vade

Building a Scalable Managed Security Service with Vade for M365

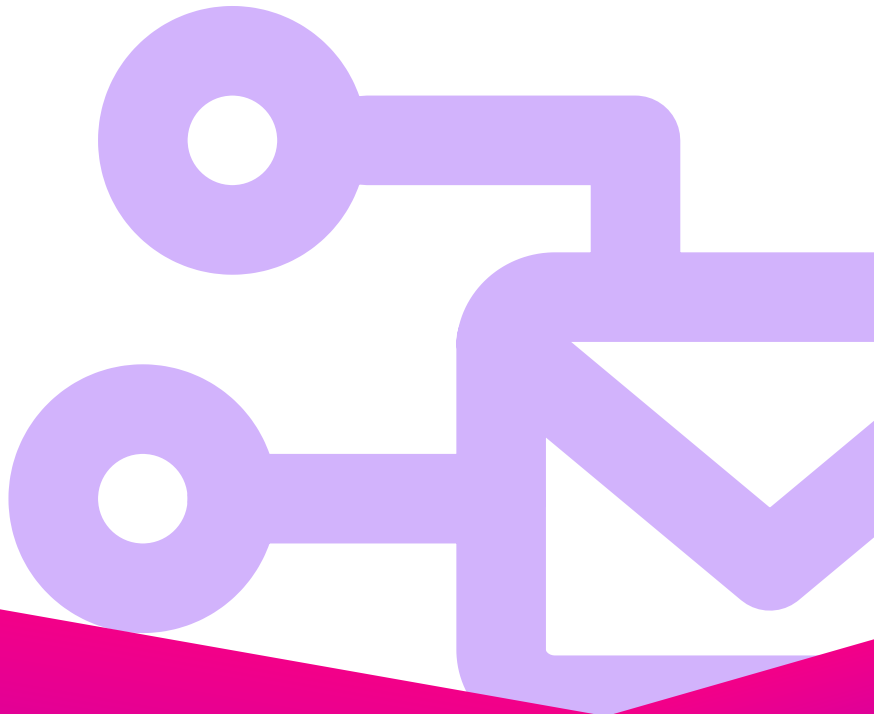


TABLE OF CONTENTS

INTRODUCTION

2020 might be over, but the profound changes resulting from the COVID-19 pandemic set in motion continue to live on. The depth and breadth of the transformation that took place in just a few short months has challenged many small and midsized businesses (SMBs)—they'll need access to new skills, competencies, and strategies in order to navigate the "new normal."

On the one hand, there's unprecedented demand for new digital products and services, and near-limitless opportunity for those businesses that can evolve to meet this demand. On the other hand, today's cybersecurity risks are more pressing—and current attack tactics more potentially devastating— than ever before.

MSPs that stand ready to help their customers set the right course through these novel and trying circumstances can expect to see their businesses grow in the coming months and years. Those best prepared to meet the demands of tomorrow's dynamic business climate stand to win against less-ready competitors.

A recent survey conducted by Datto highlights the widening gap between the top performers and the slowest-growing MSPs: only 20 percent of MSPs report growth rates of more than 20 percent per year that have been sustained over the last three years.[1] What sets these leaders apart is that they generate a higher portion of their revenue from managed services. They're able to maintain steady cash flow with high levels of recurring revenue while providing the benefits that their customers need most: high-value offerings that help businesses stay productive and profitable.

Managed services, including email security and endpoint management, currently generate 53 percent of MSPs' annual revenue, while break-fix services generate only 10 percent. And for every 10 percent increase in the proportion of revenue an MSP generates from managed services, its annual growth rate will increase by 0.25 to 0.75 points.

> ***For every 10 percent increase in the proportion of revenue an MSP generates from managed services, its annual growth rate will increase by 0.25 to 0.75 points.***

This trend will likely continue over the next few years. According to a 2020 CompTIA survey, 67 percent of business stakeholders reported that their organization was looking for additional third-party assistance to shore up its ability to protect remote workers, and 75 percent of IT security and managed services professionals said they'd seen an increase in business opportunities since the start of 2020.[2]

The bottom line is that MSPs wanting to reach their growth targets should look for opportunities to generate ongoing revenue, particularly through managed service offerings that are easy to administer, highly valuable to customers, and increasingly in demand.

[1] Datto. *Datto's 2020 State of the MSP Report.* https://www.datto.com/resource-downloads/Datto2020_State-of-the-MSP-Report.pdf

[2] CompTIA. *The Sudden Shift to Remote Work is Driving Business for Tech Firms During COVID-19.* https://connect.comptia.org/blog/tech-business-covid-19

I. Email security: A critical business need for your clients, a world of opportunity for you

Email has long been the most common entry point for malware-based cyberattacks as well as social engineering scams, but the number of email-borne threats further increased in 2020. Phishing played a role in 36 percent of the breaches analyzed in the 2021 Verizon Data Breach Investigations Report, making it the most frequently-exploited threat action of the year.[3] This represents a significant increase in prevalence from 2019's numbers (25 percent). And, according to the FBI's 2020 Internet Crime Report, the raw number of phishing attacks doubled from the year before.[4]

A majority of these email-based attacks found targets within the Microsoft 365 application ecosystem. Demand for cloud services like Microsoft 365 skyrocketed during the pandemic as businesses sought a solution that would enable a quick transition to remote work. Already the world's most widely-used software suite at the end of 2019, Microsoft 365 then boasted 200 million active users; by the end of the second quarter of 2020, its user base had expanded to 258 million.[5]

This growth in the number of Microsoft 365 users, combined with the number of email-borne cyberattacks, means that Microsoft accounts are especially likely to be targeted by malicious actors. After all, Microsoft's market dominance already made it the top target for attackers, with the tech giant remaining the most impersonated brand in phishing attacks in four of the last six quarters.[6] Research also reveals that 71 percent of Microsoft 365 users have experienced an account takeover attack within the past year.

> ***71 percent of Microsoft 365 users have experienced an account takeover attack within the past year.***

[3] Verizon. *2021 Data Breach Investigations Report.* https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.42100261.1805425503.1621456782-104164624.1620685073

[4] Federal Bureau of Investigation. *Internet Crime Complaint Center. Internet Crime Report 2020.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[5] Microsoft. *"Earnings Release FY21 Q2: Microsoft Cloud Strength Drives Second Quarter Results".* https://www.microsoft.com/en-us/Investor/earnings/FY-2021-Q2/press-release-webcast

[6] Vade. *"A Year Like No Other: Phishers' Favorite Brands of 2020".* https://www.vadesecure.com/en/blog/phishers-favorite-brands-2020

II. Protecting your customers' email hasn't been easy — until now

Clearly, there's a strong and growing need among MSPs' customers for better safeguards to protect their users' email accounts, and along with them, the entirety of the IT environments to which email serves as a gateway. That an attack against a Microsoft 365 account might succeed isn't a risk that anyone should be willing to take.

While some organizations may be tempted to rely on Microsoft's built-in security solutions, these haven't proven effective in independent third-party testing. Microsoft Exchange Online Protection (EOP) and the add-on service, Defender, formerly Advanced Threat Protection (ATP), ranked dead last and second-last in terms of detection and false-positive rates when compared with other security vendors' email security solutions by expert advanced threat researchers.[7]

However, creating new managed security services offerings isn't always simple. Adding standalone cybersecurity solutions to your toolset can increase your employees' workload and administrative burden. This may require you to hire additional employees or certify existing team members in newly adopted solutions. This can be an expensive and time-consuming process, particularly given the size and extent of the current cybersecurity skills gap.

The reality is that although offering cybersecurity services (including email security) promises to be one of the fastest-growing sources of ongoing revenue for MSPs this year,[8] the margins you're hoping to see won't materialize if administrative costs are too high. Hence, there's enormous need for a solution that's easy to administer for a wide array of clients, from a single dashboard—one that doesn't require advanced technical skills or a specialized certification to work with.

> ***Although offering cybersecurity services promises to be one of the fastest-growing sources of ongoing revenue for MSPs this year, the margins you're hoping to see won't materialize if administrative costs are too high.***

[7] SE Labs. *Email Security Services Protection. Jan-Mar 2020.* https://selabs.uk/reports/email-security-services-protection/

[8] Altaro Software. *"70% of MSPs saw increased revenue as companies work from home"*. https://www.altaro.com/msp-dojo/msp-survey-microsoft-365/

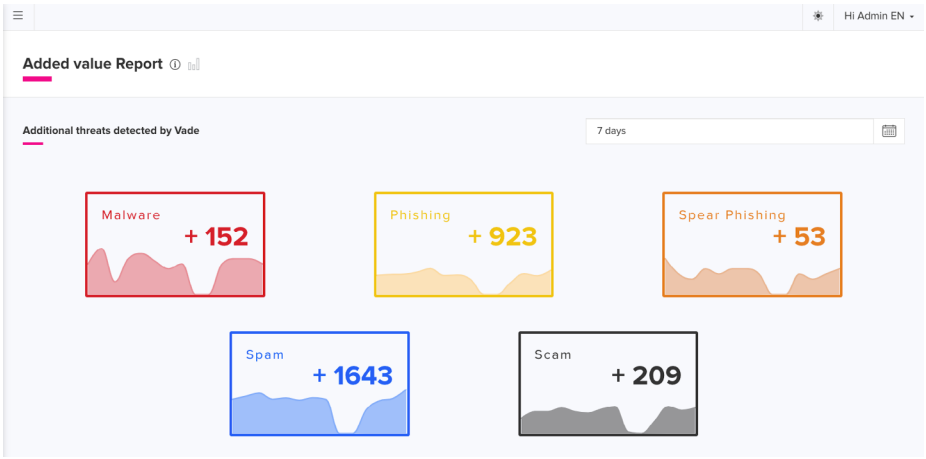
III. Introducing Vade for M365: The driving force behind robust managed security service offerings

Vade for M365 is purpose-built for MSPs and designed to empower them to create a robust managed security service that is easy to bundle, sell, and manage. The solution's architecture leverages API integration with Microsoft 365 to enable fast deployment and a native Outlook experience for end users. API integration also enables a range of features and benefits for MSPs:

- No MX changes required
- Invisible in MX record queries
- Post-delivery remediation capabilities
- Easy to configure (on/off toggle settings)
- Automated feedback loop
- Ingests Microsoft Exchange settings

Vade for M365 protects against today's dynamic email-borne threats by using machine learning (ML) and computer vision to detect phishing and spear phishing attempts (business email compromise). Vade's Filter Engine combines heuristics and AI to identify malware and ransomware in real-time, with no quarantine and no latency to end users. In a 2021 benchmark assessment of 330,000 emails on a production tenant configured with Microsoft EOP and Defender, Vade blocked nine times more advanced threats than Microsoft Defender. Advanced threats are threats that were not detected by Microsoft EOP.

> ***In a 2021 benchmark assessment of 330,000 emails on a production tenant configured with Microsoft EOP and Defender, Vade blocked nine times more advanced threats than Microsoft Defender.***



Threats missed by Microsoft and blocked by Vade for M365

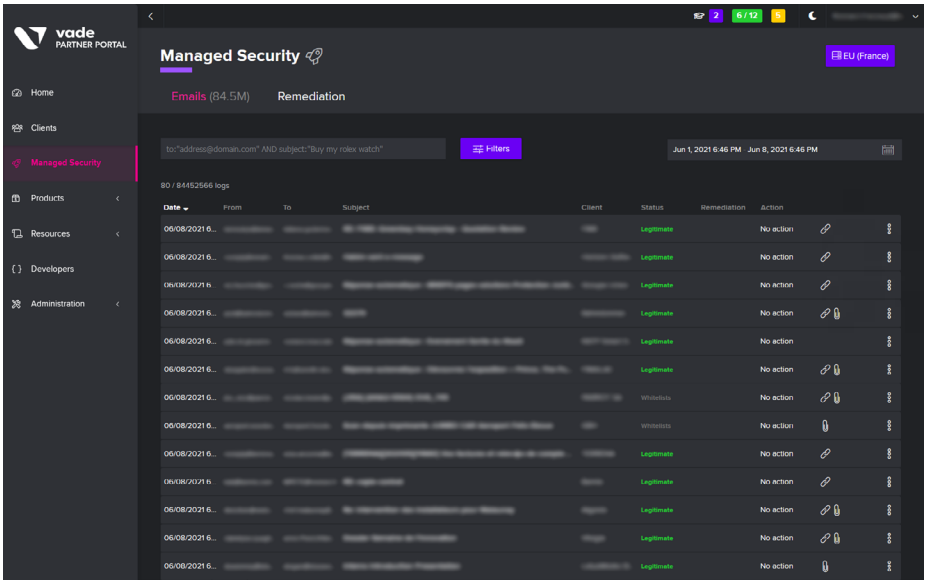
In addition to threat protection, Vade for M365 comes with no-cost, integrated features. MSP friendly, these automated features are designed to empower MSPs to move beyond selling licenses and toward building a scalable managed service business–without needing to hire expert security staff or incur more licensing or add-on fees.

> ***Automated features are designed to empower MSPs to move beyond selling licenses and toward building a scalable managed service business***

Integrated, MSP-friendly features

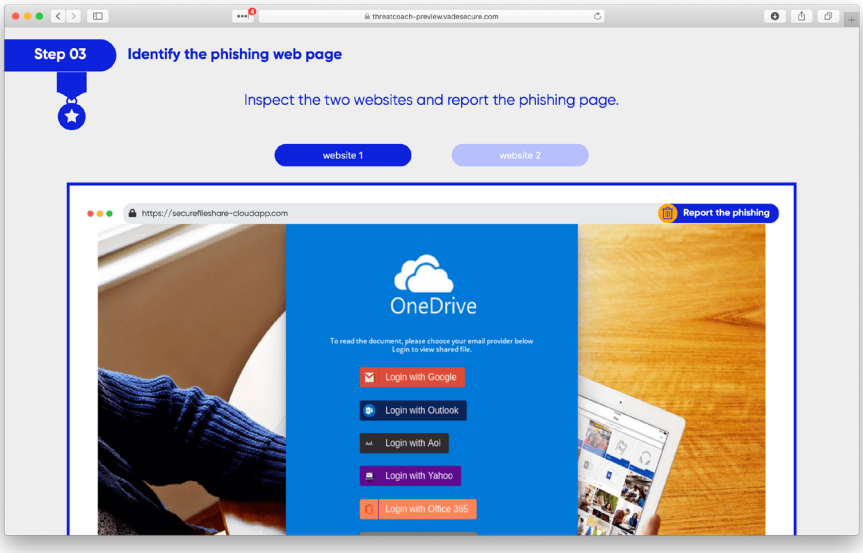
MSP Response

MSP Response provides unified threat management and incident response capabilities in a single dashboard in the Vade Partner Portal. MSP Response features a cross-tenant interface that aggregates all your Microsoft 365 tenants in a single dashboard. If you identify a threat in one client's email logs, you can quickly see whether that email was delivered to other clients, and you can then remediate all examples of that email, across your entire client base, with a single click.



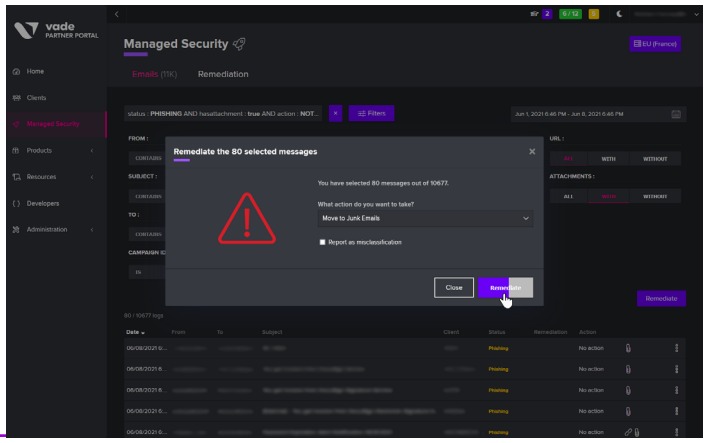
Threat Coach

Threat Coach is an automated user awareness training tool that launches a targeted awareness campaign based on the end user's behavior. Leveraging current, real-time examples of phishing emails and other threats, Threat Coach fills the gap between simulated phishes and routine user awareness training. Unlike simulated phishing exercises built from templates, Threat Coach features real phishing emails captured by Vade. Phishing samples used in training exercises are automatically generated at the user level on the types of emails the user typically receives and from the brands they typically receive them from.



Auto-Remediate

Vade's Filter Engine scans an average of 100 billion emails per day from its database of 1 billion protected mailboxes. The self-learning AI engine scans mailboxes continually and removes email threats post-delivery, with no action required by the admin. Admins can also manually remediate emails with one click. Auto-Remediate is powered by a continual stream of intelligence from threats detected, from user reports, and from our research and SOC teams that continually fine-tune the engine.



The power of artificial intelligence

Artificial intelligence (AI) is the scientific pursuit of developing computers that can mimic the problem-solving and decision-making abilities of the human mind. In advanced email security solutions like Vade for M365, AI enables the software to go beyond simple signature-based threat detection methods to identify the sophisticated, evasive threats that other tools (including Microsoft's built-in capabilities) will miss. AI achieves this by constantly learning from Vade's user base. With over 1 billion protected mailboxes to draw upon as a source of information on the latest threats, Vade for M365's intelligence is always being updated to reflect the latest global attack tactics.

Vade for M365 was built to be user-friendly. Designed to deploy in ten minutes, it offers set-it-and-forget-it configurability and a native Outlook experience that intuitive and simple.

IV. Conclusion

By protecting your customers with AI-based predictive email defense, you're safeguarding their productivity and profitability. With a single solution designed first and foremost for ease-of-use, you can build a scalable managed security service offering without creating burdensome administrative overhead. You'll enjoy some of the most comprehensive sales, marketing ,and technical support in the industry. And you can rest easy, knowing that your business is on the road to success.

About Vade

Vade helps MSPs and ISPs protect their users from advanced cyber-threats, such as phishing, spear phishing, malware, and ransomware. The company's predictive email defense solutions leverage artificial intelligence, fed by data from 1.4 billion mailboxes, to block targeted threats and new attacks from the first wave. In addition, real-time threat detection capabilities enable SOCs to instantly identify new threats and orchestrate coordinated responses. Vade's technology is available as a native, API-based offering for Microsoft 365 or as lightweight, extensible APIs for enterprise SOCs.

Follow us

Subscribe to our blog
www.vadesecure.com/en/blog