IS OFFICE 365'S EOP SEAWORTHY?

THE CASE FOR TIGHTER EMAIL SECURITY

WHITEPAPER

July 2016

Vircom

www.vircom.com

EXECUTIVE SUMMARY

There is no question that Office 365 is a boon to businesses large and small as they move their apps, and in some cases, their entire 'ops', to the cloud. With O365, Microsoft has not only developed one of its strongest product offerings in decades, but provided resounding proof that it can hold its generation-long grasp on the digital office. Any doubt about that was dispelled back in 2015 when, with its big Office 365 push, Microsoft more than quadrupled its market share (from 6% to 25%)[1], leaving Google a much slower growing second.

And while the market speaks in Microsoft's favour, lingering concerns over the seaworthiness of its bundled Exchange Online Protection (EOP), continue to plague Office 365. While critical reviews and security vendor whitepapers like this one would seem to paint a one-sided picture, one needn't look further than Gartner to see the flies in the ointment as their own independent analysis shows Microsoft's flagship cloud suite failing to deliver on email security.

"Microsoft is accelerating feature improvements at an impressive pace; however, reference customer satisfaction with spam detection rates remains low, and Gartner customers continue to report Microsoft's spam detection rates lag other leaders and visionaries,"

Gartner, 2015

In an era of rampant cybercriminality and untenably high costs associated with data breaches, security that is merely "good enough" simply won't cut it. And yet, a large majority of Office 365 environment IT Managers pin their reputations as security administrators to Microsoft's "best effort" email security, Exchange Online Protection (EOP).

At the heart of the issue with EOP is an apparent disconnect with the industry and its buyers, and this manifests in three ways that cast severe doubts on EOP's status as a true business-class email security solution;

1) Performance
2) Features
3) Value

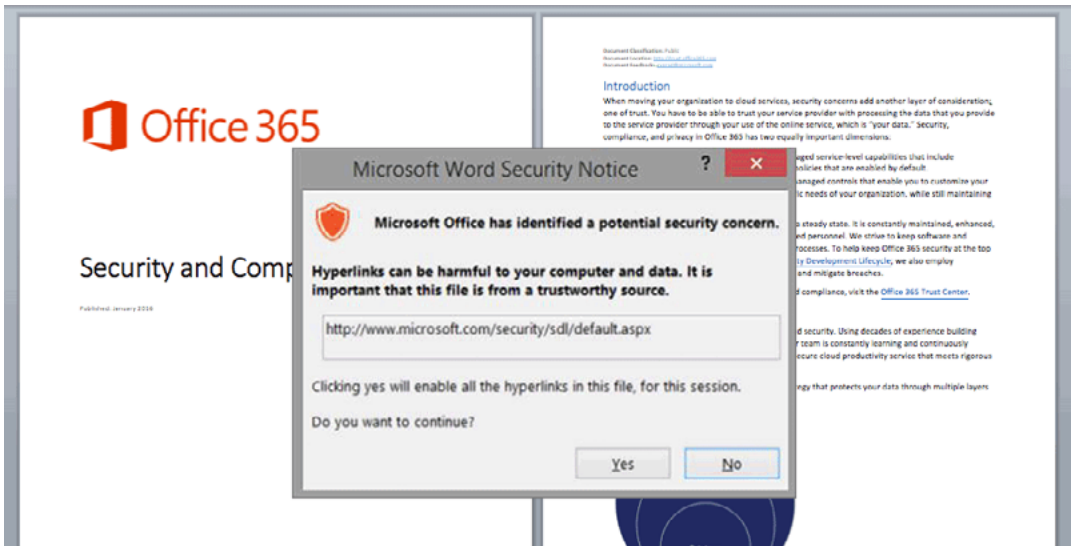
Combined, these pillars reveal the core benefit of any product, not just a security solution. But in the security space, and particularly for regulated and compliance-bound industries, failings on the first point alone, "Performance", would represent a show-stopper.

In this whitepaper, we're taking a data-driven look at Office 365's EOP suite to gauge its standalone viability verses the need for tightened security via third-party solutions.

INTRODUCTION

Critical to the job of securing any network and its data is the ability to benchmark the performance of tools put to that task. Microsoft's "go-it-alone" strategy has worked well in the world of business apps where it dominates, but in the highly competitive, data-defined world of security, any vendor worth its salt needs to go toe-to-toe with the competition to prove their value.

We start here because this represents a telling signal to buyers that the "company that brings you everything", doesn't necessarily "get it" when it comes to security. Case in point, we've included below a rather telling Microsoft Word Security Notice we got while researching the O365 security offering within an 0365 environment. While not directly related to EOP, it provides both a humorous and disconcerting perspective on Microsoft security.



Note both the source document and the 'offending' hypertext URL

Despite Microsoft's somewhat notorious failings on the security side of the ledger, today the vast majority of Office 365 environment admins settle on EOP to protect their networks. But are they getting value for their money? And is that creating a false sense of security? It's very difficult to know since Microsoft doesn't publish data on EOP's performance and doesn't submit itself to standard peer review or industry-trusted benchmark tests like Virus Bulletin and others. This has two important and related impacts. 1) It reinforces doubts about EOP's performance, 2) It leaves EOP buyers wondering if they are getting value.

For the purposes of this discussion, we will rely on Microsoft's own reported performance data and direct customer testimonials from trusted sources like Gartner to paint a picture of EOP's performance and what that may mean for companies that rely exclusively on EOP.

THERE'S NO CLOUD,

JUST SOMEONE ELSE'S COMPUTER

As every network admin knows, the cloud is simply a way to host and serve content, data and applications from a computer other than your own. But how secure is that computer? While early skeptics cited the cloud's not-so-silver-lining when it comes to security, our ascent into the cloud was inevitable given all of the advantages on both sides of the monthly subscription. From 'anywhere accessibility' to seamlessly pushed updates and as good as 99.99999% uptime, it's no wonder so many mission-critical apps, services and even entire networks have flocked to the cloud. By 2015, the cloud market for small and medium businesses (SMBs) in the US alone topped $25 billion according to ODIN 2015 SMB Cloud Insights[2]. According to a recent Forbes magazine cloud services roundup, by 2016, revenues from public cloud Infrastructure-as-a -service will reach $38B, growing to $73B by 2026[3].

Microsoft may not have been the first company to get the memo, but its well-established role of "strong follower" is playing out yet again. Since launching Office 365 in 2011, the company has tied up a tidy quarter of the cloud business app market and nearly a third of the high-growth SMB market, beating out rival Google and reestablishing its tenure as the global business app leader. By 2018, Morgan Stanley predicts Microsoft cloud products will represent 30% of revenues[3].

Drawing customers with its well-known apps, interfaces and formats, now in a more accessible, sharable, upgradable environment, business and consumer customers have plenty to cheer about with O365. Still, in a world of mounting cyber risks, has Microsoft delivered the goods on the security side of the equation? What can buyers expect from EOP when it comes to features, performance and ROI? And what are the options and considerations should you elect to bring third party solutions into the mix to strengthen your company's security?

LIMITATIONS OF O365'S EOP

PERFORMANCE ANXIETY

While we're not yet at the stage of demanding SLAs from our security vendors, we're not that far off, and in some highly-regulated industries, it has already arrived. And yet, one of the world's leading business technology companies stands on a certain side of history when it comes to providing mission-critical data on their product's performance. This issue was recently presented in an article by Vircom CEO Mike Petsalis asking the rhetorical question, "Microsoft, where's your performance data?"[4], referring to Microsoft's unwillingness to put its products to the test by third party organizations, preferring to publish their own unverifiable data. Most glaring, as Petsalis points out, is their absence from the industry's top benchmark test, the Virus Bulletin VBSpam+ report, and specifically its most critical data point, an email security solution's spam catch rate.

Microsoft's decision to opt out of peer review raises several issues not least of which, their own apparent lack of confidence in the product they sell to address the need. As Petsalis points out, Microsoft does state EOP's spam catch rate on the EOP product page at 99%. On the face of it, and assuming the figure is accurate, this rate would seem to make EOP a top performer. However, and as anyone in the email security business knows, the performance battle in the industry happens on the other side of the decimal point.

Of the 21 products tested and reviewed by the Virus Bulletin in their most recent VBSpam+ test, only 2 of the lowest performers fall under 99% and they are both provided by the same company, Spamhaus. All of the other vendors are competing for percentages well above 99.5%. So even if buyers were to take Microsoft's self-reported spam catch rate of 99% at face value, and in line with VB's stringent tests, Microsoft comes in at the very bottom of this most critical test.

But how important is the spam catch rate really? Does it really make that much difference? The answer is a resounding yes.

Applying a simple hypothetical scenario in which an average business person receives 50 potentially dangerous spam emails a day, the difference between a 99.96% catch rate (Vircom modus' most recent VB Spam+ result, March 2016[5]) and Microsoft's 99% catch rate is significant.

Stretched over the course of an average month of spam, a product like modus would allow less than one spam message through, while Microsoft would permit 15. That constitutes a considerably higher risk for exposure to malware, phishing ransomware and other email-borne attacks. When multiplied by a typical SMB's O365 or Exchange environment of say 100 users, that would mean some 1500 pieces of spam entering the network over a given month.

Taking our scenario a step further, how would we calculate the potential risk in costs of such a performance discrepancy? According to IBM's 2015 Cost of Data Breach Study, the average cost of an individual malicious breach was $170. If according to spamlaws.com, only 2.5% of all spam is malicious, and only 40 of those 1500 pieces of uncaught spam make it through, and just 20% of them get acted upon, the conservatively-calculated potential cost of a 99.00% catch rate would be somewhere in the neighbourhood of $16,000 annually.

FEATURE POOR

For the purposes of this examination, we are looking exclusively at O365's Exchange Online Protection (EOP) product. Microsoft customers can expand their security capabilities with Exchange Online Advanced Threat Protection, but as of the writing of this whitepaper this add-on does not improve O365 in the area of email security and thus not germane to this discussion.

Before getting into the details of EOP's feature set and areas where we'll argue that it falls short, it is important to understand the context in which EOP comes to market and how it is presently offered with Office 365. O365 offers Exchange Online Protection replaces its EOL'd predecessor, Forefront Online Protection for Exchange or FOPE. A very popular solution within the Microsoft user and IT community, its discontinuation and replacement with EOP has not been positively received.

"Why is the EOP spam filter so much worse than Forefront? We just had 100 clients which were migrated and without exception we have gotten complaints. It seems to have moved from a solution that "just worked" with very little tweaking to something that needs a lot "care", and even then doesn't work as well."

Anonymous User
msexchange.org forum

Email security is by its nature not the most interactive or engaging category of software. Ideally, in most cases it is a set-it-and-forget it type solution, that is primarily judged on its performance. That said, and aside from the experience of setting up and configuring the solution there is one key area of interaction that many IT Manager and Sys Admin buyers look to as the measure of an email security solution's viability. This is in the all important areas of quarantine and retention. Thus, in our exploration of the features of 0365, we start here.

QUARANTINE-LITE & RETENTION HEADACHES

In Microsoft O365 EOP, administrators have important configuration decisions to make right from the start that will determine how junk, spam and malicious email will be dealt with by the system. As we will show however, regardless of the way an administrator elects to handle unwanted or malicious email, there are significant feature limitations that make this, the most interactive aspect of email security, a workflow headache or worse.

THE NOT SO GOOD OLD JUNK E-MAIL FOLDER - BY DEFAULT

Out of the box, EOP defaults to sending all incoming email determined to spam to the recipient's Junk Email folder. A familiar item to any user of Outlook or Exchange, it is known well both for the many legit emails found in it and the many not so legit emails it doesn't filter. By default, the spam protection is on but the protection level is set to "low", in an effort to avoid trapping legitimate email in the Junk folder. This at least partly explains the common complaint about the amount of spam reaching O365 inboxes. But as we examine the solution, we'll show that from its default settings to more highly configured environments, O365's EOP provides questionable performance on both ends of the anti-spam continuum (false positives to false negatives), and fails to provide adequate control to admins to help them improve it.

If left in default mode, all filtered email will go to the Junk Email folder including what they define as "Spam" and "High Confidence Spam", - a phrasing that would suggest that they don't have very much confidence in first category. We'll look at the issue of Microsoft's approach and performance with false positives later. Here we are looking at the system's default settings and many critical security issues that result.

As stated, all teir-1 filtered "Spam" and "High-Confidence Spam" is placed in the user's Junk Email Folder where it will remain for 14 days by default before being deleted permanently. For most admins, this is not an ideal configuration for a variety of reasons. 1) It gives each user on a network unilateral freedom to move, open and otherwise act upon potentially hazardous emails. 2) The default period is not long enough to ensure that false positive emails filtered as junk don't get wrongly, and permanently deleted.

Take for example a common situation where a C-suite executive (many of whom get more than their share of spam), is on vacation for longer than two weeks. It's very possible that a piece of high-value email, say an invitation to dine at the Whitehouse, would be determined to be spam and moved to that folder. Upon the ex-

-ecutive's return three weeks later, that email would be unretrievable. Additionally, and by default the executive would have received no notification about the email as the default configuration in EOP disabled end-user spam email notifications.

Most admins would instinctively jump right in to change these settings as they invite the risk of a breach, data loss and welcome false positives right our of the gate. However, even reconfigured, the Junk Email retention issue does not go away entirely. While the system defaults to 14 days, which is far too short, it can't be extended beyond 30 days without custom add-ons. And even this extended period is too short and has proven to be more than a mild annoyance for IT administrators.

"Message retrieval is a common pain point for admins. With Office 365, that pain can be unbearable, as Office 365 doesn't perform message retrieval beyond the deleted item retention limit, which is 14 days by default."

J. Peter Bruzzese,
Microsoft MVP
TechTarget Contributor

The lack of flexibility with EOP's retention period can also present a compliance issue in highly regulated industries and many that simply work with or handle email content from compliance-critical businesses. The good news it most comprehensive third party email security solutions allow for lengthier retention and more flexibility so that users can customize the retention period.

LACK OF FLEXIBLE & TRULY CENTRALIZED QUARANTINE CONTROL

To activate EOP's Spam Quarantine features, administrators must log in to Exchange Administration Center (EAC). While not excessively complicated, this is not recommended territory for people not experienced setting up email handling policies and transport rules.

When first released, EOP restricted spam quarantine release to system administrators. This gave admins the difficult choice of letting *all* users release their email (by staying with the default Junk Email set up), or allowing *none of them* to by activating Spam Quarantine. In its most recent release however, admins can now allow users to release emails from quarantine. However, and ironically, the options include letting *all* users release *all* quarantined spam, or allowing no users to have that privilege. Go figure. So essentially admins are given the same Sophie's choice when it comes to acting on filtered email as prior to the "fix".

While activating quarantine, one of the first limitations admins will notice is that its retention period is even more restrictive than that of the Junk Email folder system it replaces. Here the default retention period is 15 days, which is also its upward limit. This presents serious issues for potential data loss and may even constitute

a show-stopper for compliance-conscious companies, who simply can't allow unprocessed email deletion at that pace. Interestingly, the way that the EOP interface is designed, it looks as though this is a number that can be freely changed, which of course it can be, as long as it's any number below 15.

Going one level deeper, Administrators should note that email sent to quarantine by way of admin-configured transport rules will be held for only 7 days by default after which they are not retrievable. This is a woefully short period by default, and represents yet another potential booby trap in EOP that administrators, and for that matter any business owner, should be aware of. Additionally, these transport rule-filtered messages are not viewable by the intended recipient, requiring additional manual and interpersonal interventions to validate email filtering and avoid false positives and data loss.

By default, your Exchange filter automatically detects and analyzes all emails coming into your network and filters those based on the originating IP address. This deletes most spam before it is even analyzed for content and the user never even sees this email. This would be an acceptable approach if the system performing these determinations was a known high-performer with a high spam catch rate, and low false positive rate. But since with EOP neither is the case, this non-consultative approach at the first gate, should be cause for concern.

Further down the pike, EOP reverts to a highly decentralized, user-rule driven system that is friendly neither to average users (with little knowledge of email risks), nor to admins. After a piece of email passes the first spam test, it is analyzed by a second O365 filter that examines message content. If considered spam, the email is treated as malicious, converted to plain text and stripped of pictures, and moved to the corresponding employee's Junk Email folder. Out-of-the-box, Office 365 allows users to review email in the Junk folder and release them. Once quarantine is activated, the reverse is true. None of the users can access or release quarantined content by default. However, turning on this global permission instantly renders quarantine a non-centralized function. Individual users can then freely remove emails from quarantine if desired by simply dragging them into another folder.

In this configuration, users can also manage lists of safe senders/domains, safe recipients, and blocked senders/domains, effectively retraining the filter by managing a whitelist of legitimate parties and a blacklist of illegitimate ones. Most admins would agree that it is not the average office worker's job to recognize and build rules around spam, phishing or spoofing. They might suggest that it's also dangerous to task them with these critical security decisions. On the other hand, while most admins would opt for complete control over no control, EOP's unique approach presents another set of issues when it comes to managing mishandled emails, releasing false positives and avoiding data loss company wide.

Opting for a comprehensive third-party email quarantine solution gives IT and network admin staff much

greater and more granular control over their security environment, allowing them customize and selectively balance between centralized and decentralized control. With Vircom's modus for example, an IT administrator can maintain global control of quarantined email to prevent any malware from reaching the company. At the same time, users can still be granted defined permissions to control their own spam filters, thus allowing them to release any mistakenly-quarantined emails from their side.

WORK-NON-FLOW

Additional headaches continue on the admin workflow side of EOP quarantine. One of the first complaints most admins cite, and this stands as a major oversight, is the quarantine display limit of 500 messages. This wouldn't be a big problem, if there was a 'next' button. Unfortunately there isn't one and so for all practical purposes the maximum quarantine holding capacity becomes 500 messages. Considering that spam represents 70% of all email[7], 500 messages wouldn't likely cover a week of spam and potential false positives in an average company.

As we dive in to begin acting on quarantined messages, we begin to see some of the more glaring shortcomings of EOP from a workflow perspective. As any rule-based filtering can sometimes be off or in need of tweaking, it's a good thing to be able to render bulk releases of emails quarantined in error. Unfortunately, EOP allows for no bulk processing of any kind, requiring admins to open each email one-by-one in order to release them. In a situation where hundreds of emails of the same sort have been wrongly quarantined, any admin would be shaking their fist at such forced inefficiency.

Another head-scratcher is the message trace feature, which forces a download for traces on messages older than 7 days. The system requires a batch submission for the creation of a .csv file that must be downloaded. While Office, Exchange, Dynamics not to mention Bing, have all reinforced the sense that search is not one of Microsoft's strong suits, the idea that a simple status verification of an email requires an admin to jump through so many hoops is unconscionable. Quite surprisingly, the primary display of quarantined messages in EOP is not only limited in rows, but limited in columns as well. The missing column in question is a message "TO" or "RECEIVED" field. This critical column cannot be added to the view and so in order for an admin to discover this basic information they must access advanced search function or actually open the email itself.

Another failure of the search functionality in EOP is the quite surprising inability to perform a search on multiple aliases for the same email user. Instead, the same search must be performed multiple times to retrieve or confirm the same data.

Once these search hurdles have been scaled, the workflow failures of the quarantine endure. As an administrator gauging the veracity of a piece of email determined to be spam, it only makes sense that should you want to

remove it from quarantine, you would naturally want to do that for yourself and not the recipient first. In EOP however, the only person that a piece of quarantined email can be released to is the original recipient.

Additionally frustrating is that through a process of checking and releasing email, there is no indication in EOP that a given piece of mail has been released. Rather it remains, quite unintuitively, in quarantine, whether it has been released or not. This is at very least a headache and annoyance, and at worst a booby trap. Imagine that a known piece of malware was accidentally released, but because it remains in quarantine display it was assumed to have been caught again. It should be noted that some of these issues can be resolved or worked around through the introduction of Microsoft's Powershell, but again, the focus of this investigation is on EOP product off the shelf, not the product customized with add-ons and other bells and whistles.

ANTI-SPAM PROTECTION & CONTENT FILTERING

Earlier in this paper, we cited EOP's gateway level filtering. This is the first filter for all incoming Exchange email, and its set up and behavior provide a good starting point for a discussion of EOP's general approach to spam protection and content filtering.

Reinforcing Microsoft's customary non-transparency around performance, the very first action this system takes in filtering messages is a complete mystery. All that is known about this level 1 gateway is that it instantly blocks any offending emails based on an unknowable, uneditable list of "bad words" and unpublished reputation data. And while EOP does provide a log of all received and actioned messages, none of these first-level filtered emails are included in the log. As the time-honoured taunt goes, "you don't know what you're missing!". In EOP this is literally true, and provides a good argument, not for merely expanding security with a third party solution, but for turning EOP off altogether and relying entirely on security from another vendor. This case can be made on issues of bad workflow, lack of transparency and untracked filtering alone, but does the argument sustain when discussing EOP purely on its performance catching malicious email content? We believe it does.

As embodied in the Office 365 message warning included in the introduction, the company has developed a "shoot first and ask questions later" reputation. This is certainly reinforced through our examination of EOP. Take the simple example of identifying and blocking or quarantining international spam. Here, a single setting change asks the admin to identify a given language or geography to filter international spam which are not at all related to spam.

Interestingly, some of the spam protection and content filtering failures of EOP were features that had been included in its predecessor product, FOPE. And while many of these may also fall under the category of workflow, they undoubtedly have an impact on overall security as well. Case in point, the inability to perform

bulk edits of any kind extends beyond quarantined emails and into the areas of IP and domain blocking. For example, it is impossible to import or copy and paste a bulk list of IPs or domains. Rather, these must be entered into EOP one by one, in single file. Also dropped from FOPE and missing from EOP is the ability to run SMTP connectivity checks.

Another notable issue for identifying potentially harmful content is the fact that EOP only identifies and blocks IPs in the Block IP list through a direct entry point connection. Were one of these IPs to connect via another server in the network, the connection would lose its originating IP and EOP would recognize it as an internal message and allow it.

It's no surprise then, that according to neutral, third party analysis like Osterman Research, "Office 365 does not offer advanced and targeted threat protection techniques"[8]. Osterman cites lacking capabilities like real-time link following and reputation checks to support the case that O365 security lacks the sophistication of other standard solutions. In a world where more than 70% of email is spam, and much of it carrying Zero-day malware (or next-generation malware), it is critical to deploy a secure email gateway that provides fully transparent, real-time updates on the latest threats before they reach the network. The good news is that many peer-reviewed, third-party tools like Vircom are available that continuously self-update to defend against the latest attacks and fill the security gaps left open by EOP.

CONCLUSION

Companies, large and small, are migrating to Office 365 with the objective of streamlining their digital operations. But with the many advantages of moving to the cloud and O365 come many risks on the security side of the equation. This is not because cloud computing is inherently risky, but rather because of Microsoft's decision to bundle a mid, to low-grade security product within its core suite. In so doing they not only provide a false sense of security to their users and admins alike, but as they underperform on both ends of the unwanted email spectrum, they also present a real risk for irretrievable data loss.

In sum, by resisting peer review and underperforming against the best in the industry, Microsoft's EOP exposes its users and their networks to an untenable risks of data breach and data loss. In the process, the product provides for a high degree of workflow inefficiency bound to frustrate admins, and even fans of the FOPE product that EOP has replaced. For these reasons, it is our opinion as security technologists that third party security is essential in O365. If your choice for that security is Vircom's modus, we commend the choice but the most important takeaway here is that in order to effect strong, reliable security, EOP on its own simply doesn't cut it.

ABOUT VIRCOM

Vircom, Inc. is a pioneer in email security software, technology, hardware and virtual appliance solutions, and professional services.

AT THE EDGE OF TECHNOLOGY

Vircom was founded in 1994 with a vision to advance technological improvements in network infrastructure through innovative products. This vision evolved as the Internet advanced, and it became clear to Vircom that it too was evolving as a company as it became a pioneer in email security and anti-spam software.

VIRCOM'S STORY SO FAR

In 1994, the Internet as we know it today was not yet to be formed. Vircom started by creating software for digital bulletin boards, the precursors of the Internet, and eventually software for the management and authentication of dial-up and DSL connectivity for service providers.

As email evolved into the killer app of the Internet, we developed one of the first secured mail servers for businesses and service providers. At the same time, we also created one of the first secured email gateways to protect any standards-based mail server. We are proud to say that both innovations (modusGate and modusCloud) were based on our own proprietary and award-winning technology.

Since then, Vircom has evolved into more than a developer of email security software. **We are the IT security partners to thousands of customers representing millions of end users.** We are an IT trend-setting company, always monitoring, analyzing and responding at the edge of the latest threats and attacks.

What makes us different is our proactive approach: by being at the forefront of technological advances, we're one-step-ahead of understanding IT threats and challenges and living up to our motto of preventing future problems before they occur.

ENDNOTES

[1] Bitglass, Bitglass Report: Microsoft Office 365 Surges Ahead of Google Apps, August 27th, 2015

[2] ODIN, DIN 2015 SMB Cloud Insights United States, retrieved June 1, 2016.

[3] Forbes, Roundup Of Cloud Computing Forecasts And Market Estimates, March 13th, 2016.

[4] Petsalis, Michael "Microsoft, Where's Your Performance Data?, July14th, 2016.

[5] Virus Bulletin "VBSpam Comparative Review?, March, 2016.

[6] IBM Cost of a Data Breach Study, June, 2016.

[7] Kurt Wagner, More Than 70% of Email Is Spam, August 9, 2013.

[8] Osterman Research, Inc., Microsoft Office 365 for the Enterprise: How to Strengthen Security, Compliance and Control, February 2014.

[9] Yves Lacombe, Interview with Yves Lacombe, Senior Sales and System Engineer, Vircom, March 27, 2015

Vircom

460 Rue Saint-Catherine West, Suite 600 Montreal, QC, H3B 1A7

www.vircom.com | 514-845-5731