

White Paper



EXPERTS ON DEMAND

Security versus Privacy: Best Practices for Spam and Virus Protection for Telecommunications Carriers and Service Providers *Europe*

A White Paper created by

Experton Group AG
Ismaning, Germany

On behalf of

Cloudmark, Inc.
San Francisco, USA

October 2007

Copyright

This survey was created by Experton Group AG. The data contained herein were gathered conscientiously and with the utmost care in accordance with scientific principles. Nevertheless, we cannot guarantee their exhaustiveness or accuracy. Nobody should act, based on this information, without obtaining professional advice and performing an in-depth analysis of the respective situation. All rights to the contents of this survey are reserved by Experton Group. For reasons of data protection, the data and information remain the property of Experton Group. Reproductions – even of excerpts – may only be made with the written permission of Experton Group AG.

Copyright Experton Group, 2007

1. Introduction

Today, spam and malware are ubiquitous, challenging both consumers and corporate IT. The Radicati Group reports that enterprise spam costs were roughly US \$49 per mailbox in 2003 and that they expect this cost to skyrocket to US \$257 per mailbox in 2007. E-mail abuse constitutes more than just a nuisance to consumers and companies, rather its impact goes deeper, compromising the personal privacy and the integrity of information systems.

While spam is by no means a new problem, it remains a growing issue. According to estimates by the Messaging Anti-Abuse Working Group (MAAWG), spam as a share of global e-mail traffic was oscillating between 75 and 80 percent from January 2006 through March 2007. This acceleration in spam activity has been driven by new attack techniques used by spammers. Now, spammers commonly use botnets to distribute spam mails. Botnets consist of millions of remotely controlled, compromised computers owned by unsuspecting consumers. These so-called “zombies“ currently account for almost 70% of worldwide e-mail traffic. In many cases, botnets also distribute malicious code disguised as videos or websites on topical events such as major European weather events, the start of the American Football season, etc. The malicious code typically turns the downloading computer into yet another zombie of the botnet. Thus, the cycle continues as these new systems are exploited for distributing more spam or conducting DDoS (distributed denial of service) attacks against targeted systems.

To combat the surge in abusive messaging, most companies have deployed some form of commercial or open source anti-spam solution. For instance, surveys conducted by Experton Group have revealed that at the end of 2006, nine of ten German companies with at least 100 employees were using some kind of anti-spam or content-filtering solution. Beyond that group, however, many organizations have not yet conquered the spam problem. According to the Experton Group, small businesses and consumers are the two groups that are most lacking in effective countermeasures against spam.

In this context, telecommunications carriers, e-mail and Internet service providers play a key role. Winning the war against spam and malware is among the current top priorities of European service providers. This is not an easy goal to achieve as the service provider's actions against unsolicited messages could potentially conflict with regulations related to user and data privacy. When using a content filter, service providers must ensure that it does not only demonstrate efficacy against phishing, viruses, spam and other messaging-borne threats, but also that the process by which it filters also respects the anonymity and privacy of subscribers and complies with regulations on data privacy and protection.

Therefore, a balance must be achieved between security and privacy. A good analogy is that of electronic surveillance techniques such as speed cameras or cctv. Too much surveillance could be an invasion of privacy, whereas too little could create an unsafe environment.

2. Challenges for Carriers and Service Providers

1.1 Business Perspective

European carriers, Internet service providers (ISPs) and e-mail service providers (ESPs) are facing internal and external pressure to take stronger measures against the increasing volume of spam, viruses and other malware. Since service providers handle all e-mail transactions between senders and recipients, they have a certain "moral" responsibility to control the overall flood of spam. The reputation of the service provider suffers from inadequate spam management.

However, there are also economic factors that favor more effective protection against spam and viruses from providers. End users, particularly those who pay a subscription fee, expect high quality e-mail services and assume that their providers will offer them protection against unsolicited e-mails, malware security threats and targeted fraud from phishers. Users who consistently experience these problems will be dissatisfied with their provider and look to switch. Therefore, effective anti-spam solutions can help to improve customer retention rates.

Operational cost savings are another driver for continued efforts to reduce spam traffic. In recent years, many service providers have focused on cost reductions. Mobile operators are outsourcing 2G and 3G network management and operations. Carriers and ISPs are migrating to highly efficient data centers and green IT concepts. However, the flood of spam threatens to neutralize these efficiency gains. Unsolicited messages, which now comprise the overwhelming majority of e-mail traffic, consume considerable storage, server and network infrastructure resources. They also increase administration, system maintenance and customer support costs.

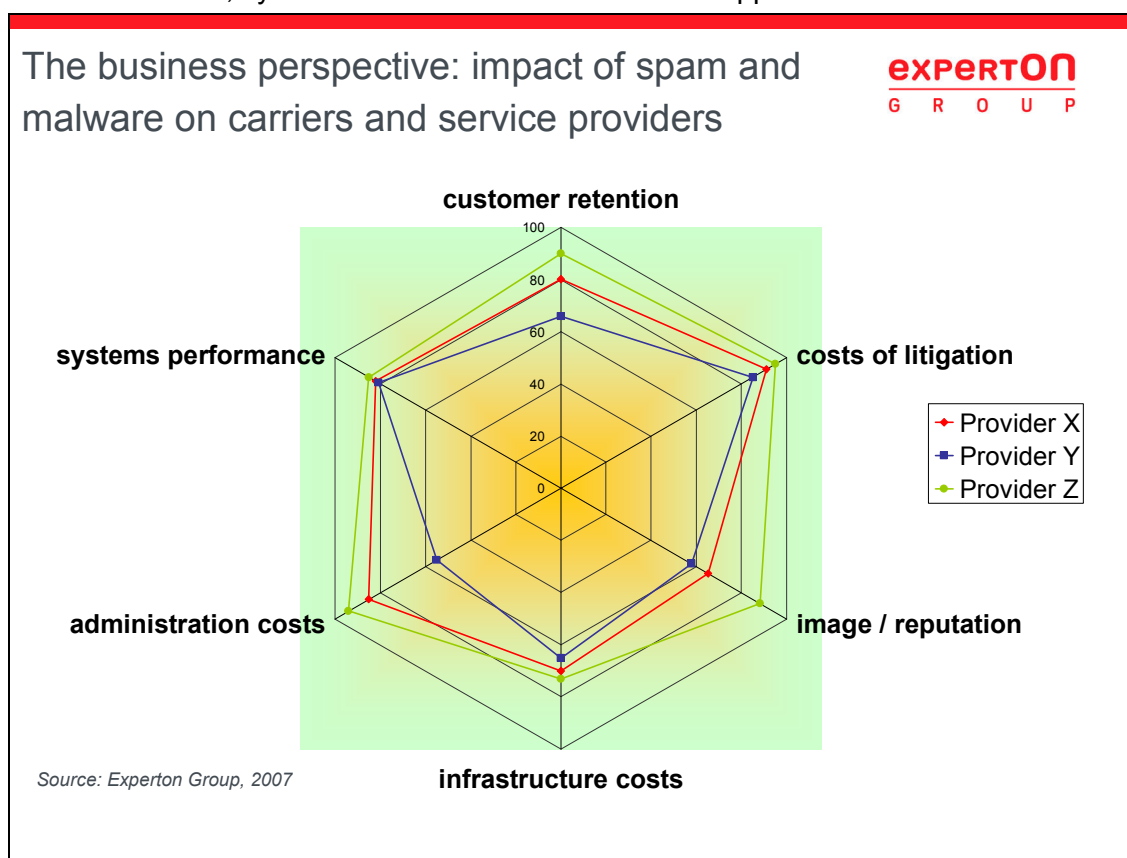


Figure 1: The business perspective – impact of spam and malware on carriers and service providers

Finally, there are legal and regulatory issues to consider. The service provider's approach to dealing with spam, in particular their way of handling "false positives" and privacy issues, can result in legal disputes and conflicts. The respective countermeasures may contrast to some extent with the service provider's objective to reduce overall administration and infrastructure cost and increase system performance.

Thus, spam and malware is not a mere technology issue. Rather, it must be addressed through a thorough risk management. It is difficult for the provider to determine the "adequate" level of spam and virus protection and the cost-benefit ratio. While it is useful to take industry best practices as an orientation, this is by no means sufficient. Risk management will help to objectively determine technical and organizational priorities.

1.2 Legal Aspects of Spam Filtering

Legal requirements for carriers and service providers in the European Union

There are EU-wide and country-specific regulations that address the spam issue and are relevant for carriers and Internet service providers, in particular, directive 2002/58/EC of July 12, 2002, of the European Parliament and the European Council concerning the processing of personal data and the protection of privacy in electronic communications (privacy protection directive for electronic communications), which also specifies requirements for carriers and service providers, including the following:

- ▶ Minimizing the processing of personal data and use of anonymous and pseudonymous data where possible;
- ▶ Appropriate measures to ensure the security of services;
- ▶ Full information to subscribers and users on existing networking security risks, including risks for which the provider cannot provide any remedies;
- ▶ Appropriate measures to protect subscribers against any violations of privacy through direct mailings;
- ▶ Prohibiting the usage of false identities or false sender addresses when sending unsolicited messages for direct marketing purposes.

The regulations of directive 2002/58/EC had to be incorporated into national law by October 31, 2003. For instance, some of these provisions were included into the German Telecommunications Act, which provides that communications systems with intermediate storage are only permitted to process messages outside the systems of a provider who uses such intermediate storage upon explicit consent of the respective subscriber. The subscriber is the only person to determine the exact content, scope and kind of processing. The service provider may only delete the content of messages according to the specifications laid down in the contract concluded with the subscriber. Transferring personal data to international non-public recipients is subject to certain restrictions.

Moreover, providers risk breaching the secrecy of telecommunications as specified in § 206 of the German criminal code (Strafgesetzbuch StGB). The StGB prohibits the unauthorized rejection of messages submitted for delivery. Also, in accordance with § 303a of the German StGB, attempting to change data is illegal. Carriers and service providers must make sure that their subscribers consent to mail filtering measures in order to be compliant with German law.

While the current regulations provide a framework to ensure the security and privacy of data, they do not recommend specific measures against spam and security threats. For carriers and service providers, this leaves a certain scope of interpretation, which is, however, substantiated through

case-law. It becomes apparent that filtering or deleting e-mails without sender or recipient notification is, for instance, a legally questionable action, even if e-mails are classified as spam. This results in a conflict of goals for the providers: On the one hand, they are obliged to ensure the security and protection against unsolicited mails, on the other hand, deleting messages without the subscriber's consent violates or restricts the subscriber's right of self-determination – unless the messages contain malware and pose a security threat to the subscriber. Filtering spam, which often involves detailed analyses of e-mail content, may be deemed a violation of the end customer's privacy. Service providers, therefore, face the dilemma of "security versus privacy" – they must pursue a balanced approach to avoid image damages and cost disadvantages.

1.3 Requirements for Technological and Organizational Spam Protection

1.3.1 Organizational Best Practices

Protecting ISP and carrier customers is not a purely technological issue; rather, it must also be addressed on the organizational level. The focus is on how to avoid and respond to spam and malicious code and how to achieve industry-wide cooperation.

Avoiding spam and malware

- ▶ Information service for customers (newsletter, web) to increase the awareness for general and current threats through spam and viruses. Specifically, by means of information services, subscribers learn how to "respond" to spam.
- ▶ Written guidelines and policies on spam and virus protection to be communicated to employees, partners and end customers. This is the basis for a joint approach to fight spam. End customers are also informed on potential sanctions in case of e-mail abuse.
- ▶ Free or funded anti-spam/anti-virus software for consumers. Some ISPs have already decided to take such steps. Providers also benefit from the lower consumption of resources through outbound spam and malware.
- ▶ Awareness training for customers. This is particularly suited for business customers and should be taken into consideration, either as a means to increase customer retention rates or to generate additional revenues.

Response to spam and malware

- ▶ Hotline and helpdesk to support customers in case of spam- and malware-related problems.
- ▶ Central point of contact for reporting cases of e-mail abuse and security problems. This may, for instance, be combined with a reputation system to generate added value.
- ▶ Notification to users whose PCs are abused for spam mails. Senders of e-mails classified as spam should be informed and requested to take appropriate countermeasures, based on the provider's policy, or resend any e-mails identified as false positives.
- ▶ Quarantine of user PCs that have been infected with viruses or have been classified as a source of spam.

Industry-wide cooperation

Internet service providers and telecommunications carriers must leverage opportunities to jointly fight spam. Standards for best practices and the exchange of information on spam can be helpful to ensure the success of such efforts. One example is the DomainKeys Identified Mail (DKIM) standard. Data sharing and analysis for early detection is another area.

1.3.2 Technological Approaches

Most carriers and service providers combine several techniques to protect their customers against spam and malware. From filtering techniques such as IP blacklists/whitelists and content inspection to blackholing and secure domain name services, carriers are taking steps to protect their subscribers with solutions that are accurate, high-performance, reliable, and protective of subscriber privacy. These techniques come from a variety of sources, including commercial vendors, open source, and even home-grown development. Payment for these measures is similarly varied. A common model is to implement a software or appliance solution on the service provider side to be used by the subscriber as an anti-spam or anti-virus service, often free of charge. A second model is based on commercial spam and anti-virus software for the subscriber's desktop, often with an accompanying fee for the software paid by the subscriber.

Blacklisting

Blacklisting blocks SMTP connections of IP addresses contained in a "blacklist" of spammers. Some blacklists can be bought on the market, others can be administered manually. The advantage of this approach lies in its simplicity and the low consumption of network resources. To ensure the quality of such lists, they must, however, be updated continuously. It may also happen that blocked legitimate e-mails ("false positives") cannot be recovered any more, since they are blocked directly at the network entrance, independent of their real content.

Whitelisting

Whitelisting is the opposite of blacklisting; mails from known and trusted sources are included in a whitelist. This mechanism can, for instance, also be used to correct entries on blacklists. Whitelists should, however, be combined with other filtering mechanisms.

Greylisting

Greylisting is a technique that rejects e-mails of unknown senders in a first attempt and only delivers these e-mails if they are resent a second time. This method is based on the assumption that a legitimate sender will undertake a second effort, while a spammer will give up after a first blocked attempt. Although this technique can be implemented relatively easily, it also has its disadvantages. For instance, legitimate e-mails may be delivered with considerable delays, which reduces the value of e-mail as a fast medium of communications.

Sender authentication

Sender authentication makes it impossible for the e-mail senders to hide their true identity. Common approaches include traditional SMTP authentication, the Sender ID Framework or Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standard. The latter two methods, however, cannot prevent spammers from authenticating themselves with legitimate DNS entries through "domain tasting", i.e., spammers register a new and legitimate domain for a temporary "trial period".

Management of port 25

Since infected host systems of ISP and carrier customers may be a source of spam, the management or blocking of port 25 is becoming an interesting option. Port 25 is used by SMTP clients to connect to their e-mail server. Port 25 is used by MTAs (Mail Transfer Agents) to talk to one another. The value of blocking port 25 for a network of computers is to ensure that none of them are behaving like MTAs and sending out spam without going through the network owner's MTAs. A secure alternative is the transmission of e-mails by subscribers through port 587, combined with

authentication procedures. This does, however, not prevent the infection of customer PCs with malware.

Frequency analysis

Providers can conduct a frequency analysis on the network level to analyze the e-mail traffic and check it for anomalies that indicate the occurrence of spam. While this method is quite promising, it requires high efforts to reliably recognize "typical" anomalies on a continuing basis.

Content filtering

If an SMTP connection to send an e-mail has been set up already, content filtering methods help to identify spam. There are two problems that must be solved in any content filtering system: 1) how to identify messages and 2) how to determine if messages are spam or legitimate. Most solutions use one or several of the following mechanisms:

- ▶ Heuristic methods (header analysis or e-mail content analysis): Rule-based analysis of e-mails to determine similarities with keywords, expressions or specific patterns (e.g., Viagra). If high volumes of e-mails are sent, this may affect the system performance. This method helps both to identify messages and determine spam.
- ▶ Statistical methods: Check for keywords and comparison with spam databases. A common statistical method is based on Bayesian filters: Whether or not an e-mail is identified as spam, depends on the frequency of certain words occurring in typical spam mails (e.g. "Viagra"). This method may, however, be compromised by spammers, the false-positive rate is relatively high and high mail volumes affect the system performance. As with heuristical approaches, this method helps both to identify messages and determine spam.
- ▶ Checksum comparison (hash): This method, used to identify messages, is based on a network of users, whose e-mails are classified by means of a checksum algorithm with a so-called "fingerprint". Checksum comparison methods usually hash some or all of the headers, body, or attachments. When combined with the collective intelligence of a reputation system, it is possible to distinguish legitimate e-mails from mass e-mails (spam). If a simple checksum comparison is the only method used, the false-positive rate could be high. However, false positives can be significantly reduced when this method is part of a hybrid approach.
- ▶ Blacklisting of URIs (Uniform Resource Identifier Domain Name System Blacklist, URIDNSBL): This is a method to check links in an e-mail that lead to the spammer's web site and to compare them with a spam database. Blacklisting of URIs helps to identify messages. However, it is useless for spam that does not contain any links.
- ▶ Reputation-based methods: Such methods evaluate users or IP addresses under consideration of their spam activity or their reliability as spam reporters, based on a centralized system or a peer-to-peer network. Reputation systems determine whether messages are spam or legitimate, based on the reputation of senders or of the content, attachments and meta-data. They should be used in hybrid approaches in combination with common filtering methods such as fingerprints or blacklists.

1.3.3 Security vs. Privacy: The Contribution of Commercial Solutions for Spam and Virus Protection

Vendors of messaging security solutions with their core expertise in spam and virus filtering can support service providers to ensure the protection of their services. They also have access to a large pool of spam data and can leverage economies of scale for spam identification to achieve a greater accuracy and benefit from reputation systems.

Some cross-industry approaches and models for spam filtering are not fully suitable for the telecommunications and ISP sectors due to legal regulations and restrictions. For example while managed services may be appropriate for enterprises, many carriers and ISPs have concerns regarding the involvement of externally hosted solutions since there are restrictions for the intermediate storage of messages outside the providers' own data center. Carriers and ISPs are also obligated to use anonymous or pseudonymous information to classify e-mails and must not delete mails classified as spam without prior notification.

For service providers, the ideal spam filtering solution must provide flexible options for handling spam and false positives. It must also allow providers to notify senders or recipients about deletion of messages. According to Experton Group, hybrid spam filtering solutions are the most suitable approach. Individually, statistical methods, blacklisting and greylisting may not comply with applicable law, for instance, due to the rather high false-positive rate.

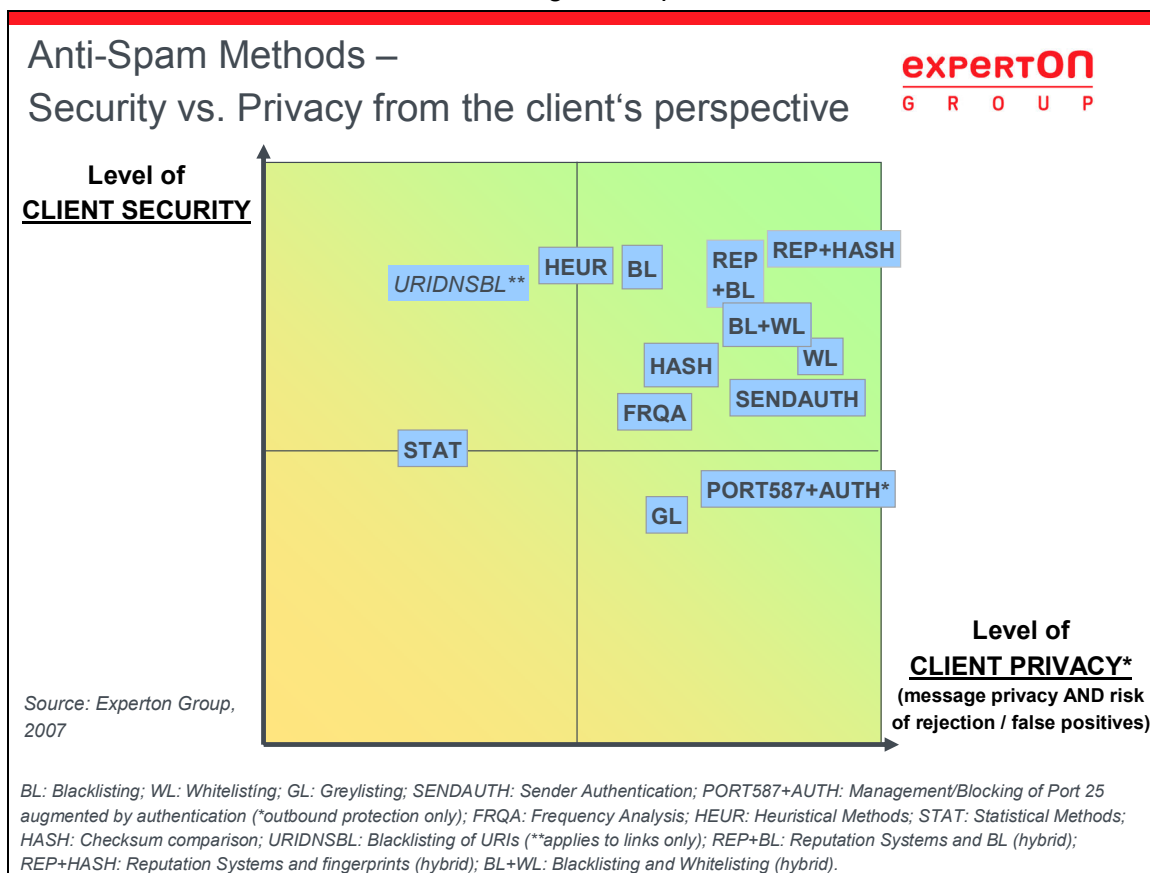


Figure 2: Anti-Spam Methods – Security vs. Privacy from the client's perspective

Figure 2 illustrates how well selected spam-protection methods meet the subscribers' requirements for security and privacy.

High security and high privacy levels:

Methods with high security and high privacy levels are solutions that are effective against spam, whilst also providing Service Providers with the flexibility to implement the system according to local laws and regulations.

- ▶ Reputation systems and hashes (hybrid): the spam-filtering mechanisms of this approach are usually very accurate. As long as the personal information (hash) is processed in the carrier's data center and the message is not "reconstructable", the privacy levels are high. Content reputation is better than sender reputation in terms of privacy, since the latter may mark legitimate senders as spammers in case of false positives.
- ▶ Reputation systems and blacklists (hybrid): This approach combines the security strengths of blacklists with the collective intelligence of a reputation system. However, the false-positive rate is higher than with the previous method (REB+HASH).
- ▶ Blacklists and whitelists (hybrid): this is a common approach. While the security strengths of blacklists complement the privacy traits of whitelists, there are some drawbacks regarding the combined weaknesses. In particular, the quality of the whitelists depends on the subscriber's contribution.

High security, but low privacy levels:

- ▶ Heuristic methods allow a high level of security, but the analysis of e-mail header or body information conflicts potentially with privacy issues, especially when the data is processed at an external site. The false-positive rate can be considerable when the underlying policies are not managed properly.
- ▶ URIDNSBL and reputation systems that rely on lookups to external systems are passing private information about the content and sender of a message. However it is possible to deploy such solutions by caching the URI and Reputation data locally and performing those lookups within the carrier data centre, thus avoiding the passing of private information to third parties. However, as the diagram shows, such systems are very prone to false positives.

High security, but medium privacy levels:

- ▶ Blacklisting methods guarantee a high level of message security and privacy, but the trade-offs stemming from false positives can be considerable – blocked false positives usually cannot be recovered anymore.

Medium security, but high privacy levels:

- ▶ Sender authentication methods such as SMTP authentication ensure that customers are who they say they are, preventing spoofing on relay and locally generated messages. However, it does not prevent spam per se.
- ▶ Whitelists are good from a privacy perspective, since the subscriber can decide on his or her own whether to trust a source or not. Nevertheless, human error or simply curiosity could make a user whitelist spam or malware sources. If not maintained properly by the user, the benefit from whitelists can turn out to be low.

Medium security, and medium privacy levels:

- ▶ Hash/Checksumming – Simple checksumming has two potentially large disadvantages. Firstly, it can be susceptible to false positives, due to the risk of collision with legitimate message checksums. Secondly, depending on the architecture of the supplier, it can cause a

lookup to an external system for every message. For example, some checksumming-based systems work by also performing frequency analysis (FRQA), i.e. comparing the rate of change of volume of certain checksums in order to detect spam. This information is aggregated at an external site, and thus could be considered a serious breach of privacy, especially if the data is sent in a way which can reconstruct the whole or part of the original message.

Medium security, but low privacy levels:

- ▶ Statistical methods have already been applied for many years, but they can be compromised by spammers and the false-positive rate may be high.

Low security, but high privacy levels:

- ▶ Management of port 25, augmented by authentication methods, is a good means to solve spam issues, but it does not entirely protect end-user devices from malware. The privacy level is high because there is not any filtering of message content involved.

Low security, but medium privacy levels:

- ▶ Greylisting is easy to implement, but also relatively easy to defeat with persistence. Delayed delivery of legitimate messages can be a nuisance factor.

3. Recommendations for Carriers and Service Providers

Experton Group recommends e-mail service providers to continue their efforts to fight against spam and malware. The following best practices should be leveraged to optimize existing approaches:

- ▶ Embed all measures into a risk management process. IT risk management must be performed continuously and in close alignment with the business side or as part of enterprise-wide risk management efforts.
- ▶ Consider differentiated measures for individual customer categories – for instance, consumers versus freelancers versus small businesses, based on the risk management approach. Individual user groups have different requirements regarding security, service and privacy.
- ▶ Be prepared for rapidly changing spam methods and attack scenarios. This is a "hare and tortoise" game requiring the providers to permanently scrutinize the efficiency of their current measures and to respond rapidly to any changes.
- ▶ Watch out for changes in legal requirements. The anti-spam regulations of the European Union are only providing a rough guideline. At present, there is much scope for interpretation for concrete anti-spam and anti-virus implementations by carriers and service providers, and in most cases, legal action must be taken to clarify such issues. In particular, providers must phrase their general terms and conditions accurately to prevent litigation. It cannot be excluded that in future, stricter regulations might apply within the European Union, which may have at least an indirect impact on the spam issue.
- ▶ Establish hybrid approaches to filter spam and malware. Providers must protect their customers and networks on various levels and must combine the specific advantages of different approaches, such as checksum analysis and reputation systems. Using commercial spam filtering solutions ensures a high degree of protection mostly at justifiable financial expenses. Such anti-spam solution should, however, provide a high degree of flexibility to be able to comply with rules and regulations and cover the span between security and privacy – as much security as possible for the users, while ensuring their privacy.
- ▶ Ensure the transparency of guidelines and problems, both internally for the provider's IT staff and externally for the customer. Anti-spam guidelines and requirements for user behavior as well as problems caused by spam and malware in the network must be communicated. The goal is to increase the spam awareness among the provider's staff and customers.
- ▶ Support industry-wide collaboration and focus on outgoing e-mail traffic. Cross-company cooperation of ISPs and carriers is desirable to get to the root of the spam problem. Key steps include the development of common best practices and standardized measures against outbound spam, e.g., egress filtering.

4. Cloudmark Profile¹

Cloudmark, Inc. is a global leader in carrier-grade messaging security, delivering the industry's most accurate and efficient real-time spam, virus and phishing protection for fixed and mobile networks. Cloudmark solutions combine Advanced Message Fingerprinting™ technology based on highly sophisticated algorithms and a Global Threat Network of trusted reporters in 163 countries, to provide filtering and security intelligence at all points of the messaging infrastructure. Cloudmark's customers include 90 of the world's largest Internet service providers and mobile operators, such as Comcast, Earthlink, Swisscom, NTT OCN, Sprint/Nextel, and Demon Internet. Cloudmark currently protects more than 260 million mailboxes around the world.

1.4 Service Provider Solutions

Cloudmark's highly scalable solutions were architected from the ground up for the most demanding carrier environments. Cloudmark frees network resources, lowers storage requirements and delivers an immediate improvement in the subscriber experience.

Cloudmark Authority™

Cloudmark Authority is the leading messaging security solution deployed on carrier mail transfer agents (MTAs). With a 100% win rate in service provider accuracy trials around the globe, Cloudmark Authority consistently blocks spam, phishing and email-borne viruses with greater than 98% accuracy and near zero false positives. In addition to this high level of accuracy, Authority requires significantly less processing power than competitive rules or heuristics-based solutions, lowering CPU requirements by up to 90%.

With Cloudmark Authority, service providers receive a secure local copy of all threat data, which is automatically updated every 45 seconds with fingerprints from new threats. This ensures immediate protection against new threats as well as filtering availability. Cloudmark Authority is compatible with virtually any commercial mail transfer agent (MTA) and plugs into the open source Apache SpamAssassin™ platform.

Cloudmark Gateway™

Cloudmark Gateway is a high-performance edge mail transfer agent (MTA) that integrates with Cloudmark Authority. Powerful enough to run policy-based protocol filtering together with full content filtering at the edge of the network, Cloudmark Gateway blocks unwanted email traffic *before* it impacts messaging servers, storage and other infrastructure. Cloudmark Gateway also performs intelligent flow control to control "botnets" and "zombies" from compromising the service provider network. Service providers benefit from lower infrastructure and operational costs and an enhanced subscriber experience free from messaging abuse.

¹ Source: Cloudmark, Inc.

1.5 Cloudmark Technology

The technology components and automated processes underpinning the Cloudmark Authority solution drive the system's high accuracy and efficiency. Only Cloudmark leverages a combination of intelligent fingerprinting algorithms, the world's largest threat detection network (the Cloudmark Global Threat Network), and a trust system that analyzes and corroborates all reporting, to rapidly detect all forms of messaging threats.

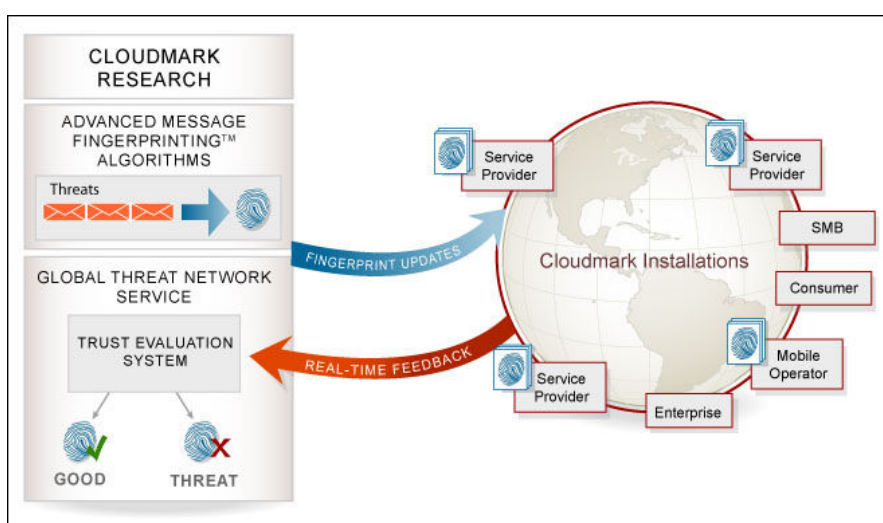


Figure 1 – Cloudmark Technology Overview

1.5.1 Advanced Message Fingerprinting Algorithms

Cloudmark has developed Advanced Message Fingerprinting™ algorithms which identify and track spam, phishing, and virus attacks throughout the network. Cloudmark's fingerprinting algorithms have been optimized for high performance and work in tandem to target different threat attributes embedded in a message. These algorithms are able to identify all mutations in a given attack, such as changes in content, image, sender, URL, or other attributes, enabling threat variants to be stopped in zero time.

Cloudmark's unique content-agnostic threat analysis enables Cloudmark to stop spam in all languages (including those using characters such as Chinese, Japanese and Cyrillic) and formats, including image spam, virus attachments and SMS/MMS spam.

Authority maintains an in-memory cache of all verified fingerprints, updating its list every 45 seconds with the latest data from the Cloudmark Global Threat Network. Authority checks each message against its cache of known fingerprints. If there is a match, Authority classifies the message as spam, phishing, virus or newsletter according to the fingerprint. This architecture enables Cloudmark Authority to achieve message processing throughput that is 20 times faster than traditional rules or heuristics-based content filtering technology.

Cloudmark Authority's performance and stability characteristics are predictable over time. Updates provided by many other messaging security solutions include new rules or other logic that can drastically change the processing complexity on a message, and thereby, impact performance and

stability. In contrast, Cloudmark updates only add to the data stored in the in-memory cache; they do not change the processing done on messages.

Each Cloudmark Authority server maintains its own cache of fingerprints enabling full redundancy and independence. If one server or all servers lose connectivity to the updates server, filtering will continue with the last updates received, which are stored both in memory and regularly backed up to disk.

1.5.2 Cloudmark Global Threat Network

Cloudmark is able to provide extremely fast coverage of new threat outbreaks and therefore, maintain consistently high accuracy, due to its Global Threat Network. Cloudmark's Global Threat Network, consisting of over 260 million reporters in 163 countries, is based on the premise of *networked collective intelligence*. Members of the Global Threat Network span service provider abuse teams, systems administrators, honeypots and end users. With Cloudmark, threat monitoring comes not just from a single department within a company or "dumb" probes, but collectively from a 24 x 7 worldwide network of reporters that can discern, for example, an opt-in newsletter from spam. The millions of Global Threat Network reporters who provide real-time feedback enable Cloudmark to block the latest threats typically within minutes of attack origination. This approach contributes to both faster detection of threats as well as more accurate classification of messages.

The Cloudmark system is able to automatically self-correct, therefore reducing incidents of false positives and false negatives. Cloudmark's global network of reporters is enabled to provide feedback any time an abusive message is missed or a legitimate message is incorrectly classified as abuse. Once this feedback is corroborated, the message is automatically re-classified without manual analysis.

1.5.3 Trust Evaluation System

All feedback by the Global Threat Network is corroborated and analyzed in real time by the Trust Evaluation System (TES). TES tracks the reputation of each reporter and determines when to mark fingerprints as a known abuse message based on the number of reports and by the reputation of the reporters submitting feedback. Trust is earned over time by consistently reporting correct abuse feedback. This system preserves the integrity of reports and ensures that the system is extremely accurate. By identifying trusted sources within the network, Cloudmark is able to fully automate the data analysis process. Since feedback is continuously corroborated, any inaccuracies in message classification are corrected in near real time. No other system offers this kind of a constant monitoring and feedback review.

1.6 Cloudmark's Approach to Security and User Privacy

As discussed in this paper, the ideal messaging security solution would combine a high degree of accuracy in filtering out messaging abuse together with safeguards in place to ensure that individual privacy and government regulations are respected.

Cloudmark's solutions were designed for maximum user privacy, and can be customized to fit the service provider's individual requirements for data security and privacy. For example, service providers can determine exactly what is to be sent back to Cloudmark for analysis — nothing, just analysis headers, or full message fingerprints. In addition, Cloudmark's Advanced Message Fingerprinting fully maintains sender and recipient anonymity as well as data protection.

Local Message Processing

Subscribers have a contract with their service provider that grants them the right to process personal information on their behalf. However, this right does not necessarily extend to third party filtering vendors who do not have a contract with the end user. Therefore, in countries such as Germany and Japan, the user must opt-in for spam filtering.

With Cloudmark, the processing of information is done locally at the service provider site. Cloudmark Authority provides a local cache of anonymous spam fingerprints that is updated every 45 seconds. Advanced Message Fingerprinting algorithms are run against a message to generate a set of fingerprints. If the message fingerprints match any of those in the local cache of known threat fingerprints, the message is marked as spam.

Message Evaluation

The service provider may choose to enable user reporting of false negative and/or false positive messages. Users can forward unwanted messages (or misclassified legitimate messages) back to their service provider or Cloudmark for further analysis and re-classification. Unwanted messages or spam are not in the same category as private communication and therefore, are exempt from data protection concerns.

Spam and false positive messages are first deconstructed into fingerprints before they are forwarded to Cloudmark. Message fingerprints generated by Cloudmark's Advanced Message Fingerprinting algorithms are one-way hashes that makes it impossible to reverse engineer and reconstruct the message. There is no way to decipher the sender, recipient or message content from the fingerprints.

Service providers may apply an additional layer of data obfuscation by choosing only to send the analysis header back to Cloudmark rather than the message fingerprints. The analysis header is just meta-data about what which signatures were applied to the message.

Effective Protection Against Spam, Phishing and Viruses

Another way that Cloudmark addresses the issue of user privacy is through the effectiveness of its solutions. Spam, phishing and virus attacks can compromise individual privacy as well as corporate data security. For example, Cloudmark is able to detect extremely targeted phishing attacks that easily evade traditional spam filters (which are only effective against large-volume outbreaks). By stopping phishing messages from entering email inboxes, Cloudmark protects end users from a significant source of identity theft and fraud.

Traditional solutions provide either security or privacy. However, Cloudmark offers the industry's highest level of messaging security without sacrificing privacy. Due to the flexibility of Cloudmark's solution architecture, the service provider can go choose a variety of configurations: they can elect to disable or enable feedback. If they enable feedback, they can send to Cloudmark the message fingerprints or just the analysis headers. They can also do a hybrid approach and have feedback go directly to them as full messages and then to Cloudmark as analysis headers. Having this flexibility is critical as legal requirements and regulations regarding spam continue to change in the future.