ZERO SPAM

OstermanResearch
Market research and insight on communications and collaboration technologies

AN OSTERMAN RESEARCH WHITE PAPER

WHAT ARE THE KEY FACTORS TO CONSIDER IN IMPROVING EMAIL SECURITY?

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 •
info@ostermanresearch.com • www.ostermanresearch.com
Twitter: @mosterman

ZERO SPAM

OstermanResearch
Market research and insight on communications and collaboration technologies

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Email is absolutely critical to the operation of business and to the efficiency of individual users. It is equally true that email is under severe and increasing attack from growing volumes and new forms of threats: ransomware, spear-phishing, malware, viruses, 0-day threats, etc. These threats can steal data, drain financial accounts, bring down networks, drive up IT costs, and generally wreak havoc on an organization.

ANY ORGANIZATION THAT USES EMAIL MUST PROVIDE ROBUST DEFENSES AGAINST THESE THREATS.

However, doing so is expensive and time-consuming for many IT staff. Defense mechanisms must continually be upgraded to combat growing volumes of spam, as well as increasingly sophisticated malware and other threats. Furthermore, email security must operate virtually 100% of the time – interruptions of even a few seconds can create major problems.

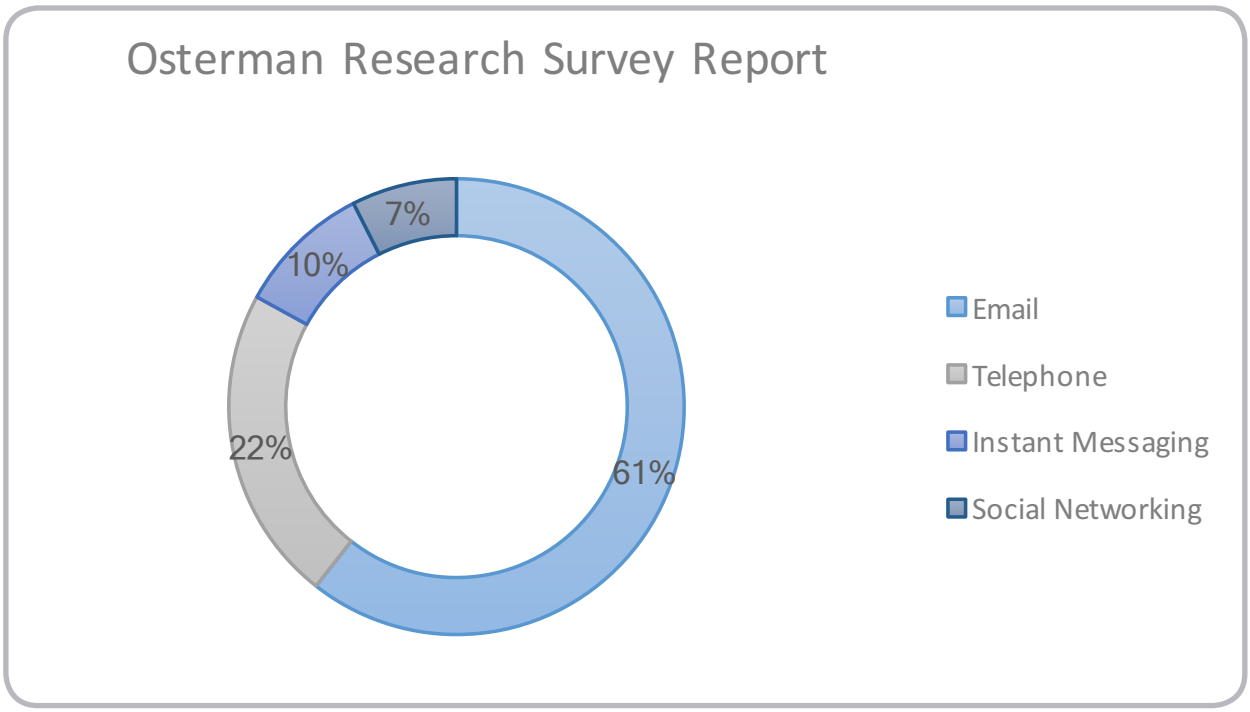
This white paper discusses the advantages of cloud-based email security and it offers some guidance on what decision makers should evaluate as they consider whether or not cloud-based email security is a good fit for their organization.

EMAIL IS UNDER SEVERE ATTACK

Because email is the venue in which the typical user spends roughly 30% of his or her day, it's no surprise that email is under severe attack from hackers, foreign actors, malware authors, phishers, organized crime and others. Email acts as both the container for malware and as the avenue through which Web-based malware can enter an organization, as in the case of blended threats. An Osterman Research found that 43% of organizations had had malware successfully infiltrate their network through email during the previous 12 months.

Spam continues to represent a major problem for organizations given that 85% to 90% or more of all email sent across the Internet consists of spam. Spam volumes consume important amounts of storage, email server CPU cycles, bandwidth and recipients' productivity.

Despite the increasing use of social networking, instant messaging, collaboration and other communication tools, use of email continues to dominate the average computer user's day. Consider the following:



- An Osterman Research survey found that the typical user spends 146 minutes on a normal workday doing something in their email client. This is significantly more than the amount of time they spend on the telephone (54 minutes), using instant messaging (23 minutes) and using social networking tools (18 minutes) combined.
- The same survey found that the typical user in an organization of up to 500 users sends and receives 173 emails on a normal workday, while users in larger organizations send and receive 160 emails – an average of one email sent or received every three minutes or less.
- Another Osterman Research survey found that email use is holding steady or increasing for 97% of email users.

WHAT'S THE BEST WAY TO ADDRESS THE PROBLEM?

There are two basic methods that organizations can employ to address email security:

a. deploy software/servers and/or appliances using internal IT staff to evaluate, configure, deploy and manage the infrastructure or

b. let someone's else's IT staff do this in the cloud.

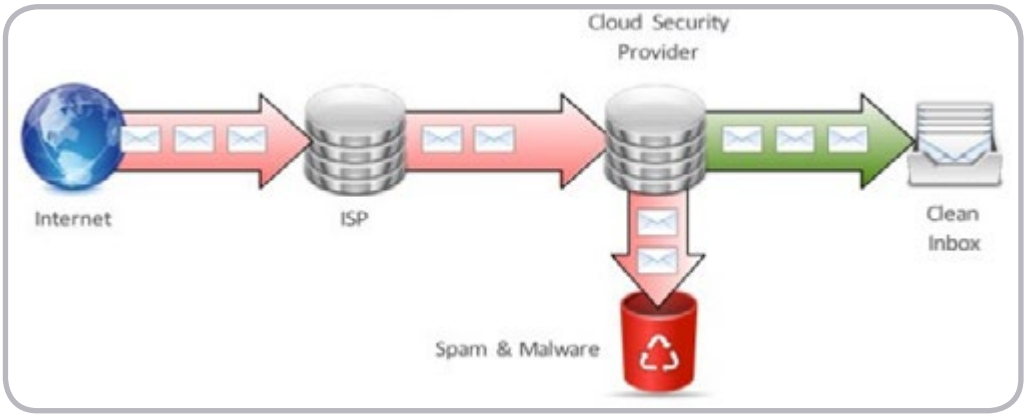
Increasingly, organizations of all sizes are opting for the latter approach because of the cloud's inherent advantages:

- It keeps threats outside of the network perimeter.
- It can significantly reduce the cost of ownership for providing email security, particularly for smaller organizations.
- It frees up highly pressured IT staff and infrastructure for initiatives that will provide more value and more competitive advantage.
- It makes the cost of providing email security more predictable because costs shift from capital to operating expenditures. This means that costs scale according to the number of users and new infrastructure does not have to be added periodically to deal with traffic increases or significant increases in the number of users resulting from mergers or acquisitions.
- It can provide a level of disaster recovery and business continuity that would be expensive to duplicate with on-premise infrastructure.

HOW CLOUD EMAIL SECURITY WORKS

Cloud-based email security is conceptually very simple. Instead of receiving email directly from the Internet, after going through the various providers that manage emails on their way from the sender to the recipient, mail is finally routed to an email security provider's data center for processing.

This is accomplished by a simple modification to a domain's MX records. For example, if a company had been receiving email sent directly to its domain "company.com", the change in the MX records will route all email sent to company.com to the cloud-based email security provider's data center. The email security provider then filters spam from the email stream; checks it for viruses and other malware; performs various checks on the content and various attributes of the email; and then sends legitimate email on to the recipients at company.com free of spam and other undesirable content. The entire process normally requires an additional one to two seconds in total message delivery time, a delay that is virtually unnoticeable to recipients.



The process is displayed conceptually in the above diagram.

6 ADVANTAGES TO CLOUD-BASED EMAIL SECURITY

While on-premise security can provide very good performance, the cloud offers a number of important benefits in the context of email security:

1. RESOURCE SAVINGS

Among the most important benefits of the cloud-based email security model – and the cloud model in general – is that it frees up IT staff time that otherwise would be devoted to management of the security infrastructure, updating and patching it, configuring new servers or appliances, etc. For example, in a major security survey undertaken by Osterman Research, it was determined that mid-sized and large organizations in North America require a mean of 27.1 person-hours of IT staff per 1,000 email users, or 0.68 full-time equivalent (FTE) staff, to manage just the security infrastructure in the average organization. For smaller organizations, this figure is substantially higher.

When using cloud-based email security, almost no IT staff time is required, freeing current IT staff for other initiatives that will provide more value to the organization. On the contrary, on-premise systems, such as dedicated appliances have to be installed, configured and monitored and they run using the email server's resources if installed on the server itself. Furthermore, a good installation also requires the development of a corpus of spam and "ham" (valid email) so that the solution's statistical engine can learn about incoming content and score it appropriately. This is a time-consuming task that also poses a security challenge: who will be trusted to read through the company's business correspondence in order to choose a sufficiently representative ham corpus?

Other resource savings arising from the use of cloud-based email security include the dramatically reduced load on email servers and on the network in general, including a dramatic decrease in network bandwidth requirements by as much as 80%. This savings comes from the fact that most of the incoming mail stream – consisting of spam and malware – that would otherwise have to be received into the network and processed is simply dealt with by the cloud email security provider before it ever reaches the corporate network. Because the vast majority of incoming email is spam, most content that would need to be processed by the internal network is eliminated before it ever reaches the corporate firewall.

2. SECURITY ADVANTAGES

Cloud-based email security provides much better protection of the network perimeter because viruses, worms, phishing, other malware and spam are eliminated before they ever reach the corporate network. This prevents malicious content from entering the network and possibly infecting computers.

Further, cloud-based email security

improves virus detection because the provider's anti-virus agents are added to the on-premise agents, thereby increasing the global antivirus spectrum.

It also provides added security by limiting incoming traffic to one trusted source (clients can use their firewall to limit incoming email to just the provider's servers), which greatly simplifies troubleshooting and disaster recovery.

Other security benefits of the cloud-based email security model include greater redundancy in malware and spam filtering, protection from Distributed Denial-of- Service (DDoS) attacks and DSN backscatter, simplified troubleshooting, remote monitoring of client gateways and transcient message encryption throuh the use of TLS.

3. GREATER RELIABILITY

Cloud-based email security providers typically offer very high levels of reliability because of the redundancy they build into their networks. This can also be accomplished using on-premise systems, but it adds significantly to the cost of providing security in-house, as clients have to double their investment, which may be more difficult to justify.

4. BUILT-IN DISASTER RECOVERY AND BUSINESS CONTINUITY TO PROTECT AGAINST THE LOSS OF IMPORTANT EMAIL

Many cloud-based email security providers offer built-in disaster recovery and business continuity capabilities in the form of email "spooling". For example, if a customer's primary email servers go down because of a power outage, natural disaster, or some other unforeseen incident, email can be received and stored by the cloud-based email security provider during the period of the outage. Once the customer's email servers are again operational, stored email is then sent to the customer in a controlled manner. Further, some providers will offer to set up temporary email accounts so that business can continue during the outage.

In a typical on-premise system, on the other hand, an outage will result in emails that are bounced back to the sender. This can result in phone calls to determine why emails are bouncing, a potential loss of reputation for the business whose email servers are down, and other negative consequences. While organizations that use on-premise

security can deploy disaster recovery and business continuity systems to prevent these problems from occurring, doing so adds to the expense of managing the system.

5. GREATER FLEXIBILITY

Cloud-based email security also permits more flexibility than is possible for on-premise security systems. For example, if an organization acquires another or otherwise adds significantly to its total employee count – or if it must undergo a major layoff of staff members – cloud-based email security can be "rightsized" in a very short period of time to meet current demand. The speed and ease with which this can be accomplished with the cloud model is simply not possible with on-premise systems.

It is also important to stress that cloud filtering is completely platform independent, which means that compatibility issues are non-existent, allowing an organization to use multiple email systems or switch to another email platform without changing its email security capabilities.

6. MORE PREDICTABLE AND OFTEN LOWER COST OF OWNERSHIP

Cloud-based email security also offers much more predictable and typically lower cost of ownership than on-premise systems. The greater predictability in the total cost of ownership for email security provided by the cloud model comes from the fact that most cloud providers offer fixed pricing for a year or more, allowing decision makers to understand what their cost per user will be during that period. Even if spam and malware increases dramatically – which is often the case during the Christmas holidays and during occasional "spam storms" or major outbreaks of malware – the cost to the customer of remediating the additional spam and malware will not increase during the contract period.

This is not the case for on-premise infrastructure that must occasionally be upgraded or added to in response to increases in traffic or the number of users. These off-budget expenditures of adding new servers or appliances can be costly and fairly disruptive to IT staff. While an on-premise infrastructure can be overbuilt at the outset to accommodate unanticipated increases in spam or malware, this adds significantly to the cost of the overall security infrastructure.

6 KEY REQUIREMENTS FOR CHOOSING AN EMAIL SECURITY SOLUTION

There are a variety of important issues that any organization should consider as it formulates its email security strategy. In particular, there are some specific issues that Canadian organizations should consider that do not necessarily apply to organizations in the United States or elsewhere.

1. PREVENTING ACCESS OF YOUR EMAIL BY OTHERS

An important consideration for any organization is the prevention of unauthorized access to corporate email and other important business content. Given that email systems today contain a substantial proportion of the content that organizations generate – including confidential statements of policy, financial records, personnel records and the like – protecting this content from access by unauthorized parties is critical.

A key issue in selecting a cloud-based email security provider must be the US Patriot Act, a sweeping set of regulations passed on October 26, 2001 that actually amended 11 existing Congressional Acts, including the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act and the Money Laundering Control Act.

A key provision of the Patriot Act is the use of National Security Letters, which are essentially search warrants written by federal agents without an examination of evidence beforehand by a judge (similar in concept to the "writs of assistance" that British soldiers were permitted to execute in the US colonies prior to the Revolutionary War).

A critical security issue for non-US organizations when selecting a cloud-based provider of any kind should be the location of the data centers it

operates. For non US organizations having data centers outside of the United States provides a layer of protection from unauthorized access to email by a foreign government.

2. INTEGRITY AND AUTHENTICATION CHECKS ARE KEY

The ability for a cloud-based email security provider to perform integrity and authentication check on senders of email is an important capability in reducing the amount of email that must be processed. For example, email senders that appear on blacklists, that have badly configured HELO banners, or that are spoofing domains protected by SPF records can be rejected before their content is inspected for spam or malware. This can result in a spectacular reduction in the number of inappropriate connections that servers must process and can dramatically reduce the size of the spam quarantine. When choosing a cloud-based email security provider, these integrity and authentication checks are an important issue on which to focus.

3. QUARANTINE MANAGEMENT

While some organizations will want all of their users to have access to spam quarantines to check for false positives – valid emails that inadvertently are trapped in a quarantine area – this is not necessarily a best practice for all users or organizations. A cloud- based email security provider should offer the option of making individual spam quarantines available only to those organizations that want them, and then only to those users within the organization that IT management feels should have access to them. Experience has shown that some users will spend an inordinate amount of time checking email in spam quarantines, thereby wasting the time the solution saves them. Further, they could actually release dangerous content into the corporate network without realizing it. This is particularly true for blended threats and phishing schemes, in which a link to a malicious Web site is embedded in a spam message. If a user releases this type of email from the spam quarantine and he or she clicks on the link, this could create enormous problems for an organization.

4. IT MANAGEMENT ISSUES

Although cloud-based solutions dramatically reduce the amount of IT staff time required to manage security, there is still some time required for

answering users' questions, investigating false negatives and false positives, managing the relationship with the provider, and the like. Any cloud-based email security system should keep IT management time to a minimum through the use of user-friendly and multi-lingual interfaces, detailed statistical reports on user behavior and system performance, and a dashboard that will keep IT staff well informed on email traffic flow and the overall performance of the system. Further, robust technical support is essential for those rare occurrences when things go wrong. Because of the critical nature of email, access to 24/7 one-on-one support should be provided.

5. RELIABILITY IS CRITICAL

The reliability of any cloud-based email security system must be as close to 100% as possible, since a breakdown of the system will permit dangerous content to enter the on-premise network, or it will result in bounced emails to senders. This is particularly important in the context of the email continuity capabilities described earlier that will queue email for at least several days in the event that a customer's email system goes down.

Another important consideration is the provision of a backup email capability for some or all users in an organization. Some cloud-based email security providers offer this capability, allowing use of temporary email accounts that can be configured for users within the customer organization. This provides a level of business continuity that could not otherwise be achieved without substantial investment.

6. OTHER IMPORTANT CONSIDERATIONS

There are a number of other issues and questions that should be posed to prospective cloud-based email security providers, including:

- Do users have the ability to easily report false negatives (spam or malware that mistakenly was delivered to users), such as through a user-friendly reporting agent?
- Must IT staff closely monitor the exact number of users being protected by the cloud provider, such as when employees are hired or leave the organization, or can they provide just an approximate number that is updated periodically?
- Is optional greylisting possible?
- Is there access to detailed statistical reports about the amount of spam and virus received?
- What is the Service Level Agreement (SLA) offered by the cloud provider? A strong SLA for both performance (spam capture rate) and availability should be expected.
- Does the provider offer convenient spooling capabilities so that important email is not lost in case of an outage?
- Are all transactions fully audited?

ABOUT ZEROSPAM

Founded in 2003, ZEROSPAM is a leader in cloud email security. Their solution is a highly effective, multi-layered system – providing high levels of efficiency and accuracy. The performance of ZEROSPAM has been validated by Virus Bulletin, a neutral third party and the industry's reference for antispam evaluation. Based in the UK, Virus Bulletin runs a well-reputed antispam testing program that many of the industry leaders are taking part in. ZEROSPAM first started with the program in March 2012 and has steadily obtained a catch-rate of 99,5% to 99,9% with a very low false positive rate. ZEROSPAM has also earned several VBSpam+ awards which require a catch-rate of 99.5% or more without any false positives.

ZEROSPAM offers a list of exclusive features, including 2 antivirus agents, superior detection of executable files, spear-phishing and ransomware protection, a safer approach to quarantine management, detailed statistical reports, optional greylisting, easy attachment management and flexible licensing. TLS and LDAP synchronization are fully supported and outbound filtering is also part of the ZEROSPAM offering. As email marketing is becoming widespread, organizations run the risk of becoming blacklisted if they send email blasts using their own gateway. The best approach is to use a specialized vendor for email marketing AND to implement outbound filtering. Outbound filtering also offers efficient protection against blacklisting caused by an organization unknowingly sending spam through an infected gateway or workstation. Made for discriminating customers, ZEROSPAM provides a best in class cloud-based email security solution with exceptional technical support at an affordable overall cost of ownership.

The company has a 15 year history of success and sustained growth and a large client base comprised of organizations of all-sizes, from 25,000 seats to very small businesses, in a large variety of sectors. It has earned the trust of leading organizations in technology, governmental agencies and industry leading think tanks. Some of their customers include government agencies, school boards, large customers from the transport, enrgy, financial and legal industries.Transcom, Telefilm Canada, Beyond the Rack, Radialpoint and Lawpro.

ZEROSPAM OFFERS ITS CUSTOMERS

A 30-DAY FREE TRIAL

WWW.ZEROSPAM.CA/TRIAL

AND BOASTS A 95% ADHESION RATE AFTER THE TRIAL PERIOD.

CONTACT INFORMATION

MONTRÉAL

2520 Beaubien St. East Suite 200
Montréal, QC Canada H1Y 1G2
+1 514 527 3232
+1 888 990 7726 (toll-free)
+1 514 527 1201 (fax)

TORONTO

+1 647 478 8336

EMAIL

Corporate Sales : gov@zerospam.ca
Government Sales : corp@zerospam.ca
General Information : info@zerospam.ca

© 2010 Osterman Research, Inc. All rights reserved.

© 2014 ZEROSPAM, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statue, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 •
info@ostermanresearch.com • www.ostermanresearch.com
Twitter: @mosterman