



# TrustedSource: The Next Generation Reputation System for Enterprise Gateway Security

## Table of Contents

Abstract	3
Introduction	3
Reactive Systems, Including Signatures, Are Not Enough	5
Phishing and Other Cyber Attacks Designed to Circumvent Signatures	6
Reputation Systems Defined	7
First-generation reputation systems	7
Second-generation reputation systems (2G)	8
Reputation Systems Reach Maturity: The TrustedSource Global Reputation Approach	9
Sender reputation	9
Message reputation	9
How Does TrustedSource Work?	10
Persistence testing: guilty until proven innocent	10
Message reputation	11
Statistical analysis	11
Social networks	11
Real-time data feeds	12
Constant feedback	12
The Next Phase: Extending Reputation System to the Internet	13
Real-World Analogy of Reputation-Based Security	13
TrustedSource Integration into McAfee Gateway Solutions	14
McAfee Web Gateway	15
McAfee Email Gateway	15
McAfee Firewall, Enterprise Edition	17
TrustedSource and unified threat management at the network gateway	18
The positive security model	18
TrustedSource Portal	19
Conclusion	20
About McAfee	20

### **Abstract**

Your enterprise network is the engine that drives the communications that fuel business. Today's network applications support mission-critical functions and transactions, customer and partner relations, meetings, financial transfers, distributed access to confidential information, and much more. Business productivity and profitability depend on these capabilities, so protecting the network is protecting the organization itself.

In this white paper, we'll explain how to use network reputation intelligence to mitigate the business risks posed by modern, targeted attacks against multiple entrance points to the organization's network:

- Email and other messaging protocol attacks including spam, phishing, directory harvesting, and denial of service
- Web-based attacks such as malware-infected URLs, unfiltered SSL encrypted traffic, and viruses
- Network attacks that take advantage of system-level vulnerabilities, as well as blended threats that combine multiple attack vectors

We'll also discuss the shortcomings of legacy security solutions—based on reactive, signature-based systems, blacklist/whitelist technology, and older, packet-based firewalls that overlook the application layer—and why these older technologies are no longer sufficient to address today's sophisticated attacks. We'll make the business case for significantly widening and strengthening your security posture—because in today's enterprise, network security truly matters.

You'll learn about the limitations inherent in a security environment that uses multiple, single-point solutions, and the advantages of a multi-layered, defense-in-depth approach that integrates reputation-based systems with best-of-breed messaging, Web, and network security technology in a single appliance. And you'll learn how McAfee's TrustedSource™ reputation system adds an extra layer of proactive, advanced protection to help your organization accurately detect and block all types of threats to your messaging, Web, and network environments.

### **Introduction**

Security challenges have changed. New vulnerabilities constantly emerge, while attacks become more sophisticated and multi-pronged. Taking charge of security means instituting proactive measures to deal with many aspects of the business, including:

- The enormous volume of traffic that moves across the many entry points of the enterprise gateway
- Expansion of the enterprise itself through the increasing use of remote connectivity
- Vital sensitivity and privacy of data, intellectual property, and financial information exchanged across the enterprise
- Supporting applications and systems that represent the life blood of your organization

With the rise of a far more dynamic, interactive, and user-driven Internet—often referred to as Web 2.0—attacks that were once limited to the messaging layer can now penetrate the enterprise through the web and network layers as well. Communications services are now embedded within systems and applications, and blended threats have become commonplace as a result. Threats are evolving and multiplying faster than ever, and enterprises don't have access to the information they need to identify threats quickly and render them harmless. To deal effectively with burgeoning, ever-more-sophisticated threats, enterprises need modern gateway security that proactively anticipates and blocks threats before they can cause damage. This requires real-time global intelligence as part of a multi-layered defense that incorporates complementing security techniques to ensure complete protection.

Yesterday's security technology fails to address the needs of the Web 2.0 world. McAfee's TrustedSource multi-protocol global reputation system bridges the worlds of messaging, web, and network security to create an umbrella of multi-platform protection that is missing from antiquated point products for Internet security.

Forming the foundation of McAfee's entire range of enterprise gateway security solutions, TrustedSource accumulates data from more than 7000 sensors in 68 countries—data that includes more than 110 billion messages per month and millions of URLs—in order to create highly accurate profiles of all sender, message, Web site, and domain activity on the Internet. TrustedSource then uses these profiles to watch for deviations in expected behavior. The system creates “reputation scores” that can be used to identify and stop spammers, cyber-criminals, targeted attacks, and fraud.

Moreover, TrustedSource doesn't just identify and block the bad. It also helps ensure that good traffic is reaches its intended recipients fast and trouble-free.

TrustedSource reputation scores are incorporated into McAfee gateway security solutions for the enterprise, forming a critical first layer of protection at the messaging, Web, and network gateways. As a result, a large percentage of unwanted traffic is rejected before it even gets to the innermost layers of protection. And because TrustedSource is highly refined and proven to be accurate and reliable, false positives are virtually a non-issue. The traffic that needs to get through reaches its destination.

TrustedSource adds a strong, extra layer of proactive protection to enterprise security solutions through reputation intelligence based on:

- *Volume of reputation data.* TrustedSource sees more email sent to enterprises and governments than any other messaging security technology in the world. Quantities are in excess of 110 billion messages per month.
- *Quality of reputation data.* TrustedSource assigns reputations to each identity by intelligently aggregating the global knowledge of behavior and sending patterns it gathers for each sender.
- *Accuracy of reputation data.* TrustedSource conducts real-time behavior analysis, using over 80 behavior classifiers that examine over 1,000 characteristics, to identify up to 400,000 new zombies in a typical day.
- *Combination of sources.* TrustedSource combines information from multiple sources including virus detection, web pages, and email traffic. This enables TrustedSource to gather more data than any single source and to aggregate intelligence to help identify and stop blended threats that use multiple protocols.
- *Strength of multiples.* By combining sender, message, domain, image, and URL reputations and correlating their relationships, TrustedSource is able to identify and stop blended threats the moment they appear. With TrustedSource, organizations no longer have to wait for reactive, signature update files to be released.

## White Paper TrustedSource: The Next Generation Reputation System for Enterprise Gateway Security

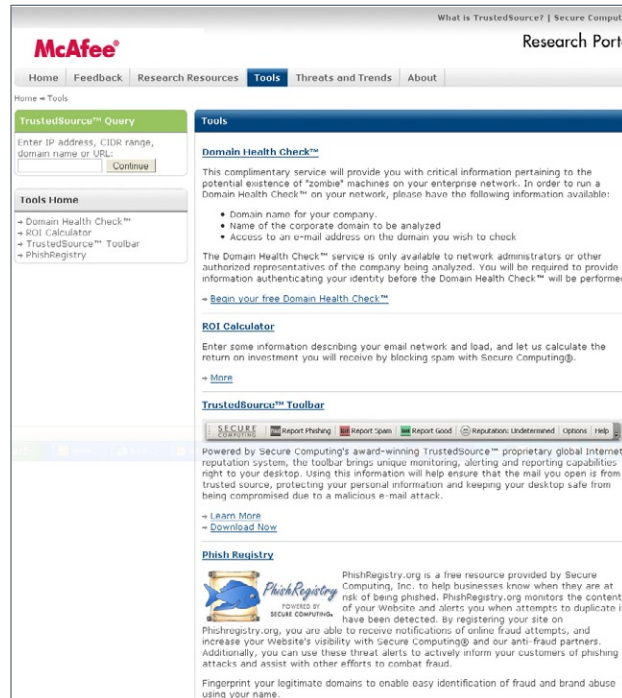


Figure 1: Located at [www.trustedsource.org](http://www.trustedsource.org), the McAfee TrustedSource Portal is a free online resource that provides precise information about sender and message reputation by domain and IP address

### Reactive Systems, Including Signatures, Are Not Enough

Reactive, signature-based security is quite effective at catching malware that has already been catalogued and included in signature databases. Signature-based prevention is an important part of reactive threat management. But what about brand new malware that has not yet been identified? What about targeted attacks that are too small or too fast-moving to catch the attention of signature anti-virus software? Depending solely on signature-based solutions is an ineffective way to prevent malware attacks. In particular, McAfee has seen a significant increase in “zero-day” attacks which:

- Target vulnerabilities that have not yet been patched
- Use new virus code that has not yet been incorporated into virus signatures
- Are simply not widespread enough to make economic sense to patch—even though they can be highly damaging to those enterprises that are affected
- Accelerate then disappear within hours

Vendors of security software, application software, and operating systems are vigilant in keeping as up-to-date as possible with security patches and updates, but attackers are aware of these inherent weaknesses, and have stepped up their own efforts as well. To combat these threats, standard reactive systems must be used in tandem with proactive front-line defenses.

Unfortunately, many enterprises rely on a few key security solutions that address some, but not all, types of threats. For example, they may be using a packet-based firewall, which is ineffective against application-based attacks. Or, they may be using anti-virus technology that is based solely on message content and identification of virus signatures. The combination of firewall and anti-virus software does not provide the one-two punch it once did, and enterprises that limit themselves to these two strategies

are not closing off all doors to attack. The exponential growth in network traffic, email volume, and remote connectivity means that substantial hardware resources and bandwidth are required in order to analyze an increasingly large volume of traffic from multiple sources, for an increasingly large variety of threats.

In addition, signature engines are unable to keep up with outbreaks caused by zombie networks, which are responsible for the majority of spam and viruses being sent today. Hundreds of thousands of new zombie machines are being created every day. These networks of hijacked computers are capable of sending millions of messages in rapid bursts and then shutting down, making them almost impossible to trace. As a result, corporate networks are being hit with a constant stream of unwanted messages that must be stopped before they can flood the mail server.

To combat the threat posed by zombies, an enterprise must be able to tell when a remote zombie network is trying to penetrate the system. Equally important, it must prevent computers within the enterprise's own network from becoming zombies—a far more common occurrence than many IT and security administrators realize.

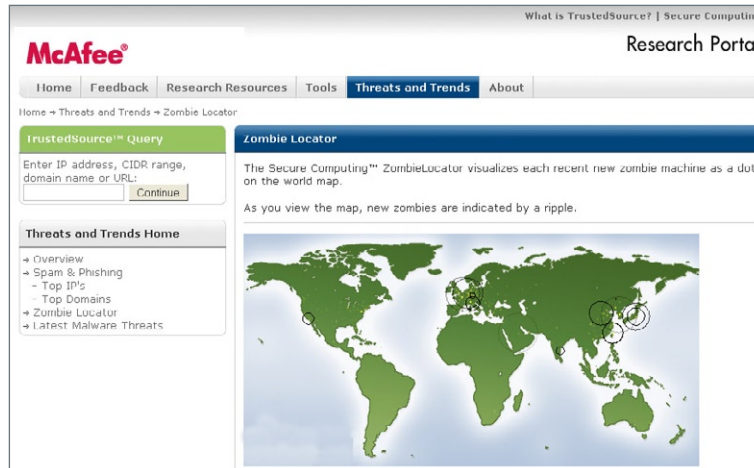


Figure 2: Zombie network

### Phishing and Other Cyber Attacks Are Designed to Circumvent Signatures

In addition to traditional viruses and spam messages, enterprises are faced with the threat of attacks from phishers and other cyber-criminals who prey on users' natural curiosity and self-interest. This class of malicious senders is becoming increasingly sophisticated in their use of common subject lines and body content to fool signature-based systems.

Many users are finally understanding the basic idea that it's unsafe to open attachments, particularly .exe files, from unknown senders. Hackers are responding by redoubling their efforts to combat the growing awareness of such threats on the part of email users.

For example, "spear phishing" attacks actually mimic the email addresses of managers and executives in a company, relying on social engineering tactics to do the dirty work. A typical employee, seeing an email that appears to be from their boss asking for a copy of their sales forecast, engineering schematics, financial projections, or product roadmaps, can be expected to hit "Reply," attach the file, and then hit "Send" without a second thought. That sensitive data has now been irretrievably sent out of the building into the hands of criminals, and no one is the wiser.

Even viruses have become more dangerous today—often propagating at real-time speeds so that it's impossible to protect against them with signature-based anti-virus technology alone. Consider the "Code Red v2" worm, which infected 400,000 hosts in about 14 hours. And while this window of time did allow leading anti-virus vendors to release signatures that prevented the worm from causing further damage, "Code Red" was only a precursor to the attacks seen more recently.

The "Warhol" worm, for example, needed only 15 minutes to infect its first 1,000,000 hosts, and the more recent "Flash" worm infected the same number in just 30 seconds. With propagation speeds like this, it's easy to see why relying solely on signature-based virus detection is no longer a viable option. You need to supplement basic anti-virus with solutions that intelligently and proactively identify threats *even before they hit the anti-virus radar*.

### Reputation Systems Defined

A reputation system tracks the behavior of network entities such as IP addresses, domains, URLs, images, and messages. Some trends that are evaluated to form a reputation include whether a sender or host engages in good behavior (such as sending legitimate email messages or hosting a malware-free web site), bad behavior (such as sending spam or malicious code) or is deviating from known historical behavior. A sender or host's affiliations can also be incorporated in the reputation—for example, taking into account whether a given IP address has hosted malicious URLs in the past.

Reputation system technology has advanced rapidly, as we'll see by reviewing the relatively brief history of this proactive approach to security.

### First-generation reputation systems

Reputation systems were first designed to help cope with the growing problem of spam clogging messaging systems and user mailboxes. In the early days of spam, circa 2001, simple blacklists and whitelists seemed like an appropriate response to the nuisance messages that had begun to show up in inboxes around the world.

Blacklists contain the IP addresses of known spammers, phishers and virus senders, while whitelists contain the IP addresses of senders known to be legitimate. Referencing these lists allowed companies to filter a segment of their total mail flow, temporarily curbing the onslaught of spam messages. When traffic was less abundant and there were fewer spammers, this approach had merit. But the shortcomings of blacklists and whitelists soon became painfully obvious:

- *Black/whitelists are reactive, not proactive.* An IP address is added to a blacklist only after a user has received an unwanted message and then manually reported it to a system administrator. By that time, it's too late. The spam has already reached the targeted inboxes, interrupting productivity and possibly inducing users to open an infected attachment or click a malicious link.
- *Black/whitelists are anecdotal.* Whitelists and blacklists may or may not be based entirely on factual information. Senders can be added indiscriminately or maliciously, with little or no investigation into their actual sending habits.
- *Black/whitelists are error-prone.* Senders of legitimate email often find themselves blacklisted due to faulty information. Unfortunately for these senders, getting removed from a blacklist can be extremely difficult. Perhaps even more troubling, some "pay-to-play" whitelists allow anyone with enough cash to masquerade as a legitimate sender and bypass spam filters.
- *Black/whitelists are slow.* Any defense technique based purely on lists will always be several steps behind the spammers. By the time a blacklist is updated with a new address, end users around the world have already received the spam message, leaving them exposed to whatever toxic cargo might be attached. Conversely, email from a legitimate sender may be falsely rejected as spam until the sender's IP address has been added to the whitelist, resulting in missed messages.
- *Black/whitelists can be hijacked.* Spoofing is a common practice, and what can appear as a trusted sender may actually be a hijacked account in disguise.

- *It's not a black-and-white world.* There are simply too many shades of grey to give senders a “thumbs-up” or “thumbs-down” based on manual, subjective, and often-faulty lists. First-generation reputation systems failed to take into account those senders who fall somewhere in the continuum between “bad” and “good.”

While other factors have contributed to a decline in the effectiveness of blacklists and whitelists, the ultimate failure of these lists as an adequate email security solution is largely due to their inability to factor message quality and speed into the equation.



Figure 3: First-generation reputation systems assigned senders either a “bad” or “good” rating based on inaccurate and anecdotal blacklists and whitelists. IP addresses that should have fallen somewhere in the middle were left for an administrator to manually determine, potentially leading to incorrect classification.

### Second-generation reputation systems (2G)

The next iteration of reputation systems added techniques to rectify the failure of early blacklists and whitelists to maintain control over the spam flood. While the lists remained an integral component, new features briefly increased the efficiency and effectiveness of 2G reputation systems. With time, however, spammers found new ways to evade detection, once again rendering this generation of reputation systems inadequate.

Among improvements seen in second-generation reputation systems were:

- *Dynamic lists.* The introduction of zombies into the email security landscape required a corresponding shift in defenses. While blacklists and whitelists had been adequate for assigning sender reputation in the early days of spam, zombies changed the playing field completely. They turned good senders into bad ones, and allowed bad senders to send their malicious messages from other peoples’ IP addresses without obvious spoofing or fear of reputation damage. The addition of dynamically updated lists allowed reputation systems to adjust to rapidly changing conditions.
- *Automatic updates.* Many second-generation systems included automatic updating—removing the burden and delay inherent in the previous requirement for administrators to manually upload their lists to central hosts for distribution across the Internet. But while automation significantly improved efficiency, the updates were still based on lists that had to be created and managed manually.
- *Message scoring.* After studying millions of spam emails, some common characteristics of these messages were identified. As a response, some second-generation reputation systems incorporated algorithms to identify these characteristics in incoming messages—assigning each message a score based on its likelihood of being legitimate.

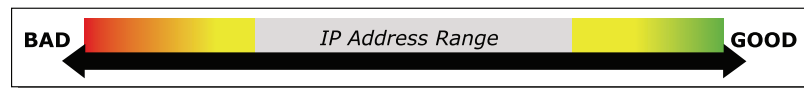


Figure 4: While some second-generation reputation systems included dynamic IP address whitelists and blacklists based on sender behavior, none combine this feature with automatic updating and message scoring.

### Reputation Systems Reach Maturity: The TrustedSource Global Reputation Approach

Today's spammers are more clever than ever, so today's reputation systems must be even more sophisticated. An effective reputation system must be dynamic, comprehensive, and precise. And crucially, it must be based on actual enterprise mail traffic in order to keep the spammers from gaining any advantage. As a rule, enterprise traffic provides a more accurate view of business-related messaging than ISP-provided spam data because it is based on actual messages encountered in corporate environments, as opposed to consumer-targeted messages.

The TrustedSource global threat correlation engine was developed to provide this view, offering enterprises the most precise and comprehensive reputation system available. In addition to general ISP spam data, which is largely consumer-centric, TrustedSource receives and analyzes over a hundred billion messages per month from McAfee's network of thousands of appliances deployed globally. Through this real-time analysis, McAfee is able to analyze more than a third of the world's enterprise messaging traffic—increasing security levels, blocking undesirable connections, and maintaining a false positive rate of less than one in a million.

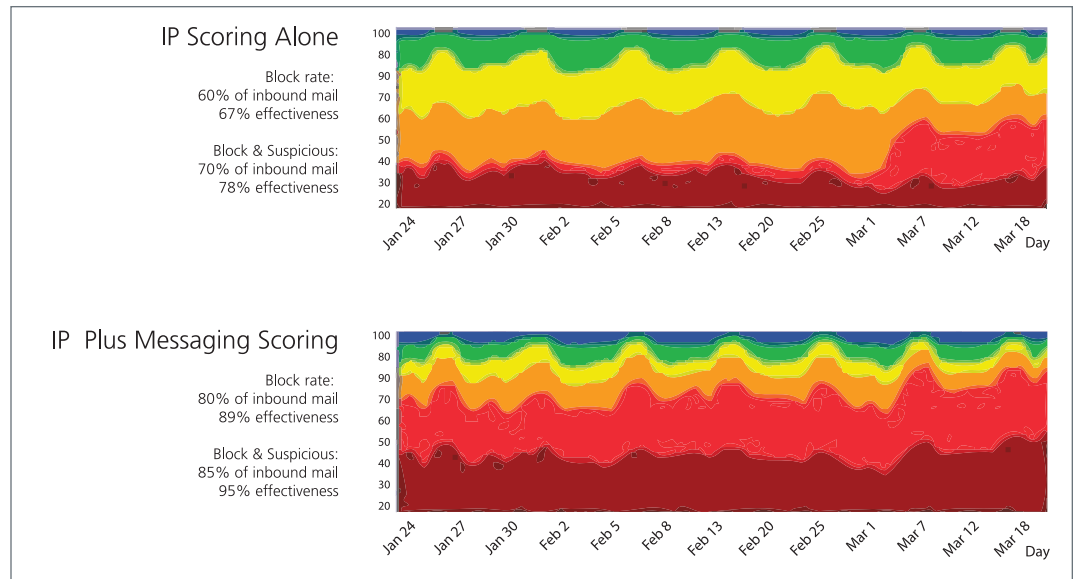


Figure 5: TrustedSource reputation service

### Sender reputation

Like a virtual credit agency, TrustedSource assigns a reputation score and further classifies senders as good, bad, or suspicious based on an in-depth analysis that takes into account more than a hundred behavior attributes for each sender. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists, and network characteristics with the unparalleled strength of global enterprise data analysis. By design, TrustedSource is able to define a precise and accurate reputation score for every sender, not just those that have been encountered in the past. As opposed to other security offerings that don't incorporate reputation in spam scoring, TrustedSource data provides the most accurate and effective protection against spam, viruses, and other unwanted traffic.

### Message reputation

Sender reputation provides only part of the solution, largely because the advent of zombie networks makes it possible to hijack an ever-shifting and growing number of unwitting "senders." By analyzing each message as well as each sender, TrustedSource can render zombies immediately useless.

By combining sender and message reputations, TrustedSource achieves an 80 percent effectiveness

rate—identifying bad messages before they even enter the enterprise’s network. And when TrustedSource technology is combined with a messaging security appliance such as McAfee® Email Gateway (IronMail), the effectiveness rate can go as high as 99+ percent.

### How Does TrustedSource Work?

By combining years of industry-leading research with advanced statistical and mathematical models taken from science and medicine, the developers of TrustedSource made ground breaking discoveries about the email sending behavior of IP addresses. Taking advantage of these insights, TrustedSource is designed to create a virtual continuum of IP scores—eliminating the estimation and guesswork required in less advanced reputation systems. Sender reputation scores in TrustedSource are based on both sender history and message characteristics. TrustedSource creates a profile view of all senders’ behaviors based on hundreds of criteria such as:

- *Persistence*: When was the sender seen for the first time?
- *Volume*: How much email originates with the sender?
- *Breadth*: Does the sender both send and receive, or only send email?
- *“Burstiness”*: Is the sender’s behavior sporadic or continuous?

TrustedSource then uses the profile it has created to watch for deviations from expected patterns for any given sender. McAfee security appliances report back to TrustedSource on all the mail flow they are seeing, giving TrustedSource a real-time view of worldwide mail traffic. Any deviations from predicted behavior are picked up by TrustedSource, and if a new reputation score is derived for a given sender, that new score is made immediately available to McAfee units in the field.



Figure 6: TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists, and network characteristics with the unparalleled strength of McAfee’s network of more than 7000 total deployments globally. The result is the most complete reputation system in the industry, with the ability to provide a score for every sender encountered.

By collecting data on email senders and what types of emails they generate, TrustedSource continues to build “collective intelligence” about senders, which becomes progressively more accurate over time.

### Persistence testing: guilty until proven innocent

Rather than give the benefit of the doubt to unknown or unfamiliar senders, TrustedSource takes a “guilty until proven innocent” approach to reputation scoring. By examining the frequency with which it has seen email activity from a particular IP address and the quality of the sent messages, TrustedSource assigns the address a probability of being a spammer or a zombie machine that has been taken over by hackers and used to send spam, viruses, or other unwanted messages.

Based on information gathered from the 4000 sensors in the field, TrustedSource has identified approximately that 50% of all spam is sent by IP addresses that are less than 6 months old, with approximately 10% being seen for the first time in the last 30-days. More than 90 percent of these messages are spam, viruses or other undesirable messages. Based on this analysis, McAfee researchers conclude that IP addresses that are encountered for the first time are very likely zombie machines. Using this principle, McAfee typically identifies more than 5,000 new zombies an hour.

### Message reputation

Sometimes, even good senders generate bad traffic. If a computer has been infected with a zombie, it can turn into a “spam cannon” in an instant, sending high volumes of spam and other malicious messages without the user even realizing it. TrustedSource weighs each message as well as each sender, checking, for example:

- Has this message already been classified as spam from another sender?
- Has this message been seen in greater volume than expected?
- Has this same message been sent by a number of other senders?

### Statistical analysis

Built into TrustedSource is a combination of several sophisticated algorithms and techniques that, when combined, create an accurate picture of each message:

- *Header analysis:* Complete analysis of the message header often identifies spoofed, corrupted, or incorrectly sized information. Checking the message header for invalid information is critical.
- *Feature analysis:* TrustedSource extracts high-level features such as the number of messages, the number of recipients, the “burstiness” of the message, and the periodicity over the last twenty-four hours.
- *Normalization:* TrustedSource performs a normalization analysis to extract the noise, unnecessary content, and obfuscations of the message.
- *Fingerprint analysis:* Thousands of hashes are created for each message, which are then intelligently processed to identify varying degrees of similarity among messages being sent from all over the world.
- *Heuristics and dictionaries:* Noting whether or not the message contains known words or phrases that are considered offensive or blacklisted.

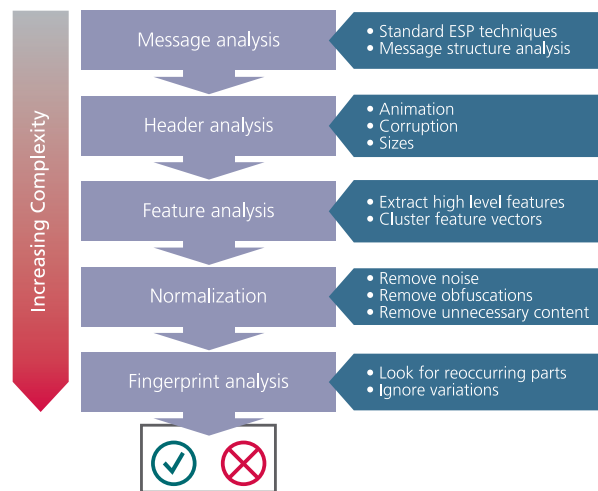


Figure 7: Message Gateway Security statistical analysis

### Social networks

One of the most effective methods used by TrustedSource to determine reputation scores for senders is the “social network” of the sender. Relationships between all senders are examined by TrustedSource to determine whom a sender communicates with and at what frequency, what volumes of email are generally transferred, and how much mail flow moves in each direction. Based on this social network, TrustedSource is able to instantly detect deviations in behavior, which are typically considered to be suspicious activity.

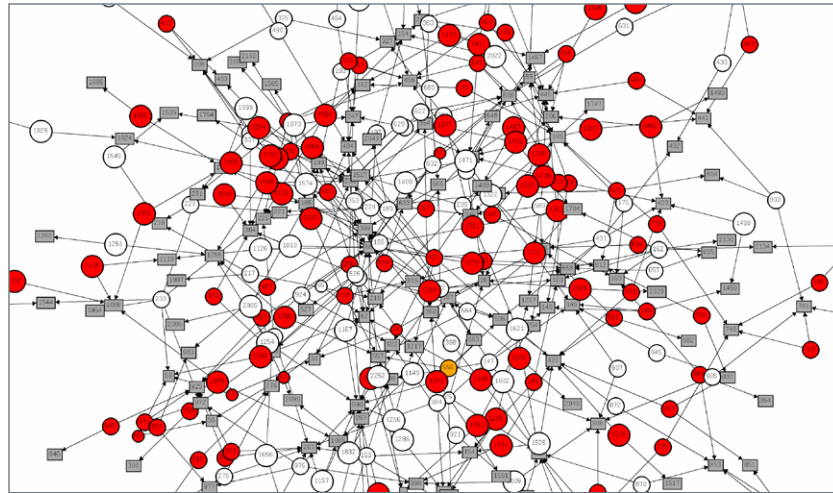


Figure 8: An example of how social networks can identify spammers.

### Real-time data feeds

Information provided by TrustedSource is streamed in real time to McAfee products around the globe, ensuring that they are always up-to-date with the most recent and relevant IP scoring data. As a primary information source for McAfee's enterprise messaging security products, TrustedSource plays a large role in ensuring that McAfee remains the undisputed leader in accuracy and performance.

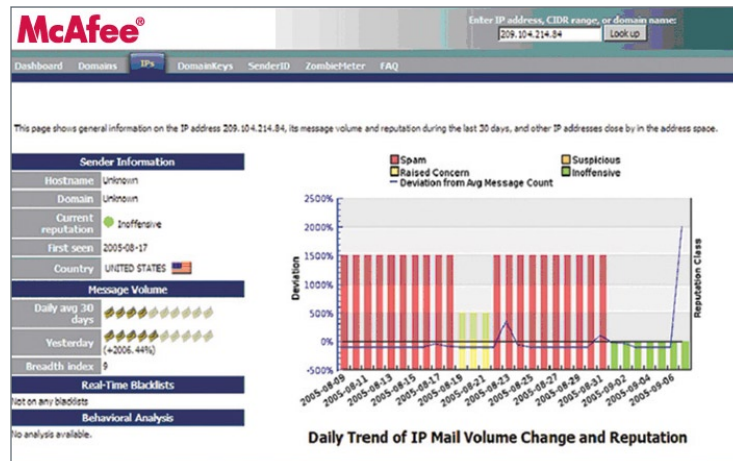


Figure 9: TrustedSource gathers IP, web, and malware data to create a comprehensive Internet reputation for all entities on the Internet.

### Constant feedback

TrustedSource is a self-learning, dynamic system which becomes more intelligent and accurate over time. The more unwanted messages and traffic McAfee security appliances encounter, the better they get at detecting and stopping threats. TrustedSource provides constant updates on sender and host status to McAfee. These updates are then sent out to other security appliances in the field via McAfee's Threat Response, creating a cycle of feedback that benefits all parties involved—except spammers and hackers—and allows McAfee to achieve the highest level of accuracy in distinguishing the good traffic from the bad. By tracking sender and host behavior over time, McAfee's database of web and email reputations is constantly becoming both more robust and more accurate at the same time.

### The Next Phase: Extending Reputation System to the Internet

The dynamic nature of today's Web 2.0 environment—where anyone can author content and publish files and applications—has dramatically increased web-based threats. And the ability of hackers to create sophisticated, blended attacks that utilize multiple protocols has blurred the lines between email-based and web-based threats.

While first-generation reputation systems focused on messaging, the Internet now requires a similar reputation system to determine the overall behavior of web sites, including:

- Whether a web site engages in good behavior, such as hosting malware-free content
- Bad behavior, such as a landing page embedded in a spam email that hosts spyware, keyloggers, or other types of malware
- Whether the site host is deviating from known historical behavior—for example, a site that has always hosted malware-free content in the past but now shows signs that it may have been recently compromised

TrustedSource is the first reputation service to gather reputation information about every entity connected to the Internet. The resulting “network effect” of TrustedSource is used to create a comprehensive repository of reputation information of IP addresses, domains, specific messages, URLs, and images. TrustedSource feeds this global intelligence to local appliances in real time, giving each enterprise the opportunity to leverage the experiences of all users.

TrustedSource is integrated into all of McAfee's enterprise gateway product lines: McAfee® Email Gateway, McAfee® Web Gateway (Webwasher), McAfee® SmartFilter®, McAfee® Firewall, Enterprise Edition (Sidewinder), and McAfee® UTM Firewall appliances. By cross-referencing knowledge from multiple products and sources, TrustedSource provides significant insight and direct benefits to an organization's ability to protect critical resources.

For example, when a McAfee Email Gateway appliance detects a phishing or other type of malicious email, the information is fed directly to TrustedSource, reputation scores are immediately generated or modified, and the results are shared with other solutions including McAfee SmartFilter, McAfee Firewall, Enterprise Edition, and McAfee UTM Firewall. Additionally, the URL from the phishing email is incorporated into the McAfee Web Reputation Database\* which then provides category-based protection for all McAfee SmartFilter and McAfee Web Gateway customers. And TrustedSource not only shares a single URL or sender IP, but also automatically analyzes other domains hosted on the same server and adjusts reputation scores and categories appropriately.

In another example, when a McAfee Web Gateway appliance in the UK detects a virus, TrustedSource extracts a signature from the virus and automatically updates all McAfee web and email anti-virus deployments around the world instantly. TrustedSource also incorporates this signature into the web crawlers used to check millions of sites everyday. If web pages are found with the newly detected virus, reputation scores are immediately changed and the sites are added to the McAfee Web Reputation Database.

### Real-World Analogy of Reputation-Based Security

To provide a real-world analogy for the proactive protection of TrustedSource, think about airport security. Increased inspections of persons and luggage are required in order to prevent attacks. Today's state-of-the-art airport security, however, is reactive—relying on what we know about the types of attacks that have already been attempted, such as shoe bombs and aerosol contaminants. So authorities make everyone, regardless of who they are or whether they actually pose any threat, to take their shoes

off and limit toiletries to small containers in quart-sized clear plastic bags. Necessary though these measures may be, they slow down the entire air transportation system. And to make matters worse, it can take days or weeks after a new vulnerability has been discovered before airports can respond by deploying new security measures.

However, if a system like TrustedSource were available for airport security, a “reputation score” would identify a known terrorist based on information about that person’s past and current suspicious behavior. Upon attempting to make an airline reservation, that person would be blocked or put on a heightened security list. Arriving at the airport, the potential suspect and his or her luggage would be subject to a thorough inspection at the airport, while people with good “reputation scores” would only be subject to normal scrutiny.

Moreover, the system would notify the airlines and the Transportation Security Administration (TSA) anytime the “reputation score” of someone holding a reservation changed. Reputation tracking would continue with any new information and become part of each flyer’s ongoing history. Like TrustedSource, the hypothetical system for airport security would operate in real time—so if someone has a good reputation upon making a reservation, but is subsequently put on a watch list or arrested for a safety violation, the system would immediately update the “reputation score” and alert the airlines and TSA. Likewise, a new terrorist attempt in Singapore would be analyzed, the details would be made available, and new security measures would be deployed at every other airport around the world—instantly.

The risk of a few “zero-day” threats that have not been seen before will always exist. But our hypothetical airport security system would reduce even these risks by providing background information on not just the person and their reputation, but also on the reputations of others with whom they have affiliated. TrustedSource provides this same benefit in cyberspace by analyzing the reputations of URLs and IP addresses that each sender is affiliated with.

When you combine a global reputation system with a content search and a whitelist of known-good senders (analogous to a Pre-registered Traveler Program), you know much more than ever before about the entities trying to gain entry to your network—enabling you to protect your resources much more effectively. And that’s exactly the confidence that TrustedSource provides.

### TrustedSource Integration into McAfee Gateway Solutions

Reputation scores were first integrated into McAfee Email Gateway in 2002. Today, TrustedSource is also integrated into McAfee Firewall, Enterprise Edition; McAfee Web Gateway, McAfee UTM Firewall, and McAfee Email Gateway—providing the most intelligent reputation system available. As a self-learning system, your TrustedSource-based appliance leverages the collective intelligence of all other systems around the world—so the day you install it, you are already gaining the advantage of all reputation information gathered since TrustedSource first started analyzing traffic.

We’ll conclude our discussion with an overview of McAfee gateway solutions and how they incorporate the TrustedSource reputation system.

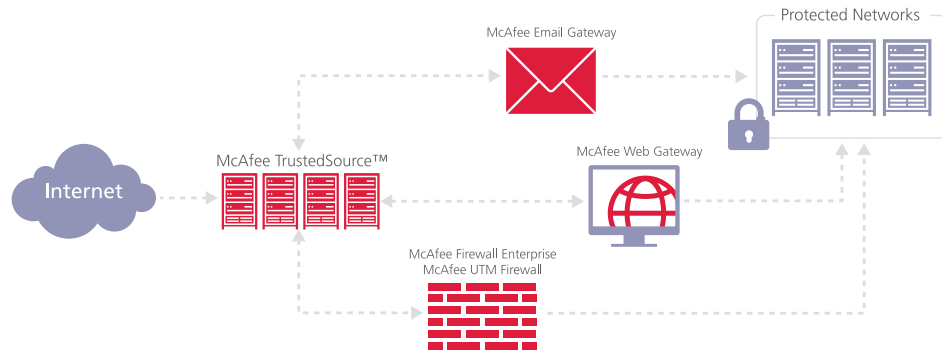


Figure 10: McAfee TrustedSource Enterprise Gateway solutions.

According to an independent report from eWeek, “The No. 1 product (McAfee Web Gateway), for example, detected 99.97 percent or all but 87 out of the 289,682 samples.” To read that report visit, <http://www.eWeek.com/article2/9,1759,2023127,00.asp>

To learn more read our white papers, “in Today’s Web 2.0 Environment, Proactive Security is Paramount. Are You Protected?” and “Why Comprehensive Malware Protection is Superior to Anti-Virus Signatures for Protecting Your Organization.”

### McAfee Web Gateway

McAfee offers a complete portfolio of web gateway appliances designed to protect enterprises from malware, data leakage, undesirable URL content, and Internet misuse—while ensuring policy enforcement, regulatory compliance, and a productive application environment. By integrating TrustedSource global reputation technology into McAfee Web Gateway appliances, we’re able to profile in real time literally billions of entities connected to the Internet worldwide, and to provide up-to-the minute host behavior analysis to create a reputation score that can be used to determine whether a connection to the enterprise network should be allowed. McAfee Web Gateway also employs the most sophisticated behavior-based heuristics and signature-based techniques for stopping malware, as well as patented content analysis software for stopping data leakage.

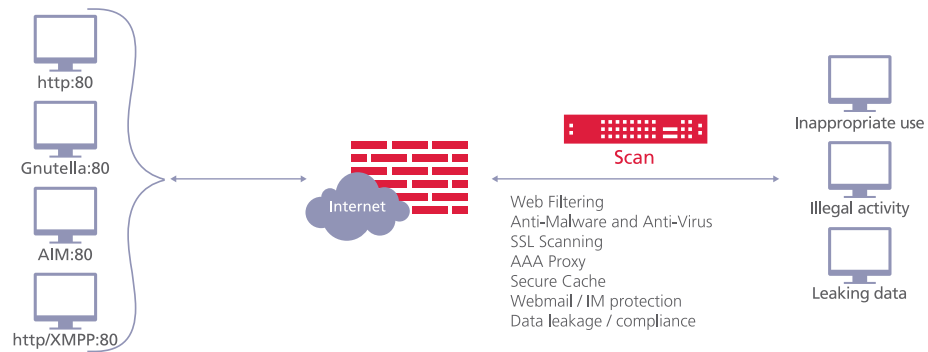


Figure 11: TrustedSource Integrated into McAfee Web Gateway

As part of the TrustedSource network, McAfee Web Gateway deployments provide automatic feedback on threats to TrustedSource for the benefit of all McAfee security gateway customers. Additionally, McAfee offers a stand-alone Web filtering solution, McAfee SmartFilter, which provides exceptional Web filtering through the powerful combination of category-based filtering and reputation-based filtering, powered by the TrustedSource reputation system.

### McAfee Email Gateway

In 2008, the volume of email sent worldwide was estimated at 100 billion per day or more, an exponential increase over the previous year. The rapidly rising volume of email brings with it a corresponding rise in the potential threats to corporate email systems.

McAfee research indicates that more than 85 percent of all email messages are unwanted spam, viruses, denial-of-service (DOS) attacks, Trojans and other malicious threats. And these threats are constantly evolving to evade detection by traditional security techniques, presenting a major challenge to all organizations regardless of the type of mail server or message transfer agent installed in the network. How can companies handle the massive increases in email volume without sacrificing accurate detection of threats and without being forced to add hardware to process the additional messages?

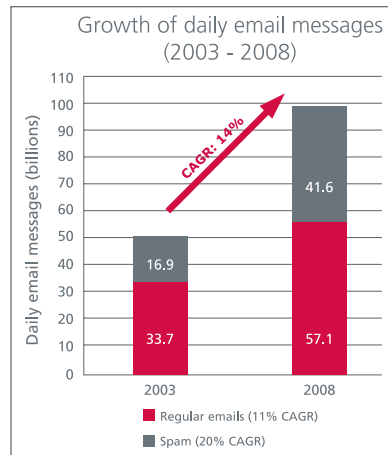


Figure 12: Increase in email volume

A comprehensive approach to email security requires correlating results from examinations of both message content and sender history. By evaluating senders based on their past behavior, a more accurate picture of their intentions and legitimacy can be discerned. Has the sender engaged in spamming, virus distribution or phishing attacks? If they have, an effective reputation system knows this and flags the message. Has the sender even been seen before? Does that sender both send and receive email? Who does that sender communicate with, and how often? Knowledge of these behavioral aspects about a sender is crucial to determining a sender's intent.

*Reputation systems add value to corporate email security efforts in multiple areas:*

- *Increased effectiveness:* If a known spammer tries to use a new technique to evade detection, an accurate reputation system will still recognize the origin of the message, causing it to be blocked. Email security solutions that do not employ reputation will be unable to maintain their effectiveness against new threats.
- *Managing email volume:* By identifying and blocking known bad IP addresses, reputation systems can reduce the intake of messages into the network by over 50 percent. This is critical in handling the constantly increasing load of mail.

To combat the real business risks posed by the growing number of messaging security threats, McAfee Email Gateway solutions protect against threats that can occur over your messaging infrastructure. These innovative, policy-based security, encryption and compliance appliances will protect multiple messaging protocols, including email, instant messaging, webmail, file transfers, and other HTTP- and FTP-based activity.

In one integrated appliance, McAfee Email Gateway provides total email protection, protecting enterprise email systems from inbound (spam, viruses, phishing, and hackers) as well as from outbound threats (regulatory or corporate policy compliance violations or theft/leakage of confidential information

or intellectual property). McAfee Email Gateway even protects enterprise email systems from threats that haven't been identified yet. By combining the spam profiler in McAfee Email Gateway with the TrustedSource reputation system, McAfee customers have a significant advantage over users of other messaging security solutions. Even more important, they also have an unmatched advantage over spammers, virus writers, phishers and other malicious senders. To learn more, read our Essential Secure Mail Guide (link to <http://www.securecomputing.com/webform.cfm?id=132>).

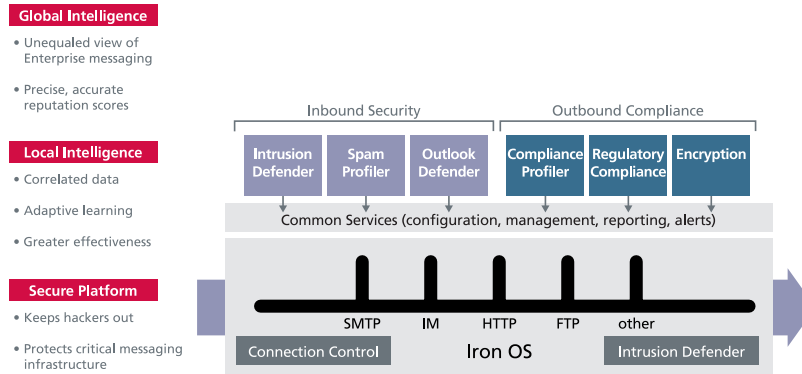


Figure 13: The McAfee Email Gateway product family provides an integrated, scalable, and secure architecture by combining the global intelligence of TrustedSource with local analysis at the appliance to provide optimum protection.

McAfee Email Gateway appliances have won several awards, including "Best Buy" from SC Magazine. Read more details on our awards page and the article itself: <http://scmagazine.com/us/products/productdetails/0d23aed1-b86e-cd6f-2e97-85ca3ce55350/ironmail-/>. For more information on our Messaging solutions, please visit <http://www.securecomputing.com/index.cfm?skey=26>

### McAfee Firewall, Enterprise Edition

McAfee Firewall, Enterprise Edition is the first and only firewall that incorporates reputation-based security for the edge of networks. The bi-directional global intelligence feed from TrustedSource is built in, enabling the firewall to make proactive security decisions based on the real-time known behavior of IP addresses worldwide. This dynamic scoring system provides McAfee Firewall, Enterprise Edition with a unique new layer of comprehensive protection.

Customers benefit from this real-time data feed reputation service because it allows McAfee Firewall, Enterprise Edition appliances to automatically drop huge volumes of unwanted and infected mail at the outer edge of our customers' networks. By rejecting connections from known bad senders of spam, infected web pages, or machines that have been taken over and turned into malware-distributing zombies, McAfee Firewall, Enterprise Edition can eliminate well over 70 percent of the ever-increasing mail traffic flooding into today's networks. As a result, huge volumes of unwanted mail can be rejected before reaching internal network resources. That means your enterprise:

- Saves on messaging servers' processing time
- Sees an increase in available network bandwidth
- Minimizes networking infrastructure expenses
- Improves the overall security posture

TrustedSource reinforces McAfee Firewall, Enterprise Edition by adding reputation-based intelligence to its other strong and comprehensive technologies, including high-speed application proxies and signature-based security services.

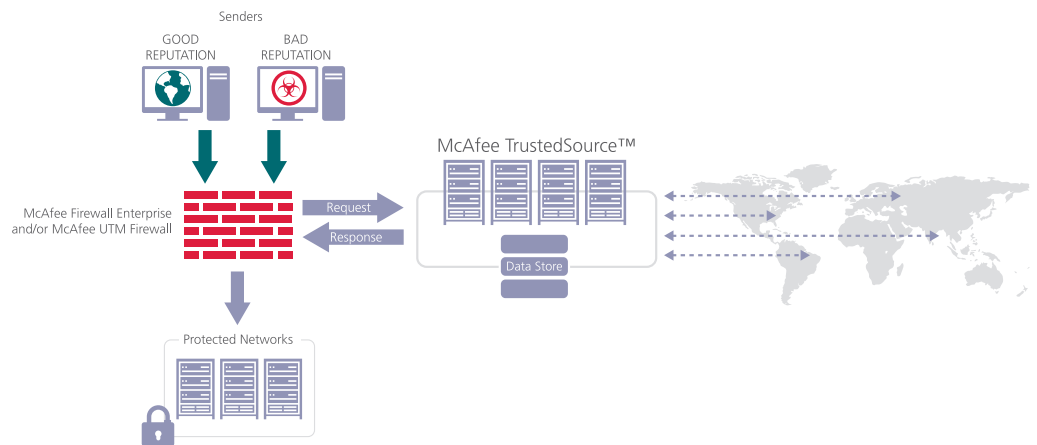


Figure 14: Based on reputation information provided by TrustedSource, McAfee appliances are able to determine with unmatched accuracy whether or not a particular entity should be permitted to connect to the enterprise network.

#### TrustedSource and Unified Threat Management at the network gateway

No single security process, no matter how efficient or technologically superior, is adequate in itself. Strong security depends on multiple strategies operating together, as a unified whole, forming a solid front against attack. Even the best firewall in the world, acting in isolation with no other features outside of basic firewalling, will not deter all threats. And even the best anti-virus software, by itself, cannot detect and prevent all threats from penetrating your network. McAfee Firewall, Enterprise Edition provides a unified set of best-of-breed security tools that are stronger together than security tools that operate in isolation.

TrustedSource works alongside the full range of network gateway security protections integrated in McAfee Firewall, Enterprise Edition. This industry-leading “all-in-one” appliance consolidates numerous security functions into one system that’s easy to manage. These functions include the world’s only uncompromised application firewall, intrusion prevention, anti-virus, anti-spyware, anti-spam, URL filtering, encrypted applications filtering (SSL/HTTPS, SSH, SFTP, SCP), and more.

For small and mid-sized businesses and enterprise branch offices, we offer these same capabilities in our McAfee® UTM Firewall appliances. For more information on our UTM firewall solutions, please visit [www.securecomputing.com/securefirewall](http://www.securecomputing.com/securefirewall). And to learn more about McAfee Firewall, Enterprise Edition, please see our paper “An Examination of Firewall Architectures and Secure Firewall (Sidewinder) v7.0.”

#### The positive security model

Two defensive approaches against both known and unknown attacks exist in network security today: The negative security model and the positive security model. The advanced application proxies of McAfee Firewall, Enterprise Edition employ the positive model of security to allow tightly defined and recognized traffic through at Gigabit speeds, ensuring legitimate use of Internet-facing applications. Both models are defined below within the industry.

- Negative security model countermeasures identify bits of traffic known to be threatening. Anti-virus and intrusion detection/prevention systems are classic examples, both of which depend upon checking traffic flows against attack signatures. With threats increasing at such a rapid pace, this results in less and less time to react to new attacks, and a steady increase of successful attacks over time.
- Positive security model countermeasures allow all legitimate, acceptable traffic requirements and deny

*“Products based upon the positive security model dramatically reduced an organization’s attack surface by automatically eliminating exposure to all sorts of attacks—unknown as well as known. Unless counter measures capable of preventing unknown attacks are employed, the result will be steadily increasing occurrences of successful attacks!”*

– Mark Bouchard,  
Missing Link Security Services  
Author of Unknown Attacks: A  
Clear and Growing Danger  
<http://www.securecomputing.com/webform.cfm?id=97&ref=tswp>

everything else. This approach is highly effective at preventing unknown attacks and dramatically reduces an organization’s attack surface by automatically eliminating exposure to all sorts of attacks—unknown as well as known.

Positive-model security tools—which apply an in-depth knowledge of how a wide range of applications work—are essential to face down today’s greatest security challenge: the unknown attack. McAfee Firewall, Enterprise Edition offers leading-edge solution incorporating the positive security model.

### TrustedSource Portal

The TrustedSource Portal is a free online resource that provides precise information about sender reputation by domain and IP address. Located at [www.trustedsource.org](http://www.trustedsource.org), the TrustedSource Portal is the only Web site in the world that provides administrators with a view into current and historical reputation and sending patterns of the senders, as well as analytical information such as country of origin, network ownership, and hosts for known senders within each domain.

Additionally, the TrustedSource Portal provides a snapshot of global email trends, including a map illustrating the country of origin for email attacks, graphs displaying overall email and spam volume trends, McAfee’s ZombieMeter™, and a snapshot view of email authentication deployments across the Internet. Using this information, administrators can troubleshoot, conduct research, and analyze various senders that may be sending mail into their environments.

IT administrators can also request a report outlining their own domain’s reputation and overall health. Called a “Domain Health Check” this report is free of charge and can be requested from the [www.trustedsource.org](http://www.trustedsource.org) website under Tools.



Figure 15: Moe page, [www.trustedsource.org](http://www.trustedsource.org)

### **Conclusion**

A traditional security approach that identifies bad traffic solely on the basis of content, characteristics, signature lists, or blacklists and whitelists, is incapable of generating adequate data about senders, URLs, and domains. In order to accurately identify connections as wanted or unwanted, corporations must embrace a more comprehensive approach that combines local message examination techniques with global enterprise email sending patterns, web HTTP traffic, network protocols and applications, as well as encrypted tunnels (SSL/HTTPS, SSH, and others). As a comprehensive, multi-protocol reputation system, TrustedSource plays a critical role in the greater security mission to protect all of these traffic pathways.

TrustedSource provides intelligent infrastructure protection. By incorporating TrustedSource into all of McAfee's enterprise gateway solutions—and even more importantly, by unifying TrustedSource installations all over the world—this engine gains tremendous power and accuracy as the cornerstone of enterprise gateway security to ensure the highest level of protection, covering multiple protocols across the enterprise environment.

### **About McAfee**

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee® is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

