Evios

A Managed, Enterprise Appliance
for Identifying and Eliminating Spam

Introduction

Electronic messaging (e-mail) is a mission-critical business tool that has been compromised by the proliferation of Unsolicited Commercial E-mail (UCE or "spam"). The excessive growth of spam has resulted in cost shifting and resource abuse for enterprises worldwide. Spam increases network congestion, drives up CPU utilization, uses bandwidth, consumes disk space and distracts employee attention.

Spam is different from postal mailings or telemarketing in that the cost of traditional marketing is paid by the sender, whereas a spammer bears a relatively small percentage of overall message delivery costs. For spammers, the enterprise receiving the spam, the Internet service providers forwarding the spam, and the other enterprises that maintain Internet hardware are the ones paying for the spam transmission. A typical spammer will send out over 250,000 spam messages each day.

"Spam will cost U.S. businesses more than $10 billion in 2003!"
- Ferris Research

According to IDC, there were 31 billion e-mails sent each day in 2002, of which 5.6 billion, or nearly 18%, were spam. Gartner research suggests that spam is growing at 1000% per year and will account for 50% of all e-mail traffic by 2004. Ferris Research estimates that spam will cost U.S. businesses more than $10 billion in 2003! Osterman Researchers estimate that in 2002, a 5,000 person company lost over $344,000 in productivity costs because their employees wasted over 12,500 hours just deleting spam. The Spamhaus Project reports that 60% of all western Internet e-mail is spam. That number is expected to grow to 70% by January, 2004.

A. The impact of spam

The cumulative costs of spam add up quickly when e-mail users spend just a few minutes a day dealing with spam. Assuming employees never open a spam, this few minutes adds up to several hours per year. When multiplied by the number of employees, the result is a significant amount of lost productivity. Spam also increases mail server processor loads, storage space and bandwidth usage.

"Chevron settled out of court with four female employees for $2.2 million after they were exposed to offensive e-mail messages"

Gartner Group suggests that up to 25% of all spam contains pornographic or otherwise offensive material. Furthermore, 70% of all Internet porn traffic occurs between 9am and 5pm. USA Today reports that 50% of employees acknowledge having received offensive or inappropriate content via e-mail while at work. Some of these e-mails will find their way throughout the enterprise. If other employees find these e-mails offensive, the enterprise could find themselves liable for the actions. In 2002, Chevron settled out of court with four female employees for $2.2 million after they were exposed to offensive e-mail messages forwarded by male co-workers, including one listing "25 reasons beer is better than women." This is not an isolated case and has compelled enterprises to fire otherwise-valuable employees under similar circumstances rather than risk high-dollar lawsuits.

Widespread use of the Internet and e-mail has made it possible for viruses to spread globally in less than 24 hours. Infected messages can be spread throughout entire enterprises via mail servers and cause immediate and costly business outages.

"Enterprises utilizing wireless device technology … are paying for spam twice - once into the enterprise, and again to the wireless device"

Enterprises utilizing wireless device technology can incur significant costs in both productivity and bandwidth due to spam. When spam is transmitted from the enterprise mail server to the wireless device, the enterprise is paying for that spam twice - once into the enterprise, and again to the wireless device. This is a significant cost if the wireless device charges per mail message or by bandwidth. As unwanted messages flood wireless devices end-users will no longer utilize the technology as a viable mode of communication

B. How can Evios help?

Evios is a dynamic anti-spam filtering appliance that analyzes all incoming messages and deals with them according to user defined rule sets and standards. Based on the analysis, the filtered mail is bounced, deleted, forwarded to your internal mail server for delivery, or tagged for special handling at the server and/or client. The dynamic nature of Evios allows filtering of Day Zero viruses and worms by special handling (or the removal of) executable attachments. This means that when a new virus is launched, your enterprise won't have to wait the days or weeks for a patch to be developed and made available for download. By removing executables from mail messages, Evios provides added protection against viruses that can cause costly network outages.

"This advanced combination of spam filtering techniques gives Evios the edge in identifying and eliminating spam before entering your network"

The Evios heuristic framework analyzes the behavior of the sender of each message, the body of the message, and the headers. Evios then utilizes Bayesian filtering, fingerprinting, blacklist/whitelist/greylisting and other technologies to determine a "score" for each message. This advanced combination of spam filtering techniques and user definability gives Evios the edge in identifying and eliminating spam before entering your network. All settings are definable by domain, sub-domain or by individual user, making Evios both powerful and flexible.

"Installation is simple and will not cause loss of e-mail, inhibit your network performance, or require complex configuration changes to your routers or firewall"

Evios is a fully secured appliance that sits in front of the firewall outside your network. Thanks to this configuration, mail is validated and spam is categorized prior to entering your network, before it can consume network and human resources. Furthermore, most viruses can be stopped before they can get into your network and cause damage. Installation is simple and will not cause loss of e-mail, inhibit your network performance, or require complex configuration changes to your routers or firewall. Evios utilizes state-of-the-art IBM X-Series servers for enhanced performance and dependability.

As a fully managed appliance, Evios does not require additional maintenance by the network admin. Occasional updates to the whitelists and blacklists (if needed/desired) through the web-based GUI (graphical user interface) require minimal input. This allows the network admin to proactively maintain the network. Mail By-Design will remotely administer any updates, patches or fixes as they become available.

Evios is built on a platform that allows incorporation of new anti-spam technologies as developed. This capability allows easy upgrades in a single location that will benefit the entire network – your network administrator will no longer need to upgrade multiple servers or hundreds of desktops to hurriedly apply a patch or block a day zero virus.

“Evios is scalable to meet the needs of large enterprises and service provider environments.”

Evios is available in multiple configurations to accommodate small businesses and large enterprises alike. Evios Lite is available for small businesses with fewer than 100 users. This version provides the power and flexibility of Evios in a cost-effective shared environment for customers with lower e-mail volume. Evios is scalable to meet the needs of large enterprises and service provider environments. High-availability designs can be implemented to handle large volumes of e-mail without degrading network performance or adding a single point of failure.

Evios has full reporting capabilities and keeps extensive logs of e-mail traffic through the appliance; reports are available through the web-based GUI.

C. Conclusion

Spam is a serious issue for practically all Internet-connected enterprises. The best solution is to filter unwanted content before it enters your network. As an external, managed appliance, Evios provides the most complete enterprise anti-spam solution and will save your enterprise time and money.

“Evios can help increase your bottom line.”

By filtering spam and unwanted content, Evios enables an enterprise to protect its network and e-mail systems. By preventing pornographic and offensive material from entering an enterprise, Evios can help reduce liability exposure. As a managed service, Evios minimizes time spent on integrating, updating, and maintaining e-mail systems. Evios will help increase your bottom line.

For a free 30 day demonstration of EVIOS, call 314.786.1000 x 103