Office 365

Why Email is the #1 Vulnerability

vircom.com

Table of Contents

Office 365 is Powerful, but Not Worry-Free

Outages are not infrequent and have broad implications.

Spam and content filtering can be weak from within O365.

Off the shelf/standard archiving is slow and inefficient.

Office 365 is a powerful productivity solution, but can be lacking in the means it provides customers to secure their email instances. While Microsoft Advanced Threat Protection (ATP) is a powerful solution to stop threats, its application is inconsistent. Its tools like email continuity and cloud archiving are not native to the platform, meaning that 3rd party vendors will always be required.

Digging deeper into these challenges, users may find a new appreciation for what they love about Office 365. With over 1 billion users and 120 million commercial customers, the breadth and accessibility of the platform is a marvel. However, within such a large swath of users going online, there are more vulnerable targets from which cyber criminals can attempt to make recurring income.

Office 365 has

1 Billion Users

120 Million
Commercial Customers

If Threats are coming from within Office 365's infrastructure how long can your organization stay protected?

This becomes most prominent in the issue of Office 365 phishing. While phishing commonly plagues all unprotected email services, Office 365 ATP does prevent most of it from getting through to users – yet it fails to protect against phishing that originates from within Office 365 accounts.

Threats are fundamentally evolving, and time-of-click URL scanning and attachment scanning beyond signatures are required to protect against modern threats. Hosted malware could be uploaded to a malicious link at any time after the email has passed through the email gateway, and attachments could contain no malicious software but instead function as forged invoices in Business Email Compromise (BEC) attacks. ATP protects against these things, but it does not apply where compromised Office 365 accounts are concerned.

Thirty-five percent of Office 365 businesses are already using third party security, primarily because phishing messages delivered through compromised accounts have so ruthlessly prevailed within this environment. Likely due to architectural constraints, most Office 365 phishing messages delivered through compromised O365 accounts reach users without any filter stopping them. This allows for the compromise of more accounts and the sending of more messages, leaving any O365 user vulnerable to malicious links, URLs and targeted phishing, BEC and more.

When combined with the concerns generated by frequent Office 365 outages, along with the inefficiency of its native archiving solutions, it is evident why many customers improve on 365 for their productivity and functionality with 3rd party solutions.

Where can Office 365 Improve?

Adding Continuity

Email outages and server downtime have always impacted productivity across organizations, but since 2015 frequent email outages on Office 365 have cost users and organizations hours and days of lost productivity with little contingency provided by Microsoft. For instance, in January 2016, some organizations reported issues for up to 9 days, with 5 more major outages occurring worldwide between that time and September 2017.

Even if Microsoft promises 99.9% uptime in its Service Level Agreement, Office 365 serves more than 1 Billion users worldwide and over 120 million commercial subscriptions, meaning in aggregate 0.1% of those users could go through an entire year of downtime without necessarily compromising Microsoft's overall SLA, averaging out to 8.76 hours of downtime per user per year.

While you might get reimbursed for an O365 failure in a particular month, there's no way to make up the costs to productivity that sort of outage causes. Every business on O365 needs to have a contingency plan for Email Continuity, or some sort of effective Emergency Inbox, in place to reduce the costs to both IT and organizations as a whole.

Protecting Against "In-Office" Phishing

Advanced Threats aren't driven by programmatic systems like spam campaigns of the past, but by individuals and groups dedicated to finding the craftiest possible way to scam your organization. This is a part of the spike we are seeing in socially engineered attacks. These targeted attacks mean you need better protection against "zero-day" email threats, where databases of sandboxed URL's and time-of-click protection against the latest threats prevent new tactics, malware or other threats from victimizing your users.

For Office 365 in particular, organizations are experiencing 2.7 threats per month on average, and email threats like compromised accounts take precedence and frequency above all:

1.3 compromised accounts each month (like unauthorized, third-party login using stolen credentials)

0.8 insider threats each month, like users downloading sensitive data and joining a competitor with it in hand

0.6 privileged user threats each month, with users taking advantage of excess administrator-provisioned permissions relative to their role

Your most effective form of email security also needs to include bulk email protection, highly accurate graymail classification and ATP features that make a meaningful impact on your users' inboxes. Phishing Protection, for instance, needs to work in concert with protection from malicious URLs and Attachments, but also needs to function without any default exclusion or discerning between sending domains.

These elements converge to detect email imposters who use "reply-to" spoofing and other tactics to visually deceive users into responding to email requests as if they were authentic. Effective URL protection needs to not only rewrite URLs as they pass through your email gateway, but also refer to complete databases of sandboxed URLs that understand the origins of both hosted malware and hosted non-malware attacks like credential phishing.

These evolving threats fundamentally require time-of-click scanning on URLs and attachment scanning that goes beyond signatures - regardless of where mail is hosted. For example, bad actors now commonly send waves of email pointing to compromised websites, but only upload malicious content after most of the wave has been delivered. They might also use attachment-based attacks where files are bulk created with changes so that hashes don't match and signatures are effectively masked, or other forms where only sandboxing can verify whether an attachment is malicious or not. Microsoft Advanced Threat Protection protects against both of these for Office 365, but does nothing to help with the primary challenge facing O365 customers, which is phishing from compromised Office 365 accounts. Given that there are over 120 million commercial users for O365, it is a fairly large security hole to leave unaddressed.

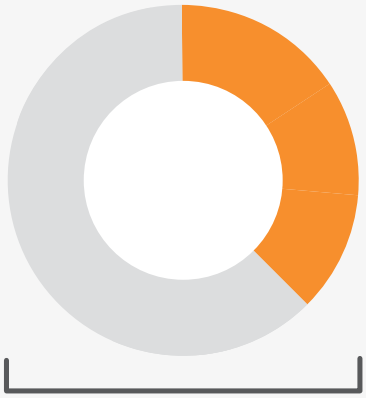
Thus, all the effort put into time-of-click URL scanning, filtering of attachments and other Office 365 ATP features are useless if threats are received from compromised O365 accounts. Whether scanning URLs, looking for malicious links or requests in seemingly benign attachments, or trying to stop credential phishing, O365 ATP's functionality is rendered null by this glaring exception.

Adding Cloud Archiving

While Office 365's comprehensive archive can collect and store data from its entire variety of apps, email is a particularly sensitive application that poses risks for your business in both regulatory compliance and legal proceedings. In-Place archiving on Office 365 makes search and eDiscovery processes slow and cumbersome, while the legal defensibility of such archiving may prove challenging.

Customizability is also important in archiving, and setting retention policies, managing users and ensuring that your off-site archive is secure and easy to search, are all features that need to be considered. Fundamentally, the faster your archiving solution works, the less time you have to devote to using it.

The Movement for 3rd Party Security with O365



35% of Office 365 organizations have already actively solicited or are using 3rd party security

–
https://www.viewpointe.com/uploadedfiles/viewpointe/pdfs/filling%20the%20gaps%20in%20office%20365%20-%20viewpointe.pdf

Research shows that 88% of Microsoft O365 user organizations view email as an application of high importance, seconded only by Exchange Online Advanced Threat Protection. It would make sense that email is the highest priority – that's what Office 365 is good at – and also that Advanced Threat Protection is the second highest priority, which is not as effective as most users require. Thus, the logical step is to not "throw the baby out with the bathwater" and keep Office 365 as a primary productivity solution while searching for better security services that truly complement its power.

So, while over 35% of organizations on O365 are already using 3rd party security, 41% of them are unsure what to do, since the one-stop-shopping benefit of Microsoft's premium plans don't leave all their bases covered.

Email is the system by which most businesses still communicate, work out their biggest deals, and stay in sync between teams. Securing this fundamental channel while also using it efficiently are twin goals of all IT departments and services providers to all businesses. Without email functioning effectively and securely, you'll find yourself "blowing in the wind" where you otherwise might be reaching the effectiveness and efficiency all Office 365 organizations aspire to.

Fundamentally, Microsoft's ATP services only work against inbound email messages and attachments, while being unable to filter outbound email, leaving organizations vulnerable to compromised accounts. There are now over 120 million Office 365 business customers, and not only are the ones relying on ATP left liable by its "one way street", but that also offers 120 million domains from which those businesses can receive unobstructed phishing, which compromises accounts and does more damage in the long term.

The growth of Office 365 only magnifies the threats and vulnerabilities created by going without 3rd party security.

The focus of Office 365 is not security. It's an amazing solution that you invest in, but you need to protect it.

–
https://www.viewpointe.com/uploadedfiles/viewpointe/pdfs/filling%20the%20gaps%20in%20office%20365%20-%20viewpointe.pdf

Reducing Total Cost of Ownership

Reducing continuity and archiving risks saves your organization time, further improving your productivity with O365.

Phishing threats not only take away IT time, but when they're successful, they also cost money.

Your users can't afford to focus on protecting themselves, and your IT departments can't afford every little thing, so you get value from going with the right solution.

Keep using Office 365, but don't put all your eggs in one basket. Each time a phishing message gets through, it can take an IT admin 10 minutes or more on average to ensure that there is no further danger to the company. In a medium-sized business, Office 365 can let through anywhere from 200-400 excess phishing messages per month, which may cost weeks of IT productivity per year if the phishing gets out of hand, or worse if it is successful at compromising a major account, system or transaction.

If you already use Microsoft's built-in Advanced Threat Protection, you can choose to take the risk of sticking with a solution that allows in-office phishing to propagate. This risk only gets larger as Office 365 continues to grow, which means there is little escape from Office 365 phishing – unless you get 3rd party protection.

modusCloud is a powerful, machine-learning driven email security gateway that fulfills the requirements you need to meet to protect against the sorts of attacks and risks discussed in this paper. With powerful filtering, Advanced Threat Protection, Email Continuity, Email Encryption and Email Archiving, you can meet all the needs your organization has in preventing and managing malicious email threats as their perpetrators work harder and harder to target your users.

At its core, modusCloud offers powerful email filtering against spam, phishing, viruses, bulk mail, gray mail, along with protection against imposter attacks, targeted phishing and malicious attachments and URLs. modusCloud's Imposter Protection, Phishing Protection, Attachment Defense and URL Defense all fulfill the key requirements that growing businesses need to protect against threats as they emerge – and further offer real protection against Office 365 phishing and other targeted email threats.

On top of filtering, modusCloud offers continuity, encryption and archiving for Office 365 that allows you to maximize the utility of your email gateway.

Email Continuity: modusCloud displays all spooled mail in the Emergency Inbox through a web-based user interface. 30-day spooling provides always-on SMTP deferral, failover & queue protection, thus allowing users to read, reply to and send new emails via the Emergency Inbox. This instantly deploys as soon as a spooling threshold is surpassed, meaning your organization can still use email even when a primary server or cloud service is down. When delivery is restored, email will automatically flow to the downstream mail server along with any replies and new emails that have been sent while delivery was unavailable.

Email Encryption: By allowing employees to send encrypted messages within and without your organizations, all made accessible through a secure hosted portal, stakeholders within your organizations can share sensitive information securely across public networks and through their mobile devices. Using this sort of technology removes your employees from the path of various malicious actors, making secure email simple as ever.

Email Archiving: Archiving in modusCloud also offer your organization an unlimited storage volume for 10 years at a fixed cost per user, featuring company-wide search, individual user search and a user-friendly web interface. Built for Microsoft Exchange, Office 365 and more, modusCloud Archiving ensures compliance and retrievability for legal, financial and other businesses while also allowing any company to fully own and understand their email data. With 55% of organizations being ordered to produce email by court and regulatory bodies, archiving can be a critical functionality that prevents both lost time and resources.

With powerful solutions that assure compliance and keep your organization running smoothly at all times, while also limiting the possibility for compromise of both accounts and sensitive information, the services you provide to your organization are no longer simply a “cost of doing business”, but play a proactive role in the function, protection and improved efficiency of all your colleagues around you.

Of course, modusCloud isn’t only geared to powerful technology, but also thoughtful people. Our support team is staffed with IT experts that are always focused on finding you solutions to problems as soon as you call. While providers like Microsoft and others have names recognized beyond the industry, they may not value individual customer relationships that every IT admin and service provider needs to get their job done efficiently.

The fact is, Vircom has been in the business of email and security for more than 20 years because of the compelling support it provides. Many customers have chosen us over other providers on the basis of our quality onboarding alone – that means that even as you get a demo or start a trial, you’ll begin to see where Vircom offers you a service advantage that other vendors simply can’t match.

Learn More About Email Threats

Office 365 Email Outages: What's Your Backup Plan?

A More Effective & Efficient Email Security for Office 365

The Office 365 Spam Filter – 3 Reasons it Isn't Enough for the Modern SMB

moduscloud Your Complete Cloud Email Security

About Vircom and modusCloud

With more than 2 decades of award-winning experience, Vircom has always been at the cutting edge of developments in email and securing your business's communications. With modusCloud, Vircom now offers powerful, AI-driven filtering with Advanced Threat Protection, Email Continuity, Email Encryption and Email Archiving, along with the great customer service and partner benefits that those who know us have always loved. A free 30-day trial on all offers means you're able to discover all the benefits Vircom gives you, from easy management and implementation to powerful protection and services that keep your business running smoothly, no matter the threats that are out there.

Contact Vircom for a technical demo

Get a live look at what attackers are doing, the heights they've scaled and how you can stop them with modusCloud.

Toll Free: 1.888.484.7266

Local: 1.514.845.1666

info@vircom.com

Vircom