

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.



TrustedSource in SnapGear: Big-Business Security for Today's SMB

What is TrustedSource?

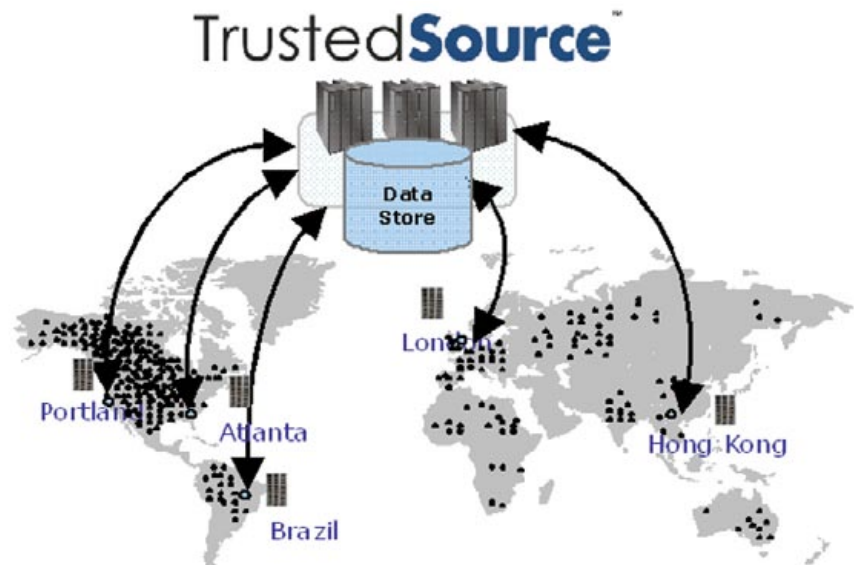
The TrustedSource™ reputation system is a cornerstone of the Secure Computing® solution portfolio. The most precise and comprehensive Internet host reputation system in the world, TrustedSource characterizes Internet traffic and makes it understandable and actionable. TrustedSource's unrivaled effectiveness is a direct result of Secure Computing's unique view into enterprise Internet traffic. TrustedSource has now been added to every current SnapGear® model, and this document will outline this exciting new functionality and what it means to you, the small- to medium-sized business (SMB).

TrustedSource is Secure Computing's IP and mail reputation service, previously available only in our enterprise-class IronMail® appliances. Rather than depending solely on localized protection using algorithms that are quickly obsolete, TrustedSource uses a global reputation approach to proactively identify and block traffic from illegitimate sources. Illegitimate sources are identified as machines that generate spam, such as those taken over by zombies or botnets.

The TrustedSource servers accumulate information about spam and malware from more than 7,000 of our appliances in 68 countries, worldwide which leads to the following:

1. More than 110 billion messages examined per month
2. Recent detection of more than 400,000 new zombies per month (18,000 per hour)
3. Ability to identify and block better than 80% of unwelcome traffic before it ever reaches the enterprise network

TrustedSource then uses this information 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.



Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

Berkshire, UK
Tel +44.0.870.460.4766

Asia/Pac Headquarters

Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel +81.3.5339.6310

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

© 2007 Secure Computing Corporation. All Rights Reserved. SNAP-TS-WP-04107NF. Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, IronIM, SoftToken, Enterprise Strong, Mobile Pass, G2 Firewall, PremierAccess, SecureSupport, SecureOS, Beta, Cyberguard, SnapGear, Total Stream Protection, Webwasher, Strikeback and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, Security Reporter, Application Defenses, Central Management Control, RemoteAccess, SecureWire, TrustedSource, On-Box, Securing connections between people, applications and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.

Actually managing this level of information on SMB devices such as SnapGear just isn't feasible, due not only to the size of the database collections, which are always growing due to continual enhancement of the quality of data, but also due to the processing power required to ensure our customers' expected performance levels. So how can SnapGear leverage this enterprise level facility?

Let's assume you have a mail server on your premises and a SnapGear appliance is leveraged as your firewall and anti-spam device connected to the Internet. Every time an incoming SMTP (email) connection request is received, SnapGear asks the TrustedSource data center (see map above) for a reputation score for the source of the connection request. SnapGear will then either accept or reject the connection—before it hits your email server. This process alleviates approximately 80% of any spam processing your email filters are doing, which extends the life of that system, and also stops a huge amount of spam getting through to your employees. In diagrams below, Diagram 1 outlines the process of an email coming from a source with a good reputation score. Diagram 2 outlines the process of an email coming from a source with a poor reputation. Note that SnapGear appliances allow every organization to tailor their own thresholds in terms of what they deem to be a good or bad reputation score.

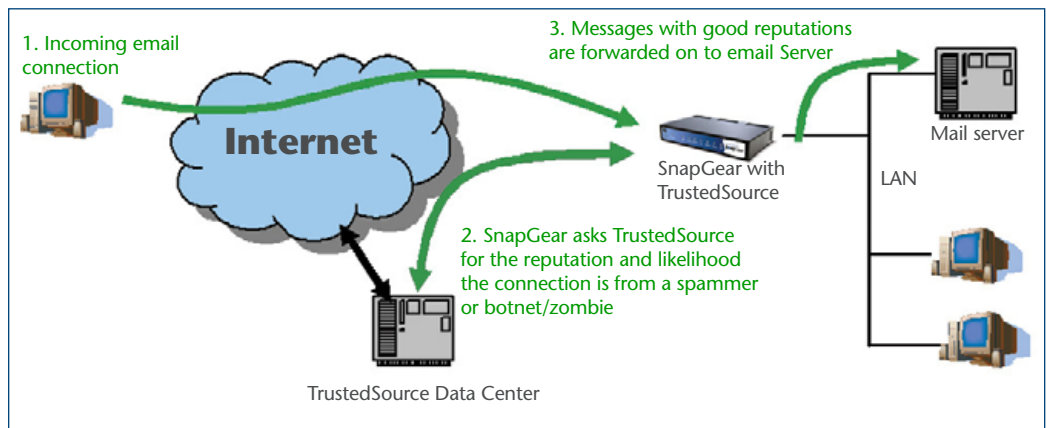


Diagram 1: Email with good reputation

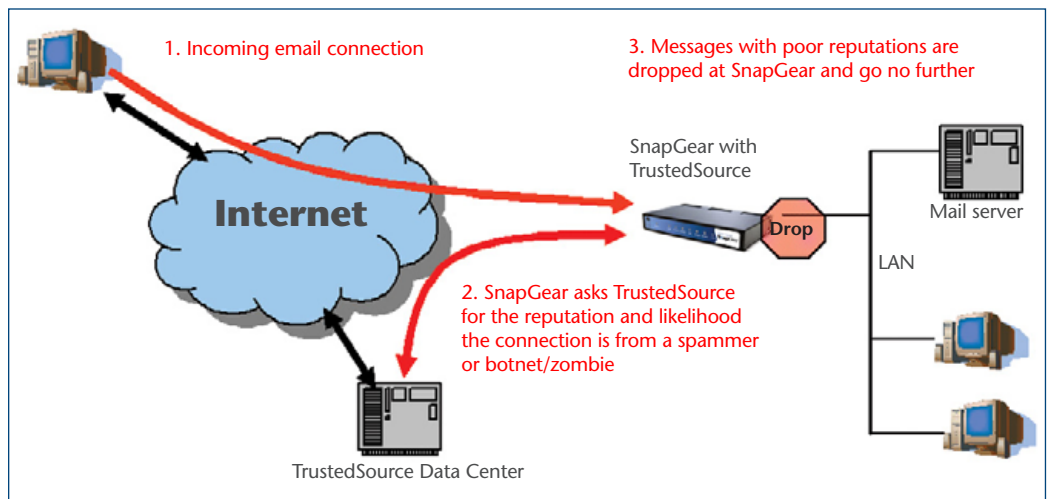


Diagram 2: Email with poor reputation

How Does TrustedSource Help the SMB?

Issues that are affecting SMBs that host their own email right now are:

1. Ever-increasing spam in users' inboxes; this costs money in lost time.
2. The continual processing of more than 90% of your mail that is spam, causing undue stress on mail servers.

3. Effectiveness of anti-spam systems based on signatures and black lists has decreased significantly due to the constantly changing tactics of spammers.
4. Anti-spam measures are being flooded, requiring significant investment money to upgrade hardware, software, and manpower.
5. Internet connection bandwidth and data center allocations are being wasted by downloading spam this wastes money.

What Does TrustedSource on SnapGear Do for You?

1. SnapGear can now block approximately 80% of all incoming connections based on sender reputation.
2. Provides your business with access to technology that had previously been available only to Fortune 2000 companies and other enterprises with large IT budgets and staffs.
3. Saves you money on bandwidth by blocking unwelcome connections 24/7.
4. Future-proofs your existing anti-spam systems, as TrustedSource's effectiveness continues to improve with each new spammer technique identified.
5. Puts your organization on the leading edge of mail filtering technology without the need to update signature databases.
6. Provides a true appliance, ensuring much higher reliability than other solutions; no moving parts to wear out or fail.

Conclusion

Secure Computing's TrustedSource enabled SnapGear appliances will:

- Reduce your spam load on your existing mail server by ~80%
- Reduce the amount of time spent by end users deleting spam, resulting in increased productivity
- Free your administrator from continually setting up filters
- Decrease your Internet bandwidth usage
- Increase bandwidth availability
- Extend the life of your email servers

Why choose SnapGear to deploy such a reputation system? Secure Computing's TrustedSource reputation system is the most robust in the world, and Secure Computing is the only company in the world to offer such a system on their SMB-level security appliances. SnapGear is the one multifunction security appliance every SMB needs.

For more information on how TrustedSource works and what sort of behaviors are analyzed please visit Secure Computing's Web site at <http://www.securecomputing.com/index.cfm?skey=1621>.

You can also see detailed records and the dynamic structure of mail volume around the world, where most zombies are popping up, and also see how much of the world's messaging is spam at <http://www.trustedsource.org>.