The Radicati Group, Inc.
595 Lytton Avenue
Palo Alto, CA 94301
Phone 650-322-8059
Fax 650-322-8061
http://www.radicati.com

The Radicati Group, Inc.

Trend Micro Anti-Spam

Innovative Defense Against Evolving Spam

A White Paper

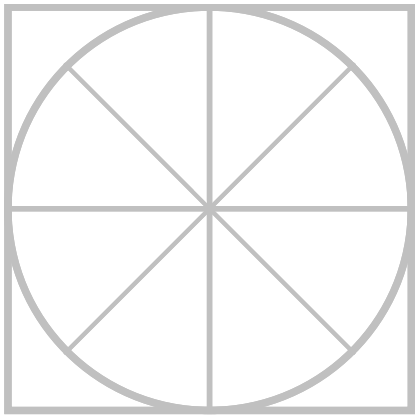

TABLE OF CONTENTS

1. INTRODUCTION

Spam has rapidly turned from a mere nuisance into a major security threat and financial drain for organizations worldwide, as they attempt to stem the flood of unsolicited bulk email while ensuring that legitimate correspondence is delivered correctly. While at first spam was relatively easy to block through the use of blacklists or basic content filtering techniques, spamming methods have advanced to the point that these technologies are no longer sufficient or cost-effective. Therefore, anti-spam technologies have had to evolve with spam to stay effective in this adversarial environment.

The financial costs associated with spam are large and growing. First, there is the loss of employee productivity due to time spent managing their inboxes and junk email folders, requiring employees to delete spam and block senders. But perhaps even more costly for businesses is the large volume of spam that enters company networks, which can choke mail servers and occupy expensive space in email quarantines and storage archives. This inundation of spam results in reduced bandwidth, slower email delivery, and higher storage costs. To make matters worse, spam is often a mechanism used to carry viruses, malware, and numerous other security threats which can compromise sensitive information, damage a network, and cause significant cost in terms of network downtimes and repairs to infected systems. Finally, there is the challenge of successfully blocking spam while at the same time avoiding the accidental deletion of valuable business email.

Table 1, below, shows the extent to which daily messaging traffic is saturated with spam, and how the volume of spam is projected to grow through 2010. In 2006, the Radicati Group estimated spam comprised 70% of the total worldwide messaging traffic, and this number is expected to increase to 79% by 2010.

Worldwide Spam Messages, 2006-2010					
	2006	**2007**	**2008**	**2009**	**2010**
Worldwide Messages/Day (B)	**173**	**222**	**282**	**357**	**442**
Worldwide Spam Messages/Day (B)	122	160	209	272	351
Total Spam%	70%	72%	74%	76%	79%

Table 1: Worldwide Spam Traffic, 2006-2010[1]

[1] From "Corporate Email Market, 2006-2010" Copyright © December 2006 The Radicati Group, Inc.

Clearly with such an influx of unwanted, dangerous junk mail, it is necessary for organizations to broaden their efforts at combating spam by applying a new generation of anti-spam solutions that leverage multiple layers of protection, including reputation services. In a nutshell, reputation services maintain an accurate knowledge about the nature of the email sender or embedded URL. If the sender is known to send spam or other malicious email or the link in the email connects to a malicious Web site, a bad reputation is assigned, ensuring that only emails from good sources are accepted.

This white paper looks at the evolution of anti-spam techniques, including reputation services and their benefits, Trend Micro's innovative approach to fighting spam, and Trend Micro's anti-spam security solutions.

2. THE EVOLUTION OF SPAM TECHNIQUES AND ANTI-SPAM TECHNOLOGIES

Unsolicited bulk emails, or spam, started in the 1990s. At that stage, no anti-spam engines existed, enabling spammers to create simple emails to convey their message. As these emails began to increase, they became an annoyance and started to hinder businesses, giving birth to the first anti-spam filters. Since then, there has been an adversarial relationship between spammers and anti-spam solution vendors. Spammers continue to evolve their techniques to bypass filters while vendors respond with more innovative approaches to defeat these spamming techniques. The following provides an overview of how spamming techniques and anti-spam technologies have progressed over time.

Whitelists and Blacklists - are a straightforward method of blocking spam using lists of email addresses, IP addresses, and/or domains that are considered safe (whitelists) or unsafe (blacklists) to determine whether to accept or block messages from a sender. There are several public blacklists that are utilized by email security vendors today, such as Spamhaus, SORBS, DSBL, and many others.

In the early days of email, companies could rely more heavily on blacklists and whitelists, as email was not used as extensively for communication as it is today. It became more impractical to rely on these techniques, however, as email traffic continued to increase. In addition, these lists depend largely on recipient submissions. However, recipients often mistakenly or inappropriately place IP or sender addresses on blacklists.

The growing usage of zombies and botnets has also made blacklists much less effective in blocking email. Zombies are computers that, unbeknownst to their owners, have been infected with malware that forces them to send spam emails. Botnets are a collection of multiple zombie computers that are controlled by a single spammer source, giving the spammer the ability to send mass emails with multiple machines. With this technique, otherwise legitimate email senders may be placed on blacklists because of their infected computer. Because blacklists are static, it can be difficult for users of infected computers to get their names removed from blacklists even if they have cleaned their computers and are once again only sending legitimate emails.

Content Filtering – was created as a complementary anti-spam technology to blacklists. Blacklists attempt to block spam from known spam senders while content filtering was introduced to prevent spam delivery from unknown spammers by inspecting the email body. This simple technique works by scanning the message body and subject line for keywords that flag a message as spam, such as words related to pornography, gambling, etc. This was one of the early anti-spam methods and is relatively easy to implement. It was initially effective because spammers were fairly straightforward in their messages, in that they did not try to bypass anti-spam filters. Content filters were able to easily detect spam keywords in the bodies of messages. This technique, however, was susceptible to false positives, because many of the spam keywords also had legitimate uses. Furthermore, spammers began using methods that could easily bypass these filters through the use of techniques that would obscure content, such as misspelling, spacing, symbols to replace letters, or more recently, images in messages.

Context Filtering – is similar to content filtering (and often labeled as such), and relies on scanning messages for specific word groups within a defined context, making it somewhat more effective than simple content filtering. This method is particularly helpful when differentiating the use of terms in a specific industry context versus spam. For example, the term Viagra can have legitimate uses in the healthcare industry but is also a strong indicator of spam. Context filtering can help identify these different circumstances.

Just as with content filtering, context filtering is easy to implement. Unfortunately, it shares the same drawbacks as content filtering in that it can be easily bypassed by more advanced types of spam.

Signature Filtering – uses a known spam email to block all identical spam messages. Initially spammers would send out the same spam email en masse. They could simply create one spam email and send it out to an extensive email list. Signature filtering was designed to combat this spam approach by capturing "signatures" of known spam emails. If an incoming email matches the signature of a known spam message the email is immediately blocked. This anti-spam technology is a good complementary technique in that it will block obvious spam messages with very low false-positive rates. However, spammers now bypass this approach by using templates to randomize spam emails. Small variations in each spam message make each email unique. A signature will not match an email if it is slightly different.

Heuristics Filtering – is a rule-based approach that looks for spam indicators in emails. Unlike simple content and context filters, heuristics filters can be coded to be quite sophisticated and complex. This approach was developed to detect the tricks spammers began using to try to fool anti-spam filters, with rules to detect several devious spamming techniques such as "transparent" font colors, tiny font, deceptive URLs, and more.

Heuristics filters are only effective when their rules are well-written and kept up to date. They require constant maintenance to remain effective, as the rules are static and spammers are continually finding ways to bypass these rules. Poorly written heuristics filters also have the tendency to have a high false-positive rate, leading to legitimate emails being misidentified as spam.

Statistical Filtering – is an advanced anti-spam technique that uses statistics to determine whether an email is spam. One approach to statistical filtering is to create a "score" for the email based on the number and weight of the spam indicators identified in the email. The email is determined to be either a spam or good email based on the score threshold. Often users can modify the anti-spam sensitivity by adjusting this threshold.

Other statistical filtering methods can "train" the filter using samples of spam and non-spam emails to determine the statistical probability that incoming emails are spam messages. This technique goes beyond the static rules of heuristics and uses a learning-based approach. The more email that is processed, the more effective the filter is.

The major downside of statistical filters is that they must be well-tuned or well-trained to keep up with newer spamming techniques. The spam indicators must represent current

spam trends and appropriate weights and score thresholds must be assigned. If using a training method, the email training sets must be updated frequently with large, representative email samples or the statistical filtering will be ineffective.

Even if statistical filters are maintained correctly, many spammers have developed methods which make it difficult to analyze the content of emails. For example, image spam displays the spam message in an image and not in text in the email body, making it more difficult to identify the spam indicators. Image spam has been successful in circumventing most advanced filters, and requires more innovative solutions than the ones listed above.

In addition, most of the anti-spam methods discussed above require emails to enter the network to be scanned. With the current inundation of spam, scanning these emails within the network can require costly resources and may overload the system. In today's spam environment, anti-spam solutions must be optimized to keep the bulk of email threats completely off of the network.

3. REPUTATION SERVICES

The problem of filtering out email without burdening the email infrastructure is almost a paradox. How does one stop spam effectively without bogging down email systems? And how does one accomplish this while keeping up with the latest threats, such as image spam, while at the same time ensuring a zero false positive rate?

The best approach to preventing the majority of today's spam from entering an organization is to block it at the perimeter, before it even enters the gateway. This is best accomplished through the use of reputation services, which are designed to accurately identify spammers and block their emails from even reaching the organization's network.

Reputation services work by leveraging a vendor's customer, partner, supplier base, or research lab to monitor messaging traffic. Unlike simple blacklists, reputation services continuously analyze the sending behavior of IP addresses and domains to determine if they are sending legitimate or illegitimate email. By identifying the sources of spam and other email threats, reputation services can block email based on the sender without having to scan the content of the email, increasing effectiveness, lowering false positives, and reducing the burden on the network.

In addition, reputation services can be applied to the URLs embedded in emails. If a link connects the user to a spam site or other malicious Web site, the URL is given a "bad" reputation. An email containing a URL with a bad reputation is automatically blocked. This keeps that email out of the inbox and prevents employees from following the link and falling victim to Web threats, such as malware downloads, phishing sites, and more.

Effective reputation services collect an email history and email samples from sending IP addresses or data on Web sites. A company that provides reputation services should be able to support why they have given an IP address or URL a "bad" reputation. Reputation services should also continually update their lists, as zombies and botnets are now responsible for most spam on the Internet. As victimized computers remove the bot code and once again send good email, they should no longer be blocked as having a bad reputation.

The main benefit of reputation services is that they keep spam and other email threats completely off of the network. Reputation services are highly effective because they block emails from IPs and domains known for sending bad email. They do not scan the body of the email, so they are not subject to the content tricks used by spammers. By keeping threats off the network, reputation services ensure the network stays secure and save costly bandwidth and storage.

Other anti-spam techniques can be highly effective at blocking spam if they are well maintained. However, the high levels of spam traffic can overwhelm the system. By eliminating much of the traffic that hits organization's email systems, reputation services have become a required component of an effective anti-spam solution.

4. TREND MICRO'S ANTI-SPAM TECHNOLOGY

Trend Micro's anti-spam solution involves a multi-level defense that strategically removes most spam before it enters the gateway and blocks any remaining email from entering the inbox. Trend Micro's anti-spam approach encompasses the following components:

- **Trend Micro Network Reputation Services**
- **Trend Micro IP Profiler**
- **Trend Micro's Anti-Spam Composite Engine**

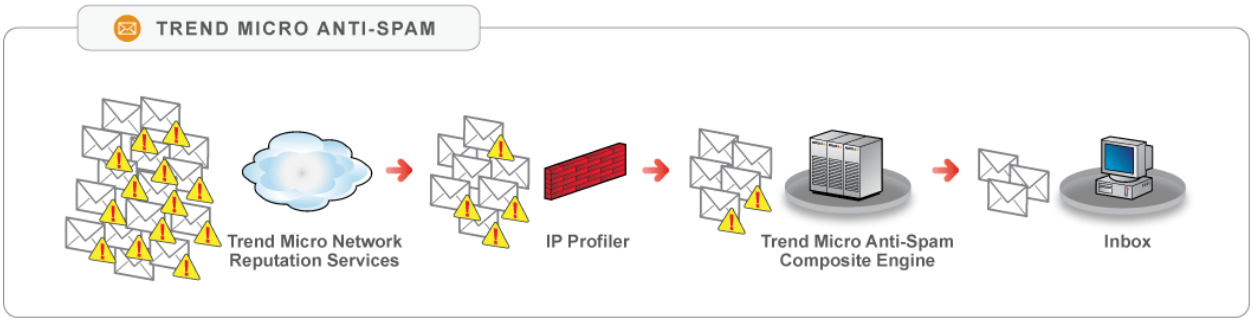

Figure 1: Trend Micro's Three-Tiered Anti-Spam Defense

Through these components, Trend Micro offers a three-tiered solution that gives its customers an impenetrable spam defense while keeping legitimate email flowing smoothly with a very low false positive rate.

Trend Micro Network Reputation Services

Trend Micro Network Reputation Services monitors millions of messages per day, identifying spam and applying a reputation to individual sender IP addresses. By blocking senders with a bad reputation, organizations benefit from increased security and reduced storage, processing, and bandwidth costs.

While several email security solutions use reputation services to help block spam messages at the SMTP gateway, Trend Micro differentiates itself by leveraging nearly a decade's worth of global network reputation information. Network Reputation Services applies ratings for over 1.6 billion addresses supported by sending histories and spam samples. With this expertise, the service is able to stop up to 80% of spam before it reaches an organization. Other similar reputation services have only been monitoring IP reputations and messaging traffic for the past few years. These other vendors do not have the breadth of email sender knowledge and they cannot support their reputation determinations with extensive histories.

The Trend Micro Threat Prevention Network deploys a global IP monitoring system that detects network behavior and anomalous activity. The network currently consists of eight data centers distributed throughout the world supported by Trend Micro's global customer base that gives the company a very large data pool with which to monitor messages and their senders.

Working around the clock, the Threat Prevention Network assures 100% availability and millisecond response times. The network even detects spamming zombies and botnets in their early stages, which other reputation services and filters are often unable to catch. Reputation investigators determine the IP source and define the threat profile, continually updating reputation ratings to ensure accuracy. Using attack behavior and history, threat experts conduct up-to-the-minute due diligence to determine new listing status and, similarly, expiration when security integrity is restored. Combining real-time availability and an auditable methodology of sender histories and email samples, Trend Micro provides a very reliable reputation service.

Another way in which Trend Micro differentiates Network Reputation Services from other vendor offerings is through its administrative console, providing companies with both in-depth insight and flexible administrative control. Organizations can play a more active role in their spam prevention efforts with the ability to access global spam information, view reports, and create or alter policies for approved and blocked sender IP lists.

The administrative console includes a global spam update that provides a brief overview and discussion of current spamming tactics and their implication for organizations. The console also displays the total spam volume received from the top 100 ISPs for a specific week. This ranking changes daily as spam sources and volumes change.

Using this spam overview and ISP information, customers can enhance the protection they receive from Network Reputation Services by creating and updating approved and blocked lists. These lists can be based on individual IP addresses and Classless Inter-Domain Routing (CIDR). Organizations can create blocked lists based on country or ISP selected from drop down lists provided in the console, making it easy for organizations to block spam sources based on current global spam information.

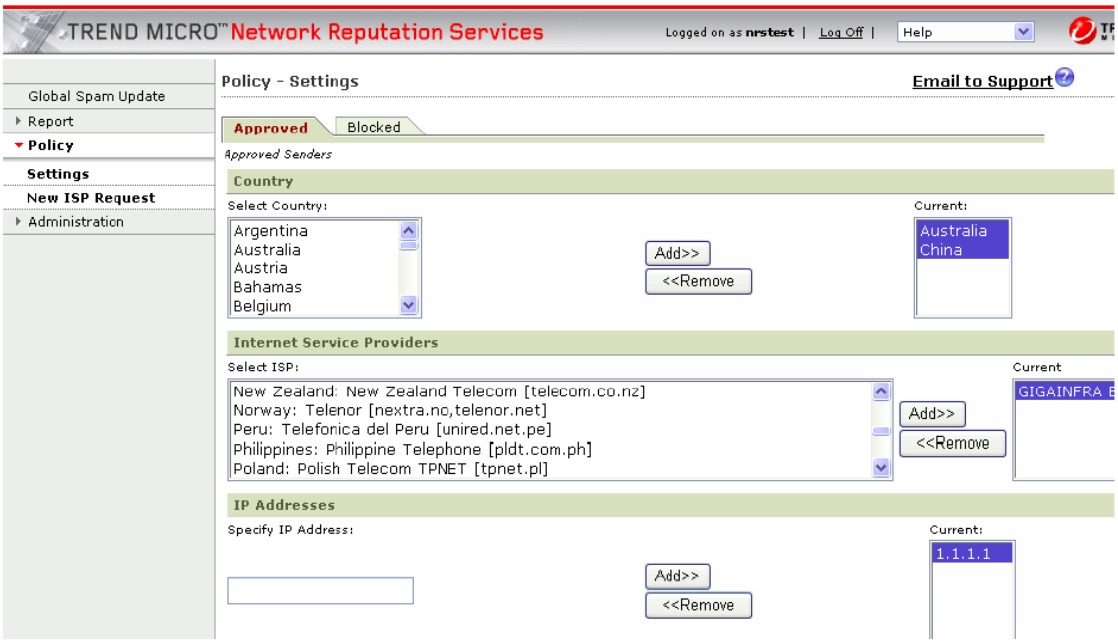

Figure 2: Network Reputation Services Administration Console, Policy Setting

Network Reputation Services is based on one of the industry's leading reputation databases and provides easy administrative options to provide additional protection. This service keeps most threats completely off of the network, preserving valuable resources.

Trend Micro IP Profiler

The second tier in Trend Micro's anti-spam approach is Trend Micro IP Profiler. This new, patent-pending technique is designed to complement the functionality of Network Reputation Services, by blocking more bulk email threats from entering the network.

IP Profiler creates a firewall against directory harvesting attacks (DHA) and bounced mail attacks with additional protection against IP addresses that only send spam and/or viruses and do not send legitimate email. Organizations can determine a threshold for how much unwanted email a specific IP can send before being blocked. In essence, organizations can customize spam policies that best fit their own messaging traffic, creating customer-specific reputation services.

Some of the custom thresholds that can be set by organizations include these parameters:

- How long the emails from an IP address will be monitored
- Total emails that need to be received to be considered a sufficient sample
- Percentage threshold of how many messages with a specific email threat will be allowed from a certain IP (percentage of spam, viruses, DHA, or bounced mail)
- The action that is applied when the threshold level is met or exceeded, including block an IP address temporarily or permanently

One example shown in the screenshot below, an IT administrator can set IP Profiler to temporarily block an IP address if it sends at least 100 emails in an hour and 90% of those are spam messages.

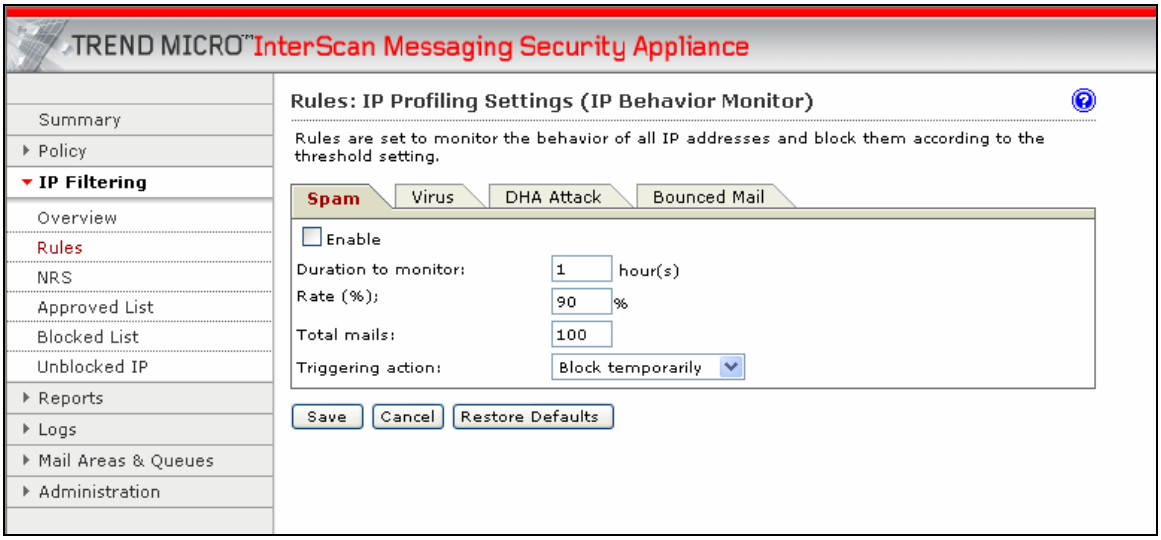

Figure 3: IP Profiler Administrator Settings

To determine if the thresholds are met, IP Profiler initially scans all emails using the Trend Micro anti-spam composite engine. If the percentage of spam sent from an IP address meets or exceeds the thresholds set by the organization, the selected action is applied. The IP address is blocked at the connection layer from that point forward, keeping spam from that IP address off of the network. For optimal results, organizations should set a high threshold. This enables Trend Micro's effective anti-spam engine to identify and block IP addresses that are only sending malicious emails. However, emails from IP addresses that are sending a mix of malicious and legitimate emails will not meet the high threshold and will continue to pass through to the anti-spam composite engine which will filter out the malicious emails while delivering the legitimate correspondence.

This approach maximizes the amount of spam that can be kept off of the network while ensuring low false positives.

IP Profiler is also a useful tool for customers to proactively protect against Directory Harvesting Attacks, as administrators can set thresholds for the total number of recipients that can be listed in a message, as well as the total number of non-existing recipients based on directory integration. Additional behavior analysis helps to create the firewall against DHA and bounced mail attacks.

IP Profiler stops even more threats before entering the gateway by looking at the traffic specific to the organization. By blocking senders of DHA, bounced mail attacks, spam, and viruses, IP Profiler further reduces the load on IT infrastructure.

Trend Micro Anti-Spam Composite Engine

The third tier of Trend Micro's anti-spam approach is its powerful anti-spam composite engine. The few remaining emails that are not blocked by Network Reputation Services or IP Profiler are stopped from entering the inbox by this anti-spam engine. The engine uses a variety of techniques to detect and block junk email, including statistical analysis, heuristics, signature filters, whitelists, blacklists, and much more. Most importantly, however, Trend Micro's anti-spam composite engine can effectively block image spam and image-based phishing attacks.

Image spam has quickly become one of the most pervasive types of spam circulating the Internet today, as the spam content is generally shown on an image embedded within the email, and often contains nonsensical text that can help bypass email filters. Spammers randomize image spam to create numerous small variations in the email, changing characteristics like image dimensions, background colors, text colors, and more. The use of images bypasses content, context, and other spam filtering techniques that focus on the email body. Standard signatures are also ineffective because the randomization technique makes each email unique.

Trend Micro's engine uses a patent-pending approach to strip away the characteristics that spammers randomize, such as color and dimensions, leaving only the core of the image. This enables the anti-spam engine to apply just a few main signatures to block all of the different variants. Through image content analysis, the engine is also able to scan the underlying composition of the message and apply heuristic rules to determine if an

embedded image is spam. Whereas many other spam filters have failed to stop image spam, Trend Micro's composite engine has had a high level of success in stopping this advanced spamming technique.

The anti-spam engine also applies embedded URL reputation. Trend Micro utilizes its expertise with reputation services to determine the reputation of URLs embedded in emails. If the URL belongs to a spam or other malicious Web site, the email containing the URL is blocked. Applying Web reputation to emails not only stops spam emails, but also prevents recipients from following links to dangerous Web sites that may download malware or phish for confidential information.

Trend Micro's anti-spam engine is powered by TrendLabs, a global network of research centers that ensures constant threat surveillance and attack prevention. With accurate, real-time data, TrendLabs is able to provide effective anti-spam techniques, such as heuristics and statistical filtering, to detect, preempt, and eliminate attacks.

Network Reputation Services and IP Profiler block emails from known spammers and keep these threats off of the network. Any remaining threats are scanned by the anti-spam composite engine. This engine is highly effective at keeping threats out of the inbox with low false positives by combining image spam detection technology and embedded URL reputation with other anti-spam techniques. All emails identified as spam by the composite engine are placed in an End-User Quarantine, allowing employees to manage their own spam while reducing the burden on IT staff.

5. TREND MICRO PRODUCTS

Trend Micro offers several products tailored to meet the needs of various organizations looking for a comprehensive and accurate anti-spam solution. Trend Micro's product line offers protection at various levels of a business's network, such as at the gateway or at the mail server, and provides solutions that are tailored to the needs of small, medium, and large organizations. Trend Micro is also one of the only vendors to offer solutions in software, an appliance, and a hosted service.

For small and medium-sized businesses, Trend Micro offers Worry-Free Solutions with all-in-one security that is more streamlined and easily managed. **InterScan Gateway Security Appliance** gives medium-sized business customers comprehensive security,

with defense against viruses, spam, spyware, Web content filtering, compliance, and more. Customers of this appliance can also benefit from Trend Micro Network Reputation Services and its anti-spam composite engine. Trend Micro also offers medium-size businesses the same comprehensive gateway security in a software solution: **InterScan VirusWall**.

For enterprise customers, Trend Micro provides a comprehensive, layered approach to network security through its Enterprise Protection Strategy. This strategy offers an effective security framework, protecting the network from the gateway to the desktop. As part of this strategy, Trend Micro offers messaging security products with anti-spam protection. These messaging security products can be integrated with other Trend Micro security products to achieve holistic protection.

At the gateway, Trend Micro offers its InterScan Messaging Security line. This includes the software solution **InterScan Messaging Security Suite** as well as **InterScan Messaging Security Appliance** and **InterScan Messaging Hosted Security**. With a broad range of form factors, customers can deploy an InterScan Messaging Security solution in the manner that best suits their network environment, whether it is an easily installed appliance, a comprehensive software suite, or a hosted service that keeps threat protection off of the network. The InterScan Messaging Security line gives customers numerous benefits beyond spam protection, including antivirus with zero-day protection, content filtering to enforce compliance and prevent data leakage, as well as a centralized management console for easy administration. Customers of the appliance and software suite version of InterScan Messaging Security can benefit from Trend Micro's three tiered spam defense, including Network Reputation Services, IP Profiler, and its anti-spam composite engine. The hosted version includes the Network Reputation Services as well as Trend Micro's powerful anti-spam composite engine.

Trend Micro's **ScanMail** line of solutions is designed to stop spam at the mail server, with a version for **Microsoft Exchange** and for **Lotus Domino** platforms. These products come with Trend Micro's anti-spam composite engine out-of-the-box, and customers can license Trend Micro Network Reputation Services for additional spam protection outside the perimeter. In addition to spam protection, ScanMail defends against viruses and other malware, as well as inappropriate content with its compliance features.

Network Reputation Services, though integrated with select Trend Micro solutions, can be purchased separately and deployed with numerous solutions. It is compatible with nearly all popular MTAs, as well as many firewall solutions, giving customers the flexibility to enjoy a powerful reputation service while keeping their current infrastructure intact.

Trend Micro provides additional products beyond messaging security to provide comprehensive network protection. For example, Trend Micro's Web security products provide a perfect complement to email security. These products apply Web reputation to block malicious Web sites, as well as preventing transmissions to phishing-related sites, dangerous downloads, and viruses in Web mail, in addition to other Web security features. Threats now span across email and the Web, requiring Web security to achieve comprehensive messaging security.

All products in the Enterprise Protection Strategy are centrally managed through Trend Micro Control Manager for a coordinated defense against network threats.

6. CONCLUSIONS AND RECOMMENDATIONS

There is no doubt that spam represents a significant, global threat to business. The costs associated with spam are spiraling out of control, as employees lose productivity and companies spend billions each year to process and store spam messages that penetrate their networks and to deploy solutions to combat the influx of spam.

While there are dozens of security products available that can block most spam, organizations are finding that, for a truly effective solution, a defense that blocks spam from entering the network is necessary, especially in instances of high messaging traffic volume.

Trend Micro offers its multi-tier anti-spam technologies in a comprehensive line of messaging security solutions, with gateway products such as its **InterScan** line, as well as mail server products, such as its **ScanMail** line. In addition, the company's **Network Reputation Services** add a powerful outer defense layer that blocks spam before it even reaches the anti-spam filters at the organizational level.

Trend Micro's solutions provide customers with truly secure email, lower the impact on IT infrastructure, reduce security costs, and raise employee productivity without the risks of high false positive rates, ensuring business-critical emails are delivered safely to the inbox.

