CLOUDMARK

Cloudmark Authority

Server-Based Spam Remediation Software

Reviewer's Guide

Cloudmark Authority Reviewer's Guide

Document version: 1.0
Last revised: May 30, 2003

All examples with names, company names, or companies that appear in this guide are fictitious and do not refer to, or portray, in name or substance, any actual names, organizations, entities, or institutions. Any resemblance to any real person, living or dead, or organization, entity or institution is purely coincidental.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Cloudmark Inc. Cloudmark makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Cloudmark shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or examples herein.

500 Third Street, Suite 265
San Francisco, CA 94107-1805

Contents

A Note To Product Reviewers

We're pleased that you have chosen to review Cloudmark Authority. It's a product we're very excited about. This guide provides you with editorial background information to assist you in writing your review and working with the product. It is not, however, a replacement for the *Cloudmark Authority Installation and Administration Guide;* you should use them together. We hope you'll find this reviewer's guide useful. We'd like your feedback on this document and look forward to reading your published review.

Additional resources are available to assist you with your review. A list of telephone contacts is provided on the next page. Don't hesitate to call when any question—big or small—arises. If this guide accomplishes one goal, it is that we want to help you publish a factually accurate and well-informed review. Also, be sure to read the printed documentation that is included with the product you received. Finally, the Cloudmark Web site, located at www.cloudmark.com provides up-to-the-minute information.

Editorial Contacts

As you conduct your review, we encourage you to call with questions. Though we've worked hard to ensure that you have all the facts needed to write an accurate and comprehensive review, occasionally a question may arise that isn't covered in this guide.

NOT for publication; For use by editors only

Media / Editorial / Press-relations contact:

Tricia Fahey
Vice President, Marketing Communications
Cloudmark Inc.
E-mail: tricia@cloudmark.com
Cell: 415.543.1220 x208

Technical support contact:

Contact Tricia Fahey

For publication

Refer your readers to:

www.cloudmark.com

Part 1

A Tidal Wave of Spam

It's costing billions in productivity and it's getting worse

UP TO HALF THE E-MAIL RECEIVED IN A LARGE CORPORATION IS SPAM

It used to be that the contents of junk e-mail shocked and outraged us. No more. Now it's the sheer quantity. And nowhere is it worse than enterprise corporations.

Up to half of all e-mail traffic coming through an enterprise gateway is spam or contains malicious content. Do nothing and that number will exceed 50 percent in 2004.[1] And spam is very expensive: according to San Francisco-based Ferris Research, spam will cost U.S. businesses more than $10 billion in 2003, up substantially from the $8.9 billion cost in 2002.[2]

The costs of dealing with spam are widespread and reach areas that would not initially seem to be affected:

- Lost productivity as workers sort through, delete, sometimes read, and sometimes click through spam messages
- Need for more servers, network infrastructure, and IT employees to deal with skyrocketing volume of mail
- Legal exposure as those offended by sexually explicit spam seek recourse, often against their employers

As far back as 1999, the U.S. Department of Justice was receiving 3,000 spam e-mails per day in a mailbox set up specifically for that purpose.[3] No doubt that number has increased many times over.

[1] Gartner Group: "Waves of Information Disruption Due in 2003," published Dec. 3, 2002.
[2] Ferris report "Spam Control: Problems and Opportunities," published Jan. 6, 2003.
[3] http://www.usdoj.gov/criminal/cybercrime/unlawful.pdf

Spam or Not Spam?

Much junk e-mail is obvious. Be it get-rich-quick schemes, home mortgage refinancing opportunities, reduce debt ploys, or inkjet cartridge sales pitches, everyone is inundated. Pornographic materials are also obvious, and raise the specter of legal exposure from offended employees.

But what about cooking instructions for roast chicken breast, medical research about breast cancer, or communications between a company purchasing agent and an office-supply vendor about printer consumables? Clearly these are not spam. Cloudmark's advanced predictive statistical analysis methods can sort out real spam from legitimate e-mail.

Calculate the Cost of Spam

Cloudmark has an online Spam Cost Calculator that your reader can use to measure productivity losses. The calculator uses employee count, average salary, daily spams per employee, and seconds spent per spam. To use the calculator, refer your readers to www.cloudmark.com/products/authority/roi.

CLOUDMARK AUTHORITY INTERCEPTS SPAM AT A COMPANY'S GATEWAY, BEFORE IT REACHES THE E-MAIL SERVER.

Distributed vs. Centralized Spam Fighting

There's no argument about the desire to block spam. But what is the best way? Unless it's done right, the cure could turn out to be worse than the disease. Consider a couple of methods:

Alternative 1:	Individual users create spam-blocking rules in their client e-mail program (Microsoft Outlook, Lotus Notes, Eudora, etc.)
Advantages:	1. IT doesn't get involved in solution 2. No budget outlay for spam-fighting solution
Disadvantages:	1. Users still have to receive and read spam in order to create spam-blocking rules. 2. Volume of spam traffic through corporate network is not reduced 3. Costs actually rise with additional loss in worker productivity as they create individual rules 4. No way to institute corporatewide policies

Alternative 2:	Install network-based spam-blocking software
Advantages:	1. Productivity is preserved as end users no longer receive spam messages 2. Corporatewide solution assures consistent policy 3. Legal exposure to offended employees is avoided 4. Reduction in network traffic, greatly reducing strain on the corporate e-mail system 5. Cost of solution is quickly returned
Disadvantages:	1. Requires IT involvement 2. Investment in software solution

Key Editorial Point

Cloudmark Authority intercepts spam at a company's gateway. It never reaches the e-mail server or individual users' desktops. Network performance is preserved, infrastructure upgrades are avoided, IT staff maintenance is minimized, workers are protected, and productivity is maintained.

It's obvious that the best way to deal with spam in a corporate environment is to get spam-fighting tools off the desktop and onto the server. Cloudmark's approach of using SpamDNA in Authority to predict spam is best; other solutions are stuck with obsolete technology that will eventually collapse under their own weight. The next section of this reviewer's guide examines the two competing technologies and explains why Cloudmark Authority is the superior solution.

Part 2

Understanding Authority

You can predict or react after the fact. Predicting is better.

It's said the only constant is change. It's true about spam. Subject text, sender's addresses, and routing continually change, making nearly every message unique.

CATCHING SPAM CAN REQUIRE THOUSANDS OF RULES REQUIRING CONTINUAL UPDATES. THERE IS A BETTER WAY.

Several techniques exist for fighting spam at the server, including whitelisting, blacklisting, and challenge/response. For a variety of reasons—perhaps most notably problems associated with scalability—using these techniques simply isn't feasible for companies with more than 500 employees.

Therefore in this guide, we'll focus on the two most practical methods of dealing with spam: **RULES-BASED** and **PREDICTIVE ANALYSIS**. Cloudmark believes the latter method is clearly superior. Before you test Authority, it's important to understand both methods. Think of this section as a crash course in spam catching.

Rules Can't Keep Up

How do individual users prevent spam? They can't; the best they can do is to try blocking it. Most often, the individual uses an e-mail client to create rules. But one or two rules won't do. Suppose a user builds rules to delete e-mail messages in these circumstances:

- Subject contains "reduce debt"
- Subject contains "!!!"
- Subject contains "Ink refills"
- Subject contains "Win a vacation"
- Sender domain is ".cz" (all mail from the Czech Republic)
- Sender name contains your own name

That works fine for a day or two. But then the user gets e-mail like this:

- Subject contains "save money"

- Subject contains "!!"
- Subject contains "I n k r e f i l l s"
- Subject contains "F r e e v a c a t i o n"
- Sender name is "magda@isp.cz" (your Czech aunt)
- Sender name is your name (you sent a copy to yourself)

In each case, the rules you created won't work at all or are likely to delete messages of great importance to you (the dreaded FALSE CRITICAL condition). You could create a rule that looks for "save money," but that won't work the next week when you get a message with "call off the creditors" in the subject.

RULES-BASED SYSTEMS ARE UPDATED MANY TIMES EACH DAY. AUTHORITY IS UPDATED MONTHLY.

Death Spiral

It's a viscous, never-ending cycle—and you are merely reacting to spam that you've already received. What good is that? You could wind up with dozens, hundreds, or even thousands of rules. Commercial rules-based spam-detection software contains tens of thousands of rules, requires a dedicated staff making it costly and error prone, and demands more and more computing resources. Rules continually need to be written every minute (by the software company, user organization, or both), and these modifications must be applied often—usually many times each day.

Authority's Smarter Way

Authority is not rules-based. Instead, it uses a variety of techniques, including message structure analysis, Internet routing analysis, Bayesian[4] statistical models, and other proprietary "classifiers" collectively called the Authority engine. In Authority, the inputs to its engine are called "spamGenes." Together, these spamGenes™ are known as "spamDNA." As the nature of spam changes over time, these classifiers work together to predict which messages are most likely to be spam. Authority is built upon a foundation of about 200 spamGenes. Only 200 are necessary because SpamGenes are highly efficient, powerful and 10 times more effective than each rule. In fact, Authority becomes more effective over time by constantly evolving the spamDNA it gets from SpamNet, thus it only requires updates every 30 to 60 days. This compared to rules-based methods recycling tens-of-thousands of rules a day and needing updates and tweaking every minute.

AUTHORITY NEEDS ONLY 200 SPAMGENES, NOT THOUSANDS OF RULES

[4] Bayesian theory is based on the work of Rev. Thomas Bayes (1702–1761). Bayes' theorem allows new data to be combined with historical data for statistical analysis. Bayesian networks organize an existing body of knowledge (a database of spam, for example) with cause-and-effect relationships among key variables, analyzing the extent to which one variable is likely to affect another. Published posthumously in 1763, Bayes' *Essay Towards Solving A Problem In The Doctrine Of Chances* calculates probabilities among causally related variables whose relationships are not easily derived through experimentation. For additional information, visit The International Society for Bayesian Analysis (www.bayesian.org) or the Bayesian Statistical Science page of the American Statistical Association (www.amstat.org/sections/SBSS). A useful New York Times article, published on April 28, 2001, discusses a real-world application of Bayesian theory in the field of medical research. (www.ai.mit.edu/~murphyk/Bayes/nyt.28april01.html)

As an example, take a look at "I n k r e f i l l s" and "f r e e v a c a t i o n" from the preceding list. Both contain lots of spaces. In fact, fully half the characters in each are spaces, a ratio that is way out of kilter with what you'd see in normal writing.

"Nothing" Can Be Everything

When you noticed these excess spaces, you ignored the other characters. The message could be about ink refills, free vacations, or anything else. This is important: In this case, structure, not content is what matters. This is an example of just one way in which Authority analyzes messages.

Of course, having an abnormal character-to-space ratio in a subject line isn't a guarantee a message is spam. But you'd take note of it, raising your confidence level somewhat. To be even surer, you'd investigate deeper, perhaps examining the message body. Suppose the body contains a Web site link. The presence of a link *and* excess spaces should make you much more confident the message is indeed spam. The actual link destination doesn't matter; it's the mere presence of one that's important.

ANALYZING A MESSAGE'S STRUCTURE IS OFTEN MORE USEFUL THAN EXAMINING ITS CONTENT

Other Spamming Methods

Repeated characters or spaces is just one way spammers try to outsmart spam-detection software. Here are two common methods.

- Messages encoded in base64 in hope that servers will blindly route message to addressee, whose e-mail client will automatically decode the message
- Forged or inconsistent list of IP addresses or sub-domains as e-mail is relayed from server to server as it travels to the intended destination

Key Editorial Point

What is spamDNA™? SpamDNA™ includes many statistical methods including message structure analysis, Internet routing analysis, Bayesian statistical models and other proprietary "classifiers" collectively called the Authority engine. *SpamDNA evolve and improve over time learning from both spam and legitimate email to deliver the highest accuracy and lowest false criticals. Rules-based technologies focus solely on spam.*

The DNA of Spam

Cloudmark's method of identifying spam is a radical departure from traditional rules-based methodologies. So how does it work? The key is **spamGenes**.

Just like the DNA in biology, e-mail messages have a certain structure. Scientists can predict the likelihood that someone will contract a particular disease by looking for specific gene mutations. This isn't any different than e-mail spam: spammers continually mutate their message structures in the hope of avoiding detection. Authority predicts whether a message will be spam by looking for specific mutations in message structure called spamGenes.

Key Editorial Point

Authority automatically becomes increasingly effective over time by continually evolving its SpamDNA which it gets from Cloudmark SpamNet.

Varying Levels of Confidence

It's important to note that you haven't made a flat-out "is-or-isn't" decision about the message being spam. But your level of confidence has risen. That's another key advantage over rules-based systems that only allow spam or not spam determination.

.

Authority lets you handle messages differently, depending on confidence level. If you're 95 percent confident the message is spam, you can reject it. If you're 75 percent certain, you might keep the message but move it to a quarantine folder. If you're 63 percent sure, you could insert text, say, "POSSIBLE SPAM" into the subject field and route it to the addressee. If you're only 5 percent confident—meaning it is almost certainly a legitimate e-mail message—just route it to the addressee.

The following chart identifies actions you might take, depending on the "confidence level" assigned to an e-mail message. Remember, these hypothetical settings are for illustration only and do not represent any actual set of processing parameters.

Spam-Handling Scenario

"Is it spam?" Confidence Level	Possible Processing Action
90% – 100%	Delete message
80% – 90%	Delete message, send refusal to sender
70% – 80%	Save message in a central location, do not deliver to addressee
60% – 70%	Insert text "POSSIBLE SPAM" in subject field, deliver message to addressee
0% – 60%	No action taken, deliver to addressee

Source: Cloudmark

SPAM DNA AVOIDS "FALSE POSITIVES" WHICH WOULD DELETE LEGITIMATE MESSAGES AND THE FAR MORE SERIOUS "FALSE CRITICAL"

Rules-based systems don't offer this luxury of multi-tiered conditional handling. With them, the instant a message fails a test (subject contains "!!", for example), it's deemed spam and flat-out rejected. This inflexible method may result in a **FALSE POSITIVE** or worse, a **FALSE CRITICAL** condition, deleting legitimate mail. That wouldn't be good if the corporate CEO sends out a companywide message with "We Have Acquired CompanyX!!" in the subject.

- A **false positive** is a legitimate message that's flagged as spam but with no serious impact. Treating a newsletter to which a user subscribes as spam is wrong, but has no serious downside.
- A **false critical** is far more serious. An example is a request from an important customer, communication with a business colleague, or worse, a directive from the CEO. All could have far more serious downside than the newsletter example cited above.

Rules Are Reactive, Not Predictive

These two tests, high spaces-to-characters ratio and link presence, are simple, yet real-world examples. Detecting excess spaces, regardless of the intervening text, can't be done by writing a rule. And what if there are two spaces between each text character instead of one? You'd have to write a rule for each text-and-space string you encounter. And you can't do that until you've already been hit by the spam. Authority catches the message before it reaches the e-mail system.

Quick Feature Overview

RULES-BASED SYSTEMS DO NOT OFFER CONDITIONAL HANDLING. WITH THEM IT'S EITHER "IS" OR "ISN'T" SPAM.

No doubt, you'll probably want to explain to your readers why Authority is different from other spam-fighting products. This chart provides a fast look at Authority's capabilities. You'll find additional information about these items throughout this reviewer's guide.

7 Cool Facts About Authority	
It's Rules Free	Uses advanced statistical methods to predict which messages are spam. No need for a gigantic rules database.
It Learns	Relies on 200 spamGenes that evolve as the nature of spam changes. No need for thousands of rules, or constant updates.
It Has 475,000+[5] Spam Researchers	Leverages trusted SpamNet users worldwide who submit genuine spam messages to Cloudmark spam database
It's Lean	Runs on the actual MTA gateway server, does not require acquisition of any additional hardware
It's Low Maintenance	No need for daily update of rules database. Updated spamDNA sent on as-needed basis, usually monthly.
It's Agnostic	Authority runs on Unix or Windows e-mail gateways
It's Ready for Windows Server 2003	Authority has been tested and runs with Windows Server 2003 and Outlook 2003
It Saves Money	Authority slashes network traffic, relieving strain and reducing need for additional infrastructure and staff
It's Secure	Makes no calls or requests outside the corporate firewall
It Relieves Stress	On the network, that is. Can cut e-mail traffic 40% or more, eliminating need for costly infrastructure upgrades

Source: Cloudmark

Spam Updates: Hourly or Monthly?

Rules-based spam-fighting software is often updated many times per day, requiring an open connection to the software provider and taking a toll in system overhead, however small it may be. That's not the case with Authority.

[5] As of June 2003.

AUTHORITY'S MONTHLY UPDATE IS A SINGLE FILE OF ABOUT 400 KBYTES

Instead of depending on a near-continuous stream of updates, Authority requires updating only about once a month. A spamDNA update is called a "cartridge," which is actually a file. The update process couldn't be simpler:

- **Windows Server.** The update "cartridge" is a single .dll (dynamic link library) file of about 400 Kbytes. This update is quickly applied without taking Authority out of service.
- **Linux, Solaris.** The update "cartridge" is a single .so (shared object) file of about 400 Kbytes. This update is quickly applied without taking Authority out of service.

Product Info Box

If your review contains a product information chart, you may find the following information useful.

Cloudmark Authority Summary	
In Brief	Spam-fighting software that uses predictive self-learning statistical analysis methods and a worldwide, 475,000-strong contributor's network, instead of a giant rules database to identify and weed out junk e-mail. Its 200 or so "spamGenes" need updating only about once a month, unlike rules-based systems that require tens of thousands of rules and constant updates, usually several times a day.
Operating systems supported	Windows Server, Linux, Solaris
Price	Pricing is based on number of users. Authority is typically deployed in organizations that support more than 1,000 mailboxes and is priced as such. A free 30-day trial is available to help companies position themselves to recover annual lost productivity estimated to be $86 per employee. Payback ROI is under 60 Days.
Vendor	Cloudmark, Inc. San Francisco, Calif.
Web site	www.cloudmark.com

Part 3

The Competitive Landscape

We believe Cloudmark Authority is better, and we'll quote a well-known competitor's own marketing materials to prove it

Cloudmark Authority is most often compared to Brightmail Inc.'s Anti-Spam Enterprise Edition product. Cloudmark's predictive Bayesian statistical method is more proactive and requires far less maintenance, updating, and intervention than Brightmail's rules-based technology. The following chart compares the two divergent approaches. Brightmail items are direct quotes from its Anti-Spam 4.5 Enterprise Edition data sheet.

Comparative Product Analysis
Cloudmark Authority vs. Brightmail Anti-Spam

Brightmail Anti-Spam 4.5 Enterprise Edition	Cloudmark Authority	Comment
"Attracts spam using e-mail decoy accounts. Collected e-mail is sent in real time to the BLOC (Brightmail Logistics and Operations Center)"	Decoy accounts not needed. Real people using their real e-mail accounts submit actual spam to Cloudmark's SpamNet network	Even several thousand decoy accounts can't compare to SpamNet's 475,000 active users with real e-mail accounts
"A 24/7 logistics & operations center where rules are created, validated, and made available to the Brightmail Server in real-time"	spamGenes use advanced Bayesian statistical methods to predict and identify changing spam patterns over extended periods of time	No need for a large staff to write or verify new rules around the clock, every day, all year long
"Continuously updated rules in the Brightmail Server check all incoming e-mail"	SpamDNA needs updating only about once a month; it checks all incoming e-mail	Rules can only react after the fact; SpamDNA is a predictive method
"Rule updates are made available every few minutes in response to spammers' changing techniques"	Updated SpamDNA file is sent to customers only when necessary; about once a month	Dozens of daily updates generate network traffic and require an open port; no need with Authority

Sources: Cloudmark,
Brightmail Anti-Spam 4.5 Enterprise Edition data sheet (www.brightmail.com/pdfs/as_4.5_ent.pdf)

Another competing solution is Postini Perimeter Manager from Postini Inc. This product is radically different from Cloudmark Authority: it is essentially an outside service to which an enterprise customer subscribes. All incoming e-mail is first sent to this service for scrubbing; spam is filtered out and legitimate mail is then re-routed to the corporate customer.

Authority is better for a couple of key reasons. First, Cloudmark strongly believes that e-mail should never be handled by an outside service; it's an enormous security risk. Diverting e-mail to an outside service may result in communications delays and certainly creates more points of potential failure. Cloudmark's small-footprint, low-maintenance solution runs at the customers' premises, is completely secure, and requires no investment in additional hardware.

The following chart compares the two divergent approaches.

Comparative Product Analysis
Cloudmark Authority vs. Postini Perimeter Manager

Postini Perimeter Manager	Cloudmark Authority	Comment
"Services over 1,000 companies worldwide"	Each Authority installation services exactly one company—yours, and does it at your premises	Diverting all e-mail to a third-party for spam processing creates multiple points of failure
"All incoming e-mail is routed through Postini's secure data centers and scanned"	Runs inside your corporation. No need to send mail to an outside service bureau, an enormous security risk	E-mail is never handled by a third-party. Do false positives and false criticals just disappear?
"Quarantines over 95% of spam"	SpamDNA assigns confidence levels up to 99.99%	95% success rate is a 5% failure rate
"Thousands of complex rules designed to check specific parts of every message"	Just 200 spamGenes use Bayesian statistical methods to predict and identify changing spam patterns over extended periods of time	No need for a large staff to write or verify new rules around the clock, every day, all year long
"Combining content filtering and managing your SMTP connection is the highest level of protection"	Stops spam at the gateway, before it ever reaches the SMTP server	We agree, but why do it at an outside location that process e-mail for dozens of companies?

Sources: Cloudmark,
Postini Web site (www.postini.com/demos and postini.com/services/perimeter_manager.html)

Part 4

Testing Cloudmark Authority

Installation takes just minutes on Linux, Solaris, or Windows

As you work with Cloudmark Authority, you'll find that it's very easy to install and that its foot print in memory is quite small. In this portion of the Cloudmark Authority Reviewer's Guide, we'll discuss the hardware environment, system requirements, installation, and testing.

AUTHORITY INSTALLS ON THE E-MAIL GATEWAY MTA SERVER AND REQUIRES NO ADDITIONAL HARDWARE

Don't hesitate to contact Cloudmark with questions as you proceed.

Hardware Environment

To run Cloudmark Authority, you'll need an e-mail gateway and an Internet connection. In a Windows environment, you'll probably want to have a client workstation running Outlook. In a Unix environment, you may find interacting directly with the server is sufficient.

Typical Enterprise E-Mail Architecture

Cloudmark Authority is compatible with just about any enterprise e-mail architecture (Fig. 4-1). You have the option to install Authority as a Sendmail plug-in (Fig. 4-2) or as a Windows application that uses the Windows SMTP Server (Fig. 4-3).

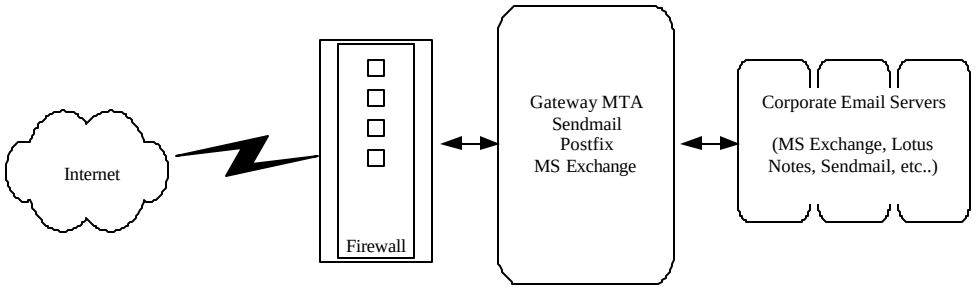
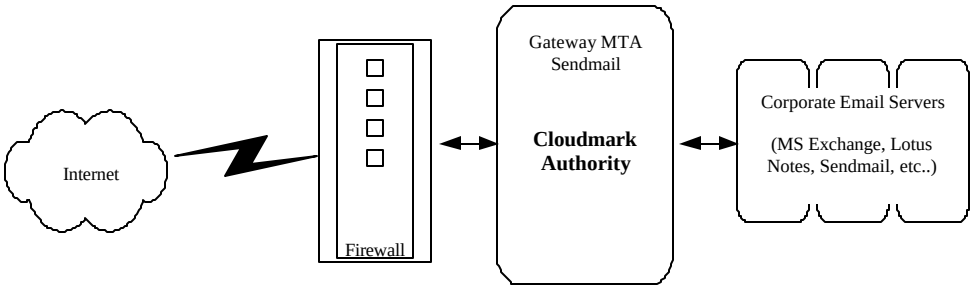


Fig. 4-1. Typical Enterprise E-Mail Architecture

Authority with Linux/Solaris Sendmail



Fi

g. 4-2. Authority in a Linux or Solaris Sendmail Environment

In a Sendmail environment, Authority is installed via the Milter interface. Authority plugs into Sendmail, using it to relay messages. Running in a Linux or Solaris environment requires Sendmail on the gateway.

Authority with Windows Server

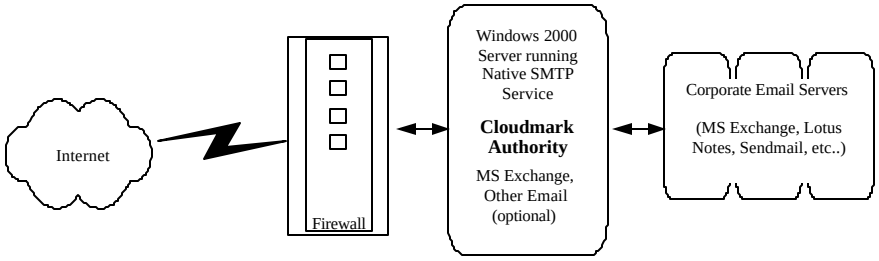


Fig. 4-3. Authority on Windows Server Running Windows SMTP Server

In this scenario, the server must be running Windows 2000 Server or later. This does not need to be a dedicated server.

In Windows server environments, Cloudmark Authority uses the SMTP Server that is part of Windows 2000 Server. Authority interoperates with all SMTP-compliant e-mail servers (Lotus, Exchange, Eudora, PostFix, etc...) via standard SMTP relay methods.

Required Expertise

To install, configure, and properly evaluate Cloudmark Authority, you should have a solid working knowledge of either Sendmail or Microsoft 2000 Server running the SMTP Server, depending on your choice of testing environment.

Software Environment

When you install Authority, it intercepts the incoming stream of SMTP mail traffic through either the Sendmail Milter interface (Linux and Solaris) environments, or the Windows SMTP Server (Windows 2000 Server or later).

AUTHORITY REQUIREMENTS			
	Linux	**Solaris**	**Windows**
Operating Systems	RedHat 7.2, 7.3 Sendmail 8.11 – 8.12.9, compiled with Milter	Solaris 8 or higher Sendmail 8.11 – 8.12.9, compiled with Milter	Windows2000 or 2003 Server with SMTP Server
Disk space	5GB –10GB or more for saved spam		

Source: Cloudmark

Operationally, Authority is simple: it receives a stream of SMTP messages from the SMTP source, filters the spam, and then returns the filtered stream back to the same SMTP source.

Installation and Configuration

To install Authority, refer to the *Cloudmark Authority Installation and Administration Guide*. It provides detailed, step-by-step instructions for installing the software in a Windows, Linux, or Solaris environment. However, the following section highlights a few items of note. Depending on the technical depths to which your review story goes, you may choose to share these items with your readers.

The Linux/Solaris version of Authority installs as an executable that is invoked from a console command line. The Windows Server of Authority is a single .dll file that is quickly installed with the included InstallShield utility.

Linux, Solaris, and Milter

The server must run a version of Sendmail that enables the Milter interface. Many Sendmail binaries are compiled with this interface enabled, but many are not. Refer to the Authority installation guide for how to determine if Milter is enabled. If it is not, it will be necessary to recompile the Sendmail binary.

Windows 2000 Server and SMTP

Refer to the Authority installation guide for how to determine if SMTP server is installed. Installation, if necessary, is quickly done through IIS (Internet Information Services).

Defining Spam Handling Policies

Authority can quarantine, delete, modify, or refuse spam. If none of those actions are taken, Authority, by default, simply routes the message to the addressee. This following chart identifies all the possible actions that Authority can take delivering high flexibility to IT managers. In this version of Authority, only one action can be applied to any given e-mail message.

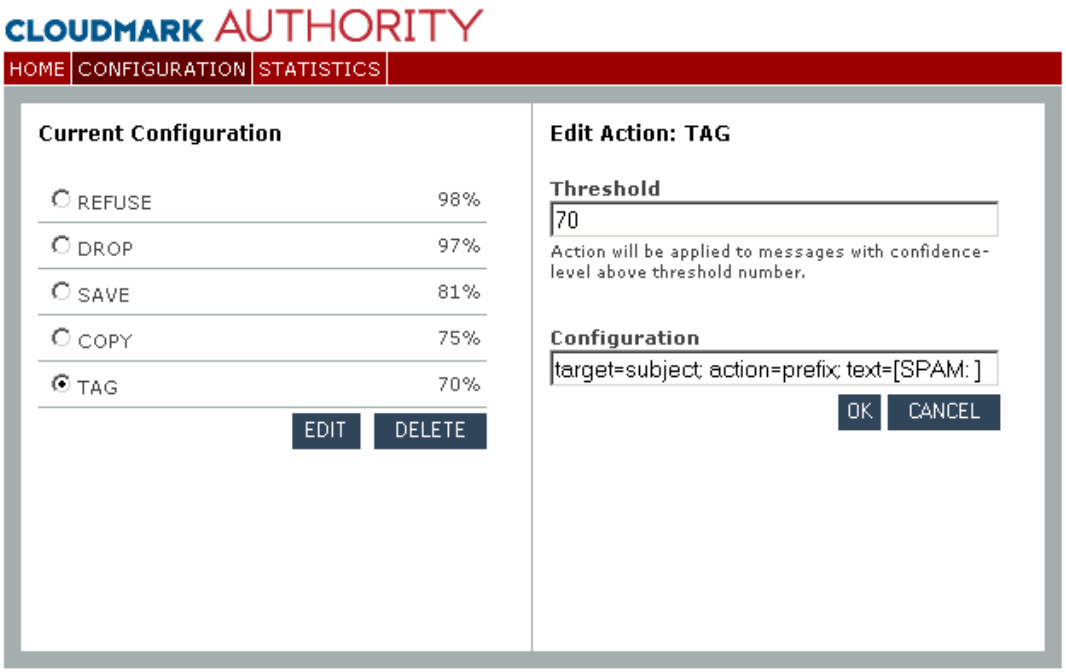
Message Handling Actions

Action	Description	Addressee Receives	Archive to Server	Message Modified	Impact to Addressee
[None]	Deliver to addressee	Yes	No	No	None
Copy	Deliver to addressee; keep copy on server	Yes	Yes	No	None
Tag	Insert text into message; deliver to addressee	Yes	No	Yes	Low
Add Header	Add message header; deliver to addressee	Yes	No	Yes	Low
Save	Keep message (quarantine) but do not deliver	No	Yes	No	High
Drop	Delete message	No	No	No	High
Refuse	Delete message; send error to sender	No	No	No	High

Source: Cloudmark

The first four actions are "non-intrusive" in that the message is sent to the addressee. The last three actions are considered "intrusive;" as the addressee does not receive the message.

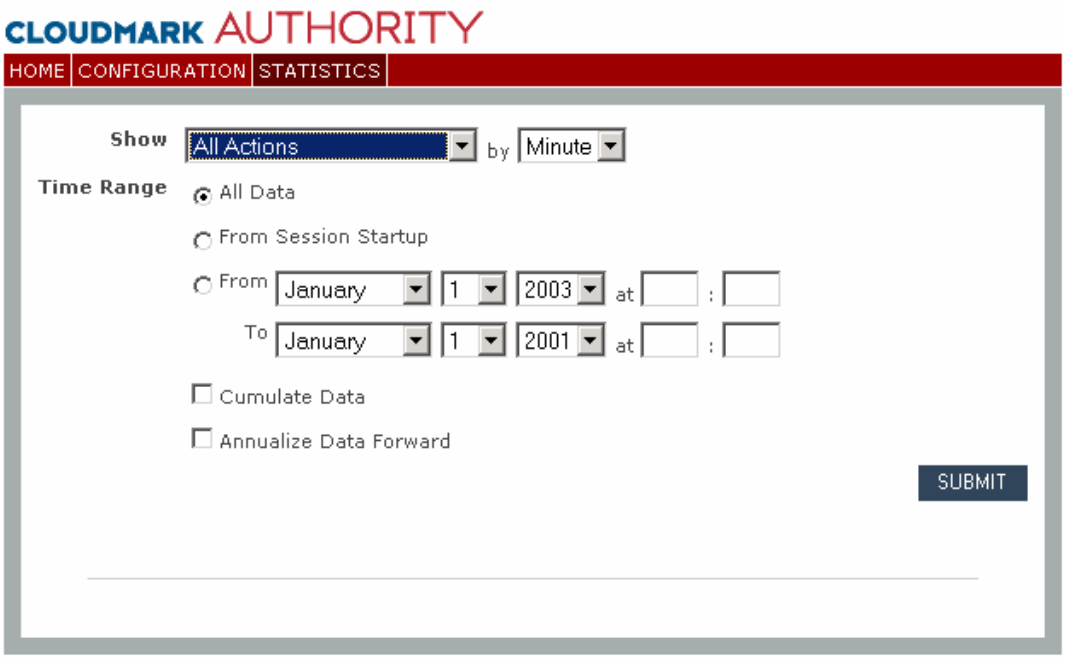
Here is an example of the web user-interface for managing actions. It is designed to make the flexibility of Authority easily manageable for IT administrators. The following shows the **Edit Action**.



To edit a current Action, click the radio button next to the Action you want to edit and then click the Edit button. In the right hand pane you will see an Action and all of the values currently associated with it. All of the data can be edited just as if you were creating a new Action. Once you click OK the changes are stored in memory.

Authority Statistics

Authority has a variety of reporting options that can be generated from the Statistics page.



Statistics can be generated from a dozen report types. Report types include:

- Spam vs. Legitimate Mail – Based on the Spam Definition %. All mail with this % and greater are considered spam and shown in this report relative to the total "legitimate mail"
- Current Actions – Based on the currently used Actions. This report would show each Action as a portion of the total email
- Save – Based on the total # of messages that had the Save Action applied to it.
- Company Dollars Saved – Based on the variables (Average salary and # seconds per email)
- Company Time Saved – Based on the variable (# seconds per email)

Authority Detention Center

The Detention Center is designed to simplify the management of detained mail. If users think a message may have been blocked, or if an incoming legitimate message is accidentally blocked, it may be necessary to Search for messages, Send a

Copy to examine their content and Release appropriate messages to their original recipients.

The Detention Center is only pertinent if you are using the SAVE or COPY actions. These are the only actions that detain messages.

When these actions are configured, you specify the location and type of detainment. (See Action Definitions in Installation Guide for details.) Authority allows detained messages to be stored in individual per-user mailboxes, or in centralized consolidated mailboxes. Consolidated mailboxes are created anew on an hourly or daily basis.

Searching Detained Messages
By selecting the Detention Center tab in the Authority Control Console, you can access the Detention Center interface. The main interface is a search form that allows a search of the detained messages to be performed.

Editorial Review Keys

Cloudmark Authority is easy to install, nearly transparent in operation, and requires only occasional updates. Here are the key editorial points that you'll discover as you work with the product.

Plugs into Existing Hardware and Software

Authority integrates seamlessly into the existing e-mail infrastructure which the IT staff already knows how to configure and operate. The result is fast installation with minimal ongoing administration.

Frugal with System Resources

Authority runs in memory and has a performance impact on the message transfer agent (MTA) of only 5 percent to 10 percent, compared with competing products that may degrade MTA performance by 40 percent or more, possibly requiring additional hardware acquisition and IT support as a result.

Firewall Security

Authority operates without a connection to Cloudmark. Other solutions require a constant connection to external servers, requiring reconfiguration of firewalls to update their rules every minute and reactively handle new spam.

Minimal Impact on IT Staff

Once installed, Authority requires only occasional updating—every 30 to 60 days. Reactive solutions require daily "tweaking" by IT staff to maintain effectiveness. These products often require several updates per day.

Keeps E-Mail Secure

Authority does not compromise security because e-mail never leaves the corporation. Other solutions send data and e-mail outside the corporate firewall.

Near-Zero False Positives

Authority's balanced approach uses knowledge about legitimate messages and spam to produce accurate results. Other solutions only look for spam.

Highly Granular Multilevel Spam Handling

Authority assigns to each message a value from 0 percent to 100 percent, indicating its confidence level that the message is spam. IT administrators can set multiple policies for handling each message. Other solutions allow only a black-and-white "is spam" or "isn't spam" that is inflexible, can generate false positives, or worse, false criticals.

Platform Independence

Authority runs on Linux, Solaris and Windows Server 2000. It is fully compatible with Windows Server 2003.

Proven Return on Investment

Cloudmark's spam-free guarantee offers a free 30-day evaluation period during which potential customers can demonstrate a return on investment before entering into a purchase commitment. Competing products require up-front fees or expensive deployment of additional servers.

Hands-On Testing

Once you have installed Authority and confirmed that it is running properly, you'll move on to hands-on testing. To test Authority, you'll need to provide it with a stream of SMTP messages. You can use your own, obtain a test stream from Cloudmark, or possibly obtain a message stream from other vendors. If you are performing a head-to-head comparison of multiple products, you'll want to run all provided SMTP streams through all solutions.

For testing, we suggest that you use the following two different scenarios:

Test Scenario 1: Prepared Message Files

To ensure that Authority is installed and configured correctly, you should first run tests using two different prepared files, one containing 100 percent spam (all spam) and another containing 100 percent legitimate mail (no spam). In this way you'll know exactly what the test results should be. Any variance might indicate a configuration anomaly.

> **All Spam.** Using a message stream consisting of all spam should result in no messages being passed back to the SMTP message stream. Cloudmark can provide you with an all-spam stream.
>
> **No Spam.** An "all legitimate" message stream is a good way to test for false positives. No messages from this stream should be filtered out. Due to privacy considerations, Cloudmark is not able to provide you with a no-spam message stream.

Should you obtain different results, contact Cloudmark. We'll work with you to find the source of the anomaly and help you to rectify it.

Test Scenario 2: Live Message Stream

After obtaining the desired result from the all-spam and no-spam prepared message-stream files, you should run a live test using actual incoming messages.

To ensure a "real-world" result, we suggest you allow a minimum of 10,000 messages to be processed.

A live message stream, one that you'd see in the normal daily operation of a business, contains both legitimate and spam e-mail. The results you obtain are what an enterprise business can expect once Authority is installed, configured, and running uninterrupted on a day-to-day basis.

Why Go Live? There's a very specific reason for using live, incoming e-mail: Prepared files (all-spam and no-spam) contain, by their very nature, only messages that have occurred in the past. Consequently, vendors of rules-based anti-spam software have probably already responded, writing specific rules for the types of spam contained in these files. That's not a true test of anything! When you test with a live message stream, you'll have an excellent opportunity to compare Authority's spamGene predictive technology with the after-the-fact method of continuously writing rules.

Even if you test Authority using your own SMTP data stream, we suggest that you first run it with a stream provided by Cloudmark. Doing so should yield very specific results; if you do not obtain these results, Authority is not properly configured and may not perform optimally.

Viewing Results

If you are testing Authority on a Microsoft Windows Server platform, you may prefer to see messages sent to the addressee (both tagged and unmodified) by setting up a client PC running Microsoft Outlook. or Eudora.

When testing Authority in a Linux or Solaris server environment, you may prefer to view these same tagged and untagged messages directly on the server using the Mutt e-mail client.[6]

Typical Results

The following chart shows results similar to those you might obtain when testing Cloudmark Authority. Your results will vary, based on the message stream presented to Authority, and on the settings of several parameters.

Test Result Samples
Subject Field Tags When Spam Confidence Level = 96%

Before	After
Got To See This CVYKBO8SR	99.97%SPAM: Got To See This CVYKBO8SR
Information you need to plan	99.97%SPAM: Information you need to plan
Need a refinance loan?	99.97%SPAM: Need a refinance loan?
Save on Dental Care	99.97%SPAM: Save on Dental Care
Be your own boss	99.97%SPAM: Be your own boss
WORK FROM HOME	99.97%SPAM: WORK FROM HOME
ADV: 30 Million Fresh Email	99.98%SPAM: ADV: 30 Million Fresh Email
Customer Get it for free!!!	99.98%SPAM: Customer Get it for free!!!
Free quotes for new home loan	99.98%SPAM: Free quotes for new home loan
Great rates (0kNV)	99.98%SPAM: Great rates (0kNV)
Holidays are coming!	99.98%SPAM: Holidays are coming!
Hundreds of Great Gift Ideas!	99.98%SPAM: Hundreds of Great Gift Ideas!
WE ARE HIRING	99.98%SPAM: WE ARE HIRING
[adv: adlt] - It's Really Free	99.99%SPAM: [adv: adlt] - It's Really Free

Source: Cloudmark

Results in the chart were obtained with the following settings

- "Tag" was the only defined message handler
- Tag confidence level was set to 96%

[6] Mutt 1.4.1 and 1.5.4 were released on March 19, 2003. Mutt is included with many Linux distributions, but you can download these latest versions from www.mutt.org.

- Parameters were set to:
  `target=subject; action=prefix; text=[%p%% confidence SPAM:]`

These settings instruct Authority to tag (insert a text string, "SPAM:") at the beginning of a message's subject field if the spam confidence level is 96 percent or greater. Messages with a confidence rating of less than 96 percent are untouched. All messages in this scenario are routed to the addressee ("Tag" does not divert messages, merely inserts the designated text).

Note: "Tag" is best for a Windows Server platform; this setting routes messages to the addressee and can be easily viewed on a client PC running Outlook. For Linux and Solaris server installations, you may prefer to specify "Save" instead of "Tag" as the message handler. Doing so keeps the e-mail message on the server, easily viewed with Mutt.

After configuring Authority, you are ready to send messages through the server. The result should be similar to what is shown in the chart, where the confidence percentage and warning text "SPAM:" are inserted into the subject field.

Keep in mind that the parameters set for this test defined only one confidence level tier and is not necessarily representative of a real-world installation.

This particular test scenario is designed to make it easy to see what is considered spam by Authority and what isn't. You also could set multiple handlers with different confidence levels to perform the "tag" action but insert a different text string for each tier. You'll still see each message and get an even more in-depth look at the confidence levels assigned to different messages.

At any time, feel free to contact Cloudmark with your questions, anomalies, or results that are not in line with your expectations.

Part 5

Additional Materials

This section contains a variety of background materials that you may find useful as you compile information for your review of Cloudmark Authority.

Authority FAQ

The questions in this FAQ are general in nature and are all covered elsewhere in this reviewer's guide. Reviewer's who prefer a question-and-answer format for product information should find this section useful.

Q Does Authority require additional hardware?

A No. Authority runs on the existing mail gateway server. Because it seamlessly integrates into the existing e-mail infrastructure, which the IT staff already knows how to configure and operate, it installs quickly and requires little ongoing administration.

Q What is Authority's operational overhead?

A Authority runs in memory and has a very small memory footprint of less than 1 megabyte. It has an impact on the message transfer agent (MTA) of 5 percent to 10 percent; other anti-spam products impact the MTA by 40 percent, and require additional hardware, configuration, and support.

Q Is Authority dependent on third-party network services?

A Authority operates without a connection to Cloudmark. Other solutions require a constant connection to external third-party servers, which means reconfiguring firewalls in order to update their rules every minute and reactively handle new spam.

Q How often is Authority updated?

A Authority only needs updates every 30 to 60 days. Other reactive solutions require updates to their rules database at least once (and usually more often) per day. This is why they require a constant network connection to third-party servers.

Q Is Authority more secure than competing products?

A Authority does not compromise security because e-mail never leaves the corporation. Other solutions send data and e-mail outside the corporate firewall.

Q How often does Authority erroneously label a genuine message as spam?

A Authority has a near-zero false positive rate. Authority uses its knowledge about both legitimate messages and spam to produce accurate results. Other solutions look for spam only.

Q Can IT fine tune Authority?

A Absolutely. Authority offers considerable flexibility for IT managers. Authority generates a confidence level between 0 percent and 100 percent for every e-mail message. IT can set a site policy that triggers different message handling based on Authority's confidence level. Other solutions only allow an "is-or-isn't" determination, resulting in false positives, and forcing continual review of detained messages by IT staff or employees.

Q What server operating systems does Authority support?

A Authority runs on Linux, Solaris, and Windows Server 2000. It has been tested with the forthcoming Windows Server 2003.

Q Can potential customers do a trial run?

A Cloudmark offers a 30-day try-before-you-buy trial with no payment of up-front fees. Competing products require up-front fees or expensive deployment of additional servers.

Q How does Authority learn?

A Authority learns and adapts to improve itself over time. Cloudmark's Bayesian Classifier learns from spamDNA generated by more than 475,000 members of the SpamNet community. Updates are contained in a single file that is e-mailed to the customer and easily applied.

Company Backgrounder

Cloudmark is the company that stops spam before it costs money. SpamNet, the company's groundbreaking, peer-to-peer (P2P) solution currently delivers immediate spam relief to nearly a half-million people, processing more than 14 million email messages each day. SpamNet, originally known as Vipul's Razor, proven effective at has been fighting spam since 1998.

Cloudmark now leverages this technology to deliver its enterprise solution, called Cloudmark Authority that stops spam at the gateway before it causes lost productivity, saps company resources and creates corporate liability. Authority prevents spam from entering your network by analyzing the DNA of spam to predict whether or not a message is spam and to constantly improve itself. Through Authority and SpamNet, Cloudmark offers the most advanced and innovative methods for countering the accelerating spam problem for both the end-user and Enterprise.

The company is leapfrogging traditional anti-spam companies and their obsolete techniques by fighting a distributed problem with a distributed solution and adding predictive technologies to crack the genetic code of spam.

CLOUDMARK

Press Release

Cloudmark Authority, the Award-Winning Enterprise Anti-Spam Solution Proves Your Corporation Can Be Spam-Free in Six Minutes

Cloudmark Sets a New Standard for Enterprise Anti-Spam Requirements in Front of Live Audience

Scottsdale, AZ. - Feb 17, 2003 - Today at the 13th annual DEMO 2003 conference, Cloudmark, the company that stops spam before it costs you money proves in a six-minute live demonstration that your company can be spam-free with Authority, its award-winning Enterprise anti-spam solution. Authority sets a new standard for enterprise anti-spam products by delivering the highest accuracy with low false positives *and* lowest total cost of ownership. Cloudmark CEO, Karl Jacob installs and runs Authority in front of a live audience demonstrating it does not require additional hardware, firewall configurations or costly professional services like competing products. Available for Windows, UNIX and Linux, the solution installs at the gateway on existing hardware and integrates with existing email infrastructure immediately preventing spam from entering your network and saving your company money.

"Authority uses our first ever spamDNA technology to deliver superior accuracy with virtually zero false criticals," says Karl Jacob, Cloudmark CEO. "Beyond that, today's corporations expect a great product with low maintenance, easy integration and most of all low total cost of ownership. By showing we can install and run Authority in under six minutes we are proving how easy it is for corporations to be spam free."

This is all possible because Authority evolves spamDNA from SpamNet, the first and largest spam-fighting community in the world with over 300,000 members.

The DNA of Spam
Spammers mutate message structure to avoid detection just like genes in DNA can be mutated. Just as scientists predict whether someone will have a particular disease by looking for specific gene mutations, Authority predicts whether a message is spam by looking for specific mutations in message structure called spamGenes. Authority uses spamDNA™, a collection of spamGenes, to feed its Bayesian classifier which learns how to stop spam more effectively. Finally, Cloudmark improves Authority's effectiveness by constantly evolving the spamDNA™ it gets from Cloudmark SpamNet, the largest spamfighting community in the world now with nearly 300,000 users and the largest database of spam.

Cloudmark Delivers on Enterprise Requirements:

- Plugs into existing hardware and software. Authority seamlessly integrates into existing email infrastructure which the IT staff already knows how to configure and operate, so it can be installed faster, more cheaply and requires less ongoing administration. Authority runs in memory and only impacts the message transfer agent (MTA) by 5-10 percent; while other anti-spam products impact the MTA more than 40 percent requiring additional hardware, configuration and support.
- Limit dependence on external network resources. Authority operates without a connection to Cloudmark. Other solutions require a constant connection to ex-

ternal servers which means reconfiguring firewalls in order to update their rules every minute and reactively handle new spam.

- Low maintenance due to limited personnel budget. Authority only needs updates every 30-60 days. Other reactive solutions require daily "tweaking" by IT staff to maintain effectiveness.
- Integrity of corporate security is maintained. Authority does not compromise security because e-mail never leaves your corporation. Other solutions send data and email outside your corporate firewall.
- Near-zero false positives. Authority's balanced approach uses knowledge about legitimate messages and spam to produce the most accurate results. Other solutions only look for spam.
- Fine grain control and flexibility for IT managers. Authority generates a confidence level between 0-100 percent on each spam message. This enables the IT manager to set a site policy that triggers what happens to each message based on how confident Authority is that it's spam. Other solutions only allow a "spam" or "not spam" determination which generate false positives and force continual detained message review by IT staff or employees. Authority runs on UNIX and Windows.
- Authority learns and adapts to improve itself over time. Cloudmark's Bayesian Classifier learns from spamDNA generated by SpamNet to constantly improve itself and free up the IT administrators valuable time.
- Proven Return on Investment (ROI). Cloudmark's spam-free guarantee offers 30 days to witness a ROI before making a commitment. Competitive products require up-front fees or expensive deployment of additional machines.

Pricing and Availability

Cloudmark Authority is currently available on Unix, Linux and Windows. It is typically deployed in organizations that support more than 1,000 mailboxes and is priced as such. To check out the spam-free guarantee, 30-day trial and witness Authority stopping spam at your gateway, go to www.cloudmark.com. People can also take advantage of Cloudmark's cost saving calculator on the site. It is estimated that a typical employee will receive ten spam messages per day, which would cost corporations $86 per employee, per year in lost productivity. This means a company with 10,000 employees can save over two million dollars a year with Authority deployed to equal immediate ROI. In addition, Cloudmark Authority protects your company against liability and morale issues generated by unwanted spam, often a more important ROI.

In addition, the beta version of SpamNet, the first, easy-to-use Microsoft® Outlook® add-in that stops spam immediately is available for free from the Cloudmark web site at www.cloudmark.com/SpamNet.