vade

The Channel Opportunity with Microsoft 365

An MSP's Guide
to Managed Microsoft Security

Table of Contents

Introduction

The growth of Microsoft 365 has created sustained business opportunities for MSPs. Margins, however, are on the downslide.

While Microsoft once offered a 23 percent margin for 2,500 seats, today, the average profit margin on a Microsoft resell is around 15 percent (for Microsoft CSPs).[1]

Some MSPs, however, are making almost no profit from their Microsoft 365 licenses. While some MSPs are focusing less on Microsoft as a result of reduced margins, others are finding creative ways to expand on their Microsoft offerings by creating value-added managed security services.

The key is in finding complementary solutions that will help you consolidate your stack in a way that is both efficient and profitable.

1 Faria, Andre. July 3, 2020. *Microsoft Cloud Solution Provider (CSP) – Reseller, Professional Services, MSP and IP Evolution.* linkedin.com/pulse/microsoft-cloud-solution-provider-csp-reseller-services-andre-faria

Microsoft growth creates new challenges and opportunities

Microsoft's dominance in the office application market reached new heights as the world came to a near standstill in March 2020. COVID-19 disrupted global business and made makeshift home offices of kitchens and living rooms around the world. The advertised "two-week pause" has now entered its second year, and while it financially devastated many businesses and workers, there were some clear winners, the most prominent being Microsoft.

258 million

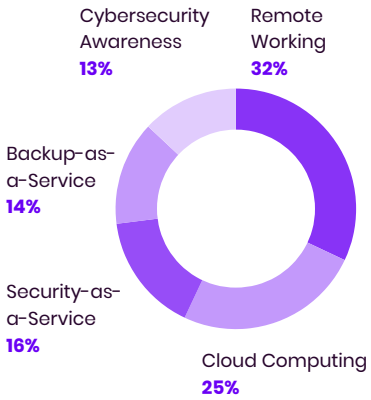
Microsoft 365 users by Q3 2020.

The great cloud migration during the first weeks of global COVID-19 lockdowns sent businesses, big and small, flocking to Microsoft 365 and Teams. In its Q1 2020 fiscal earnings report, Microsoft reported 200 million Microsoft 365 business users.[2] By Q3, Microsoft reported 258 million Microsoft 365 users and 75 million daily active users on Teams. In the words of Microsoft CEO Satya Nadella, the shift amounted to "two years' worth of digital transformation in two months."[3]

> SaaS that enables remote work drove the bulk of business opportunities for MSPs during the pandemic.

MSPs felt the effects of this transformation firsthand. Like Microsoft, many MSPs benefited from the move to remote work. As businesses shifted operations from offices to their employees' homes and apartments, they turned to MSPs to help make the transition. From teleconferencing software to cloud computing to remote monitoring, SaaS that enables remote work drove the bulk of business opportunities for MSPs during the pandemic.[4]

Best Revenue-Generating Opportunities



SOURCE: Altaro Software

2 Protalinksi, Emil. *Microsoft reports $33.1 billion in Q1 2020 revenue: Azure up 59%, Surface down 4%, and LinkedIn up 25%.* VentureBeat. venturebeat.com/2019/10/23/microsoft-earnings-q1-2020

3 Protalinski, Emil. *Microsoft Reports $35.0 Billion in Q3 2020 revenue: Azure up 59%, Surface up 1%, and LinkedIn up 21%.* April 29, 2020. VentureBeat. venturebeat.com/2020/04/29/microsoft-earnings-q3-2020

4 Altaro Software. *The Impact of Covid-19 on MSPs Revealed.* altaro.com/msp-dojo/covid-19-msp

While some might have expected the workforce to return to normal as the pandemic loosened its grip in many parts of the world, that expectation has fallen flat. One by one, the world's largest and most influential companies made clear that **remote work is here to stay** when they announced that a significant portion of their workforce could work from home permanently.

While Google and Salesforce may not be representative of most businesses, that these large corporations could make such a change inspired businesses of all sizes and across markets to follow suit. For MSPs, what seemed like a short-term opportunity has transitioned to long-term viability, with Microsoft 365 leading the pack of both in-house and remote-work solutions.

"For MSPs, what seemed like a short-term opportunity has transitioned to long-term viability.

The massive cybersecurity opportunity with Microsoft 365

Cybersecurity, already a lucrative business before the pandemic, created an explosion of opportunities as remote work took hold. More than 40 percent of MSPs reported that demand for managed security services increased in 2020, and 89 percent reported that managed security will be the top driver of business growth in the next two years.[5]

In 2020, MSPs reported that 62% of their clients are using Microsoft 365, and they expect usage to increase to 70% in two years.[6] The product, though superior, has its security flaws, and despite the security challenges that Microsoft 365 presents, it presents even bigger opportunities for sustained business and new revenue opportunities.

40%

of MSPs reported that demand for managed security services increased in 2020.

62%

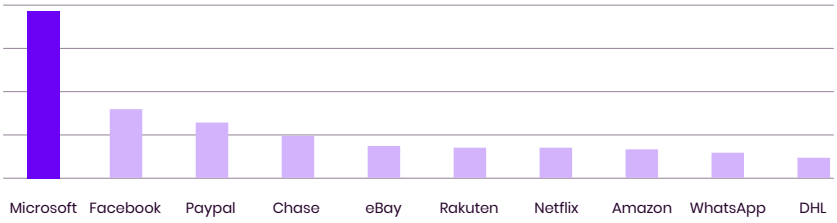
of MSPs' clients are using Microsoft 365 in 2020.

No. 1

Microsoft is the #1 target for email-borne cyberattacks with more than 39,000 unique phishing URLs detected in 2020.

Email Security

Because of Microsoft's dominance in the business email market, it is the #1 target for email-borne cyberattacks. **Microsoft was the most impersonated brand in phishing attacks in four of the last six quarters**, with more than 39,000 unique Microsoft phishing URLs detected in 2020, surpassing other big-name targets, including PayPal and Facebook.[7]



5 Acronis. *Pulse of the MSP Survey 2021.* acronis.com/en-us/blog/posts/pulse-msp-2021-survey-reveals-trends-it-channel
6 Datto. *2020 Global State of the MSP Report.* July 2020. datto.com/resources/dattos-global-state-of-the-msp-report-2020
7 Vade. *Phishers' Favorites 2020 Year-in-Review.* February 2020. info.vadesecure.com/en/ebook-phishers-favorites-2020-year-in-review

Unlike phishing emails of the past that were sent in waves, today's attacks are highly targeted, leveraging sophisticated obfuscation techniques designed to bypass Microsoft's defenses.

EOP – Exchange Online Protection, Microsoft 365's built-in email security, offers adequate protection from reported or known spam, malware, and phishing emails, but it's known to be **weak at blocking sophisticated attacks**.

64% of MSPs reported ransomware attacks within Microsoft 365, and phishing emails were named the leading cause (54 percent) of ransomware attacks against SMBs.[8]

Frustrated SMBs look to their MSPs to provide a solution to the relentless attacks against Microsoft 365. As a result, MSPs have had to seek **third-party solutions to layer with EOP to provide adequate protection**, which in turn, enables them to offer email security as a managed service.

64%

of MSPs reported ransomware attacks within Microsoft 365.

No. 1

Phishing is the leading cause of ransomware attacks according to 54% of MSPs.

SEG – In the past, secure email gateways (SEGs) were the the go-to staples for email security, but they are not optimal for Microsoft 365. Because they sit outside the M365 tenant, a SEG:

- Requires a mail exchange (MX) record change
- Is visible to hackers in an MX record query
- Cannot remove emails post-delivery
- Does not protect from insider threats/breached accounts

CESS – Email security solutions that are integrated with Microsoft 365 via API sit inside the Microsoft tenant and layer with EOP. Also known as a cloud email security supplement (CESS), they offer a few additional advantages for MSPs:

- No MX change required
- Invisible to cybercriminals
- Ingests Microsoft Exchange settings

Finally, a CESS offers one of the most important features that SEGs cannot offer: remediation. With a SEG, a delivered email cannot be removed from Outlook. With a CESS, an admin can remove it from an Outlook inbox post-delivery, eliminating the threat before a user has the chance to click.

"With a SEG, a delivered email cannot be removed from Outlook. With a CESS, an admin can remove it from an Outlook inbox post-delivery.

8 Datto. *2020 State of the Channel Ransomware Report*. November 2020. datto.com/resources/dattos-2020-global-state-of-the-channel-ransomware-report

User Awareness Training

While they tend to shoulder the brunt of the blame after a cyberattack or breach, users are the last line of defense when cybersecurity fails, which it will at one point or another. A common managed security offering among MSPs, user awareness training can significantly cut down on the user errors that lead to breaches. The data available on this point, however, is conflicting.

According to Verizon, phishing click rates have reached industry lows—3.4 percent in 2020.[9] Yet 54 percent of MSPs say that phishing was the #1 cause of ransomware attacks against their clients, 27 percent blamed poor user practices/gullibility, and 26 percent blamed lack of cybersecurity training.[10] If users are being trained, it's clear that something is awry, and MSPs have an opportunity to take advantage.

> 54 percent of MSPs say that phishing was the #1 cause of ransomware attacks against their clients.

Offering user awareness training as a managed service hits two targets with one weapon:

1. **It reduces the likelihood of a breach**, which saves the MSP precious time and resources.
2. **It reduces the likelihood of an MSP being held liable for a cyberattack**, and many are held financially responsible by their customers.

Offering user awareness training enables MSPs to add an additional managed service on top of the Microsoft email security offering, and one that is highly specific to the Microsoft environment and its SMB users. Corporate and consumer users receive different types of emails: training should be tailored to the types of phishing emails users receive.

An automated solution that delivers contextualized training can cut down on the time MSPs and admins spend on creating simulated phishes from templates. It can also provide real-world examples that are more likely to resonate with the user.

9 Verizon. *2020 Data Breach Investigations Report*. 2020. enterprise.verizon.com/resources/reports/dbir
10 Datto. *2020 State of the Channel Ransomware Report*. November 2020. datto.com/resources/dattos-2020-global-state-of-the-channel-ransomware-report

M-SOAR

Coined by Gartner, M-SOAR (Mail Security Orchestration, Automation and Response) is yet another potential managed security service for Microsoft 365 focused solely on email security. No security solution catches 100 percent of threats, so the odds of a phishing email winding up in your clients' inboxes are good. When it does, MSPs need to be able to detect, respond, and remove it post-delivery.

Adding an M-SOAR service to the Microsoft 365 offering enables MSPs to **provide more comprehensive protection by reducing phishing response and recovery time**. Once again, SEGs are not optimal here, as post-delivery remediation in Microsoft 365 is not viable with a SEG.

> A CESS that is deeply integrated with Microsoft 365 can continually scan and remove emails post-delivery in an automated fashion.

A CESS that is deeply integrated with Microsoft 365 can continually scan and remove emails post-delivery in an automated fashion—an added service that does not require adding to the MSPs headcount or workload.

To optimize M-SOAR, MSPs should seek a CESS that auto-remediates post-delivery threats that are captured by both the filter and by data from user reports. This is an added benefit of using a CESS: threat reports sent to Microsoft via Outlook are captured by the CESS and used to enhance the filter's intelligence. With a SEG, an MSP must manually investigate and respond to user reports.

Challenges to creating new managed services

For many MSPs, creating more managed services equates to acquiring more tools. Unfortunately, having more tools does not necessarily equate to more revenue or better security. In fact, adding more tools can increase costs and reduce efficiency for MSPs, especially if the tools are complex and require in-house expertise.

Consolidation

To create revenue-generating managed services, MSPs must consolidate their security stacks in a way that allows them to do more with less. Looking at your current managed service offerings and deciding what new services you want to offer is the first step in consolidating your current stack. Find your redundancies and eliminate tools that do not significantly add to the bottom line. Below are three key points to consider when consolidating your stack:

1. **Vendors –** Reducing the amount of vendors you work with will help you save money and create efficiencies. Work with a select group of vendors that can offer multiple products and solutions to help you deliver your managed services as well as the training and support you need to build a lucrative partnership. Fewer vendors equals less complexity, more discounts, and stronger relationships.

2. **Day-to-day management –** Screen switching eats up a considerable portion of an MSP's day and only gets worse as more tools are added. Search for all-in-one security tools that will help you do more for your Microsoft 365 clients with less, including tools that offer cross-tenant Microsoft 365 client management. If you offer or plan to offer SOC-as-a-service, your security stack should plug easily into your SIEM (security, information, and event management) and help cut back on screen switching.

3. **Maintenance –** Security tools that are overly complex and require specialized security staff are productivity killers. MSPs need tools that can be quickly deployed, are easy to use and manage, and don't require hiring and retaining specialized staff. The less complexity that is built in, the less time it will take to get up and running with new clients.

> "To create revenue-generating managed services, MSPs must consolidate their security stacks in a way that allows them to do more with less.

About Vade

Vade helps MSPs and ISPs protect their users from advanced cyberthreats, such as phishing, spear phishing, malware, and ransomware. The company's predictive email defense solutions leverage artificial intelligence, fed by data from 1 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.

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

Follow us

@vadesecure

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