Cisco Email Security Enhances Office 365 with Advanced Malware Protection

What You Will Learn

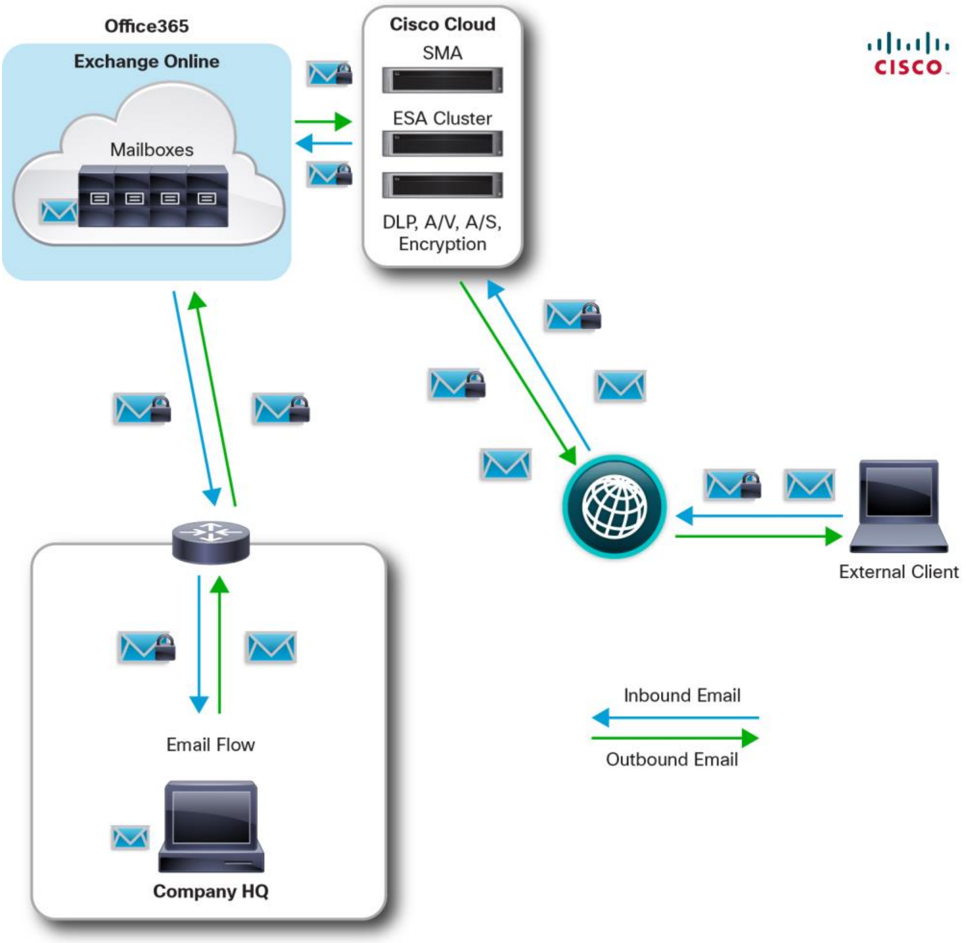
Microsoft Exchange has become the standard email system used by midsize to large-scale organizations globally. With the rise of cloud applications, Microsoft has introduced Office 365. This paper explains how Office 365 customers can boost their email security by integrating with Cisco® Cloud Email Security (CES).

White Paper Conclusions: Why You Need CES with Office 365

CES offers:

- Industry-leading protection from email based threats, including phishing and targeted attacks, with the highest efficacy (99 percent catch rate, less than one in one million false positives)
- Static and dynamic malware analysis (sandboxing) with AMP Threat Grid
- Integrated controls for data loss prevention and highly secure messaging
- Message-level encryption; no third-party products necessary
- Dynamic updates from Cisco Talos services for protection against multivector advanced malware attacks
- Near real-time graphical message tracking, with real-time tracking available from the command line interface
- Dedicated client infrastructure, reducing the risk of outages caused by another customer
- Dedicated monitoring and support for hosted Email Security customers
- Customer-controlled reporting with Cisco support available if needed

Figure 1. Cloud Email Security with Office 365



Note: The Cisco Cloud Email Security components include the Content Security Management Appliance, Email Security Appliance clusters, data loss prevention, antivirus and antispam tools, and encryption.

The Current Environment

We've all been witness to the cloud evolution. Organizations are increasingly moving their operations and resources off site to provide services that were traditionally housed internally. The migration to online services has provided many benefits to companies. Even small businesses can now have enterprise-class redundancy and disaster recovery without the capital outlay for telecommunication, network, and server resources.

Companies looking to gain competitive advantages are realizing that email, once thought not to be mission critical like financial concerns, has become business critical. Companies conduct a large portion of their business by email. Banking, trading, sales contracts, and legal documents, whether secure or not, are all transferred by electronic mail. Companies have realized that a logical step in moving to the cloud is moving mailboxes to the cloud.

Despite the many operational advantages offered by cloud email, these systems are just as likely to be compromised by sophisticated attacks as email hosted on-premises. These threats include zero-day malware, including new, widespread malware distribution and targeted, low volume attacks. Snowshoe spam, which involves sending low volumes of spam from a large set of IP addresses to avoid detection, is an emerging threat. All of these methods have been found to be very effective and often successful at passing through less-powerful spam filters.

The result: Even in the cloud, organizations are bombarded by incessant email attacks from highly sophisticated malware threats with the goal to steal your data and those of your customers.

Microsoft Exchange Online Protection (EOP)

Microsoft EOP is a hosted filtering service that provides protection for Office 365. EOP provides the following features:

- Antispam filters
- Antivirus protection
- Policy enforcement
- Disaster recovery
- Directory services

More information is available at https://technet.microsoft.com/en-us/library/dn762130%28v=exchg.150%29.aspx.

These SLAs and Microsoft Exchange's market position would seem to point customers toward using Office 365 with EOP as their email security solution. However, customer demand for a more in-depth security solution has led Microsoft to provide mechanisms for Office 365 to operate with third-party systems. These include RSA Data Loss Prevention and industry-leading solutions such as the Cisco Email Security cloud and on-premises solutions.

Cisco Cloud Email Security

Cloud Email Security is based on the same industry-leading technology that protects 40 percent of Fortune 1000 companies from inbound and outbound email threats. Customers can reduce their onsite data center footprint and out-task the management of their email security to trusted security experts. Cloud Email Security provides dedicated infrastructure in multiple resilient Cisco data centers to provide the highest levels of service availability and data protection. Customers retain access to (and visibility of) the hosted infrastructure. Comprehensive reporting and message tracking supports exceptional administrative flexibility. This unique service is all-inclusive, with software, hardware, and support bundled for simplicity.

The service offers these best-in-class features:

- **Talos/SenderBase:** Scans traffic around the globe to help protect you from both known and emerging threats, dynamically updating Cisco Email Security solutions every 3-5 minutes.
- **Antispam:** To stop spam from reaching your inbox, a multilayered defense combines an outer layer of filtering based on the reputation of the sender. It also executes an inner layer of filtering that performs a deep analysis of the message. Reputation filtering blocks more than 80 percent of spam before it even hits your network. All this culminates to an industry leading spam catch rate of greater of 99.999+% and a false-positive rate of less than 1 in 1,000,000.
- **Graymail detection:** Graymail consists of marketing, social networking, and bulk messages. The graymail detection feature precisely classifies and monitors these types of emails entering your organization. An administrator can then take appropriate action on each category of graymail.
- **Graymail safe-unsubscribe:** This feature tags graymail with a safe "unsubscribe" option. This option uses the cloud to safely process an unsubscribe request on behalf of the end user. It will also monitor the different graymail-unsubscribe requests. All of this can be managed at a policy, LDAP-group level.
- **Anti-virus:** We offer the choice and flexibility to deploy either Sophos or McAfee Anti-Virus engines. These engines can also run both in tandem, providing a layered approach for additional anti-virus protection.

- **Outbreak filters:** Outbreak filters defend against emerging threats and blended attacks. They can issue rules on any combination of six parameters, including file type, file name, file size and URLs in a message. As Talos learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Outbreak filters can also rewrite URLs linked in suspicious messages. When clicked, the new URLs redirect the recipient through the Cisco Web Security proxy. The website content is then actively scanned, and outbreak filters will display a block screen to the user if the site contains malware.
- **Web interaction tracking:** This fully integrated solution allows IT administrators to track the end users who click on URLs rewritten by Cisco Email Security. Allowing tracking of messages with malicious links, including who clicked on the link and the results of their actions.
- **DLP:** We partner with RSA, a leader in DLP technology, to provide an integrated, all-in-one DLP solution**.** This solution helps ensure compliance with industry and government regulations worldwide, and helps prevent confidential data from leaving your network. This integrated solution enables DLP policy implementation in as little as 60 seconds.
- **Email encryption:** Cisco's encrypted email provides the ability to keep your email confidential — only the sender and the recipient can read the email. Including Secure/Multipurpose Internet Mail Extension (S/MIME) Transport Layer Security (TLS) encryption support.
- **AMP add-on:** This feature delivers improved inbound threat-detection and monitoring. It provides retrospective security, which identifies areas of the network affected by a breach and helps quickly return operations to normal.
  - The AMP license includes the following three features:
    - File reputation: Examines every aspect of a file to determine its security risk.
    - File analysis (sandboxing): Analyzes files in a secure space to determine malicious intent before they enter the network.
    - Retrospective security: Continuously monitors files seen and any disposition changes trigger dynamic reputation analysis and alert the administrator. Detailed information on malware enables remediation prioritization.

Additional benefits include role-based administration, 99.999 percent uptime, co-management, multiple U.S. and European data centers for redundancy, Dedicated IP addresses to avoid shared-fate blacklisting, and financially backed SLAs.

Cisco is proud to be recognized as a leader in the Gartner Magic Quadrant® for Email Gateways 2015.

The Cisco Talos Security Intelligence and Research Group (Talos)

Email Security is part of Cisco's comprehensive family of network security products and services. Organizations are better positioned to detect and respond to threats when using industry-leading products and services that fall under one vendor's umbrella.

Email Security uses Talos, which sees 35 percent of the world's enterprise email traffic, 75 TB of web data per day, 13 billion web requests, 1.6 million deployed devices, and more than 150 million endpoints. Cisco products integrate technology from solutions like Cisco Web Security and Cisco Advanced Malware Protection (AMP) Threat Grid, which address unwanted and potentially malicious URLs and file attachments in email. Organizations need this multivector intelligence to have best-in-class security and protect themselves from the latest of blended threats.

Integrating Office 365 with Cisco Cloud Email Security

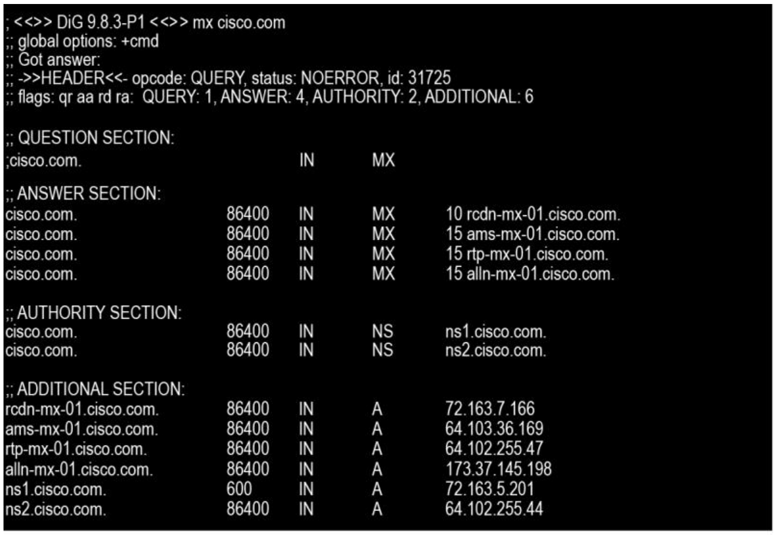
Fortunately for Office 365 customers, Microsoft has made integration with third-party systems fairly easy. The ability to create smart-host connectors for EOP to route email to these systems is well documented. See the Microsoft Exchange library.

Routing Inbound Mail for Spam Filtering to Cloud Email Security

Email routing takes place through the use of mail exchange (MX) records. These records are DNS entries that tell systems where to deliver email. The MX records point to the IP address (usually an inbound NAT translated address on the firewall), which accepts incoming (SMTP) connections. The MX record typically points to an MTA (message transfer agent), which could be a secure email gateway such as the ESA, Microsoft Exchange, Lotus Notes, or an Open Source solution such as Sendmail.

As seen in Figure 2, customers may have many MX records pointing to various IP addresses for redundancy. Cisco Cloud Email Security provides customers with two MX records to provide MX redundancy in addition to data center redundancy.

Figure 2. MX Records of IP Addresses



```
; <<>> DiG 9.8.3-P1 <<>> mx cisco.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31725
;; flags: qr aa rd ra:  QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 6

;; QUESTION SECTION:
;cisco.com.                      IN      MX

;; ANSWER SECTION:
cisco.com.              86400    IN      MX      10 rcdn-mx-01.cisco.com.
cisco.com.              86400    IN      MX      15 ams-mx-01.cisco.com.
cisco.com.              86400    IN      MX      15 rtp-mx-01.cisco.com.
cisco.com.              86400    IN      MX      15 alln-mx-01.cisco.com.

;; AUTHORITY SECTION:
cisco.com.              86400    IN      NS      ns1.cisco.com.
cisco.com.              86400    IN      NS      ns2.cisco.com.

;; ADDITIONAL SECTION:
rcdn-mx-01.cisco.com.   86400    IN      A       72.163.7.166
ams-mx-01.cisco.com.    86400    IN      A       64.103.36.169
rtp-mx-01.cisco.com.    86400    IN      A       64.102.255.47
alln-mx-01.cisco.com.   86400    IN      A       173.37.145.198
ns1.cisco.com.          600      IN      A       72.163.5.201
ns2.cisco.com.          86400    IN      A       64.102.255.44
```

The Story of Acme Inc.

Let examine how the customer Acme Inc. (a fictitious company) would migrate its email security to Microsoft Office 365 and Cisco Cloud Email Security.

Today Acme houses its email systems internally, and all messages are filtered by a homegrown application that hasn't provided the level of protection necessary for Acme's employees. Acme wants to move the employee mailboxes as well as the email security infrastructure to the cloud. To do this, it has selected Microsoft Office 365 and Cisco Cloud Email Security.

Acme's IT staff has arranged for both services to be active and has configured the Office 365 environment with the users' mailboxes. Acme's current MX record points to mail.acme.com. The Cloud Email Security environment has been configured and is ready for production traffic. MX records of mx1.acme.iphmx.com and mx2.acme.iphmx.com have been created. These records point to the Email Security Appliances hosted in redundant Cisco data centers. Acme and its business partner have configured the Cisco cloud protection to route email received for Acme's domain to the Office 365 servers, where they will be delivered to the end users' mailboxes.

Acme's IT staff changes the company's Domain Name System (DNS) MX records from mail.acme.com to mx1 and mx2.acme.iphmx.com. Over a period of up to 24 hours, DNS servers around the Internet will detect this change and begin forwarding email to the Cloud Email Security Appliances for Acme.

Incoming messages will be scanned for spam, viruses, malicious file attachments, and malicious URLs. Other email hygiene will also be performed prior to delivery to Office 365.

Routing Outbound Email to Cloud Email Security

Acme's executive staff has made it clear they want email leaving the organization to adhere to various government regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act. To accomplish this, Acme's IT staff routes outbound email through the Cisco cloud, where policies are enforced using RSA DLP modules as well as the integrated Cisco Email Encryption.

To route the email messages from Office 365 mailboxes to Cisco, an outbound connector must be configured in the EOP system. Customers can follow these steps:

1. In the EOP Admin Center, select Exchange, then go to Mail Flow and click Connectors.
2. In the Connectors, select Outbound Connectors and then Add.
3. Name the connector: Outbound to Cisco Cloud.
4. Specify the recipient domain as *.*
5. Deliver all messages to the following destination: mx1.acme.iphmx.com and mx2.acme.iphmx.com.
6. Select Transport Layer Security (TLS) and select Validation Against Self-Signed Certificate.
7. Save your changes.

In the Cisco Cloud Email Security configure the following:

1. Mail Policies/HAT Overview
2. Add the Office 365 domain: acme.onmicrosoft.com to the RELAYLIST policy and Commit changes.

For more information see:
https://technet.microsoft.com/enus/library/ms.exch.eac.connectorselection%28v=exchg.150%29.aspx

Conclusion

By integrating the two solutions, Acme has all the benefits of hosted mailboxes by Office 365 and the industry's best email protection from Cisco Cloud Email Security.

For More Information

More information about Cisco Cloud Email Security for O365 can be found at the http://www.cisco.com/go/cloudemail or try Cisco Email Security for free.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-727691-01 07/15