

Industrial Strength Email Security. For All.

Why You Need the IronPort C-Series Email Security Appliance



COMPANIES OF ALL SIZES MUST BE ABLE TO COMBAT THESE THREATS:

SPAM

- Spam has become the most recognizable threat to e-mail. No longer simply a nuisance and distraction, it now has a direct impact on employee productivity.
- In some cases, spam can be as much as 80% of a corporate inbound mail, and it often seems to increase overnight.

IronPort Defends With its unique ability to track a sender's behavior over time, IronPort has invented the world's most sophisticated spam filtering technology. Used by large companies such as AOL and Cisco, IronPort appliances recognize more than 96% of all incoming mail as spam, viruses or malicious traffic – stopping it before it even enters the corporate network.

VIRUSES

- The industry has seen a consistent increase in e-mail as the transport for over 80% of virus exploits today and growing.
- Virus writers continue to become more creative, often using social engineering techniques, increasing the cost to clean up an outbreak.
- Disaster recovery costs increased by 23% in 2003.

IronPort Defends By monitoring email traffic patterns, IronPort appliances can recognize anomalies associated with virus proliferation on a global level. IronPort Virus Outbreak Filters have the unique ability to predict virus outbreaks.

FALSE POSITIVES

- Attempts to eliminate spam with old or inadequate solutions can often result in false positives.
- Many enterprises have been found expending additional resources to sift through mail trash, in search of legitimate communications.
- Often, users simply stop trusting the e-mail system and ask to see all mail being sent to them. Although the cost of these types of actions can be extremely high, it is also difficult to calculate.

IronPort Defends IronPort Reputation Filtering technology identifies both benign and malicious senders. Mail from known and trusted sources is automatically routed around the content based spam filters, significantly reducing the potential for false positives.

DIRECTORY HARVEST ATTACKS

- By validating the legitimacy of receiving addresses, this threat exposes enterprise users to future spam and viruses.
- These attacks waste time and critical system resources, strictly for the benefit of malicious email senders.

IronPort Defends All IronPort appliances have unique directory harvest attack prevention capabilities. If a malicious email sender attempts to deliver messages to more than a specified number of invalid addresses, the IronPort appliance will continue to accept these messages. This protects the email directory by making it that much more difficult for the sender to determine which addresses are actually legitimate receivers.

REGULATORY COMPLIANCE

- New Federal and State regulations require businesses to be responsible for filtering outgoing mail and stopping the spread of unauthorized information.
- Failure to fully comply with these regulations can result in both severe legal penalties and government fines.

IronPort Defends IronPort not only makes it simple to become fully compliant with regulations, but also helps implement corporate policies to ensure companies remain in good standing. To keep your internal data safe and secure, IronPort provides easy-to-implement modules for Sarbanes-Oxley, HIPPA and GLB compliance.

WHAT'S NEXT?

The nature of email threats is continually changing. Motivated by the potential for profit, malicious email senders are creating new ways to obfuscate their identities and sell products or swindle financial information from end users. These techniques can be highly disruptive to business and drive up IT costs considerably. IronPort is committed to stopping these dangers in whatever form they take. To identify and block harmful mail, IronPort appliances receive more than 40,000 daily rule updates. At the same time, IronPort is working with ISPs and corporations to create new standards that will greatly diminish these threats by providing the world's leading email security solution.

