



CloudFilter™ Total Email Security

Email-based threats to the security of your business continue to grow increasingly sophisticated as spammers innovate new tactics for evading spam and virus filtration systems. CloudFilter puts your email security in the cloud, so you never again have to worry about keeping up with these malicious attackers. Your email security stays current, automatically protecting your business around the clock.



Policy enforcement and regulatory compliance

CloudFilter enforces email security policies and helps assure legal and regulatory compliance across your organization for inbound email. CloudFilter enables your organization to delegate management privileges for multiple administrators with different roles and access levels. It also allows administrators to configure email policy management according to global, user group, or individual user requirements. In addition, CloudFilter email security service improves email security management through a convenient web console that provides real-time configuration and policy modifications, monitoring, and alerting, as well as comprehensive reporting for administrators. If your business requires secure, encrypted delivery, Transport Layer Security (TLS) protocol enforcement is available through our SafeSend™ enhanced outbound service.

Primary Features

Benefits

Server attack rejection

- ✓ Bounces directory harvest attacks and denial of service attacks before they reach your server

Spam filtering/blocking

- ✓ Delivers extremely high filtering accuracy with virtually zero false positives

Multi-layered virus defense

- ✓ Provides up to date protection from rapidly spreading viruses

TLS encryption enforcement (via SafeSend™)

- ✓ Secures email transmission

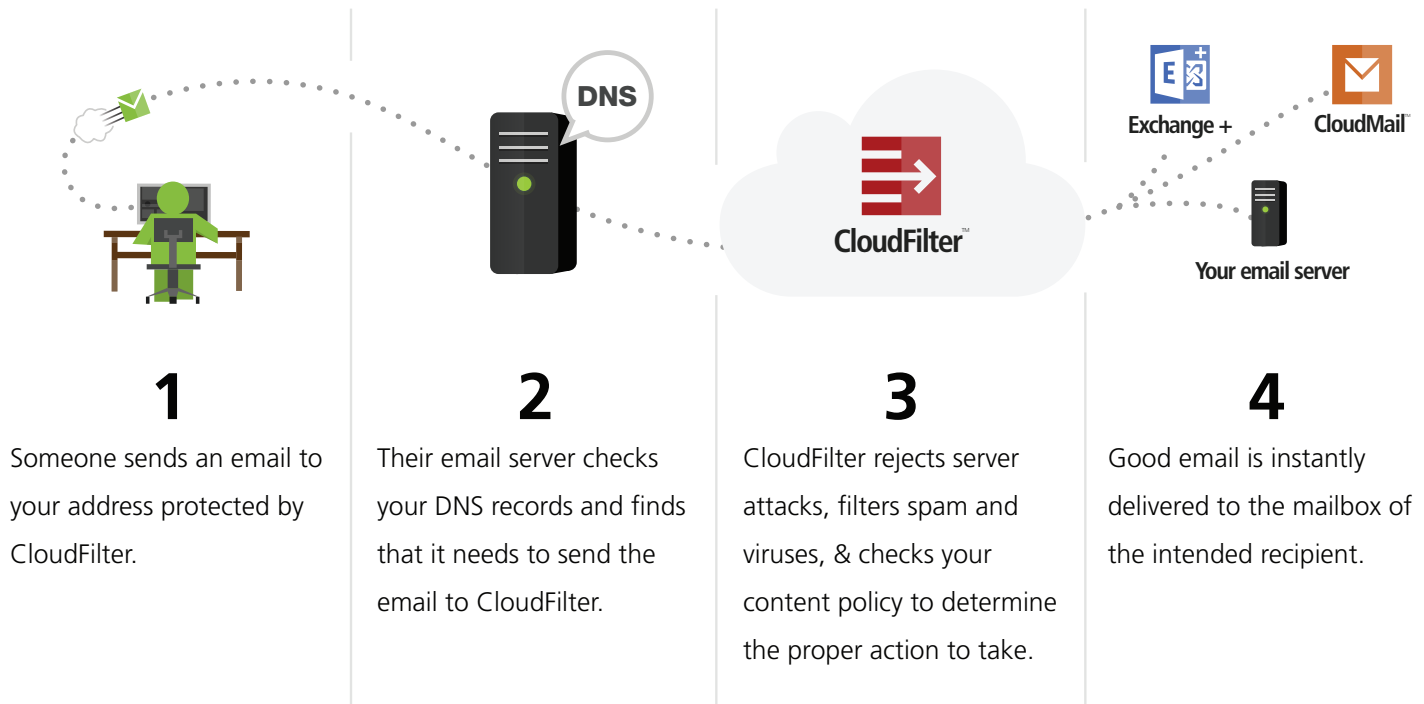
Content policy enforcement

- ✓ Manage your organization's acceptable use policies and content compliance on messages and attachment types

Instantly deployable and easy to manage

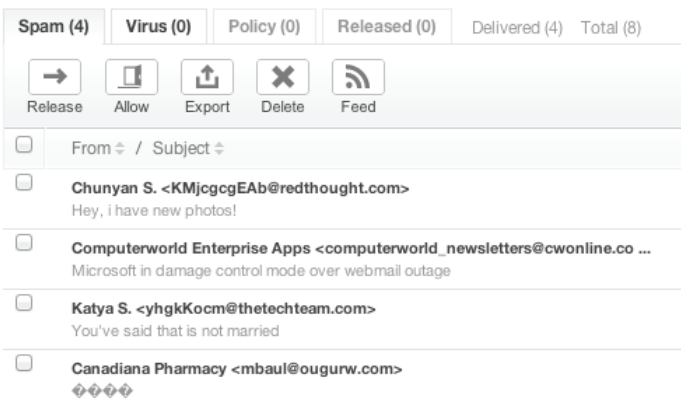
All that is required to enable CloudFilter is a quick MX record change to route your email through our systems. Once all DNS servers fully propagate the change (usually within 24 hours) all email sent to your domain will be safely and quickly filtered in a matter of milliseconds. Messages receiving a low spam score are delivered to the intended recipient with no latency. Messages receiving a higher spam score are quarantined. Admins may choose to let users release messages held in quarantine from the web console, via daily email digest report, or by establishing a handy live RSS quarantine feed directly in their email client.

How CloudFilter works



Intuitive web console

CloudFilter reduces the burden on your IT staff by providing a clean, easy to use console interface for your end users. With CloudFilter, you can choose to allow your users to manage their own message quarantine or add addresses to their allow/block list to further achieve the optimal level of protection.



Time-saving daily reports

CloudFilter users can receive a daily summary email which informs them of what email has been held in quarantine.

Unique to CloudFilter is the fact that our daily digest report only shows the top 25 messages which received the lowest spam score from our spam filtering systems. This saves users from having to scroll through hundreds of messages that are obviously spam to find the one message that might be right on edge of the spam threshold.

Your users won't even have to log in. When enabled, CloudFilter lets end-users release messages from directly within the email report itself by clicking a "release" link next to the email they wish to receive in their inbox. Admins control the delivery time and frequency of these reports.

Content policy management

CloudFilter's content policy tools give you the ability to define policies for inbound email which filter based on message content, originating URL extension, attachment type and more. Messages which trigger content policy rules can have specific actions assigned to them. They can be destroyed, sent to quarantine, or you can specify custom actions. Custom actions let you tag a message (in the subject, header, or footer) or forward the message to multiple addresses.

Allow/block lists

Be sure that you are getting the messages you want with granular allow/block list modifications.

Pre-defined content lexicons

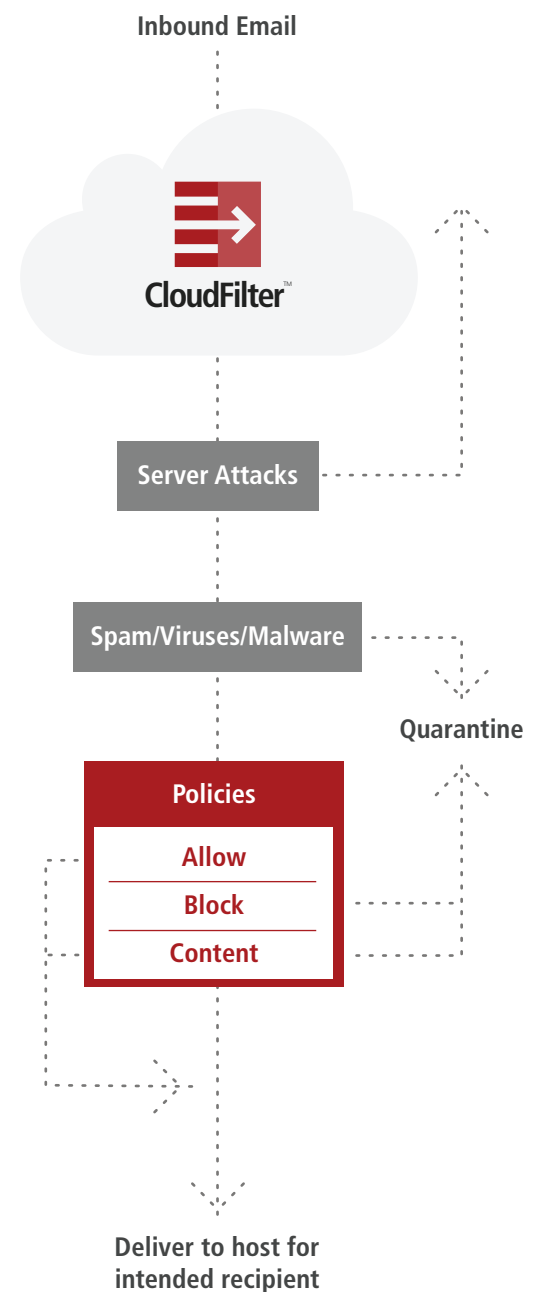
CloudFilter provides a comprehensive set of standard predefined lexicons for commonly filtered content such as explicit language, credit card numbers, and social security numbers. Rules can be enabled/disabled for an entire domain all the way down to the individual user level.

Explicit Language	Sensitive Data	Custom
Inbound Rules		
		Status
<input type="checkbox"/> Safe for TV		<input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Profanity		<input checked="" type="checkbox"/> ON
<input type="checkbox"/> Sexual		<input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Racial		<input checked="" type="checkbox"/> ON

Custom content rules

Also available is the option to create your own content filtering rules by combining a myriad of different criteria. Build your own unique rule/action combinations and create content filtering criteria which are custom-tailored specifically to the operational policies of your organization.

Criteria	
The sender's domain is:	<input type="text" value=".co.uk"/>
— AND —	
Text in the body contains:	<input type="text" value="free prescription drugs"/>



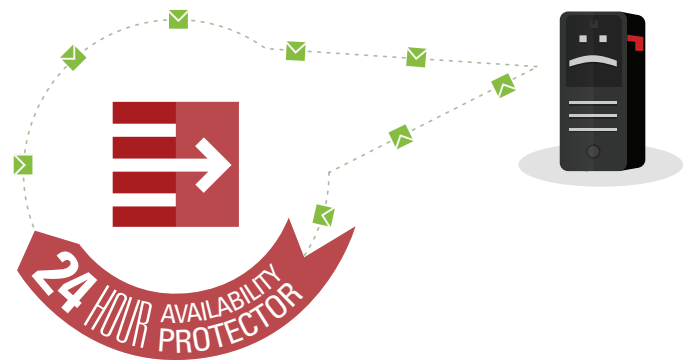
A scalable email infrastructure

Companies in today's business marketplace need to keep current with email-based threats on an hourly basis. In-house email security solutions can be unnecessarily costly and time consuming, and as your organization grows, further hardware and software licensing purchases are required, along with constantly increasing bandwidth needs. CloudFilter is built on a highly reliable and scalable SAAS platform with over 12 years of proven experience, performance, and high availability. CloudFilter can be deployed immediately and requires no upfront hardware or software investment. Adding new users to the service is as simple as adding their email address to the user list on the web console or syncing directly with your in-house LDAP server.

Availability protection

When your mail server is down, CloudFilter keeps trying to deliver email to your systems instead of bouncing the messages.

As soon as your systems are back online, your email will be immediately delivered to your users in a flow-controlled manner so your systems don't choke from the traffic increase.



CloudFilter includes:

- ✓ Inbound/Outbound spam/malware blocking
- ✓ DHA and DoS protection
- ✓ Content policy enforcement
- ✓ Intuitive web console
- ✓ Full Knowledge Base access
- ✓ Quarantine access for all users
- ✓ Daily filtering digest reports
- ✓ Admin delegation for certain roles

