Cisco IronPort Cloud Email Security

Customers of all sizes face the same daunting challenges - higher message volumes and new, evolving email threats. Cisco IronPort® Cloud Email Security delivers leadership with choice, providing superior protection and control with the cost-effective convenience of a cloud deployment model. Based on the same industry-leading technology that protects 40 percent of Fortune 1000 companies from inbound and outbound email threats, the Cisco IronPort Cloud Email Security service allows customers to reduce their onsite data center footprint and out-task the management of their email security to trusted security experts. The service provides dedicated email security instances in multiple, resilient Cisco® data centers to enable the highest levels of service availability and data protection. Customers retain access to (and visibility of) the cloud infrastructure, and comprehensive reporting and message tracking assures maximum administrative flexibility. This unique service is all-inclusive, with software, computing power and support bundled together for simplicity.

The Cisco IronPort Difference

IronPort-powered email security is the foundation of Cisco IronPort Cloud Email Security. This service combines best-of-breed technologies to provide the most scalable and sophisticated email protection available today. Exclusive preventive and reactive technologies, including spam protection, data loss prevention (DLP), virus defense, email authentication, and tracking and reporting tools, work together to enable a powerful security service.

Cisco IronPort Cloud Email Security offers customers the ability to outsource their spam problem to a vendor that provides better efficacy and higher accuracy while allowing more control and visibility into their cloud solution.

Features

Today's email security threats consist of various viruses, spam, false positives, distributed denial of service (DDoS) attacks, spyware and phishing (fraud). IronPort® technology blocks all types of threats, ensuring that companies only receive legitimate messages. Cisco uses multiple methods to provide the utmost in comprehensive email security, incorporating preventive and reactive measures to maximize defense.

Proven Spam Protection

IronPort technology blocks all types of undesirable email messages using a multilayered scanning architecture. This enables Cisco IronPort Cloud Email Security to deliver the industry's highest spam catch rate, greater than 99 percent, with a less than one in one million false-positive rate.

Cisco IronPort Reputation Filters provide an outer layer of defense using data from the Cisco SenderBase® Network to perform a real-time email traffic threat assessment and identify suspicious email senders.

Cisco IronPort Anti-Spam uses the industry's most innovative approach to threat detection, based on Cisco's unique IronPort Context Adaptive Scanning Engine (CASE). This engine examines the complete context of a message, including: **what** content the message contains, **how** the message is constructed, **who** is sending the message, and **where** the call to action of the message takes you. By combining these elements, IronPort Anti-Spam stops the broadest range of threats with industry-leading accuracy.

Powerful Virus Defense

By offering a high-performance virus scanning solution integrated at the gateway, Cisco IronPort Cloud Email Security provides a multilayered, multivendor approach to virus filtering.

Cisco IronPort Outbreak Filters are a critical first layer of preventive defense against new outbreaks - detecting and stopping viruses hours before traditional virus signatures are available.

Integrated McAfee and Sophos antivirus technology is fully integrated to enable multiple traditional virus detection methods and to ensure maximum protection against even the most complex virus attacks.

Advanced Controls

Users can take advantage of IronPort technology innovation to deliver the highest levels of security and control. A range of email authentication solutions are supported by the Cisco IronPort security gateway, including Cisco IronPort Bounce Verification technology and a sophisticated feature set for signing outbound email with SPF. These enable the intelligent mail system to make more accurate decisions.

Sender Policy Framework (SPF) verification and signing means that messages are digitally processed to establish and protect identities with email senders and receivers on the Internet.

Cisco IronPort Bounce Verification tags messages with a digital watermark to provide filtering of bounce attacks at the network edge.

Directory Harvest Attack Prevention (DHAP) tracks spammers who send to invalid recipients and blocks attempts to steal email directory information.

Sophisticated Outbound Filtering Protects Sensitive Information

Outbound filtering is just as important as inbound security. By applying additional message safeguards and policies, outbound filtering helps protect and secure sensitive information.

Content filtering can be used to add headers or footers to email, or to keep email with confidential or inappropriate information from entering or leaving your network.

Transport Layer Security (TLS) uses digital certificates to authenticate the user as well as the network.

Comprehensive Administration and Easy Access for Co-Management

A comprehensive support portal ensures that customers always have access to an extensive knowledge base of subject matter expertise to assist with their needs. Using the Cisco Security Portal, customers can create a customized homepage to quickly access their unique security interests, including the ability to view all current and historical events/tickets, geographical data, security graphics, trends, and network status and performance.

Consolidated and robust reporting options analyze traffic data from geographically diverse infrastructure deployments to provide fully integrated security reporting. IronPort's third-generation reporting technology enables unprecedented insight into even the highest volume networks in the world. Detailed and accurate information is coalesced into clear and informative reports, suitable for all levels of an organization.

Message tracking gives customers real-time visibility into messages. This feature can help resolve help desk calls quickly by determining the exact location of a message. Instead of having to search through log files, the administrator can use the flexible tracking interface to locate messages.

Benefits

Industry-leading technology. A key benefit of Cisco IronPort Cloud Email Security is the opportunity for customers to have their email protected and managed by best-of-breed products and email security specialists. In addition to maintaining the industry's highest spam catch rate and lowest false-positive rate, IronPort technology has been honored with numerous awards. One such accolade is the **SC Magazine** (U.S.) Award for "Best Email Security Solution." Forrester also stated that IronPort email security technology provides "best-in-class" antispam performance.

Dedicated infrastructure. Each customer has a dedicated email security instance, which is racked and stacked in multiple Cisco data centers. The benefit of this is to ensure that your data is protected out of the box, prohibiting data contamination. In addition, the data center is equipped with redundancy, ensuring that your email infrastructure is highly available.

Simplified pricing. The pricing model is based on the number of users per year, and includes all computing power, software, service, and support for the number of users in the contract. If the customer decides to change the type of service, or spam volumes increase drastically, there is no extra charge for additional equipment and protection.

Capacity assurance. Cisco IronPort Cloud Email Security provides a service with the capacity to protect users and maintain peak performance. When spam volumes increase, organizations typically have to purchase new hardware to maintain protection. Cisco IronPort Cloud Email Security alleviates worry from increasing spam volumes and last-minute budgeting for the cost of new hardware. Additional capacity is always included with the simple per-user, per-year pricing model.

Availability. Cisco IronPort Cloud Email Security guarantees 99.999 percent uptime, ensuring that security is always available and working for you through multiple data centers.

World-class support team. Cisco IronPort Cloud Email Security uses industry-leading operational management practices. The team's diverse background is based on knowledge gained from the implementation and operation of advanced security solutions, including the analysis and remediation of millions of security events.

Summary

Cisco IronPort Cloud Email Security is an industry-leading email security service that offers superior choice. With the most flexible service offerings, it provides customers with a powerful solution to meet their unique needs. Customers maintain control and visibility into their cloud infrastructure, while reducing their onsite footprint with a robust, multilayer email security solution that resides in Cisco data centers. This out-tasking model gives customers peace of mind, knowing that their organization is protected by email security experts.

Try Before You Buy

The best way to understand the benefits of Cisco IronPort Cloud Email Security is to participate in the "Try Before You Buy" evaluation program. For additional information, please visit: http://www.ironport.com/try.

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 C78-701313-00 02/12