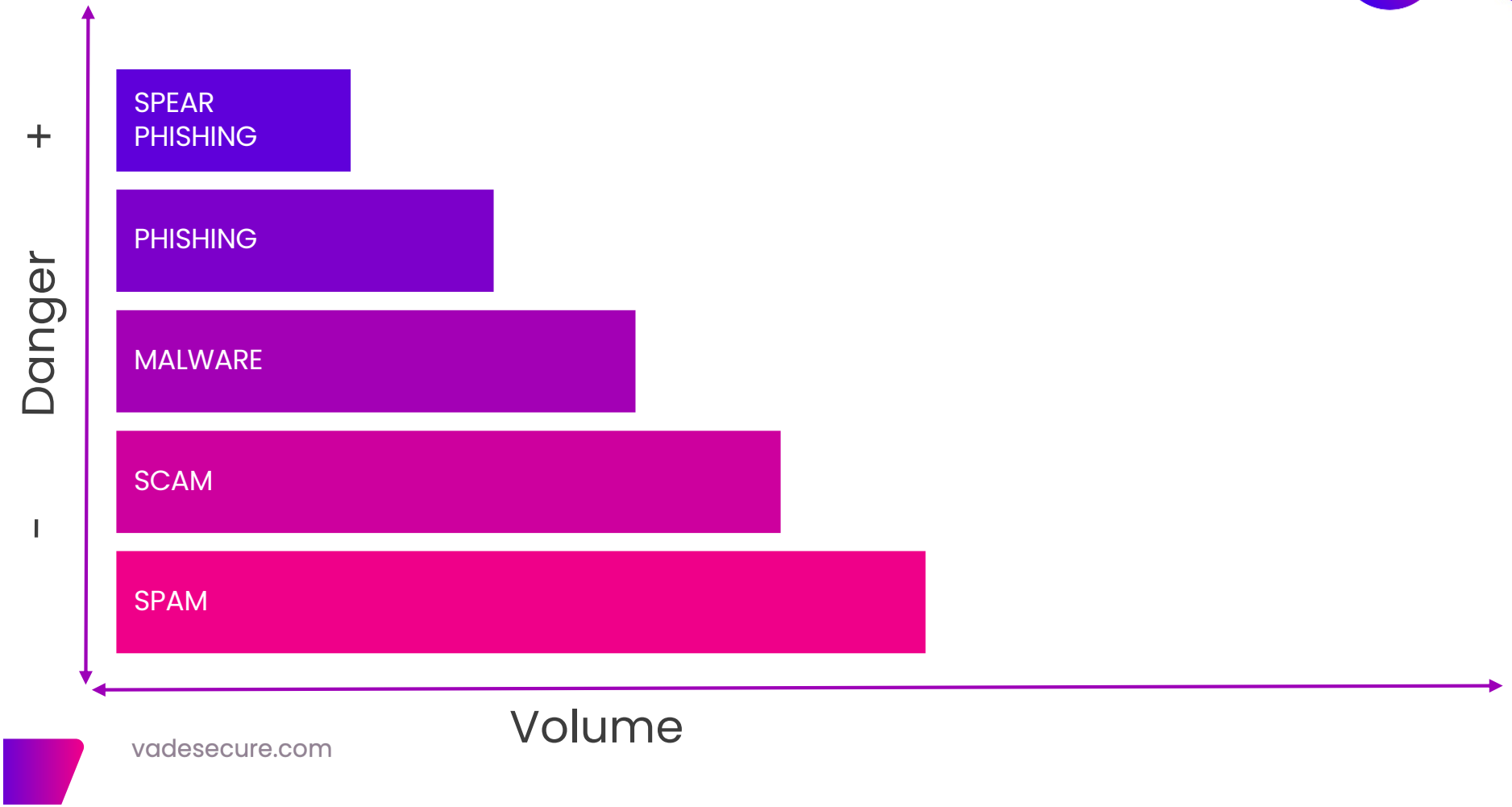
Unidentified cyberattackers force Alaska Court System to disconnect from internet

Author: James Brooks | Updated: May 1 | Published May 1

JUNEAU – A cyberattack has caused the Alaska Court System to disconnect most of its operations from the internet, an act expected to block electronic court filings, disrupt online payments and prevent hearings from taking place by videoconference for several days.

The Courtview system used to look up court records has been taken offline, as has the court system's website.

The pyramid of Threats



Who are we?

Global leader in Predictive Email Defense since 2004

vadesecure.com

European editor specialized in email security

- **Leader**

  Of proactive email protection

- **Specialty: the fight against cyber attacks**

  Phishing
  Spear phishing
  Malware
  Ransomware

- **Services**

  Threat detection, user awareness and incident response

vade

Consumer email through ISPs & Telcos

Largest US ISP

BT

orange

EarthLink

AOL

vodafone

SoftBank

NTT docomo

Spark nz

1 billion mailboxes protected

Corporate Market through Channel

THOMAS & PIRON

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Leonidas

AIRBUS

LADURÉE Paris

CHAMPAGNE POMMERY A REIMS-FRANCE

synchronoss

croix-rouge française

FAYAT

OEM Market

cisco

mimecast

SONICWALL

OVHcloud

La FRENCH TECH FT120 La FRENCH TECH NEXT40

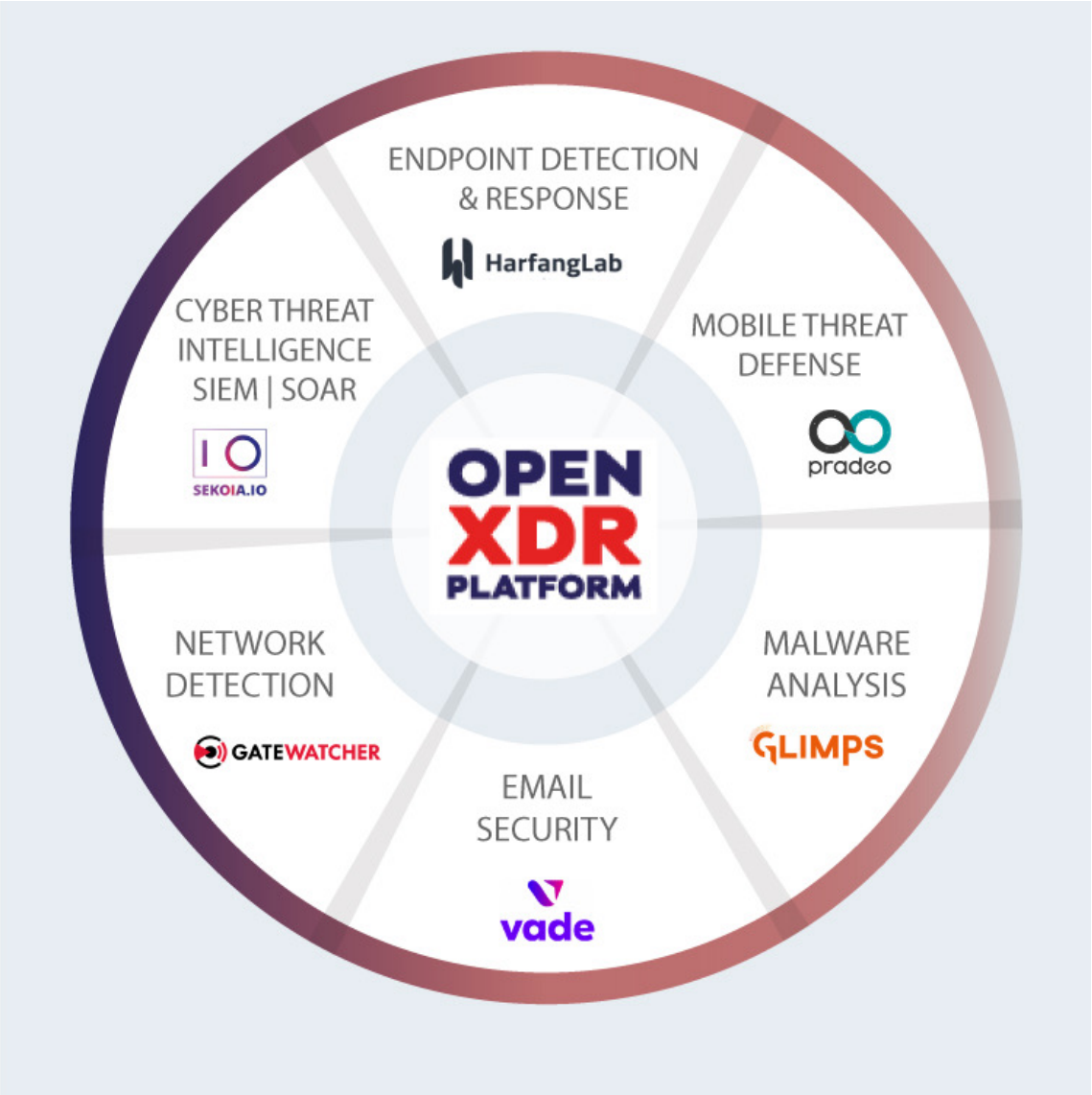
Awards

vade

Open XDR Platform

Innovative cybersecurity technologies in one platform

- XDR, Cyber Threat Intelligence, and SOAR par **SEKOIA**
- Endpoint Detection & Response, by **HarfangLab**
- Mobile Threat Defense, by **Pradeo**
- Malware analysis, by **GLIMPS**
- Email Threat Detection & Response, by **Vade**
- Network Detection, by **Gatewatcher**



Product Offering

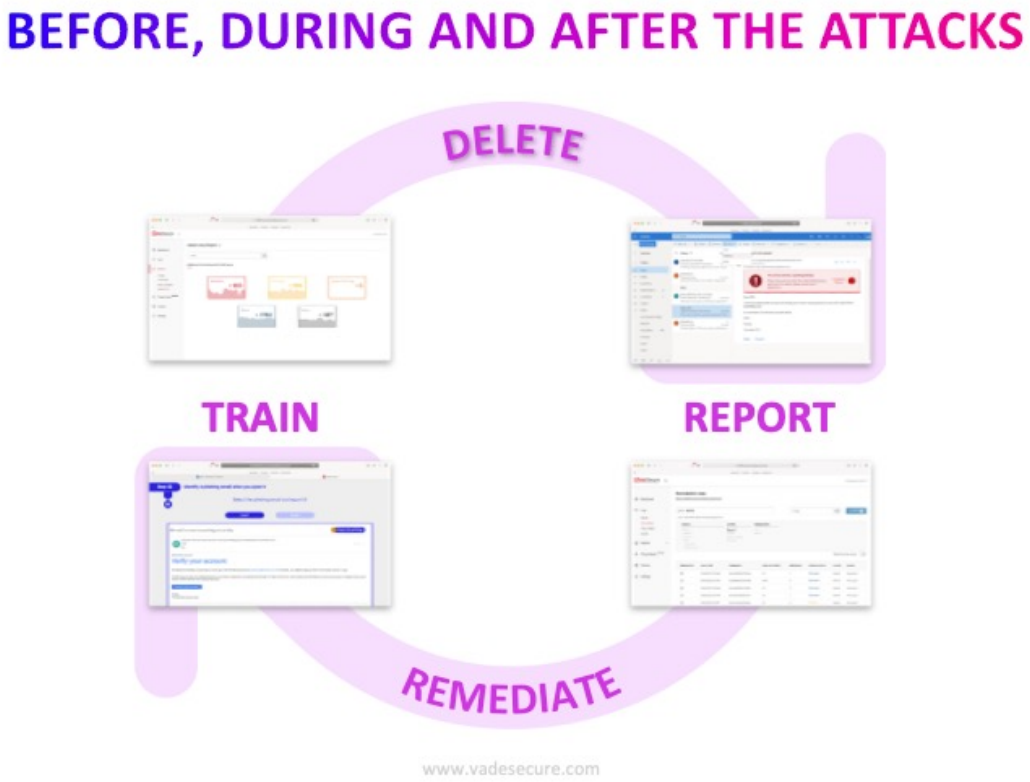
PRODUCT OFFERING

vade FOR M365

Fully integrated API

vade CLOUD

Easy and quick setup



For each threat, an integrated Vade feature

CORE DATA & AI TECHNOLOGIES

100 BILLION

Emails analyzed / day

- Machine Learning
- Natural Language Processing
- Deep Learning for Computer Vision

10+ MILLION

items blocked by Computer Vision / day

- 10,000 predictive algorithms
- Anomaly detection
- Written by humans and machines

Vade's approach

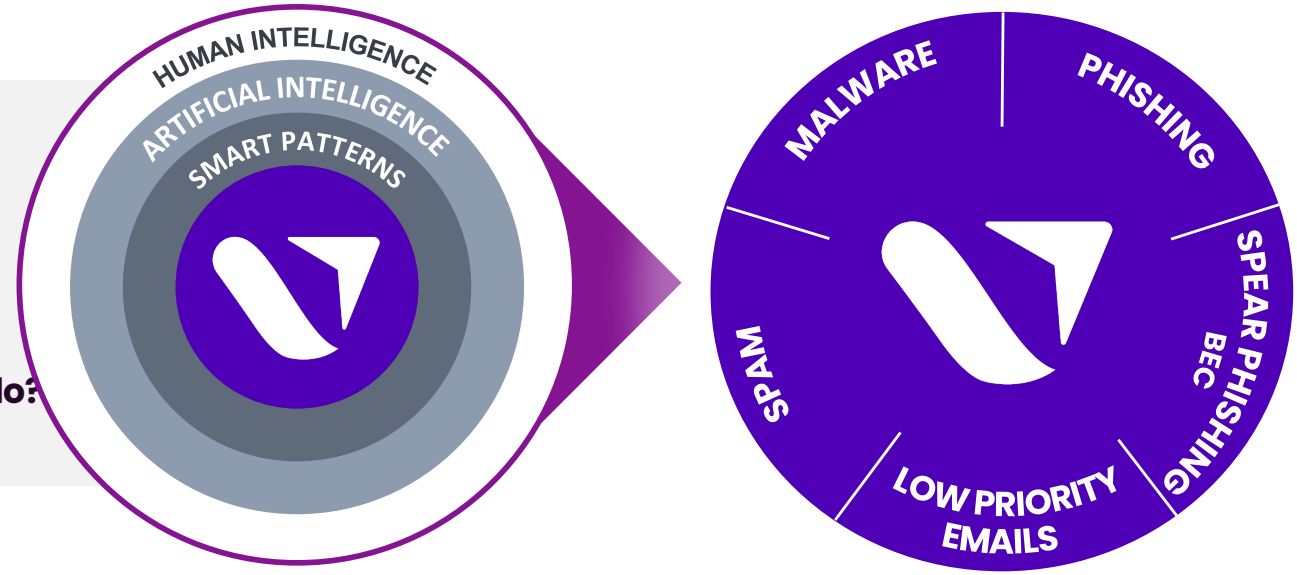
Understanding the purpose of an email

How was the email designed?

Why was it sent?

Does its behavior make sense?

What does the code in its attachment do?



Brand impersonation

Microsoft

Microsoft account

Hi [redacted],

Your password for [redacted] is set to expire on 5:19 AM, 21 Dec 2021 EST.
Keep same password with the button below.

Keep My Password

Do not ignore this email to avoid login interruption.

Thanks,
The [redacted] Team

Update Request [redacted]

[redacted]

CEO
France

From: [redacted] <personal@staff-secured-portal.com>
Date: Mon, Jan 28, 2019 at 1:30 PM
Subject: Direct deposit info
To: <[redacted]>

Hi Jon,

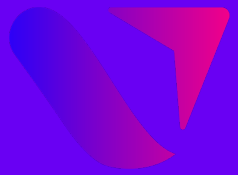
I need to change my direct deposit info on file before the next payroll is processed.
Can you get it done for me on your end?.

Regards,

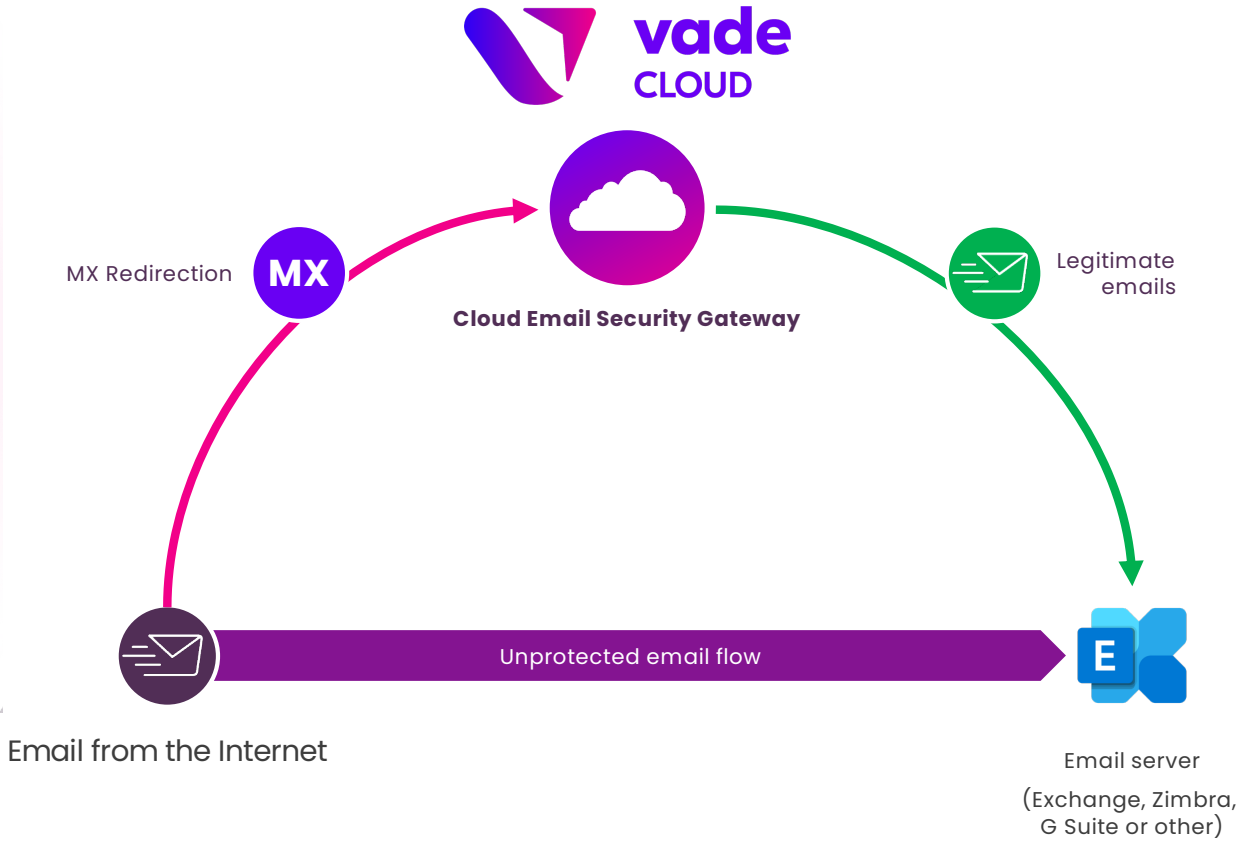
[redacted]

User impersonation

Vade Cloud



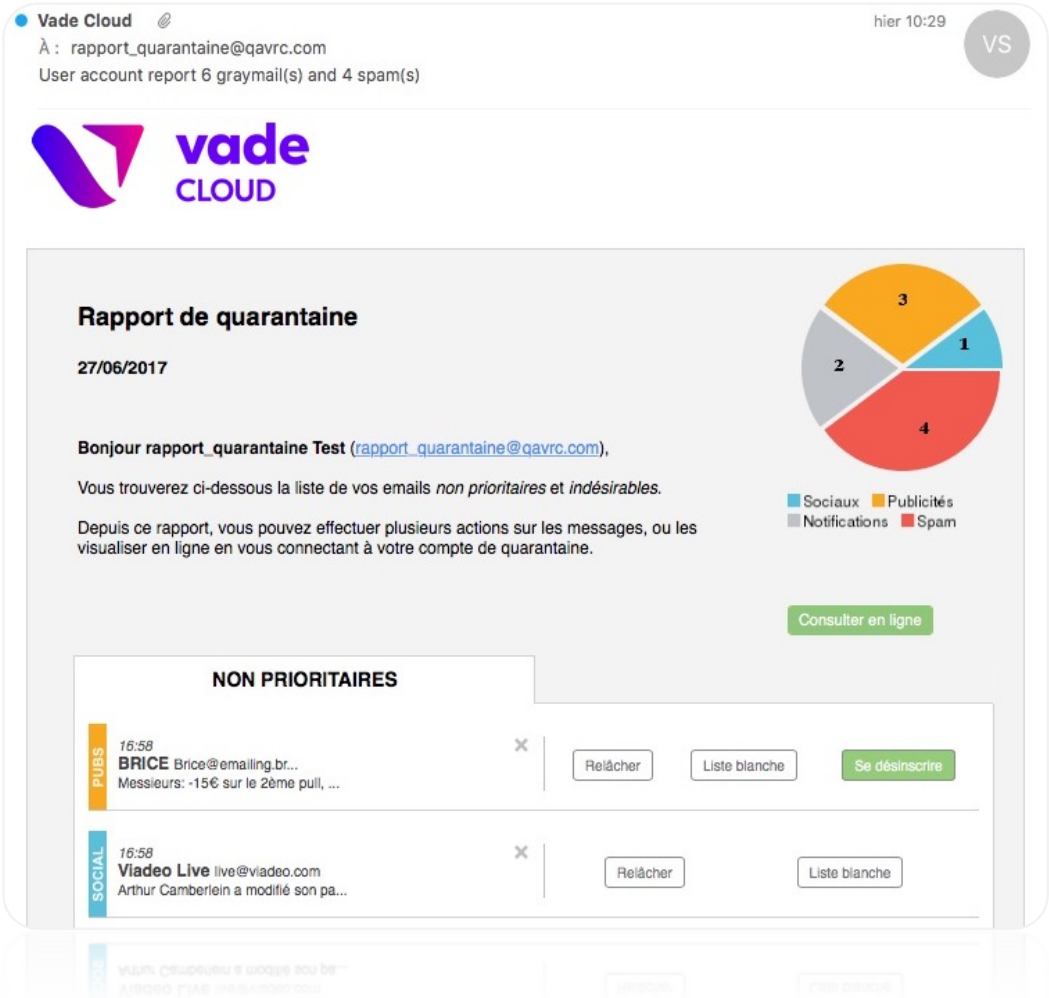
Vade Cloud Architecture



User experience

Individual quarantine report

Real time attack reports for admins



Advantages of Vade Cloud

Multi-platform solution

- Interfaces with all email platforms

360-degree protection, IP reputation and domain conserved

- Filtering of the full spectrum of non-priority threats and messages
- Filtering of incoming and outgoing emails

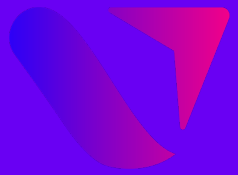
High availability and guaranteed continuity of service

- SLA 99.99% - 24/7 technical service – GRT 2 hours
- SMTP retention of 7 days

Data sovereignty

- Data housed in France by French hosts

Vade for M365



Microsoft : A great opportunity

Criminals are coming for Microsoft 365

(and have been
for the past 3 years)

#		Brand	Unique Phishing URLs
1	-	Microsoft Category: Cloud	39,621
2	↑2	Facebook Category: Social Media	14,876
3	↓1	PayPal Category: Financial Services	11,841
4	↑4	Chase Category: Financial Services	8,832
5	↑28	eBay Category: E-Commerce/Logistics	6,918
6	-	Rakuten Category: E-Commerce/Logistics	6,452
7	↓4	Netflix Category: Cloud	6,417
8	↑2	Amazon Category: E-Commerce/Logistics	6,063
9	↑5	WhatsApp Category: Social Media	5,322
10	↓1	DHL Category: E-Commerce/Logistics	4,403
11	-	Credit Agricole Category: Financial Services	
12	↑6	Wells Fargo Category: Financial Services	
13	↑3	Adobe Category: Cloud	
14	↓9	Bank of America Category: Financial Services	
15	↑2	Google Category: Cloud	
16	↑8	Comcast Category: Internet/Telco	
17	↓11	Apple Category: E-Commerce/Logistics	
18	↑22	La Banque Postale Category: Financial Services	
19	↑9	LinkedIn Category: Social Media	
20	↓8	Dropbox Category: Cloud	

Why is Microsoft 365 so attractive to hackers?

- **One target**
  258 million + corporate users
- **Single entry point**
  to the entire suite
- **Compromised accounts**
  for lateral attacks

Microsoft 365

Problem:

The Microsoft EOP / ATP security solutions detect some threats, but not all.

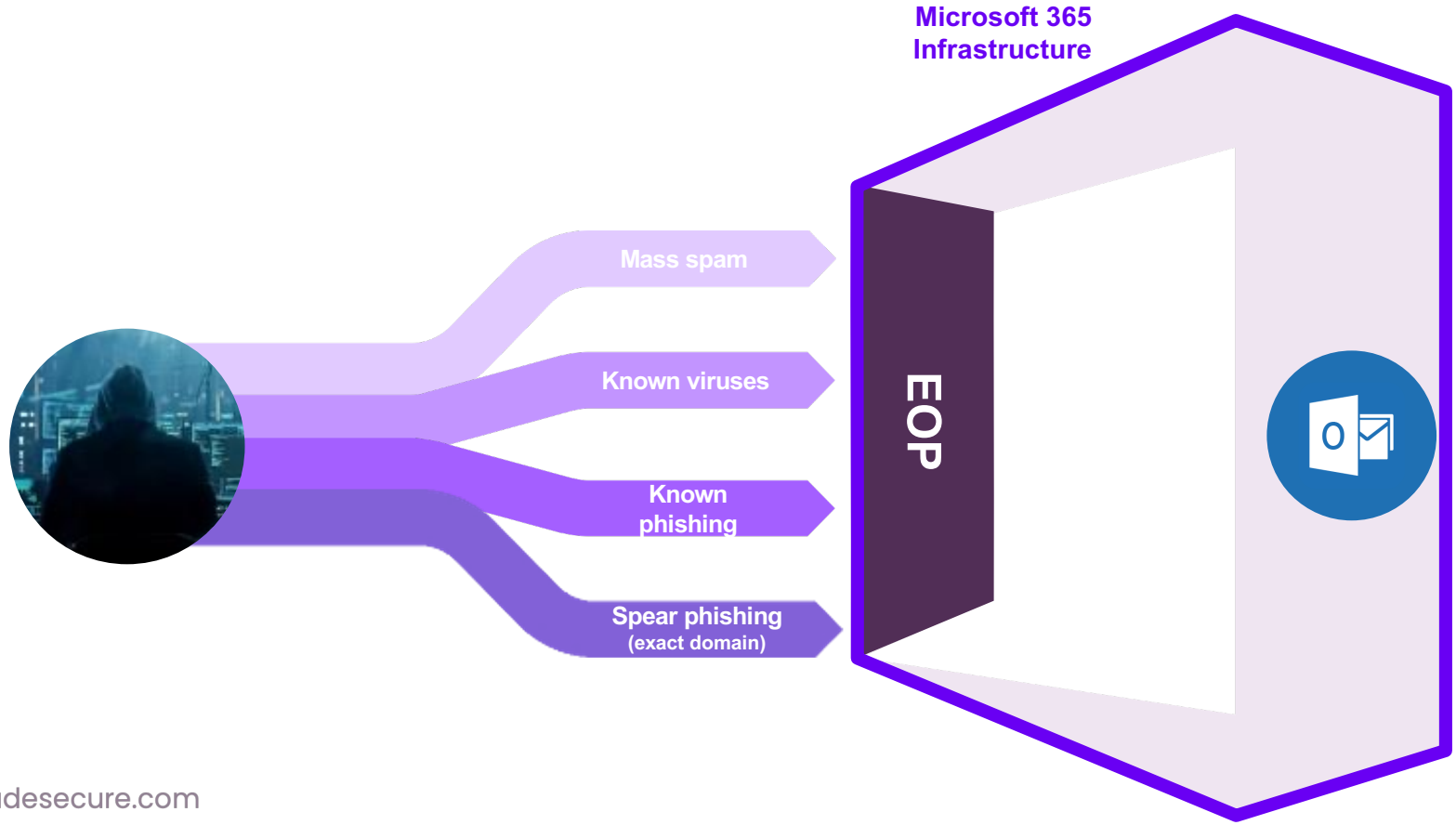
Solution:

Additional protection is needed against targeted attacks.

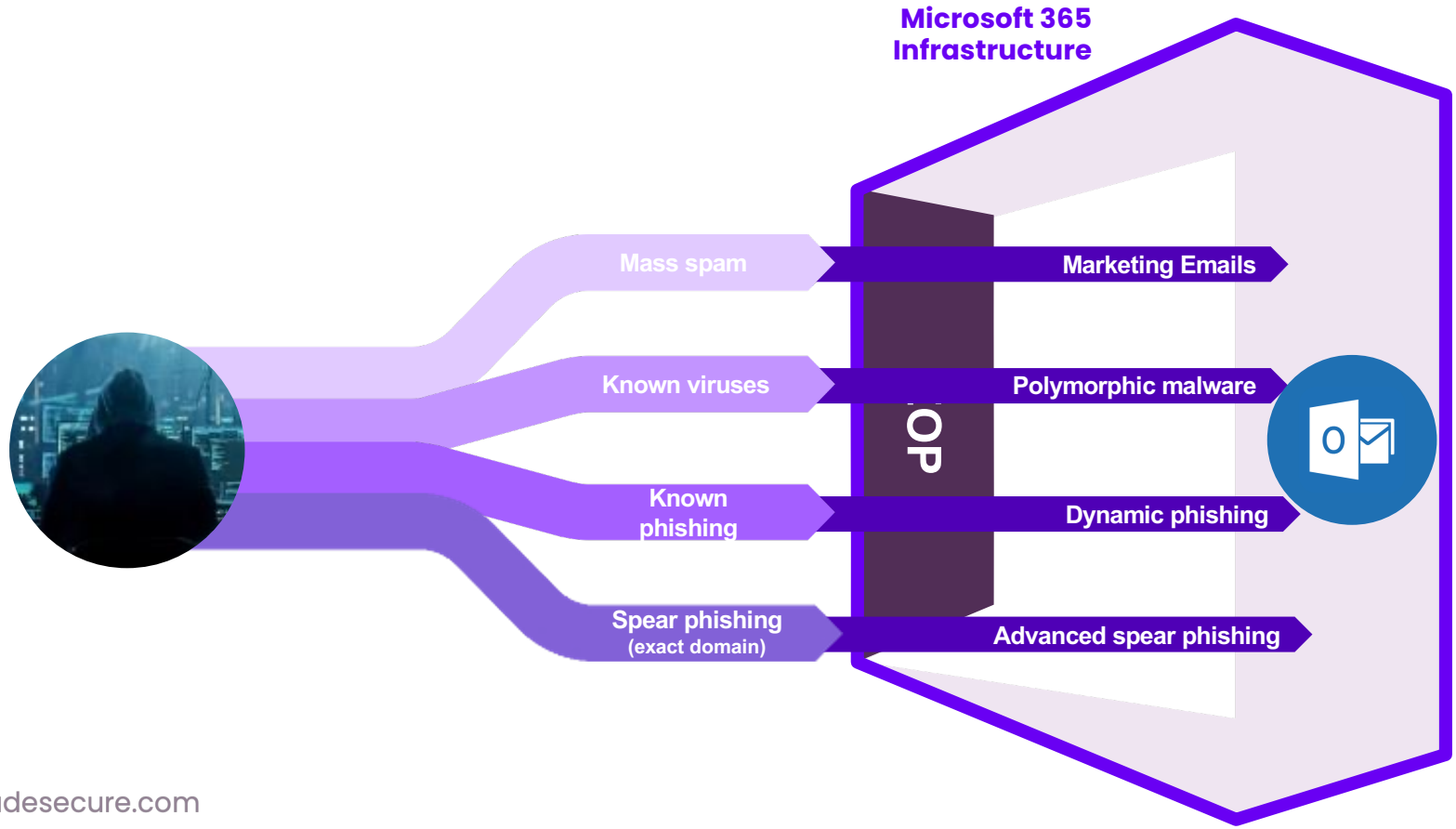
Email Security in Microsoft 365

vade

M365 EOP Security layer blocks known threats relying on standard techniques (signatures, IP reputation, etc.)

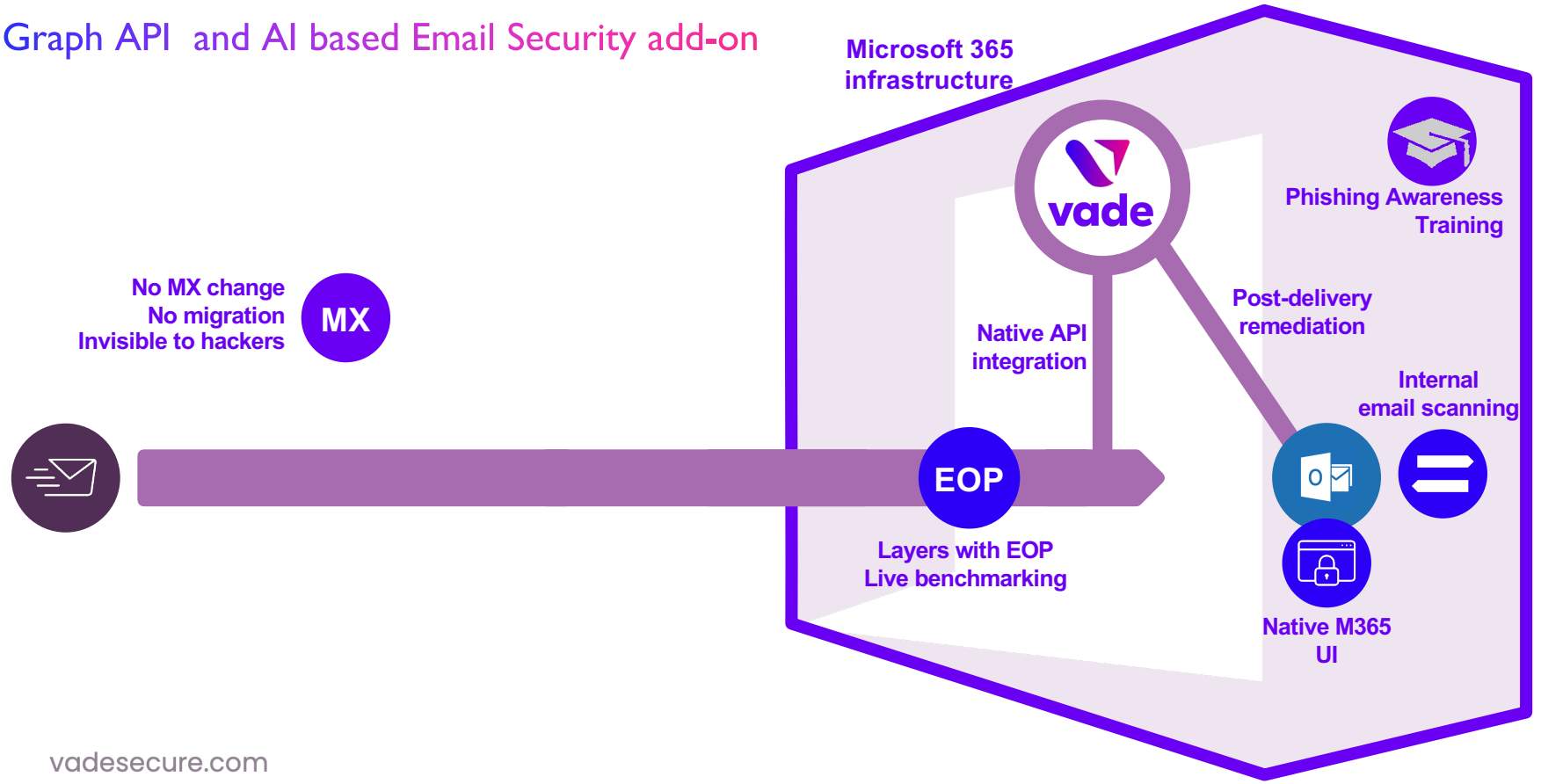


Additional protection is required to block advanced threats (highly targeted, low volume, short waves)



Vade for M365: Perfect fit for Microsoft 365

Graph API and AI based Email Security add-on



vade
FOR M365

AI based Email Security add-on for Microsoft 365

- Threat Detection
- Incident Response
- User Awareness

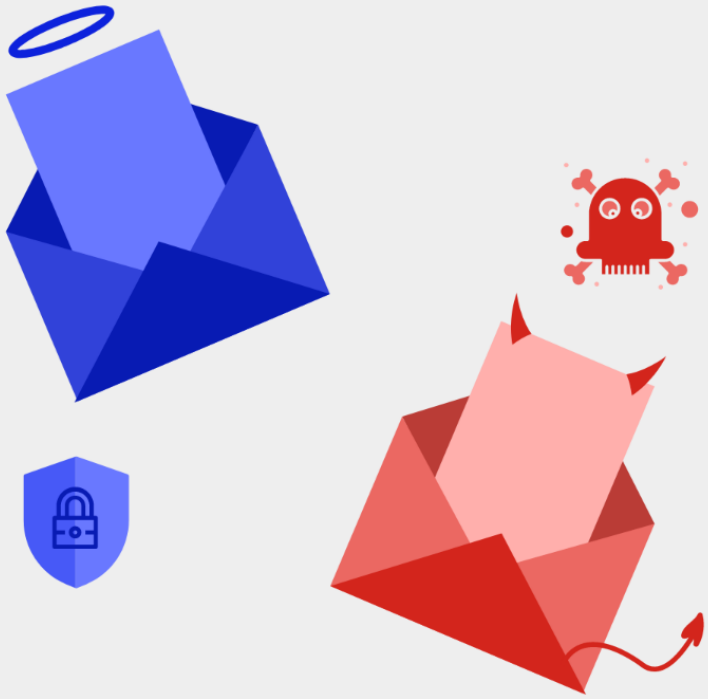
Vade Threat Coach™

- Automated phishing awareness training fully integrated into Microsoft 365
- Delivers training to users who engage with phishing emails
- Features real phishing samples, contextualized by brand and delivered at the moment of need
- Consists of a brief interactive quiz that assesses your users' phishing awareness
- Augments normal phishing awareness training by filling the gaps

Key Benefits and Features

On-the-fly	Contextualized	Dynamic
• Delivers training content at the moment of need—when user opens or clicks.	• Generates training content based on email attack type and spoofed brand.	• Features real phishing emails, updated daily with examples from top brands.

vade



Can you identify phishing emails?

Test your knowledge in 3 steps!

Let's go!

SECURED BY vade

Vade for M365, ‘Perfect Fit’ for System Integrators and MSPs

Easy to Activate:

- Quick activation & set-up
- No MX redirect

Easy to sell:

- Only 1 product
- Automatic detection of the number of users
- Monthly Billing

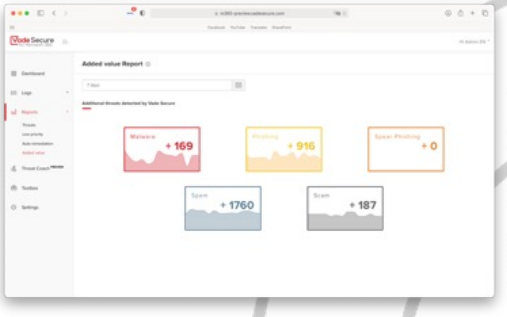
Easy to manage:

- Low maintenance
- Unchanged user experience
- User friendly administrator interface

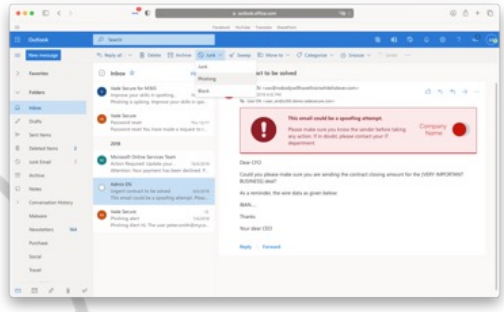
Vade for M365 provides a holistic approach to email cybersecurity.

DECIMATE

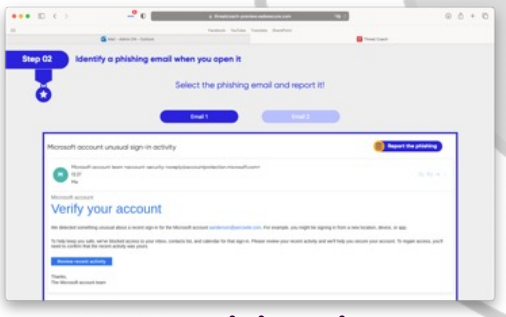
Decimates attacks with a demonstrated added value after Microsoft's security layers



Users, Admins, MSPs report emails and participate in the Intelligence Community

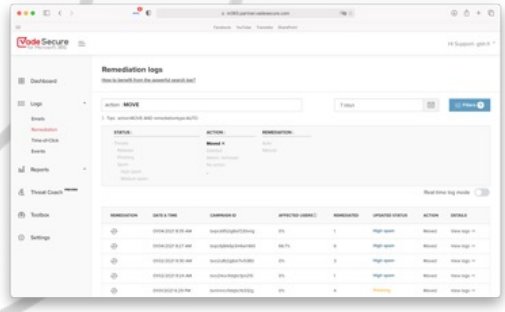


TRAIN



Automated training with real-life examples

REPORT



Fully automated Email Response / M-SOAR

REMEDIATE

VALUE OF SERVICES BASED ON VADE'S FUNCTIONS

Threat Coach™

Automated and contextualized training for end users instead of generic template-based training.

MSP Response

Cross-client security console
For threat management and incident response (Remediate and Auto-Remediate)

Threat Intel & Investigation

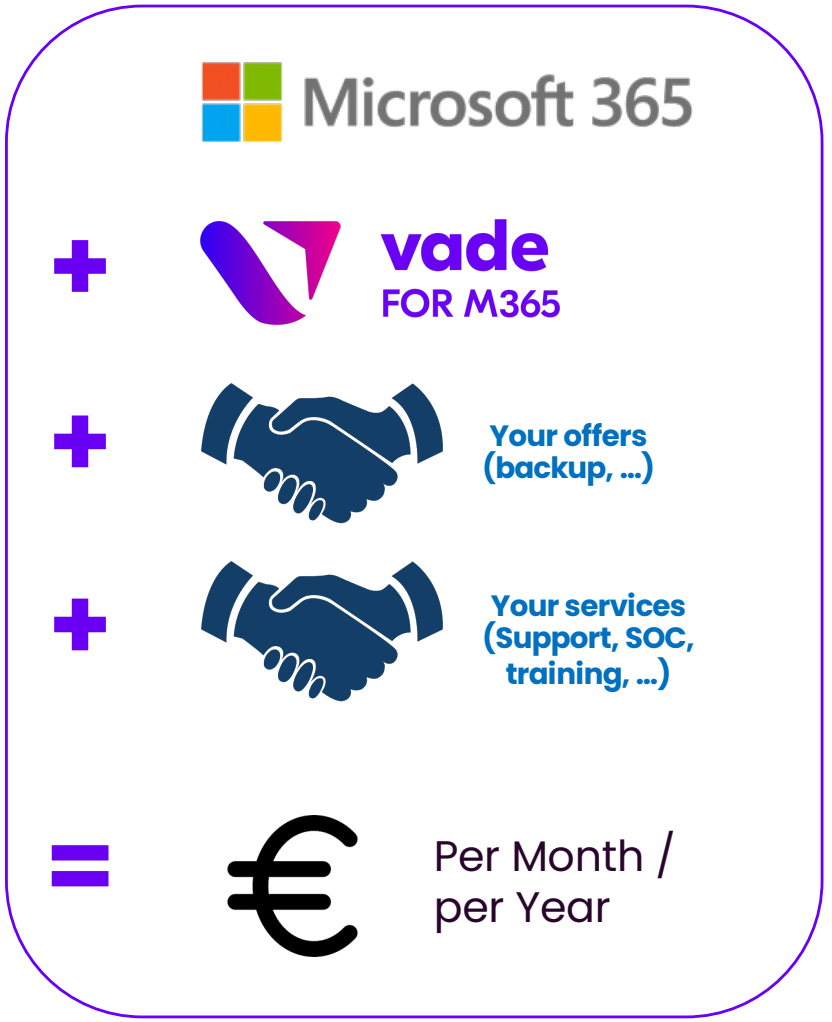
Premium functionality for SoCs or internal security teams. Proactive defense through analysis tools and SIEM integration.

vade
FOR M365

A range of services for optimal security

Ready-to-use incident response for your customers, by your teams

- Analysis of **user feedback**
- **Targeted remediation** of escalated threats
- Identification of **users who opened the threat**
- **In-depth investigation** of attachments
- **Correlate** security information with other solutions



Partner program

Being partner vade

Leader in innovation

18 U.S. patents

Numerous security industry awards

1 Billion mailboxes protected

95% renewal rate

Consistent revenue

Margin higher than the market average

Low cost of administration

Fast return on investment

Fast sales cycle

Easy demonstration

Free trials for customers

100% indirect model

Purpose-built for MSPs

Becoming a Vade Partner is a Prime Business Opportunity for Microsoft Resellers and MSPs

- NFR Licenses
- Selling support
- Marketing resources
- Partner portal
- Training website
- Technical support

Public price per end user

vade FOR M365

Range	Monthly	1 Year	3 Years
1 to 250 users	2.84 €	30.00 €	77.70 €
251 to 1000 users	2.27 €	24.00 €	62.16 €
1001 to 3000 users	1.82 €	19.20 €	49.73 €
3001 to 5000 users	1.56 €	16.40 €	43.16 €
5001 to 10 000 users	1.29 €	13.60 €	35.79 €
10 001 to 15 000 users	0.88 €	9.30 €	24.47 €
15 000+ users	0.71 €	7.50 €	19.74 €

Peace of mind costs the price of a cup of coffee per user per month!

First step to begin:

partner.vadesecure.com

Let's Demo

vade