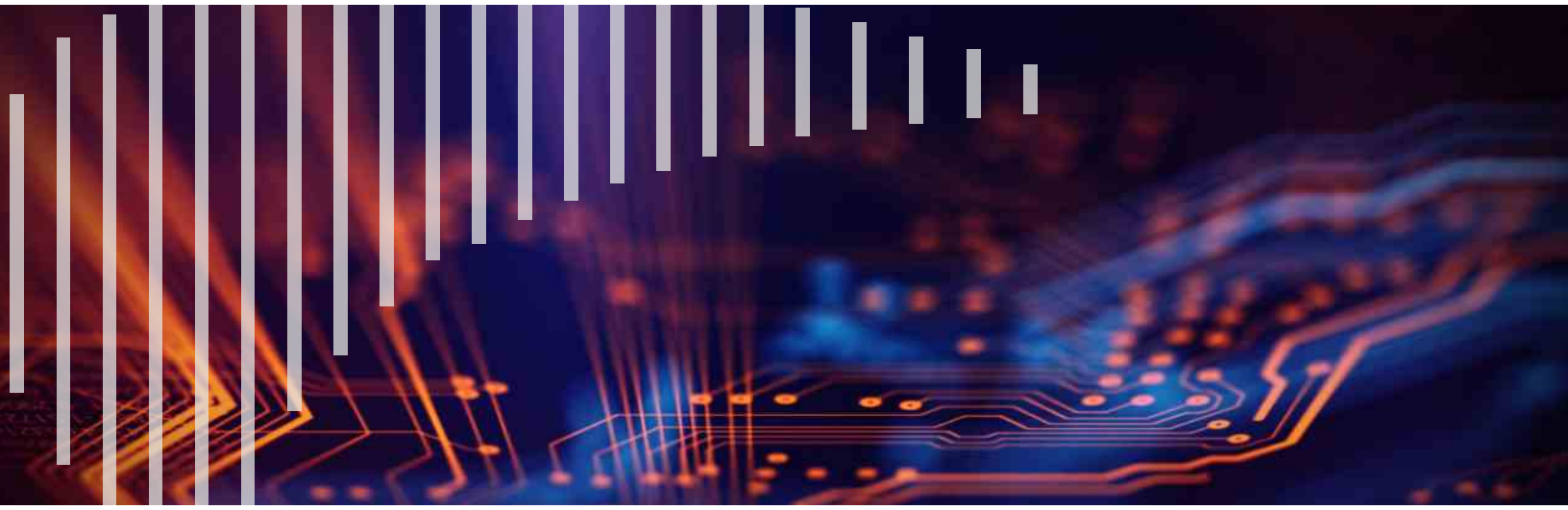
SONICWALL



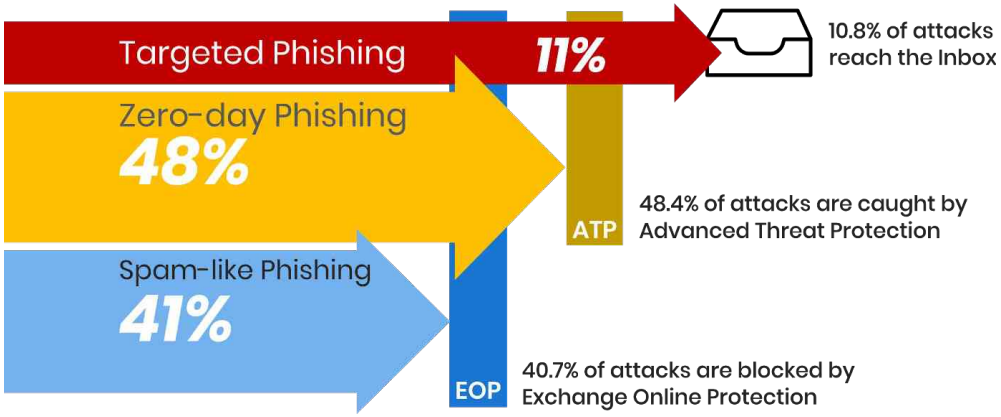
The 2020 Microsoft ATP Report

The definitive evaluation of Advanced Threat Protection (ATP) effectiveness against phishing threats to Office 365.

Executive Summary

How effective is Microsoft Advanced Threat Protection against attacks that bypass the default Exchange Online Protection?

In the most thorough analysis of its kind, security analysts classified over 500,000 malicious emails sent to real end-user mailboxes protected by Microsoft's Advanced Threat Protection (ATP). This research identified the types of attacks that were blocked by ATP or EOP, and the types of attacks that were missed by both.



Overall results:

When looking over all malicious email, the analysis concluded:

- EOP catches widespread, previously known methods — about **41%** of all attacks.
- ATP catches many zero-day attacks that bypass EOP — **48%** of malicious email.
- **11%** of malicious email reaches the inbox, bypassing both EOP and ATP.

When measuring ATP as an independent layer of security, it misses 18% of the malicious email that bypasses EOP. In some environments, the miss rate can be much higher.

Introduction

Advanced Threat Protection (ATP) is marketed by Microsoft as an improvement on the built-in Exchange Online Protection (EOP) that defends against spam and known email threats. Microsoft ATP offers an improvement against unknown threats, but the end-user experience has not matched the ATP promise.

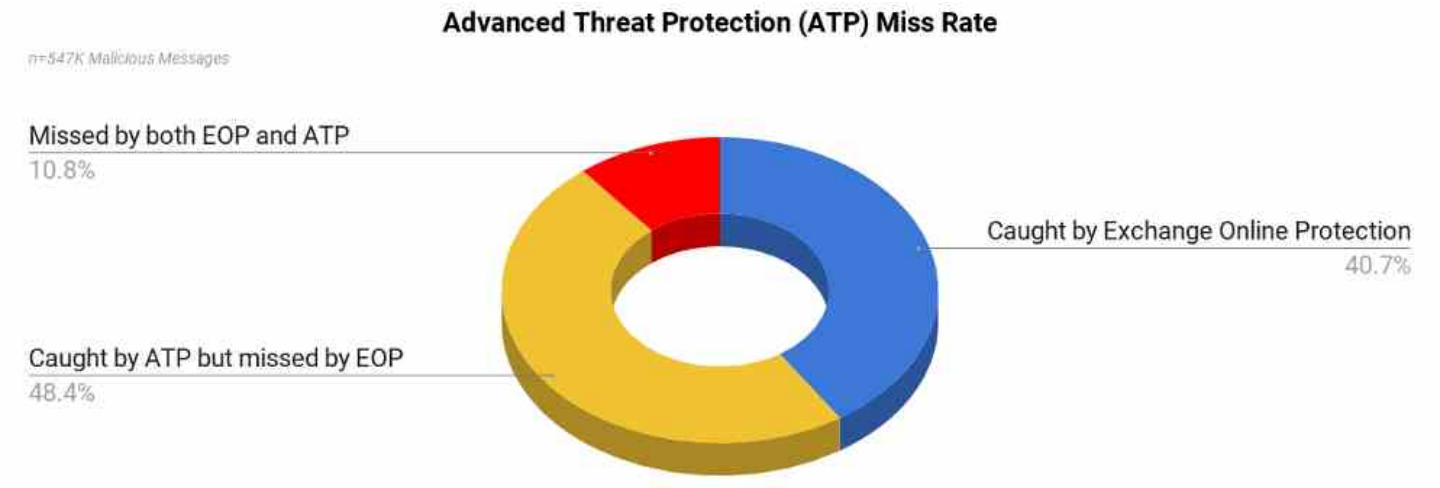
> "We are a financial institution under constant email attacks. We tried Microsoft ATP, and it reduced the number of attacks getting through from 1,000-2,000 per week to 500-800. Still way too many attacks for our company to feel secure." https://www.gartner.com/reviews/review/view/1014969 (CTO, Finance Organization)

To determine the real-world effectiveness of ATP, this research analyzed over 500,000 phishing messages during a two-week period at organizations deploying Microsoft Advanced Threat Protection. The dataset includes information about each email before and after Office 365 EOP and ATP filters, as well as before and after each message reached user inboxes. See *Appendix 1: How We Measure ATP Miss Rate* below for more details on the methodology.

EOP | ATP Effectiveness

Approximately **41%** of malicious email was caught by the built-in EOP, which performed best when blocking well-known, spam-like attacks previously seen across multiple organizations. Microsoft ATP was able to block an additional **48%** of malicious email beyond those caught by EOP.

More than one in 10 **(10.8%)** attacks were missed by both EOP and Microsoft ATP for a variety of reasons. Most (8.7%) were able to bypass due to the use of specific attack methodologies that were designed specifically for ATP. The remaining 2.1% were able tow bypass ATP by taking advantage of a variety of common ATP misconfigurations and whitelists.



This chart represents the results over all organizations sampled for this analysis. The miss rate varied greatly between organizations and between types of attack.

Attack Analysis by Organization

The graph above describes the aggregate results over all accounts, hiding the "bursty" behavior of the typical phishing attack. To better understand the end-user experience and analyze the targeted campaigns, this section looks at individual organizations over a typical seven-day period.

The figure below shows the daily miss rate Office 365 suffered within each organization over the course of a week. Each value represents the daily miss rate: the percentage of malicious emails that bypassed both EOP and ATP on a given day.

EOP|ATP Miss Rate Each Day for a Given Organization

	Type	Users	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	7-Day Miss Rate
ORG-01	MUNI	4,073	6%	20%	11%	38%	24%	24%	3%	8.9%
ORG-02	MUNI	279	36%	26%	0%	42%	9%	18%	7%	17.4%
ORG-03	MUNI	2,010	2%	4%	0%	17%	8%	1%	9%	3.5%
ORG-04	MUNI	1,006	10%	25%	25%	7%	6%	6%	10%	8.2%
ORG-05	UNIV	17,768	2%	0%	3%	1%	4%	2%	0%	1.1%
ORG-06	RSCH	17,104	0%	0%	0%	0%	0%	0%	0%	0.1%
ORG-07	MKTG	1,139	11%	0%	0%	0%	0%	0%	1%	0.3%
ORG-08	ENGR	14,462	34%	3%	3%	0%	5%	4%	9%	4.0%
ORG-09	UNIV	4,073	6%	1%	4%	1%	1%	2%	3%	1.5%
ORG-10	AERO	10,048	18%	8%	12%	31%	41%	11%	13%	14.7%
ORG-11	MNFG	22,145	17%	14%	15%	3%	16%	4%	2%	7.4%
ORG-12	FINC	6,934	0%	16%	9%	8%	13%	1%	0%	4.1%
ORG-13	HLTH	6,594	6%	4%	1%	6%	5%	8%	3%	3.0%
ORG-14	MUNI	8,778	1%	2%	0%	2%	8%	5%	0%	1.6%
ORG-15	K-12	3,669	4%	4%	3%	1%	2%	2%	5%	4.5%
ORG-16	MUNI	29,776	13%	6%	1%	9%	11%	12%	1%	4.3%
ORG-17	ENGR	5,629	0%	3%	17%	46%	6%	0%	1%	16.6%
ORG-18	UNIV	22,177	3%	2%	15%	7%	6%	2%	6%	3.0%
ORG-19	UNIV	53,124	11%	3%	5%	2%	3%	1%	1%	2.6%
ORG-20	TRNS	7,431	10%	16%	12%	8%	17%	29%	7%	3.3%
ORG-21	UNIV	3,669	0%	0%	2%	2%	1%	2%	1%	1.4%
ORG-22	FINC	5,068	31%	7%	4%	13%	16%	10%	4%	5.3%
ORG-23	MNFG	755	8%	17%	15%	11%	10%	23%	5%	13.2%

EOP/ATP miss rates during a 7-day period within each organization

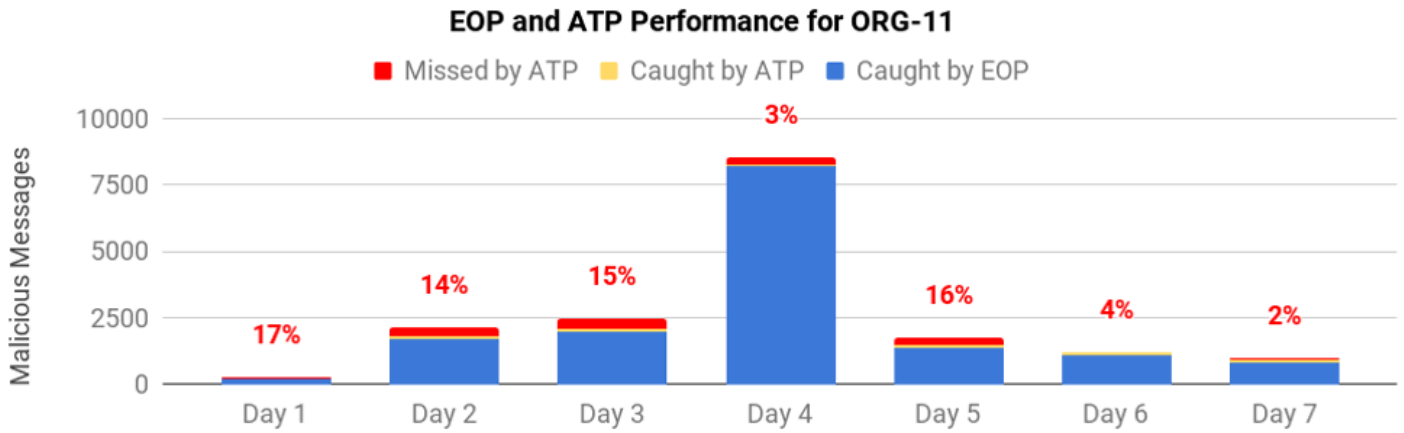
For a couple of organizations (ORG-06 and ORG-21), this was a quiet week with very few targeted attacks that bypassed ATP. To clarify, they received thousands of phishing emails, but they were of the type easily blocked by EOP and ATP, thus the miss rate for each day was near zero.

In contrast, many other organizations were subjected to targeted phishing attacks that bypassed Microsoft's filters. ORG-10, for example, never had a quiet moment, with miss rates above 10% on most days, reaching 41% during one day's worth of attacks.

These results confirm the experience of most ATP users. On a typical day, a small, even manageable, percentage of malicious email will reach user inboxes. Occasionally, however, an overwhelming burst of activity from a targeted attack will be seemingly invisible to Office 365 filters.

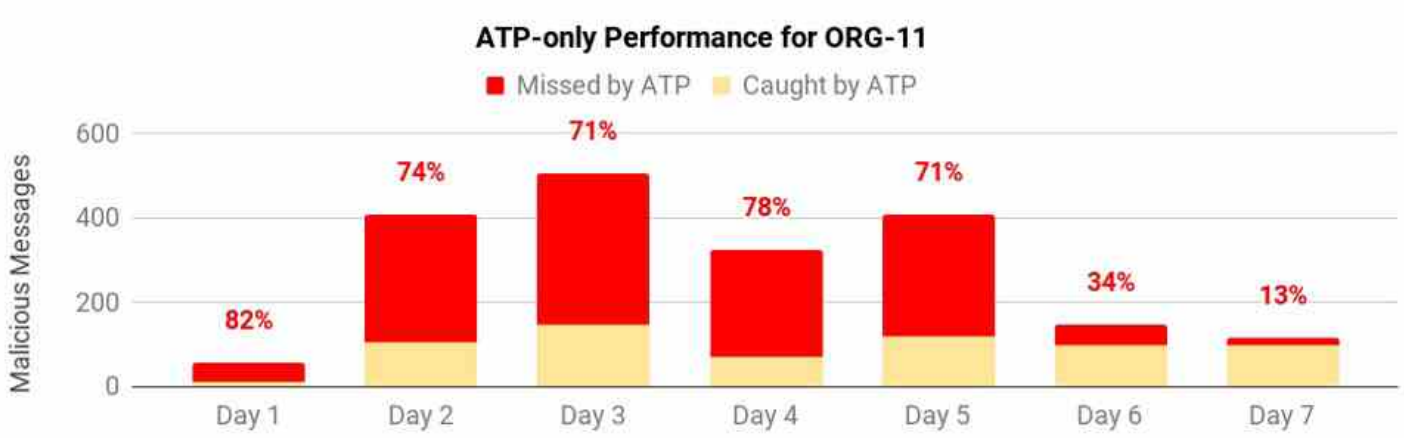
Office 365 is Susceptible to Targeted Attacks

How ATP and EOP perform can be better seen when drilling down into a single organization. This chart shows the same week for ORG-11 with the total number of attacks per day and how they were handled by the two layers of Office 365 filters.



Most of the phishing attacks during this week were blocked by EOP, suggesting they were of the type that are widespread and previously known.

During this week, ORG-11 was subjected to multiple types of attacks. Most were the type of high-volume, widespread, spam-like attacks that are easily blocked by the default EOP filters (blue). Because the goal of this research is to understand the added value of deploying ATP and the effectiveness of ATP for targeted attacks, it is helpful to eliminate the volume and noise of the attacks that were blocked by EOP.



Eliminating the attacks blocked by EOP makes it easier to see the miss rate for ATP.

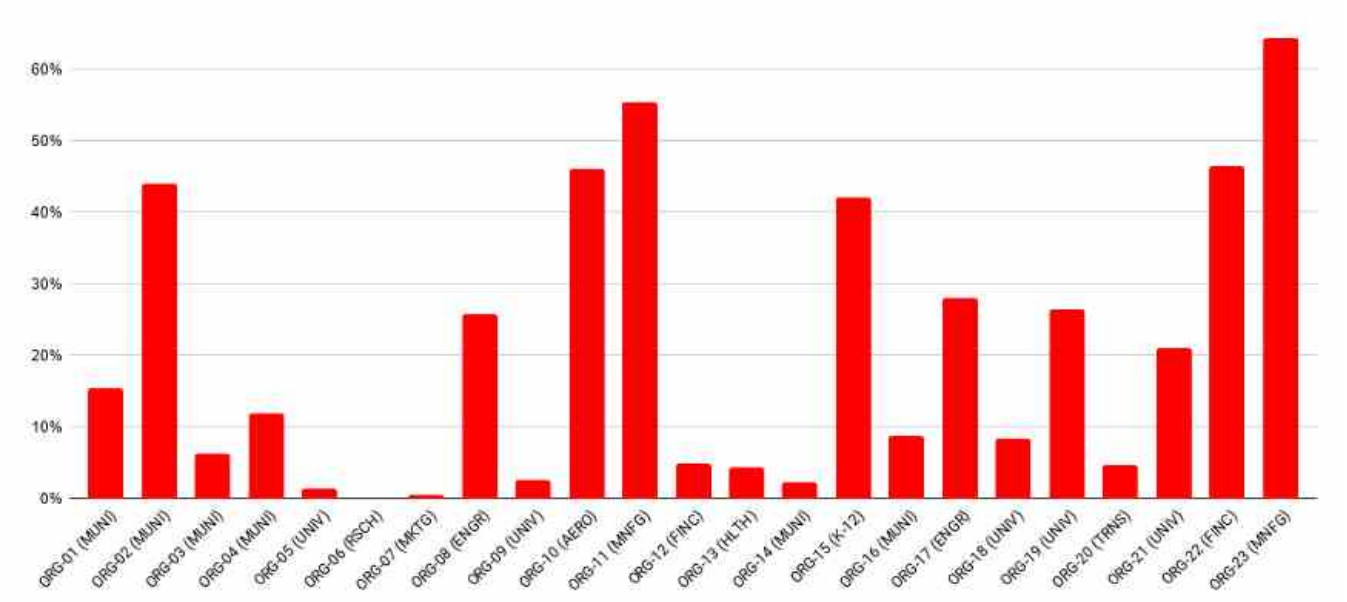
This is a much more usable way to represent the additional benefit of ATP over the default EOP. On Day 4, a large volume of spam-like phishing hit the organization, skewing results in the previous graph. While the combined miss rate for both EOP and ATP was 3% on Day 4, most of the filtering was done by EOP. The miss rate for ATP on that day was over 78% of the malicious messages that bypassed EOP.

Most organizations deploy ATP as additional protection beyond the default EOP, so it is reasonable to only look at the zero-day events that EOP cannot block. Eliminating these and measuring over the remaining volume of malicious email, the ATP miss rate is much greater, climbing to very high levels when a targeted phishing campaign is in play.

Microsoft ATP Miss Rates Across Each Organization

Looking again at the miss rates for each organization and excluding those attacks that were caught by EOP provides a better measure for ATP effectiveness.

ATP Miss Rates When Excluding Attacks Caught by EOP



ATP miss rates surpassed 50% when measuring over the attacks blocked by EOP.

In the graph above, the miss rate varied greatly, demonstrating that the ATP results in aggregate may not match the experience of an individual organization.

Hacker Behavior and Growth in Targeted Office 365 Attacks

Office 365 is the Most Targeted Email Application

The annual Verizon Data Breach Report has consistently reported that 90% of breaches start with an email and "60% of the time, the compromised web application vector was the front-end to cloud-based email servers." Hackers are redirecting their attacks to services like Office 365 and G Suite, the two most popular services for both personal and business email. In the another recent report, security researchers saw twice as many phishing attacks on Office 365 (1.04% of all email messages) as compared to Google G Suite (0.5%).

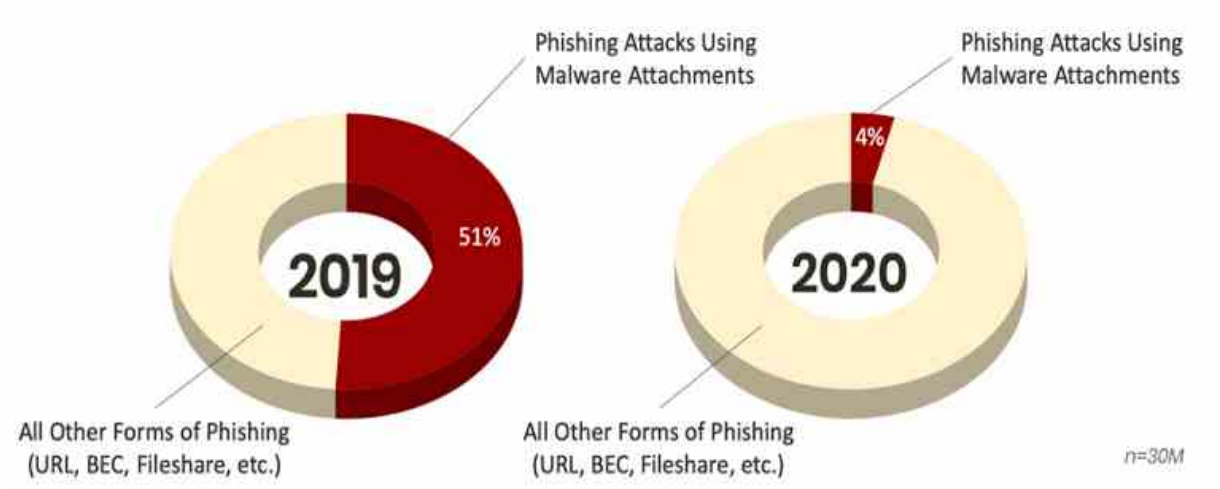
Account Harvesting is the Primary Objective

The second trend specific to Office 365 is the lateral movement of modern attacks. When hackers manage to compromise a single Office 365 account, they will use it to identify and target users both in the same organization and among trusted partners. In 2019, the most successful account harvesting methodology used emails from one user's inbox to create malicious "in-thread" attacks that looked like a reply to a previous conversation.

If the initial attack is able to bypass Office 365 defenses, the odds of subsequent compromise is high. Account-harvesting methods are designed to be stealthy and do not capture the headlines of data-destruction or data-ransom campaigns, but they're often the silent predecessor of such attacks.

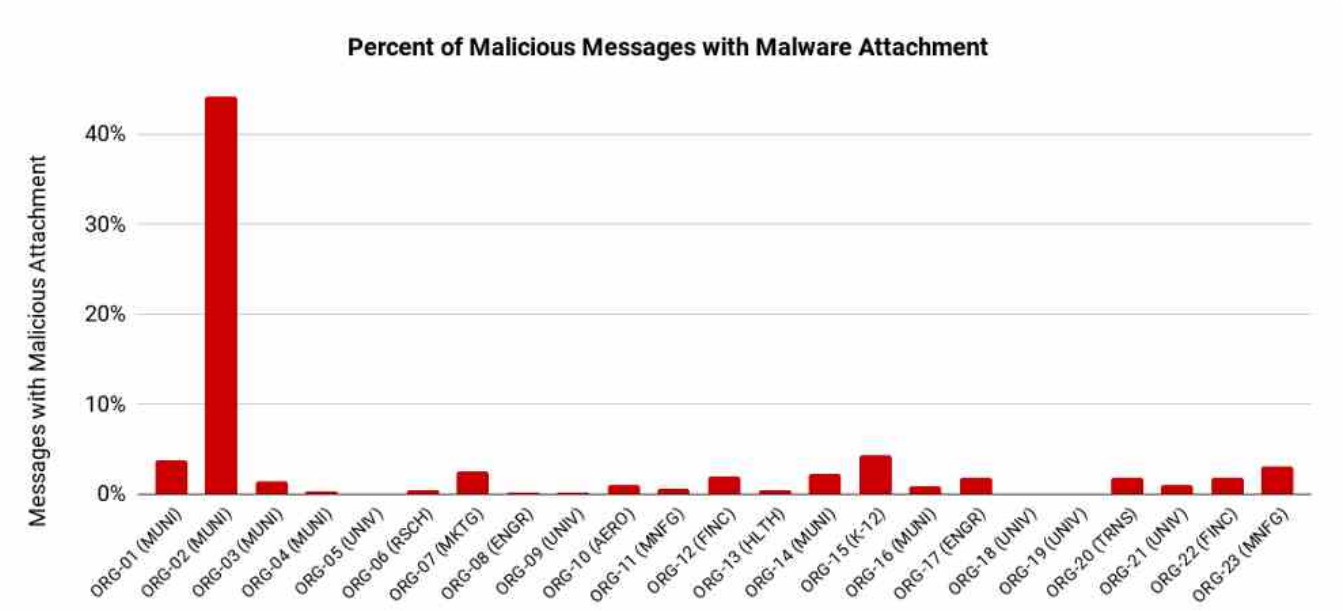
URL Phishing Has Replaced Malware Attachments

The third major trend is the usage of URL phishing over malware. The percentage of malware attachments as a portion of malicious email has dropped from over half in early 2019 to less than 4% in early 2020.



Malware attachments have dropped dramatically in favor of links to a hosted file.

When seen in the wild, malware attachments are most often part of a highly targeted campaign against a selected set of targets that are likely to be susceptible to the strain. For example, municipal organizations using weaker file-scanning tools and older versions of desktop software are likely targets for malicious attachments that would otherwise be ineffective against newer versions of Windows.



Typically, less than 4% of malicious email contains a malware attachment — unless an organization is under a targeted campaign, like this municipal organization.

SONICWALL

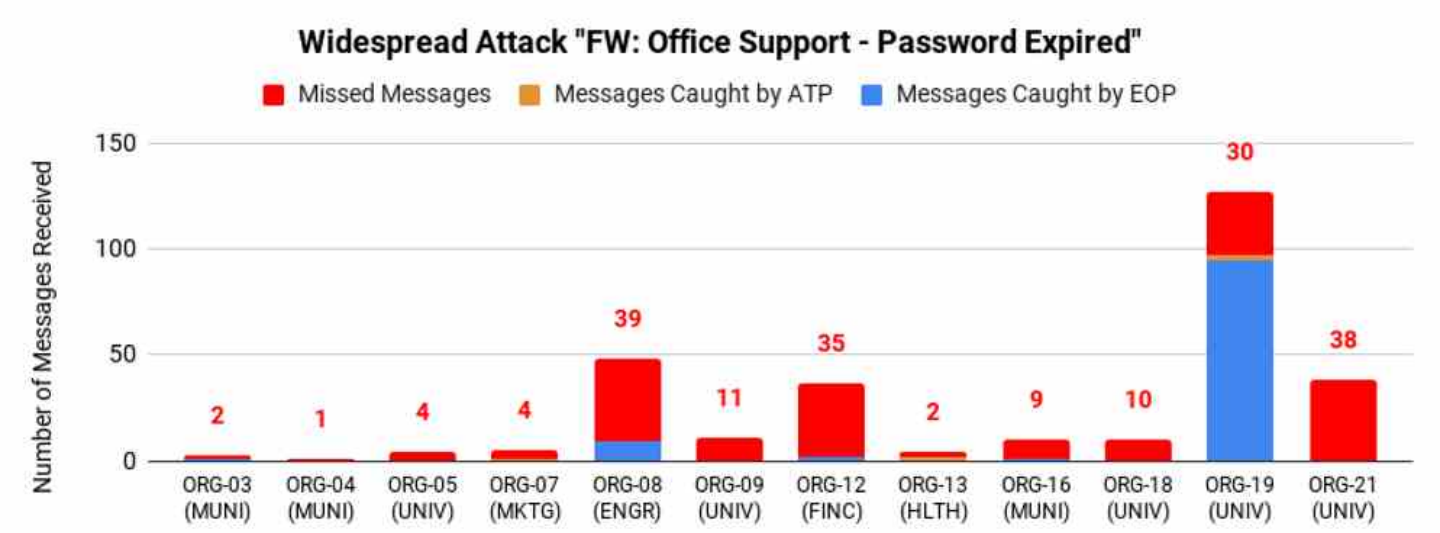
Some of the malware attachments seen during the testing period included weaponized .doc and .pdf files that are able to bypass Microsoft ATP sandboxing. These malware samples were not seen within organizations that were using other mail services, and when tested against Gmail and other email gateways they were quickly blocked, suggesting they were designed for, and tested against, ATP.

Examples of Microsoft-targeted Attacks

It is easy for an attacker to identify Office 365 accounts through a simple DNS lookup. Attackers that use EOP- or ATP-specific attacks will not send them to other mail services. For the sake of this research, any widespread attack that is seen across a large number of organizations — but only those utilizing Office 365 — is considered an Office 365-targeted attack. Most attacks were seen across multiple organizations during the test period, but occasionally a campaign would specifically target a certain organization.

Example: Widespread Harvesting Attack Targeting Multiple Organizations

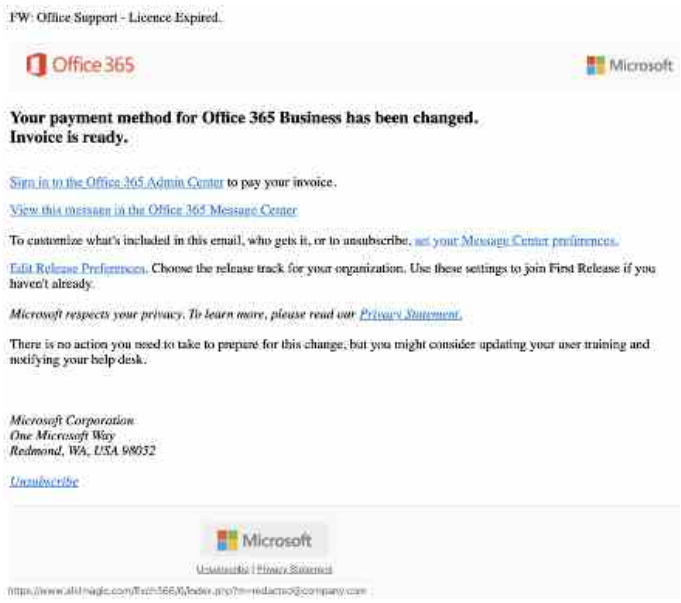
Even though many of the attacks that bypassed ATP targeted only Office 365 users, they were otherwise indiscriminate. For example, one widespread password-harvesting attack has been notoriously persistent and continues to bypass ATP. Every organization was targeted by this attack at some point or another, and during the two-week period it was seen by a dozen of the sampled companies.

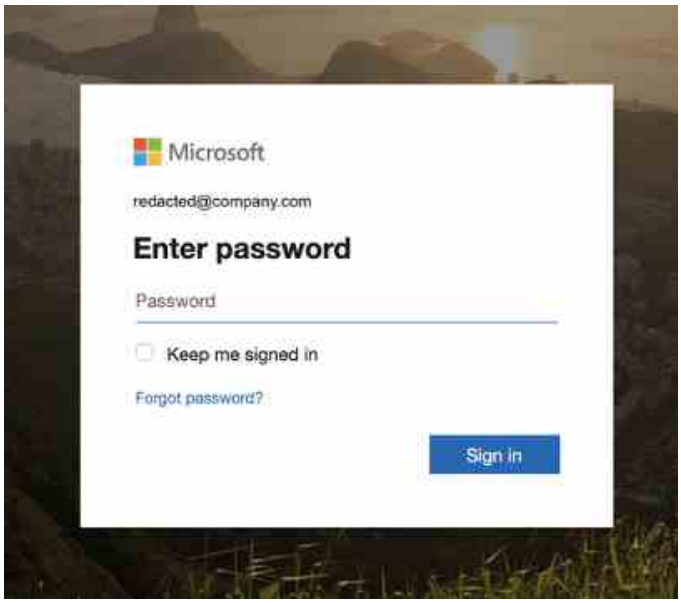


This particular attack was seen across 12 organizations during the sample period. It is difficult to see, but ATP caught only 5.

As shown in this chart, Microsoft was only able to block a small percentage of attacks. In the cases where Office 365 was able to block the malicious messages, the majority were detected by EOP.

This particular attack is sent from thousands of compromised Office 365 email accounts with the format "Exchange-BnHYMQd0iaUL@compromisedaccount.com." They appear to be legitimate messages from Office 365, and each of the links in the email point to one of hundreds of otherwise-benign WordPress accounts hosting a password-harvesting page. Because each URL embeds the target email address, it takes the user to the *second step* of the Office 365 login, asking only for the password. The "Sign In" button takes the user to their own account page, making them oblivious to the fact that they have just entered their password into a fake site.





Example of a widespread attack that continues to bypass ATP

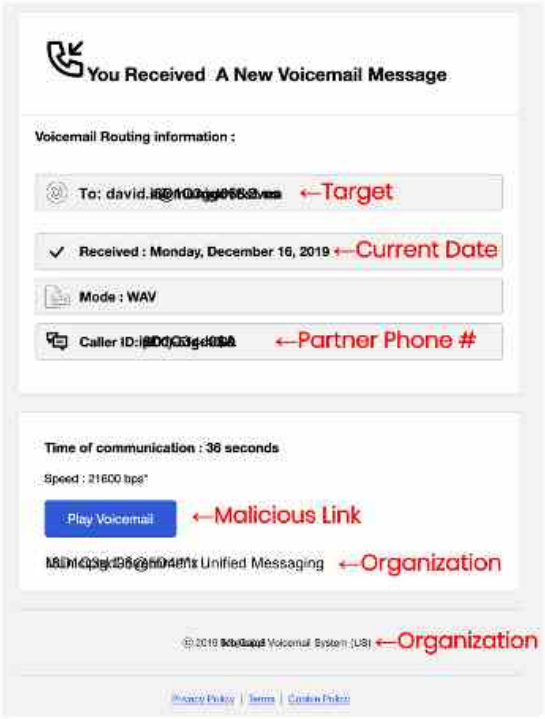
Every step of the campaign depends upon the user being an Office 365 account user. Every successful email leads to another compromised account from which to send more attacks. In one variation of this attack, a second page asked for a multi-factor authentication code, implying a live login attempt is occurring on the back end.

Example: Narrow Attack Targeting Specific Organizations

Certain types of organizations are subject to more advanced, highly targeted attacks. For example, during the sample period, a single attack targeted two separate organizations: a high-profile financial firm and a large U.S. municipality.

These attacks utilized organization-specific information that would be relevant for specific users inside the organization. In the example here, a fake voicemail message included the phone number of a partner organization. The user-facing message differed in each email and between different attempts to the same user. But all email in the attack utilized the same Microsoft ATP vulnerability and the attack persisted for several days, sending a relatively small number of samples each day to the same targets.

Some high-profile organizations were subject to multiple attacks — some lasting minutes, others spread over multiple days. All utilized a variety of ATP-specific vulnerabilities from a large number of sources. In some cases, the attacks came from specially crafted domains that would resonate with the recipient.



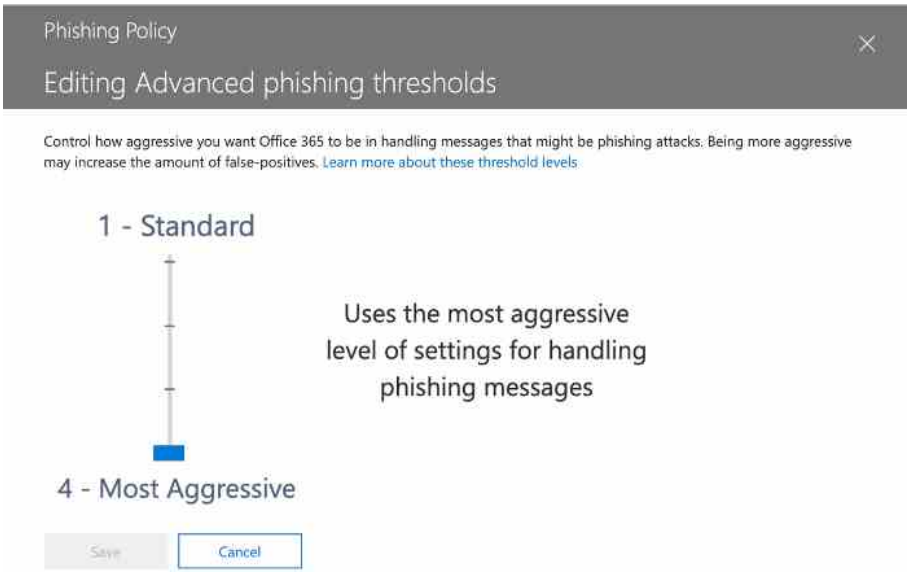
SONICWALL

ATP Configuration Challenges and Whitelist Vulnerabilities

ATP Configuration Choices and End-User Whitelists

A portion of malicious email (1.2%) was able to reach user inboxes due to overzealous or poorly maintained whitelists. Attackers have learned to take advantage of this large and easily exploitable vulnerability.

The root cause of the problem lay in the challenge of configuring ATP sensitivity.



Increasing Microsoft's Phishing Aggressiveness leads to false positives.

The trade-off of making ATP more aggressive is an increase in false positives. The organizations in this analysis were evenly split between the "2 - Aggressive" or "3 - More Aggressive" policy settings, as the "4 - Most Aggressive" setting provided little additional protection but resulted in too many false positives.

When an increase in sensitivity results in blocking legitimate messages, users and administrators pull messages from quarantine and add senders to the whitelist. In those organizations that had increased ATP sensitivity, there was a greater tendency to have longer and more permissive whitelists.

Ultimately, the whitelists became a vulnerability. In limited cases, they included branded services like Amazon or even Microsoft. Most often, though, the whitelists included partner domains that have been a source of sophisticated attacks in the last year. Emotet and other malware methods will download an inbox worth of messages and reply with malicious files from a spoofed version of the sender's domain, which would normally be caught by EOP. The attackers are counting on these addresses to be in a whitelist or pulled out of junk folders.

Selective Use of ATP (High Volume Targets vs. High Zero-Day Attack Targets)

Many organizations only apply ATP to a select group of users, leaving many accounts unprotected. This is often done to save money. A large number of attacks had to be excluded from this analysis because the recipient account did not have ATP enabled. (In one case, it had been licensed and paid for, but not turned on!)

Unfortunately, many of the assumptions made when selecting which users to protect are wrong. A naive selection might just use the volume of email an individual receives. Or it will select 'high-value' executives and finance employees but exclude human resources or operations. Many simply base the decision upon whether a user needs the Office E5 Suite of applications (which includes ATP) or the simpler Office E3 set of tools (which does not).

Ideally, everyone in the organization is protected — but if decisions are to be made, it is important to include users that have been the targets of zero-day attacks, no matter the volume.

For example, in one organization these users experienced completely different types of attacks. In this organization, the largest number of malicious messages went to a C-level user and a finance user, but most of them were common phishing attacks easily blocked by EOP. The most serious zero-day attacks targeted a sales user and a contractor.

	Number of Malicious Messages	Zero-Day Attacks (Able to bypass EOP)	Zero-Day Ratio
C-Level User	72	2	3%
Executive User	27	3	11%
Mid Manager	14	7	50%
Finance User	119	14	12%
Marketing User	74	15	20%
Sales User	52	45	87%
Contractor	16	16	100%

While some users receive more phishing emails, others receive a higher percentage of zero-day attacks. (See Appendix 3: "Am I a Target?" and the Zero-Day Ratio)

Microsoft 'Whitelists'

An administrator cannot control how Microsoft rates its own services, but this is an inherent factor when using Microsoft email filters. Messages sent from Microsoft applications (e.g., an invitation to share a file or web document) or a link to a file hosted within Microsoft services (e.g., OneDrive or SharePoint) seem to reach the inbox with less scrutiny. For example, a recent attack utilized Microsoft Sway to host a malicious link.

Conclusions

Microsoft is a victim of its own success. As more organizations move to Office 365, attackers have followed. The EOP/ATP monoculture has made it increasingly likely that malicious researchers will seek out, discover and exploit vulnerabilities in their security layers. The Office 365-targeted phishing economy has led to a number of changes in the email hacking industry:

- Attack methods are specifically designed and tested to bypass EOP and ATP.
- More than half the malicious messages that target Office 365 are able to bypass the default Exchange Online Protection (EOP), necessitating additional security.
- Attackers assume the additional security is Advanced Threat Protection (ATP).

Anti-phishing technology is not a static science: Microsoft continues to adapt to new methods and attackers continue to respond to new defenses. As such, ATP miss rates are a snapshot of the current state of this arms race. During the two-week period of this analysis, the attackers sent over 500,000 malicious messages to these 23 organizations.

- **EOP caught only 40.7% of attacks**
- **ATP was only able to catch an additional 48.5%**
- **10.8% of attacks were able to bypass both layers of Office 365 protection**

The miss rate for individual organizations varied widely and the results above would most likely change depending upon the organization and the choice of sample dates. Even organizations with near-zero miss rates during this analysis period are subjected to targeted attacks a few times a month.

In every arms race, both the attacker and defender must invest time, research and money to stay ahead. As Microsoft adds millions of new users every month, its value as a target will grow just as quickly.

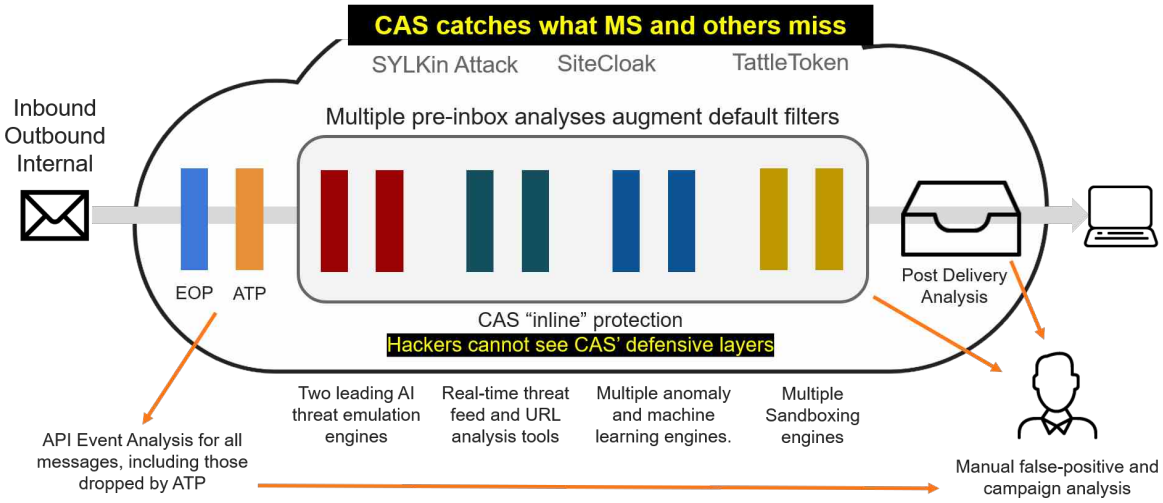
Recommendations

While this research focused solely on organizations deploying Microsoft Advanced Threat Protection (ATP), the data analysis leads to a number of important recommendations, no matter the security solution.

- **Deploy additional security beyond Office 365 Exchange Online Protection.**
  It is very clear from the data that more than half of malicious email is able to bypass EOP. While the volume of zero-day attacks might differ from organization to organization, all are going to be subject to methods that bypass EOP.
- **Deploy a technology that includes post-delivery protection.**
  A common method to bypass ATP is to host a page on a benign website that only becomes malicious after the email campaign. To mitigate this risk, look at security solutions that also provide post-delivery capabilities such as link rewrites, email retraction, user feedback and account compromise protection. Both pre-delivery and post-delivery should be a requirement for your solution of choice.
- **Prefer a third-party email security vendor.**
  As attackers focus their efforts on the ever-increasing population of Office 365 users, they are developing tactics specifically for both EOP and ATP. Highly targeted organizations are more than likely to be attacked using ATP-specific methodologies, and non-Microsoft technology is less likely to be subject to the same vulnerabilities.
- **Be vigilant with whitelists.**
  As false positives increase, the impulse to whitelist senders can leave the organization vulnerable. Sender hygiene (SPF/DKIM/DMARC maintenance) can reduce false positives without the need for whitelisting. Do not exclude users from email filters: spam-like phishing will continue to attack the CEO, but targeted campaigns are looking for less-likely candidates.
- **Do not assume you are not a target.**
  While the types of organizations used for this analysis ranged from the highly targeted to the much-less-so, all were subjected to targeted attacks that were able to bypass Office 365 filters.

Appendix 1: How We Measure ATP Miss Rate

To measure Microsoft Advanced Threat Protection's (ATP) phish-blocking capabilities, researchers analyzed over 500,000 malicious messages received by organizations that had enabled ATP.



The SonicWall solution is uniquely positioned for this type of analysis. Because it is deployed after existing security filters, but *before* the inbox, SonicWall has access to every email that bypasses Microsoft EOP and ATP. SonicWall employs multiple proprietary and third-party technologies to scan for phishing and malware:

- Two leading sandbox emulation engines to test email attachments
- Multiple threat feeds and URL analysis tools from a variety of vendors
- Natural language, anomaly detection and other anti-phishing algorithms
- Machine-learning engines trained for individual organizational dynamics
- End-user reporting of missed phishing messages.

SonicWall leverages its API access to the full Office 365 Suite in order to capture the EOP and ATP verdict in multiple ways:

- Email headers added by EOP and ATP after files have scanned but before they are put into quarantine, junk or user inboxes
- The ATP and EOP event logs to capture files that might have been deleted by ATP
- Post-delivery events from SafeLinks and ZAP determinations made after delivery

Analysts excluded customer sites deploying external Secure Email Gateway (SEG) or similar MTA-based proxy because previous tests found that a third-party gateway actually reduced EOP and ATP effectiveness, skewing results.

No Inboxes Were Harmed in this Analysis

All results are presented as they were categorized by ATP. In practice, all malicious messages were quarantined by SonicWall before they reached the inbox. The results describe how each message would have been handled without SonicWall deployed. Because all the SonicWall filters are deployed after EOP and ATP, but before the inbox, they have no effect on the Microsoft analysis. Because SonicWall utilizes the Microsoft infrastructure for quarantine and user interaction, EOP and ATP continue to benefit from end-user feedback.

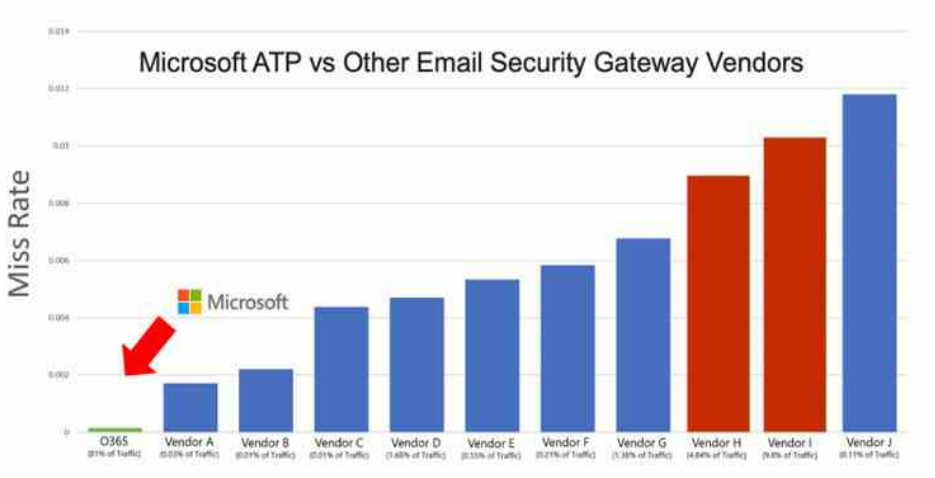
Appendix 2: Microsoft ATP vs. Leading Email Security Gateways

Most organizations using Office 365 are already aware of the need for additional email security beyond default Exchange Online Protection. But in Microsoft's attempts to convince users that ATP is the best alternative, they have shared some data about the miss rates of other vendors.

Microsoft Effectiveness Claim

At their most recent Ignite Conference (November 2019), Microsoft made the claim that ATP offered the lowest miss rate when compared to the leading email gateway products.

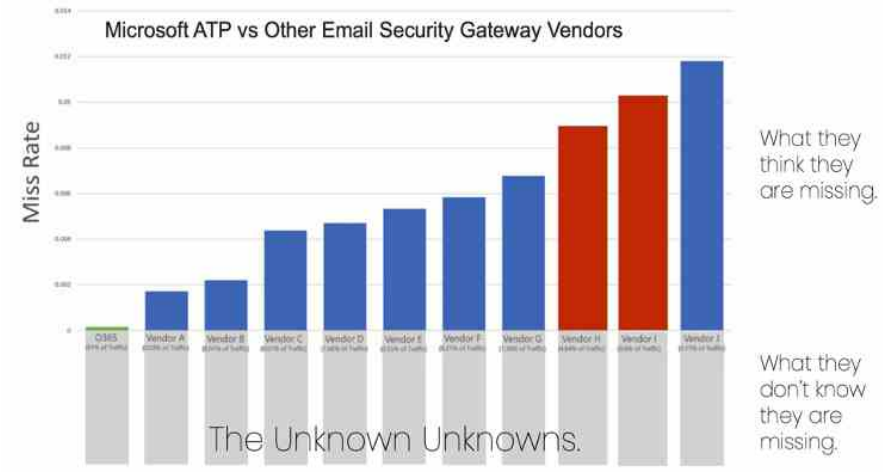
This is an impressive chart that seems to show that Microsoft ATP is orders of magnitude better than every brand of Secure Email Gateway (SEG), including the two market leaders (shown in red). When the chart was presented, Microsoft's claim produced vocal objection from users of Office 365 in the audience, as it did not meet their daily experience.



A Measurement Challenge

While Microsoft methodology was sound when measuring the attacks missed by their email gateway competitors, it was flawed in its measurement of its own effectiveness.

Because any email that was let through by Microsoft security would, by definition, not be considered malicious, they had to rely on end-users reports of phishing to know what they missed. But there's no guarantee or estimation of what percentage of attacks that reach the inbox would be understood by end users as an attack, and what percentage of users actually bother to report those as phishing. The correct method to measure missed attacks would have been to include one or more third-party tools after their own layer, in addition to some manual analysis by security experts. The research in this document hopes to fill that gap.



SONICWALL

Appendix 3: "Am I a Target?" and the Zero-Day Ratio

A question that often arises when determining whether to devote more resources to email security is whether an organization is being subjected to targeted attacks. In the last year, many organizations — especially local governments — were caught off guard when they became victim of sophisticated, organized campaigns. While the answer might be obvious to a name-brand bank, others might wonder if they can continue to fly under the radar.

The Zero-Day Attack Ratio

Every organization studied was subjected to multiple campaigns at some point during the sample period, but a very clear trend emerged from the data differentiating highly targeted organizations from those subject to only widespread, spam-like attacks. The difference was not in the volume of malicious email, but the ratio of zero-day attack methods.

Because EOP, the default Office 365 protection, is effective against previously known attacks but misses more advanced, zero-day methods, a rough but meaningful differentiator between different organizations arose in the ratio between those attacks that were caught by EOP and those that bypassed EOP.

Two organizations of similar size but with very different Zero-Day Attack Ratios.

For example, these two organizations of similar size (approximately 4,800 users) had completely different attack profiles. The K-12 school district had twice as many malicious email messages during the same period of time, but most were well-known methods that were easily stopped by EOP. Only 19% of malicious messages bypassed the EOP filter, giving it a Zero-Day Ratio of 19%.

The municipal government received half the number of total messages, but nine out of 10 were able to bypass the EOP filter, resulting in a Zero-Day Ratio of 90%. A naive metric based only on the volume of malicious traffic might assume the school district was more aggressively targeted, but the Zero-Day Ratio is an easy way to determine the true threat. Organizations with a high Zero-Day Ratio are being targeted by sophisticated methods that may also be able to bypass ATP. Of course, all organizations should assume that they will be a target one day.

The same analysis can be done within an organization to identify users that might be the target of more sophisticated attackers.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

MSFT-ATP Report-US-VG-2558

SONICWALL®