



## Cisco Email Security Appliance Keeps your Critical Business Email Safe

### BENEFITS

- **Faster, more comprehensive email-protection** often hours or days ahead of the competition
- **The largest network of threat intelligence** with Cisco Talos built on unmatched collective security analytics
- **Outbound message protection** through on-box Data Loss Prevention (DLP), email encryption, and optional integration with RSA's Enterprise DLP solution
- **Lower total-cost-of-ownership** with a small footprint, easy implementation, and automated administration that yield savings for the long term

Email is the #1 threat vector for cyber-attacks, according to the 2014 Cisco Annual Security Report. The increasing amount of business-sensitive data sent via email means the potential for leakage is great. Cisco helps you protect your email and eliminate data leakage.

The email threat landscape contains increasingly sophisticated blended threats and targeted attacks. But mass spam campaigns and unsafe email attachments are no longer the only security concerns. By scouring social media web sites, criminals now find information on intended victims and create sophisticated and highly targeted attacks using personal information and social engineering tactics that may be tied to global news events to deceive users.

There are more opportunities for attacks than ever before, according to the Pew Internet and American Life Project Report (May 2011). Employees once checked text-based email from a workstation behind a company firewall. Today they access rich HTML messages from multiple devices, anytime and anywhere. Ubiquitous access creates new network entry points that blur the lines of historically segmented security layers.

It's time to secure your network and protect your users' credentials. The Cisco Email Security portfolio - including the Cisco Email Security Appliance (ESA), Cisco Virtual Email Security Appliance (ESAV), and Cisco Cloud Email Security (CES) solutions - delivers inbound protection and outbound threat control through advanced threat intelligence and a layered approach to security including URL categorization and reputation filtering, antis spam, antivirus, outbreak filters and Advanced Malware Protection (AMP).

## Protecting a Vital Business Asset

Businesses consider email one of their most important systems. Employees and management are more apt to send email than they are to make a phone call, send a package, write a fax or even send a text message. Email is still the number one form of communication, especially for business, according to the “Email Statistics Report, 2012-2016” by the Radicati Group. And email volume is rising. So, a solid email security gateway to help protect your business is vital.

### Changing Email Habits

People aren't just sending email from their desktop computers anymore. They're using mobile devices or laptops to send email from coffee shops, corporate HQ, home offices or airports. Fueling this change is the need to be always connected. By 2016, it has been estimated that at least 50 percent of enterprise email users will rely primarily on a browser, tablet or mobile client instead of a desktop client (“Email Statistics Report, 2012-2016,” Radicati Group). And today's devices are just the beginning - more and more devices are introduced each year and access email through your network.

### Changing Threats

Spammers are making a lot of money. Malware companies are making a lot of money, some more than some of our competitors, which is pretty scary. Email attacks are a multi-million dollar business and they're here to stay.

Spam and viruses aren't going away any time soon. You're going to see things like targeted attacks, advanced persistent threats (APTs) and blended threats. Cyber criminals are getting smarter and more creative.

At the same time, it's more important than ever to protect your organization's sensitive data and to meet the compliance regulations for your industry.

“With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam [are] a reality.”

— Kenichi Tabata, Komatsu. Ltd., Japan

## Cisco Email Security Overview

All Cisco Email Security solutions share a simple approach to implementation. Three Cisco Email Security software license bundles are available, as well as one separate, standalone offering. These are Cisco Email Security Inbound, Cisco Email Security Outbound, Cisco Email Security Premium, and Advanced Malware Protection, respectively. These licenses are supported physically on our x70 or x80 appliances as well as virtually through VMware's hypervisor appliance.

In addition we offer a cloud-based solution that is a complete and highly reliable service with software, computing power, and support. The co-managed user interface is identical to that of the Cisco ESA and Cisco ESAV. You therefore get outstanding protection with little administrative overhead and no onsite hardware to monitor and manage.

Our hybrid solution gives you advanced outbound control of sensitive messages onsite while enabling you to take advantage of the cost-effective convenience of the cloud.

On-premises hardware and virtual appliances come ready to plug in. You can choose the model that works best for your environment to protect inbound and outbound messages at your gateway.

**Table 1. Software Components**

Bundles	Description
<b>Cisco Email Security Inbound Essentials</b>	The Cisco Email Security Inbound Essentials bundle delivers protection against email-based threats, including antispam, Sophos antivirus solution, virus outbreak filters, Category and Reputation-based Web Filtering and clustering.
<b>Cisco Email Security Outbound Essentials</b>	The Cisco Email Security Outbound Essentials bundle guards against data loss with DLP compliance, email encryption, and clustering.
<b>Cisco Email Security Premium</b>	The Cisco Email Security Premium bundle combines both inbound and outbound protections included in the two Cisco Email Security Essentials licenses noted above, for protection against email-based threats and essential data loss prevention.
Standalone Offerings	Description
<b>Advanced Malware Protection</b>	<p>Advanced Malware Protection (AMP) can be purchased à la carte along with any Cisco Email Security Software bundle. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting.</p> <p>AMP augments the antimalware detection and blocking capabilities already offered in Cisco Email Security with file reputation scoring and blocking, file sandboxing, and file retrospection for continuous analysis of threats, even after they have traversed the email gateway.</p>

## Cisco Email Security Features

Feature	Cisco Solution
<b>Threat Defense</b>	<p>Effective protection against email-transported threats requires an informed vision of the threat landscape. That means bringing to bear a global threat perspective and an email protection infrastructure that responds rapidly. Cloud-based intelligence, combined with real-time analytics, is essential to generating zero-day responses.</p> <p>Cisco Email Security delivers inbound protection and outbound threat control through advanced threat intelligence and a layered approach to security including URL categorization and reputation filtering, antispam, antivirus, outbreak filters and AMP.</p> <p>Before an attack, stay protected against the latest threats with Cisco Talos. With a 24x7 view into global traffic activity, Talos analyzes anomalies, uncovers new threats and monitors traffic trends to provide proven, zero-day threat defense often well ahead of competitors. Cisco's broad view of dynamic threats includes:</p> <ul style="list-style-type: none"> <li>• Over 1.6M global devices</li> <li>• Historical library of 40,000 threats</li> <li>• 35% of global email traffic seen per day</li> <li>• 13B+ web requests seen per day</li> <li>• 200+ parameters tracked</li> <li>• Multi-vector visibility</li> </ul> <p>Talos consists of three pillars to provide proactive email protection: SenderBase, Threat Operations Center, and Dynamic updates.</p> <p><b>SenderBase</b></p> <p>Encounter fewer false positives with Cisco's email reputation database, SenderBase. SenderBase, part of Talos, compiles over 200 parameters of data including email volume, domain blacklists and safe lists, domain registration dates and how long domains have been sending email to create a composite IP reputation score. This score ensures email from suspicious senders is blocked.</p> <p><b>Threat Operations Center</b></p> <p>Stay ahead of evolving threats with Cisco's around-the-clock, global coverage that generates new rules using machine-based technology with human ideas behind them. Cisco's Threat Operation Center runs 24x7x365 in five centers worldwide, covering 95 percent of Internet languages. Data feeds from email security devices are compiled along with those from IPS, Firewall and web products. In addition, penetration testing, botnet infiltration, malware reverse engineering and vulnerability research provide insight into current and future threat trends. Those insights are used to create updates that feed into Cisco Email Security.</p> <p><b>Dynamic Updates</b></p> <p>Receive automatic updates to the Anti-spam, Anti-virus and Outbreak Filter engines of your Cisco Email Security solution every 3-5 minutes - over eight million rules each day. Reputation updates also provide real-time protection against known bad senders. Automated content updates reduce exposure windows, eliminate processing of most spam messages and minimize security management overhead.</p> <p>Other solutions for threat defense include reputation filtering, category-based Web filtering, and antivirus.</p> <p><b>Reputation Filtering</b></p> <p>Block known bad email with Reputation Filtering, which is based on threat intelligence from Cisco Talos's reputation database. For each embedded hyperlink, a reputation check is performed via Talos to verify the integrity of the source. Websites with known bad reputations are automatically blocked. Reputation filtering stops ninety percent of spam before it even enters your network, allowing the solution to scale by analyzing a much smaller payload.</p> <p><b>Category-based Web Filtering</b></p> <p>Administrators have the ability to filter specific categories such as gambling and adult sites. If the associated website violates their policy, the URL may be dropped, quarantined or disarmed accordingly.</p> <p><b>Antivirus</b></p> <p>For multi-layer anti-virus protection, choose to deploy either Sophos or McAfee anti-virus engines - or both. Run both antivirus engines in tandem to dual-scan messages for the most comprehensive protection.</p>

Feature	Cisco Solution
	<p>During an attack, use a multi-layered anti-spam approach for comprehensive protection. Cisco combines the outer layer of filtering based on sender reputation and an inner layer of filtering that performs a deep analysis of each message for a defense that stops spam from reaching company inboxes.</p> <p>The emails that pass through Reputation Filtering are scanned with Cisco's anti-spam engine for a greater than 99 percent catch rate and a less than one in one million false positive rate. Drop spam and determine if you want to drop, quarantine or deliver messages suspected of being spam. Cisco also offers optional multi-engine spam scanning technology to catch corner-case spam.</p> <p>Additionally, determine whether you want to deliver, quarantine, drop or bounce marketing messages. Marketing message detection identifies and offers policies for messages typically coming from an aggressive marketer - ones that stem from agreeing to the terms and conditions on a site that shares your data with affiliate companies.</p>
<b>Data Security</b>	<p>Cisco Email Security offers effective, accurate DLP policy enforcement and email encryption. Centralized management and reporting simplifies data protection.</p> <p>Flex and scale to meet the demands of your business with your choice of appliance-based, virtual, cloud-based and hybrid solutions. Cisco's Email Security Appliance and virtual appliance keep sensitive data on-premises. Alternatively, reduce your on-site data center footprint in the cloud. Cisco takes care of policy changes for you, or you have full access to create policy changes as needed. A hybrid option allows for the benefits of the cloud while controlling sensitive data on-site before it leaves your network border.</p> <p><b>Data Loss Prevention</b></p> <p>Protect outbound messages with Cisco Email Security DLP integration with RSA. Ensure compliance with industry and government regulations worldwide and help prevent confidential data from leaving your network.</p> <p>Choose from an extensive policy library of more than 100 expert policies, with a push-of-a-button interface to activate compliance requirements. The predefined data loss prevention policies are included with Cisco Email Security solutions and simplify the application of content-aware outbound email policy. Through Cisco's partnership with RSA, the leader in DLP technology, the email security solution supplies predefined policies covering government, private sector and custom company-specific regulations. Remediation choices include encryption, adding footers/disclaimers, BCC, notify, quarantine and more and can be applied in different fashions depending on the level of severity of the policy violation. For companies needing a complex custom policy, the building blocks of the predefined policies are readily available to make the process quick and easy.</p> <p><b>Encryption</b></p> <p>Give <b>senders</b> control of their content, even after messages have been sent. With Cisco's email encryption, senders don't fear mistyped recipient addresses, mistakes in content or time-sensitive emails because the <b>sender</b> always has the option to lock the message. The sender of an encrypted message receives a read receipt once a recipient opens a message, and secure replies and secure forwards are automatically encrypted to maintain end-to-end privacy and control.</p> <p>Take advantage of the most advanced cloud-based encryption key service available today. Manage recipient registration, authentication and per-message/per-recipient encryption keys with Cisco Registered Envelope Service (CRES). CRES provides all user registration and authentication as a highly-available managed service. There is no additional infrastructure to deploy. For enhanced security, message content goes straight from your gateway to the recipient, and only the encryption key is stored in the cloud.</p> <p>Meet encryption requirements for regulations such as PCI, HIPAA, SOX and GLBA - as well as state privacy regulations and European directives - without burdening the senders, recipients or email administrators. Offer encryption not as a mandate, but as a service that's easy to use and gives the sender complete control.</p> <p>Enable the sender to manually encrypt a message with a simple feature key requiring no desktop software or additional management. CRES can also scan the outbound email and automatically encrypt that message. An email containing encryption-required content is automatically enrolled into the key management system. Once the message has been sent, the sender can log into the registered envelope service and deal with tracking, secure, reply, recall, etc. The administrator can set configurations so that senders receive automatic read receipts.</p> <p>Facilitate easy yet secure access for recipients. The recipient simply needs to open the message, confirm his identity and view the message. If this is the first time a user is asked to register credentials, he will be directed to a site to create an account and establish a password. That password will be used to open this email and all other secure emails sent from the company or from any one of the over 5,000 companies using CRES.</p>
<b>Manageability</b>	<p><b>Universal Device Support</b></p> <p>Ensure all users can access messages when needed, regardless of whether they are on smartphones, tablets, laptops or desktop computers. Universal device support guarantees that secure messages can be read by any recipient, no matter what device is used to open the message. Dedicated plug-in applications offer an enhanced user experience for Microsoft Outlook and on Apple iOS and Google Android smartphones and tablets.</p> <p><b>System Overview Dashboard</b></p> <p>Monitor and report on outbound messages from a centralized, custom System Overview dashboard. Unified business reporting offers a single view for comprehensive insight across your organization. Drill down into any report for advanced visibility.</p> <p><b>Detailed Message Tracking</b></p> <p>Track a message by envelope recipient, envelope sender, subject, attachments, message events including DLP policy or IDs. When you send a message to the Cisco Email Security solution, the message tracking database is populated within a minute or two, and you can see what happened to the messages that are crossing the system at every step of processing.</p>

## Related Cisco Services

<b>Cisco branded services</b>	The Cisco Security Planning and Design Service enables you to deploy a strong security solution quickly and cost-effectively. The Cisco Email Security Configuration and Installation Remote Service mitigates security risks by installing, configuring, and testing your solution. The Cisco Security Optimization Service supports an evolving security system to meet new security threats, with design, performance tuning, and support for system changes.
<b>Collaborative and partner services</b>	The Cisco Collaborative Professional Services Network Device Security Assessment Service helps maintain a hardened network environment by identifying security gaps. The Cisco Smart Care Service keeps your business running at its best with proactive monitoring using intelligence from highly secure visibility into a network's performance. Cisco partners also provide a wide range of additional services across the planning, design, implementation, and optimization lifecycle.
<b>Cisco financing</b>	Cisco Capital <sup>®</sup> can tailor financing solutions to business needs. Acquire Cisco technology faster and see the business benefits sooner.
<b>Cisco SMARTnet Support Services</b>	To get the most value from your technology investment, you can purchase the Cisco SMARTnet <sup>®</sup> Service for use with Cisco ESAs. The Cisco SMARTnet Service helps you resolve network problems quickly with direct, anytime access to Cisco experts, self-help support tools, and rapid hardware replacement.

## Customer Case Studies

**Customer Name:** KOMATSU

**Headquarters:** Japan

**Business:** Worldwide industrial equipment and vehicle manufacturer

Cisco Email Security provided:

- Proactive and reactive threat prevention and management with powerful email security and security management appliances
- An estimated 75 percent increase in the detection of spam within one week of deployment
- Seamless management and updating for low cost of ownership with reduced administrative burdens and downtime

**Customer Name:** Noble Foods

**Headquarters:** United Kingdom

**Industry:** Food production, agriculture, and retail

**Location:** United Kingdom

With Cisco Email Security:

- Over 2 million threats were blocked and 99.3 percent less spam was received in the first six months
- There is now less risk of delays to legitimate email
- An 80 percent decline in spam and virus related IT Service Desk calls was achieved, releasing IT to focus more on business enablement projects

**Organization:** Gobierno de Castilla-La Mancha

**Location:** Spain

**Industry:** Government

With Cisco Email and Web Security:

- Significantly reduced external Internet access malware threats, improving user experience
- Stabilized email security, dramatically improving performance
- Provided easy-to-deploy and manage solutions, freeing up IT staff time to handle other initiatives

**Figure 1.** X80 Appliance



## Why Cisco?

Security is a top priority for Cisco. We've backed that focus with over \$1 billion spent in dynamic threat research and development. Cisco was cited as a leader in the Gartner Magic Quadrant for email and Web security, next generation IPS, and next generation firewalls. Our 37,000 content security customers around the world trust Cisco's high catch rate, low false positives, and low solution complexity along with Talos, the industry's largest collection of real-time threat intelligence. Cisco also has over 10 JD Powers award-winning security support centers to serve customers around the globe and globally dispersed escalation experts, quality assurance, and development staff to meet our customers' needs 24 hours a day, 365 days a year.

**"We needed an intelligent pre-gateway filtering solution that would make it easier to enforce policies and to protect users, without being overzealous and bringing the business to a grinding halt."**

— Ben Gordon, IT Infrastructure Manager, Noble Foods

## Next Steps

Find out more about the Cisco ESA at <http://www.cisco.com/go/esa>. Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner, or systems engineer.




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](http://www.cisco.com/go/offices).

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)