Best Practices In Securing Office 365 Email

Joel Snyder
jms@opus1.com
Opus One[1]

Introduction

Microsoft Exchange deployments traditionally have depended on third-party email security gateways for critical anti-spam, anti-malware, and mail control features such as encryption and data leak protection. This design philosophy extends to Microsoft's Office 365, a full-featured offering with dozens of options and an extensive capability for collaboration and communication. However, it has a more modest set of tools when it comes to email security.

The goal of this paper is to go beyond "check list" comparisons and look at how well Office 365 performs when compared to Cisco Email Security in critical edge-of-the-network email security.

We evaluated seven specific areas in Office 365 and Cisco's Email Security solutions (on-premise and cloud) to see how well each product executed key requirements in:

- ability to find and track messages and assist in troubleshooting;
- provide meaningful reports on message flows;
- manage zero-day incidents;
- filter spam, phishing, and other unwanted mail;
- identify advanced malware;
- prevent data loss; and
- encrypt email traffic at the enterprise edge.

Our testing of these mainstream features has found that Office 365's security services don't match those of many on-premises and cloud-based email security gateways. Enterprise email administrators must consider layering dedicated email security services to enhance what is offered in Office 365. Two products working together provide a total solution, enhance end-user satisfaction, and maintain consistency during and after the transition to cloud services.

Many enterprises consider migration of *services* to cloud-based SaaS providers to also include a migration of *responsibility*, not just for uptime and performance but also for security. Our testing shows that Office 365 by itself presents greater security risks to end-users when compared to a combination of Office 365 and Cisco Email Security. Email administrators need to be informed about the additional risks associated with a "bare" Office 365 deployment, and should carefully consider adding cost-effective solutions such as Cisco Email Security to Office 365 to mitigate these risks.

[1] Opus One is an information technology consultancy with experience in the areas of messaging, security, and networking. Opus One has provided objective testing results for publication and private use since 1983.

Executive Summary

Organizations migrating to Office 365 for their email and other collaboration tools anticipate the same quality experience that they had with traditional on-premises Exchange. In objective testing, we find that Office 365's email security features can be improved to match the experience email administrators had when protected by dedicated email security gateways. Based on customer demand, Microsoft fully supports hybrid cloud/on-premises deployments. The result is that it is easy to combine tools such as Cisco's Cloud Email Security or on-premise email security gateways with Office 365.

Our testing focused on seven specific areas where Microsoft Office 365 is complemented by a third-party email security gateway. The results are summarized in the table below.

Security Area	Cisco Email Security	Microsoft Office 365
Message Tracking & Troubleshooting	Searching for messages using more than 10 different criteria is possible; full results are returned; narrowing down to specific messages is fast	Searching for messages is limited and critical search criteria are not supported; full information is not returned; email administrator cannot control age of logs
Reporting	Over 20 types of reports which can be scheduled, run ad-hoc, or controlled through an API; full export capabilities on all reports	Fewer report types and much less granular time windows available; current information not available; most reports cannot be scheduled and data cannot be easily exported
Zero-Day Incident Management	Full support for all phases of incident management, including identifying, blocking, and cleaning up attacks	Minimal support for identifying and cleaning up attacks; good capabilities for blocking incoming attacks
Catching Spam	Catches more spam with fewer false positives in 12 consecutive tests in 2015 than Office 365's native anti-spam solution	Allows through more spam and has more than 3 times the false positive rate; will negatively impact user satisfaction when transitioning from a better anti-spam filter
Blocking Advanced Malware	In zero-day testing, Cisco Email Security's AMP blocks more malware than Office 365 Advanced Threat Protection.	Office 365 Advanced Threat Protection is less effective than Cisco's AMP, letting through 46% more advanced threats to end-user mailboxes
Data Leak Protection	DLP testing with typical US sensitive data caught 14 or 16 test cases	DLP testing caught 3 of 16 tests and failed to identify sensitive data in most common scenarios
Encryption Capabilities	Greater features, including low-level and high-level encryption tools, are all included in the base product	Encryption controls only available for Business-to-Consumer type messages.

Organizations must consider Office 365 deployments carefully to weigh the benefits and costs of a cloud-based solution. However, when Office 365 is right for an enterprise, we advise retaining a third-party email security gateway such as Cisco's Email Security to complement Office 365 and provide a full-featured and highly secure solution.

1. Message Tracking and Troubleshooting

One of the most common questions email administrators have to address is “what happened to my message?” This makes timely and accurate message search and tracking (commonly called “Message Tracking”) a basic functionality.

Both Cisco Email Security and Office 365 have Message Tracking capabilities. However, Cisco Email Security goes beyond what Office 365 offers with the ability to search using diverse criteria, and providing more details on a message’s path through the network.

We looked at the Office 365 web-based GUI and the Cisco Email Security GUI to compare message tracking capabilities. We also tested the command-line (CLI) message tracking feature, using either Secure Shell (Cisco Email Security) or Windows PowerShell (Office 365). The capabilities of the products are somewhat different when using the CLI. We’ll discuss PowerShell more below.

Message tracking in Cisco Email Security starts with having the data immediately available by letting the email administrator choose how little or how much message logging they will keep. In contrast, Microsoft Office 365 limits tracking information to 90 days.

Message Searching Capabilities Examined In Depth		
Search Criteria	**Cisco Email Security**	**Microsoft Office 365**
Sender	✔	✔
Recipient	✔	✔
Subject of Message	✔	✗
Date Range	✔	✔
Sender IP address or Domain	✔	✗
Attachment Name	✔	✗
Message ID (RFC822)	✔	✗
Internal Message ID	✔	✔
Status of Message	✔	✔
More than 90 days of data	✔	✗

The table above summarizes searching differences between the two products. While both can search in terms of sender or recipient, Cisco Email Security lets the email administrator quickly narrow down a search based on other message attributes if precise information on the sender or recipient are not available.

There is also a significant difference in the depth of the data returned. Searching in Cisco Email Security returns a list of matches, allows the email administrator to export this information, and provides extensive detail on the messages including their flow through the system, the security parameters, policies that were matched, and provides a full picture of the envelope of the messages.

We found that Office 365 returned results less helpful to the email administrator. For example, results cannot be easily exported. The information provided can obfuscate the message flow, message structure (such as messages with multiple recipients) or hide important information, such as IP addresses. When email administrators working in separate organizations collaborate on tracking a message, simple questions like “what IP address did you send this outgoing message from” and “how did the receiving MTA acknowledge the message?” cannot be answered by the Office 365 administrators. This can result in lengthy or inconclusive support tickets.

Office 365 does have an advantage because it ties both the MTA and message store functions together. Administrators can see a message enter the Office 365 network and, with the same interface, see the message delivered into a particular mailbox. This capability of Office 365 reduces the number of interfaces they need to search to track down a particular message. Because Cisco Email Security is not directly tied to the message store, email administrators must use two different interfaces to see message delivery all the way from Internet to mailbox.

Message Tracking Results Examined In Depth		
Information Returned	**Cisco Email Security**	**Microsoft Office 365**
Both incoming and outgoing IP addresses	✔	✗
DNS information about IP addresses	✔	Sometimes
Security attributes of the message	✔	✗
All recipient information	✔	✗
Exportable Summary	✔	✗
Exportable Message Report	✔	✗
Email Policy Information	✔	✗
Date/Time Stamps	✔ (Local Time)	✔ (UTC)
Delivery status to end-user mailbox	No	✔
Subject Line	✔	✔
Spam Status	✔	✔
Anti-Virus Status	✔	✗
User Authentication Status	✔	✗
Can link messages on same connection	✔	✗

Email administrators with an extensive background in Microsoft Exchange and PowerShell have another option for message tracking. With Remote PowerShell, they can run commands to do message tracking directly from their desktop. This gives them more capabilities than are shown here (such as easy exporting of information).

While PowerShell provides greater functionality than the web interface, it is also a specialized skill. Some email administrators may embrace this functionality, and the required training. In that case, the daily stability of Office 365 depends on these same staff members who often the ones being reassigned after the enterprise migrates to Office 365.

Our testing shows that Cisco Email Security strongly complements the capabilities of Office 365 by adding in stronger message tracking features. Cisco Email Security lets the email administrator quickly narrow the search, finding messages with less information, and see deeper message details from search results. Cisco's Message Tracking speeds time to debug problems and to resolve user questions.

2. Reporting

Email administrators use reporting to watch aggregate trends, identify changes and threats, and establish baselines for capacity and cost planning. Good reporting gives the ability to drill down to recent events, as well as zoom out to big pictures of mail flow in the organization.

As with troubleshooting, there are differences between Cisco Email Security and Office 365 because of the different focus of the products, email security versus collaboration server. The Office 365 reporting interface provides a small number of reports (5) related to email security, email policy, and DLP (another 30 types of reports cover other areas of the product), while Cisco Email Security has more than 20 significantly different security reports, covering a greater range of information.

Another benefit of Cisco Email Security is the ability to schedule all reports for automatic creation and distribution (Office 365 only supports scheduling a subset of the reports). Cisco Email Security reports always have current information, while Office 365 delays available of information so that real-time or same-day reporting is not usually possible.

The table below summarizes some of the major differences in reporting between the products.

Reporting Capability Major Differences		
Reporting Area	**Cisco Email Security**	**Microsoft Office 365**
Messaging Security Reporting (reporting areas)	• Incoming & Outgoing Sender/Recipient • Incoming & Outgoing Destinations • Message Delivery Status • DLP Reporting • Message and Content Filters • High-Volume Mail, • DMARC Verification • Outbreak Filters & File Analysis • Virus Types • URL Filtering • Advanced Malware Protection • TLS & SMTP Authentication Usage • Rate Limiting	• Sender/Recipient • Spam Detected • Malware Detected • Sent/Received Mail • Policy Matches • DLP Reporting
Report Contents	Time window to the minute	Time window to the day
Report Currency	Up to current time	Previous day's information
Scheduling	Any report can be scheduled	4 reports can be scheduled
Ad-Hoc Report Format	Web, PDF, CSV	Web
API Control of Reports	RESTful API available	No API available

As with troubleshooting, additional capabilities are available to email administrators who are able to connect and use PowerShell to retrieve data. Microsoft offers a plug-in for Excel that will enable Windows systems to directly pull some reporting data into Excel spreadsheets, a unique feature for Office 365.

Our testing shows that Cisco Email Security widens the variety of email reports beyond what are available in Office 365. Reports are available in a large variety of formats, with detailed information, and with full scheduling capability. These additional reporting capabilities save time over a standalone Office 365 deployment, and keep the email administrator better informed about the performance of their email system.

3. Zero-Day Incident Management

Spam filters and anti-malware scanners work very well, but they cannot be 100% effective. The right combination of elements will eventually get through and infect an end-user's system. When that happens, the email administrator has to act quickly, because minutes count—delivered messages are ticking time-bombs sitting in inboxes, and more attacks are sure to come quickly.

The email administrator has to be able to answer questions and take actions very quickly to protect the enterprise. We call this "Zero-Day Incident Management," and it includes three distinct phases:

- identifying the attack
- blocking the attack
- cleaning up the attack

Our testing found that Office 365 has a good set of features for managing zero-day incidents. However, Office 365 does not have some key features in each management phase that are available in Cisco Email Security. In a world where the attackers often have the upper hand, giving email administrators even a small edge in zero-day attacks can save hundreds of thousands of dollars.

Phase	Features Cisco Email Security adds to Office 365
Identifying Attack	Attachment identification and tracking; displaying all recipients of a message; searching on a wide number of message attributes (such as subject line, IP address, or attachment name)
Blocking Attack	Blocking messages based on URL categories or reputation, attachment file type, IP address reputation, defanging URLs or blocking specific URLs
Cleaning Up	Identifying affected users by specific message attributes

When time-critical zero-day incidents have to be remediated, ease-of-use and broad feature flexibility are benefits in a stressful situation. While Office 365 has many useful features for the zero-day life cycle, email administrators have additional power at their fingertips and more accurate information when Cisco Email Security is in place in front of Office 365 email.

4. Catching Spam and Phishing Attacks

An email security solution must block spam, phishing, and other types of unwanted email. Our testing shows that the spam content filter in Cisco Email Security consistently catches more spam than the filters in Office 365, offering end-users a better experience with less missed spam and fewer false positives.

Since both products continually improve their performance, we've compared only the recent testing to show how well each content filter catches spam and avoids false positives. (Note that reputation services are not included here; we are focusing only on true false positives that would be undetected by the recipient or sender.)

Comparing Spam Catch Performance		
Month	**Cisco Email Security**	**Office 365**
July, 2015	98.37%	97.15%
August, 2015	98.78%	98.42%
September, 2015	99.19%	97.30%
October, 2015	99.26%	97.53%
November, 2015	98.44%	97.83%
December, 2015	96.19%	96.15%
Average for all 2015	**98.04%**	**97.02%**

Comparing False Positives		
Month	**Cisco Email Security**	**Office 365**
July, 2015	0.02%	0.10%
August, 2015	0.03%	0.23%
September, 2015	0.09%	0.07%
October, 2015	0.11%	0.15%
November, 2015	0.04%	0.17%
December, 2015	0.01%	0.23%
Average for all 2015	**0.05%**	**0.16%**

End-users who have previously worked with the Cisco Email Security solution may react poorly to an increase in false positives and additional time spent in spam-related email management.

Our testing proves that Cisco Email Security's spam content filter has a consistently higher catch rate and consistently lower false positive rate than Office 365. Across all of 2015, Office 365 had more than three times as many false positives as Cisco Email Security. End-users who are particularly sensitive to spam and false positives will have a better user experience when Cisco Email Security is added to Office 365.

5. Blocking Advanced Malware

Email administrators know that traditional anti-malware tools can't catch every bit of malware entering their networks. Even when configured perfectly, there is always malware that signature-based tools cannot catch.

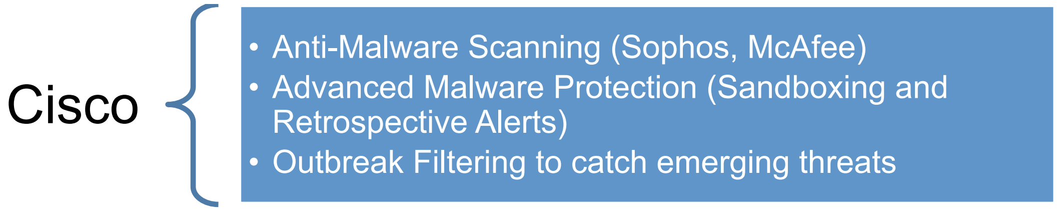
Cisco Email Security offers the option of either Sophos' or McAfee's anti-malware solution for scanning incoming email. Email administrators can select a tool that complements their existing desktop and server-side anti-malware tools. Microsoft Office 365 includes a multi-layered anti-malware scan of incoming messages as well. Email administrators can't select individual engines from Microsoft's offering, but Office 365 has "partnerships with multiple best-of-breed providers of anti-malware technologies [and] all of our customers are automatically protected by multiple anti-malware partners at all times."

Cisco's ESA has an additional feature that can add a higher level of malware protection: Outbreak Filters. Outbreak Filters are a way for Cisco's security team to react to emerging threats while waiting for anti-malware vendors to develop signatures for the threat.

With Outbreak Filters, certain messages may be automatically delayed on an urgent basis in a quarantine based on characteristics such as file size, URLs, or file names. When the emerging threat is fully understood, these messages are released from the on-board quarantine, where they are blocked by the updated anti-malware engine, or passed on through if there was no real threat. Released messages will have suspicious URLs rewritten so that the recipient's browser will be directed through Cisco's web security proxy, which will scan all downloads using both traditional and advanced malware protection tools.

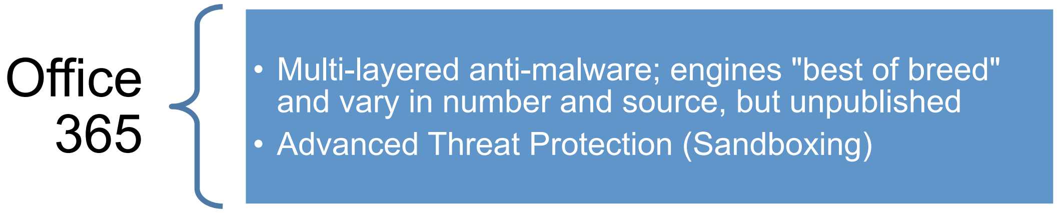
Advanced Malware Protection (AMP) is Cisco's file reputation system based on cloud-based sandboxing technology. With AMP, each attachment to an email message is hashed and the hash sent to Cisco for a reputation verdict. Files without reputations are analyzed and, if malware is found, all Cisco Email Security customers who received that file will be alerted. Advanced Malware

Protection is subject to an additional license fee. Microsoft's sandboxing technology is called Advanced Threat Protection, available at extra cost to some customers.



Cisco

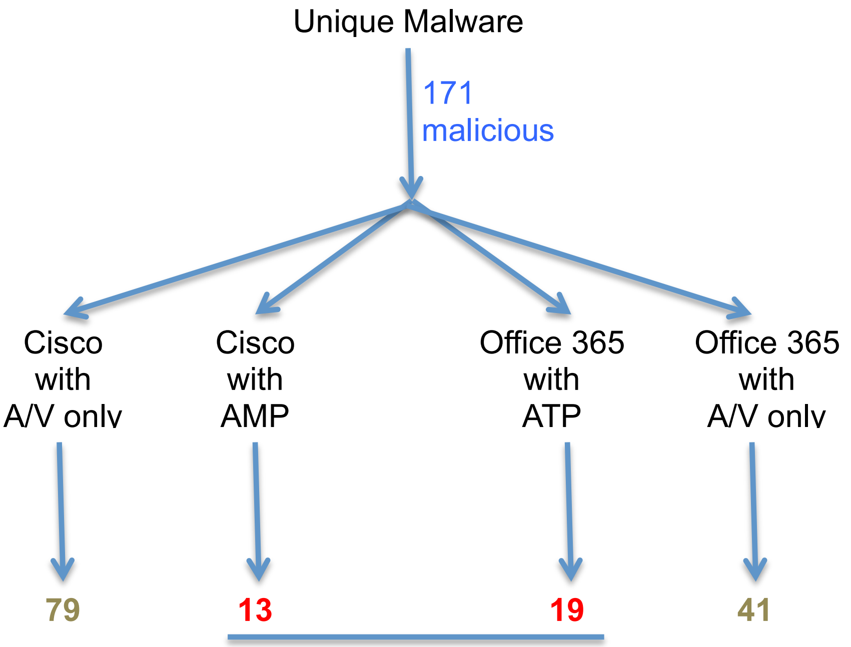
- Anti-Malware Scanning (Sophos, McAfee)
- Advanced Malware Protection (Sandboxing and Retrospective Alerts)
- Outbreak Filtering to catch emerging threats



Office 365

- Multi-layered anti-malware; engines "best of breed" and vary in number and source, but unpublished
- Advanced Threat Protection (Sandboxing)

In testing with zero-day threats, we found that Cisco Advanced Malware Protection delivered a more secure experience than Office 365 with Advanced Threat Protection. To perform a head-to-head test, we focused on the real bottom line for malware: how many malicious messages were delivered to end user mailboxes with and without advanced threat protection? The diagram shows the results of a testing with 171 different malicious advanced threats.



Unique Malware

171 malicious

Cisco with A/V only: 79

Cisco with AMP: 13

Office 365 with ATP: 19

Office 365 with A/V only: 41

Office 365 with ATP delivered **46% more** malware to the end user than Cisco AMP

In our testing, we found Advanced Malware Protection to be a significant addition to traditional anti-malware/anti-virus scanners used in both Cisco Email Security and Microsoft Office 365. When compared head-to-head with Office 365's Advanced Threat Protection, Cisco Email Security delivers less malware to the end user, reducing the risk of infection.

6. Data Leak Protection Testing

Email administrators who depend on correct operation of Data Leak Protection to reduce risk will be very disappointed in the operation of Microsoft Office 365. In our testing, we found it difficult to trigger Office 365's DLP alerting and blocking. Unless the enterprise DLP administrator is simply looking for "check box compliance," using Office 365 DLP would open the organization to claims of negligence and irresponsible security policies.

Office 365's built-in DLP features for sensitive data such as social security or credit card numbers can only be triggered for messages that essentially begin "Here are a bunch of credit card numbers" followed by the numbers (without critical information needed to make them useful, such as names, expiration dates, or CVV codes). Social Security numbers behave the same way: a message saying "here are social security numbers" with a list of numbers would trigger the DLP, but a more typical presentation, such as numbers followed by names and birth dates, slips through Office 365 DLP.

For policy definition, the two products offer similar capabilities, including pre-built policies that help the DLP administrator to get started, forcing transport encryption for known partners, and triggering different actions based on the severity of the violation.

We tested the detection system to determine how well the DLP actually works. We focused on US-centric and global DLP policies. At first glance, the products seem similar, supporting almost an identical set of sensitive data types. However, the capabilities advertised in the GUI are not matched by the performance of the DLP engine. In tests with the most important sensitive data types (credit/debit card numbers, social security numbers, and bank account numbers), we found significant differences in detection capability.

The table below shows the results of testing the DLP features of each product on real data in various formats. We tested each type at least twice: once with a label, such as "here are the social security numbers you asked for" and once without a label. We also varied the format, trying "raw data" of numbers without any other associated information, and a more natural presentation adding in information such as personal name, expiration date, and so on.

DLP Test Results: Detecting Sensitive Data

Test Type	Cisco Email Security	Microsoft Office 365
Unlabeled Credit Card full data	Pass	Fail
Unlabeled Credit Card number only	Pass	Fail
Unlabeled Social Security and Name	Pass	Fail
Unlabeled Social Security number only	Pass	Fail
Unlabeled ABA Numbers	Pass	Fail
Labeled Charge Card Full Data	Pass	Fail
Labeled Credit Card Full Data	Pass	Fail
Labeled Charge Card number only	Pass	Fail
Labeled Credit Cards number only	Pass	Pass
Labeled Social Security and Name	Pass	Fail
Labeled Social Security number only	Pass	Pass
Labeled Social Security re-formatted	Pass	Pass
Labeled Passport Numbers	Pass	Fail
Labeled Passport Number and Name	Pass	Fail

Our testing suggests that Microsoft Office 365 DLP offers little or no benefit, while Cisco Email Security (based on an embedded RSA DLP engine) does a good job of identifying, blocking, and reporting on sensitive information about to leave the enterprise.

While Microsoft Office 365 and Cisco Email Security DLP capabilities look similar in a feature-for-feature comparison, our testing shows that Office 365's ability to actually detect data leakage falls far behind the Cisco Email Security. Email administrators who need DLP technology for inbound or outbound mail must not depend on Office 365 for protection.

7. Encryption Capabilities

A growing concern of email administrators is the protection of sensitive information in email. While DLP may help to block accidental or malicious transport of sensitive information, partner organizations still have to communicate, bringing requirements for the email administrator to apply additional security, especially encryption.

We looked at the encryption control and encryption capabilities of both Cisco Email Security and Microsoft Office 365 to understand how they support the requirement to keep email communications secure. We looked at multiple levels to see where the big differences are.

The products differ considerably in their feature set. Because Office 365 is a multi-tenant cloud-based service, control of parameters such as TLS cipher set and digital certificates is not available. For security-conscious teams, the lack of configuration control can be important. (Cisco Cloud Email Security is a cloud-based service, but its design delivers a dedicated virtual appliance to each customer, offering the same level of control as in the on-premise appliance.)

Cisco Email Security and Microsoft Office 365 have similar feature sets when it comes to enforcing TLS transport between partners, but Office 365 does not offer higher-level encryption, such as automatic use of S/MIME.

Support for Encryption		
	Cisco	**Office 365**
Low-Level TLS Controls		
Control of TLS and certs, inbound and outbound	Full control	No
Control of TLS encryption on GUI	Full control	No
Select digital certificate for session	Full control	No
Server-to-server encryption		
Enforce TLS encryption for transport	Full controls	High level of control
Business-to-Consumer Encryption		
Send encrypted message based on policy	Yes (included in all licenses), "Cisco Registered Envelope Service"	Yes, requires E3 license, "Office 365 Message Encryption"
Gateway Applied S/MIME		
Detect S/MIME encryption and take actions	Yes	No
Perform S/MIME encryption on messages	Yes	No

Both products offer a service that enforces email encryption, most useful in a business-to-consumer environment. Cisco's product (Cisco Registered Envelope Service, CRES) is included in all Cisco Email Security solutions, while Microsoft's (Office 365 Message Encryption) requires the Enterprise

E3 license. We found Cisco CRES to be more sophisticated than Microsoft Office 365 Message Encryption. For example, CRES lets the system administrator control how replies are handled, while Office 365 Message Encryption does not.

Cisco Email Security and Microsoft Office 365 offer a similar level of encryption support, with Cisco Email Security having a slight edge both in maturity of product and security controls.

8. Action Items for Email Administrators

Email administrators should review the seven risk areas identified in this white paper and compare them to their own requirements and operational environment. Based on the test data provided, administrators should determine the level of additional risk to their organization when using a pure Office 365 solution with no third-party email security gateway.

Based on the additional risk, email administrators should then determine what level of mitigation is needed to match their organization's risk appetite.

Organizations that match one of more of the following categories should strongly consider a third-party email security solution to help mitigate the risks identified:

- organizations that are highly risk averse, or,
- organizations that are sensitive to high levels of spam and false positives, or,
- organizations that have high customer support expectations and requirements, or,
- organizations that experience significant malware issues, or,
- organizations that depend on proper operation of DLP for data protection.

Our testing shows that Cisco Email Security is very effective when combined with Microsoft's Office 365 email services, at reducing security risks and at delivering a higher-quality experience to end users and email administrators.