Addressing Advanced Email Threats:

Protect Your Data and Brand

What You Will Learn

Since the 1990s, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged.[1] Security has naturally become a top priority. But mass spam campaigns are no longer the only security concern. Today, spam and malware are just part of a complex picture:

- Inbound threats are becoming more organized, more personal, and more pervasive.
- Meanwhile, the potential for outbound leakage is great, with devastating consequences to your reputation and finances.

To combat these threats, Cisco® email security solutions deliver:

- Advanced threat defense
- Superior data security
- Simplified management

A Broadening Inbound Threat Landscape

Email attacks have become increasingly complex and sophisticated.

More Organized

Skilled criminals now form enterprises to create malware, discover exploits, build kits to install malware, and sell botnet spam networks and distributed denial of service (DDoS) attack services. Others sell services that make these ventures more successful. To improve the deliverability of payloads and malicious links, criminals offer programs that test spam against open-source spam filters as well as low-volume spam-bot networks that stay under the radar of many blacklist services.

More Personal

Attacks have become significantly more targeted as well. By scouring social media websites, criminals find information on intended victims and socially engineer spear-phishing emails. These relevant emails targeted to individuals or population segments contain links to websites hosting exploit kits. According to the *Cisco 2015 Annual Security Report*, "Spear-phishing messages, a staple of online criminals for years, have evolved to the point where even experienced end users have a hard time spotting faked messages among their authentic emails."[2]

The report also notes that spam, a primary delivery method for malware-laced email messages, increased 250 percent in volume from January to November 2014.[3]

More Pervasive

Employees once checked text-based email from a workstation behind a company firewall, but today they interact with rich HTML messages from multiple devices, anytime and anywhere. HTML provides more avenues for blended attacks, while ubiquitous access creates new network entry points that blur the lines of historically segmented security layers. Unwitting recipients of email-bound malware propagate the attack by opening an attachment or clicking a URL, thus exposing more employees and infrastructure.

Outbound Email Risks

In addition to threat defense, data security is a top priority for most organizations. The increasing amount of business-sensitive data and personally identifiable information (PII) sent by email means the potential for outbound leakage is great. In July 2014, for example, the global investment banking firm Goldman Sachs Group warned customers of a data breach that occurred when an outside contractor emailed client data, including "highly confidential brokerage account information" to a stranger's Gmail account by mistake; it is not known how many Goldman Sachs clients were affected by the breach.[4]

[1] *Email Statistics Report*, The Radicati Group, Inc.; 2012–2016.; [2] *Cisco 2015 Annual Security Report*, Cisco, Jan. 2015.; [3] Ibid.; [4] "Chronology of Data Breaches," Privacy Rights Clearinghouse, updated Dec. 31, 2013.

In many countries, any email with PII must be sent encrypted. If any unauthorized person can read unencrypted emails, an organization is not in compliance with the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Sarbanes-Oxley Act (SOX), depending on the industry. Hundreds of highly variant regulations add to the complexity and importance of outbound control. Most security solutions offer no way for senders to retract a PII violation or know whether recipients have read the message.

Lastly, compromised email accounts can propagate a virus by launching sudden outbound spam bursts. This leads to a blacklisting of the organization's email domain, even if emails are signed.

The Cost of Inadequate Protection

Given the widespread level of basic protection against unsolicited and malicious email, companies may think they are adequately protected, but new methods are constantly being developed to elude this level of defense. The costs of security breaches then nullify any short-term savings gained from settling for basic protection.

One hundred banks in thirty countries lost hundreds of millions of dollars—and could lose even more in related costs—due to hackers who used botnets to send email containing malware to unsuspecting bank employees.[5] When the employees inadvertently opened the emails, the hackers were able to gain control of the banks' systems using employee credentials.[6]

Outbound mistakes can also damage brand equity, customer trust, and a company's email reputation. A rogue internal sender may drastically reduce an entire company's ability to send email to legitimate recipients. Mistakes may also come with fines for regulatory violations and can result in other financial losses. An email phishing attack that targeted a third-party vendor was reported to be at the root of the Target Corp. data breach in 2013, which exposed the credit card and personal data of more than 110 million consumers.[7] As of February 2015, the U.S. retailer's net breach costs had reached $162 million.[8]

Challenges

Effective email protection requires a global, multiprotocol threat perspective and an infrastructure that addresses the entire attack continuum—before, during, and after the attack. Also required are scalability, flexible outbound compliance and encryption capabilities, and the ability to avoid burdensome demands on the infrastructure.

Cisco email security delivers **advanced threat defense**, **superior data security**, and **simplified management** while lowering total cost of ownership and reducing administrative effort.

Advanced Threat Defense

Fast and Comprehensive Email Protection Using the Largest Threat-Detection Network in the World

Advanced threat defense from Cisco starts with the work of Cisco Talos Security Intelligence and Research Group (Talos). Talos, which is composed of leading threat researchers, is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem. The CSI ecosystem includes Threat Response, Intelligence, and Development (TRIAD), Managed Threat Defense, and Security Intelligence Operations. Cisco CSI is shared across multiple security solutions and provides industry-leading security protections and efficacy.

[5] Jose Pagliery, "What We Know About the Bank Hacking Ring–And Who's Behind It," CNN Money, Feb. 16, 2015.; [6] Ibid.;
[7] Bryan Krebs, "Email Attack on Vendor Set Up Breach at Target," KrebsOnSecurity blog, Feb. 12, 2014.; [8] John Fontana, "Breach costs at $162 million, Target reports," ZDNet, Feb. 17, 2015.

Talos calls on an unrivaled telemetry data set of billions of web requests and emails, millions of malware samples, open-source data sets, and millions of network intrusions to create intelligence that provides a holistic understanding of threats. This capability translates to the industry-leading effectiveness of Cisco security solutions. Our security intelligence cloud produces "big intelligence" and reputation analysis for tracking threats across networks, endpoints, mobile devices, virtual systems, web, and email.

Talos constantly tracks more than 200 parameters, including:

- Reputation lists of domains, URLs, IP addresses, and files to be blocked
- Spam traps that catch emails that may not pass through Cisco appliances
- Honeypots that find attackers so Cisco can analyze their methods
- Crawlers that scan the web making note of malicious content
- Deep file inspections that apply analytics to spot malicious content
- Domain and WHOIS information that is used to build a database of malicious domains

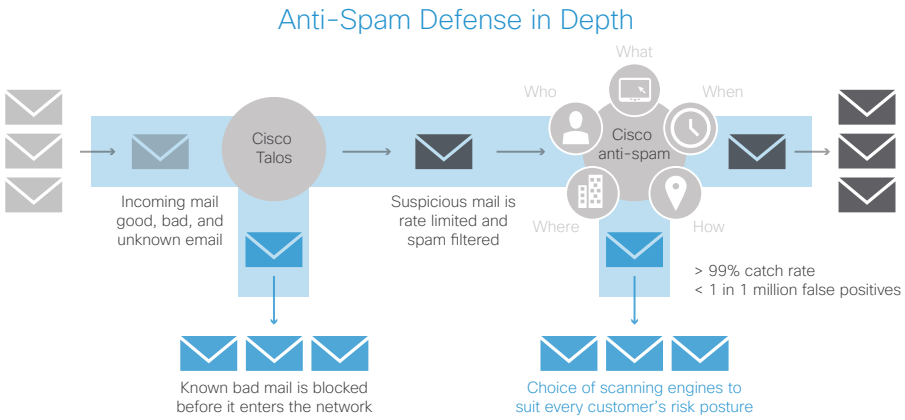
Antispam Defenses

Spam is a complex problem that demands a sophisticated, multilayered solution. Cisco Anti-Spam delivers the highest spam capture rate, with an industry-low false-positive rate of less than 1 in 1 million.

To stop spam from reaching inboxes, Cisco Anti-Spam combines an outer layer of filtering based on the reputation of the sender and an inner layer of filtering that performs a deep analysis of the message. Reputation filtering stops 90 percent of spam before it even enters the network, allowing the solution to scale by analyzing a much smaller payload. The rest is scanned by the Cisco Anti-Spam engine where we ask: Who sent the message, what are its characteristics, and when was it delivered? How long has the email domain been active? Where does a URL in the message take you?

Cisco Anti-Spam determines the reputation and category of the URL as one of the determining parameters. Figure 1 shows how Cisco Anti-Spam works.

Figure 1. Cisco Anti-Spam



Antivirus and Malware Protection

The industry's only proven zero-hour antivirus solution protects against new viruses in less than 60 minutes.

Advanced Malware Protection Add-On

Cisco Advanced Malware Protection (AMP) provides malware detection and blocking, continuous analysis, and retrospective alerting to the Cisco email security solution license. Cisco AMP uses the vast cloud security intelligence networks of Talos to provide superior protection across the attack continuum—before, during, and after an attack.

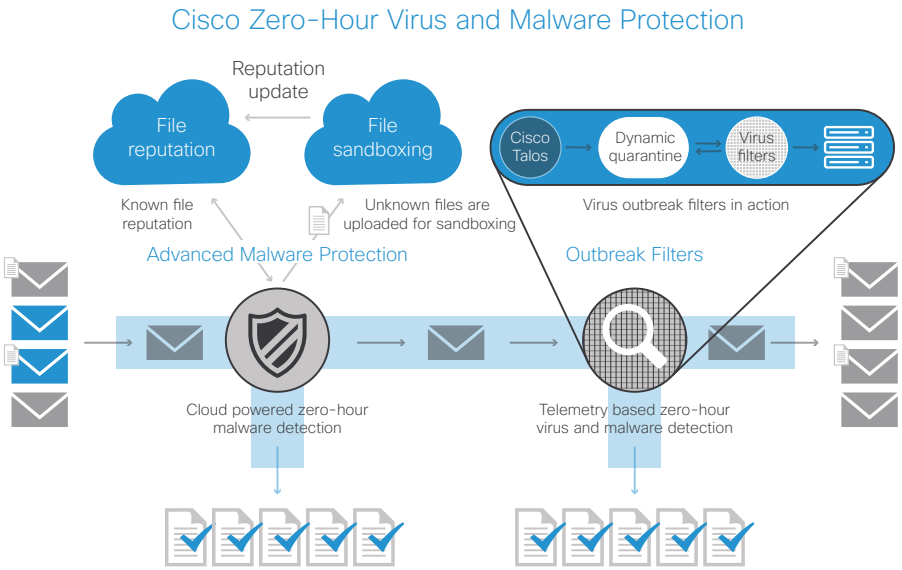
Cisco AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum. Features include the following:

- **File reputation** captures a fingerprint of each file as it traverses the Cisco email security gateway and sends it to the AMP cloud-based intelligence network for a reputation verdict. With these results, you can automatically block malicious files and apply administrator-defined policies. The Cisco email security user interface is the same as the Cisco web security interface, and the policy-reporting frameworks are similar to the ones you already know.
- **File sandboxing** provides you with the ability to analyze unknown files that are traversing the Cisco email security gateway. A highly secure sandbox environment makes it possible for AMP to glean precise details about a file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into the Talos threat intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection.
- **File retrospection** solves the problem of malicious files that pass through perimeter defenses but are subsequently deemed a threat. Even the most advanced techniques may fail to identify malware at the perimeter because techniques such as polymorphism, obfuscation, and sleep timers are highly effective at helping malware avoid detection. Malicious files simply wait until they are inside the network to do their dirty work.

  That's where file retrospection comes in. It provides a continuous analysis of files that have traversed the security gateway, using real-time updates from Talos to stay up to date on changing threat tactics. Once a file is identified as a threat, AMP alerts administrators and gives visibility into who on the network may have been infected and when. As a result, AMP helps you to identify and address an attack quickly, before it has a chance to spread.

Cisco Virus Outbreak Filters provide a critical first layer of defense against new outbreaks an average of 13 hours ahead of signatures used by traditional reactive antivirus solutions. The Cisco Threat Operations Center (TOC) analyzes Talos data and issues rules to quarantine suspicious messages worldwide (Figure 2). As the TOC learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Messages with attachments are held in quarantine until Sophos or McAfee releases an updated signature.

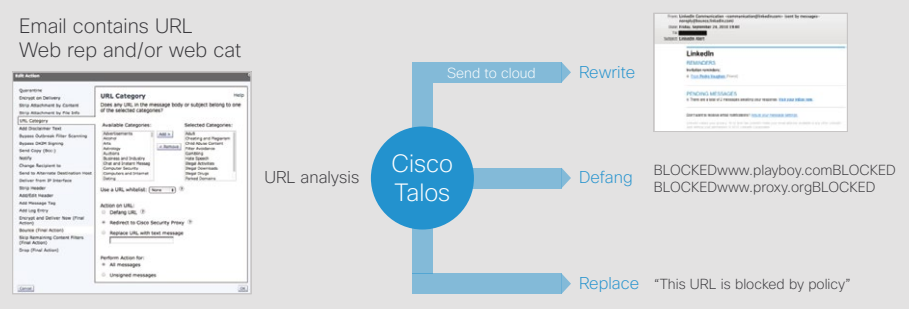
Figure 2. Cisco Virus and Malware Protection



Cisco Virus Outbreak Filters also protect against blended threats or targeted attacks with URL filtering linked in suspicious messages. Cisco email security can either automatically or manually rewrite the URL in order to:

- Redirect the recipient through the Cisco web security proxy; the website content is then actively scanned, and Cisco Virus Outbreak Filters display a splash screen, warning the user that the site contains malware.
- "Defang" the URL, rendering it unclickable.
- Replace the URL; it is removed completely and a message displays, informing the user that part of the email's content was blocked.

Figure 3. Outbreak Filters Defend Against Blended Threats and Targeted Attacks



Superior Data Security

Effective, Accurate, and Simple Data Loss Prevention Policy Enforcement and Email Encryption

Data Loss Prevention: Zero to Compliant–in 60 Seconds

Data loss prevention (DLP) filters are included with Cisco email security solutions. Through a partnership with RSA Security, the leader in DLP technology, our email security solution supplies more than 100 predefined policies covering government, private sector, and custom company-specific regulations. Remediation choices include encryption, adding footers and disclaimers, adding blind carbon copies (BCCs), notifying, quarantining, and more. The RSA Security Information Policy and Classification Research Team creates and automatically updates predefined policies with proven methodology for best-in-class accuracy. With a filter such as "HIPAA," "GLBA," or "DSS," outbound email can be scanned automatically and encrypted accordingly.

For companies needing a complex policy, the building blocks necessary for customization are readily available and make the process quick and easy.

Encryption: Complete Sender Control, No Extra Overhead

Cisco email security is the only solution to offer per-message, per-recipient encryption key revocation that can be done by either the sender or the administrator. The sender of an encrypted message receives a read receipt once a recipient opens a message. Replies and forwards are encrypted automatically to maintain end-to-end privacy and control. To recall a message, the sender can lock or expire a key at any time.

The Cisco Registered Envelope Service provides user registration and authentication as a highly available managed service, with no additional infrastructure for clients to deploy. For enhanced security and reduced risk, only the key is stored in the cloud. Message content goes straight from the sender's gateway to the recipient.

Simplified Management

Complete Control, Always Up to Date

A centralized, custom, consolidated system overview dashboard provides system and work queue status, quarantine status, and outbreak activity, among other critical metrics. The centralized quarantine system provides a single location for email users to self-administer their spam quarantines and administrators to manage policy and DLP quarantines.

Threat-message-detection rules and updates apply automatically without downtime or the need for human intervention. The result is hands-off management and superior protection.

> "With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality."
>
> – Kenichi Tabata, department supervisor, Komatsu Ltd.

Conclusion

Cisco delivers market-leading solutions at scale, using the method that makes sense for your organization.

Cisco offers the following appliance-based, cloud-based, and hybrid solutions:

- **Cisco Email Security Appliance (ESA)** keeps sensitive data on premises, 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.

For More Information

Find out more at www.cisco.com/go/emailsecurity. Work with a Cisco sales representative, channel partner, or systems engineer to evaluate which Cisco products are best for you.