Email Security:

A Buyer's Guide

Email Security: A Buyer's Guide

Introduction

The increasing amount of business-sensitive data and personally identifiable information (PII) sent by email means the potential for data compromise and leakage has never been greater. The email threat landscape contains increasingly sophisticated blended threats and targeted attacks. These attacks are aimed at delivering malware that infiltrates the data centers where high-value, business-sensitive data resides. Traditional defenses, including firewalls and endpoint antivirus solutions, cannot deflect these types of attacks.

To meet these challenges, today's organizations need an email security solution that provides layered security. This document examines the requirements that businesses should consider when purchasing an email security solution to defend themselves against spam and viruses, blended threats, and data loss and how Cisco® email security solutions can help.

Buyer's Criteria for Email Security

When evaluating email security solutions, organizations need to assess the following criteria to help ensure they will receive the deeply layered protection needed to defend their business from today's inbound and outbound email threats. An email security solution should offer:

- Big data analytics and collective global security intelligence
- Spam and virus protection
- Threat remediation
- Data loss prevention and encryption
- Deployment options

*Email is the leading threat vector for cyber attacks, according to the Cisco 2015 Annual Security Report.**

Requirement 1: Big Data Analytics and Collective Global Security Intelligence

The increase in big data traversing web and email gateways has gained the attention of hackers. To protect customers from the ever-growing volume of known malware, traditional endpoint security providers introduced "cloud-assisted antivirus," essentially moving signatures to the cloud to provide their entire customer base using collective immunity. However, this solution alone does not protect against advanced malware designed to evade traditional signature-based detection.

Holistic protection can only be achieved through continuous analysis, monitoring a file's behavior even after it has been allowed into your environment. If a file's disposition does change, constant monitoring allows you to detect, contain, and remediate the threat while tracing the infection back to its source.

The Cisco Approach:

- Support from millions of known malware samples and the collective immunity of the Cisco customer community
- Analysis by the Cisco Talos Security Intelligence and Research Group
- Identification of malware based on what it does, not what it looks like, allowing detection of even the newest zero-day attacks
- Cisco Advanced Malware Protectiotn (AMP) to provide deeper visibility, control, and retrospection

*Cisco 2015 Annual Security Report, Cisco, Jan. 2015:

Requirement 2: Spam and Virus Defense

Spam is a complex problem that demands a sophisticated, multilayered solution. According to the Cisco 2015 Annual Security Report, the latest attack methods being used are designed to evade traditional email spam filters by sending "showshoe spam." This attack method entails sending small volumes of spam from many servers and rapidly changing the message content to evade detection. This tactic is a prime example of the need for multilayered email security that provides multiple engines to work together to not only increase protection rates but reduce false positives by serving as a system of checks and balances against one another.

The Cisco Approach:

- Multilayered antispam engine
- Combination of outer- and inner-layer filtering that considers sender reputation to protect spam from hitting inboxes (See Figure 1)
- Cisco Context Adaptive Scanning Engine (CASE) which provides spam capture rates greater than 99 percent and an industry-low false positive rate of less than one in one million
- Scanning of message context as well as content to provide more accurate filtering
- Comprehensive virus defense layered with either Sophos or McAfee antivirus engines (See Figure 2)

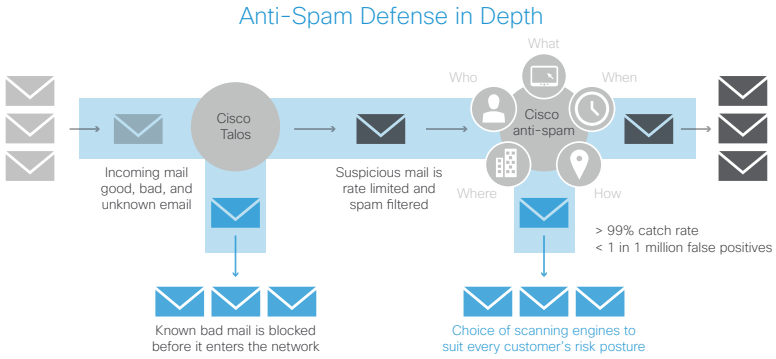

Figure 1. Cisco Antispam Defense in Depth

Requirement 3: Threat Protection and Remediation

Even with a layered approach to email security, some sophisticated attacks will manage to get through the first few layers. Continuous analysis and retrospective security are needed to identify malicious files that evade initial detection and to help defenders determine the scope of the attack so they can quickly contain and remediate the threat.

The Cisco Approach:

- Additional layer of security with Cisco AMP
- AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis; Cisco AMP can identify and stop threats across the attack continuum (See Figure 3)
- Advanced outbreak filters that leverage Cisco Threat Operations Center (TOC) and Cisco Talos threat intelligence to identify, quarantine, and modify rules as they learn more about an outbreak
- Automatic or manual URL rewriting to redirect recipients through security proxy, "defang" URLs, or replace URLs with a notification to the user that part of the email content was blocked

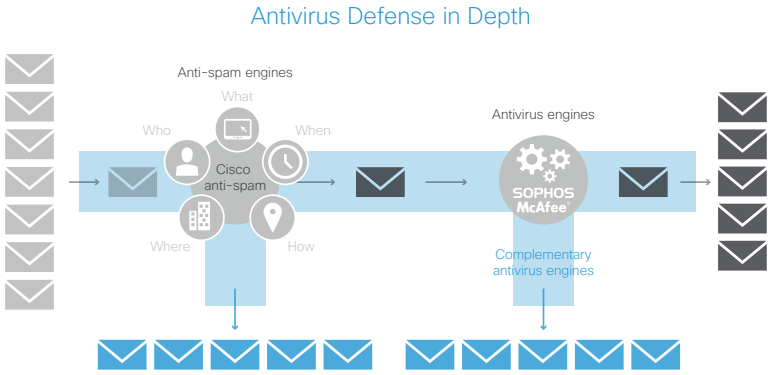

Figure 2. Cisco Antivirus Defense in Depth

Requirement 4: Data Loss Prevention and Encryption

Modern email security solutions that provide the ability to detect, block, and manage risks in outbound email can help reduce the chance of critical data leaving the network either by accident or by design. Solutions with content-aware, policy-based data loss prevention (DLP) and encryption capabilities can offer that protection. Outbound antispam and antivirus scanning, along with outbound rate limiting, helps organizations prevent data leakage, stay in compliance, and keep compromised machines or accounts from ending up on email blacklist solutions.

The Cisco Approach:

- Partnership with DLP leader RSA to deliver more than 100 predefined policies
- Per-message, per-recipient encryption key revocation by either sender or administrator
- Cisco Registered Envelope Service (CRES)—providing user registration authentication as a highly available managed service

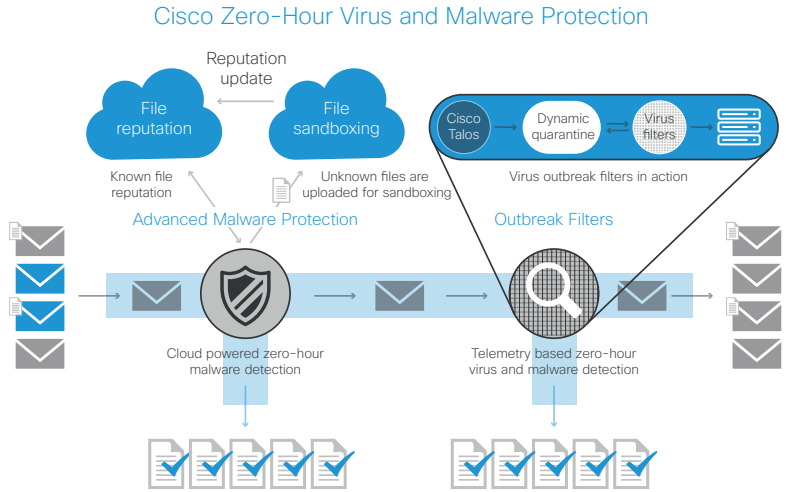

Figure 3. Cisco Zero-Hour Virus and Malware Protectiont

Requirement 5: Flexible Deployment Options

No two organizations have their networks and infrastructure designed the same way. To meet your security as well as operational needs, your email security provider must have flexible deployment options that allow you manage the security solution in a way that makes the most sense for your business; either an on-premise, cloud-based, or hybrid model.

Cisco Email Security Solution

Cisco provides a flexible set of deployment options for the Cisco Email Security Appliance (ESA) (figure 4). Cisco offers these options with support across multiple devices–including desktops, mobile phones, laptops, and tablets–and for Android, iOS, Mac, PC, and Linux.

On-premise – Cisco ESA can be deployed on-premise with an appliance or a clustered group of appliances, either hardware or virtual. Multiple clusters can be used if needed.

Cloud or hybrid – Through these deployment approaches, organizations can handle all inbound and outbound security in the cloud if they don't want the appliance on-premises or would prefer that a third party manage it.

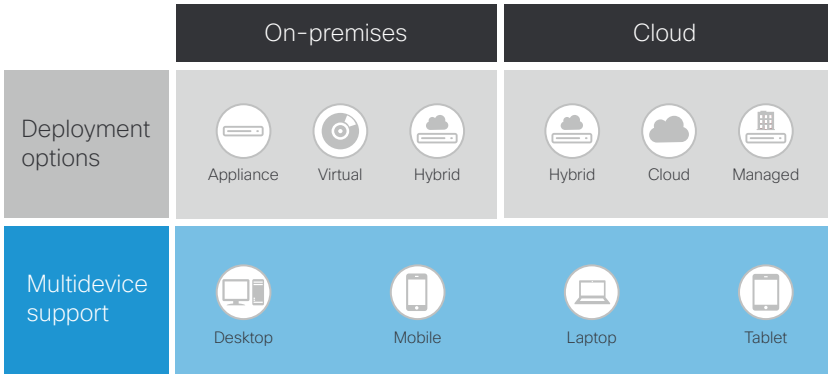

Figure 4. Cisco Email Security Deployment Options

Cisco Email Security Appliance (ESA)	Keeps sensitive data on-premise, with strong performance and easy management
Cisco Email Security Virtual Appliance (ESAv)	Provides quicker deployment, scalability on demand, and the operational efficiencies gained from using existing investments
Cisco Cloud Email Security	Delivers a flexible deployment model for anytime, anywhere email security
Cisco Hybrid Email Security	Provides advanced control of messages on site while taking advantage of the cost effective convenience of security in the cloud
Cisco Managed Email Security	Offers the performance and security of an on-premises ESA with the confidence of Cisco TOC management

Conclusion

To protect data, networks, and users, today's organizations need a threat-centric email security model. They must be able to address all attack vectors and to respond to threats in a continuous fashion at any point, before, during, or after an attack. Robust email security solutions, like those from Cisco, are a core component of a modern security strategy because they rely on real-time intelligence; provide precise access control; and are content-, context-, and threat-aware.

With Cisco email security, organizations can monitor and control data flowing into and out of the enterprise. Advanced threat defense from Cisco starts with the work of Talos. Composed of leading threat researchers, Talos is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem, which includes Threat Response, Intelligence, and Development (TRIAD), Cisco Managed Threat Defense service, and Cisco Security Intelligence Operations (SIO). Cisco CSI is shared across multiple security solutions and provides industry-leading protections and efficacy.

Cisco email security provides:

- **Threat focus** – The solution offers high-availability email protection against the constant barrage of rapidly changing and increasingly sophisticated threats that all modern businesses face.
- **High performance** – Cisco ESA features a layered defense built into a single appliance; it quickly blocks new email-sent threats and spam and stops or encrypts sensitive outbound email.
- **Continuous innovation** – Cisco email security offers the broadest deployment options in the industry. The solution reduces costs with fewer devices, faster integration, and simplified training.

For more information on the Cisco email security portfolio, visit www.cisco.com/go/emailsecurity. A Cisco sales representative, channel partner, or system engineer can help you evaluate how Cisco email security solutions will meet the unique needs of your organization.