Email Security with FailSafe

Anti spam and anti virus protection and email continuity for your mail server

Email Security provides comprehensive and highly effective virus, spam and content filtering of emails before they arrive at your server. If your server should go offline for whatever reason, **FailSafe** automatically protects from any bounced or lost mail and can even allow your staff to continue to send and receive email whilst your server is being fixed.

- Blocks 99% of viruses, spam and other unwanted content before it gets to your mail server.
- Carry on sending and receiving emails even if your in-house server goes offline.
- Simple set-up in minutes – no expensive hardware or software required.
- Fair pricing policy – you only pay for "real" users - alias domains, aliases and distribution lists are all free of charge.
- No complicated agreements or long term lock-in.
- Backed by a cast iron UK facilities and 100% Message Delivery SLA.
- UK based service and support by knowledgeable email specialists.
- Tried and tested since 2002.

Effectiveness

The email security system achieves at least 99% effectiveness with a virtually zero rate of false positives. The system benefits from the collective intelligence of millions of trusted spam reporting sources – all feeding back into the system in real time ensuring near instantaneous protection from 'zero hour' threats not picked up by conventional 'signature' based scanning mechanisms. Not only that, but the system has the ability to learn and adapt to each customer's unique pattern of email usage. This combination, in conjunction with other layers of filtering ensures that the system gets more and more effective over time.

> *" I was receiving over 20,000 junk emails into my inbox every day – I literally spent the first part of every morning trying to find important mail such as sales orders which we receive a lot of. The morning after switching to the Email Security service, my inbox had reduced to 25 unwanted emails and now, after a few months I hardly receive any. I save at least 8 hours a week and am able to concentrate on processing orders and dealing with customers.* ***David Lakey, FE Page Ltd****. "*

- Users receive only legitimate emails they actually want
- Less time spent searching for falsely blocked emails
- More productivity

SLA

We've learned what it takes to keep email flowing 24/7 year in year out – we've been doing so since 2002 with very little interruption. During this time we've refined and enhanced our systems, techniques and processes for speed, reliability and security. We've invested in multiple data centres and built redundancy into every layer of our platform. This gives us the confidence to offer a cast iron Service Level Agreement that you can rely on:

- 100% Service Availability
- 100% Email Delivery Guarantee
- Maximum 60 second email latency

Support

When it comes to a mission critical service such as email, you need to be dealing with experts. Email configuration, DNS and message tracing can be hard to understand, especially in a pressure situation. We do it all day long - there are not many scenarios we haven't already encountered so if you need help or have an issue we'll explain how to resolve it quickly, accurately and succinctly, usually first time.

UK Sovereignty

We go to great lengths to protect your data and to ensure that our email equipment is hosted only within the United Kingdom – our Tier III UK data centres are in London and Manchester. The equipment which backs the service is owned by us and we are a UK limited company. All of this costs us more in the long run (it's much cheaper to host in the USA), but we feel it's a vital to give you peace of mind.

Simple and Quick to Set-up

Getting up and running is a snap using our real time provisioning portal. Add the domain (2 minutes) and the service will be live and ready to process email!

Comprehensive and Highly Effective Protection

99%+ effectiveness, multiple layers of technology including updates every 30 seconds from over a billion reporting sources AND self learning technology unique to each domain – the system is highly effective and results in almost zero false positives.

FailSafe – Email Continuity and Disaster Mitigation

Stores up to 30 days of incoming emails in the event your sever goes offline and will automatically re-deliver the stored mail as soon as it comes back online.

Allows your users to send and receive email whilst your server is offline – email your users send and receive will be repatriated back to your in-house server once it is back online.

Keeps a rolling 30 days of historic email so that, at any time, users can login and recover an email they might have accidently deleted on your in-house server.

NB – features depend on FailSafe edition.

Advanced Configuration Capabilities

Fully delegated, real time control over all configuration options:

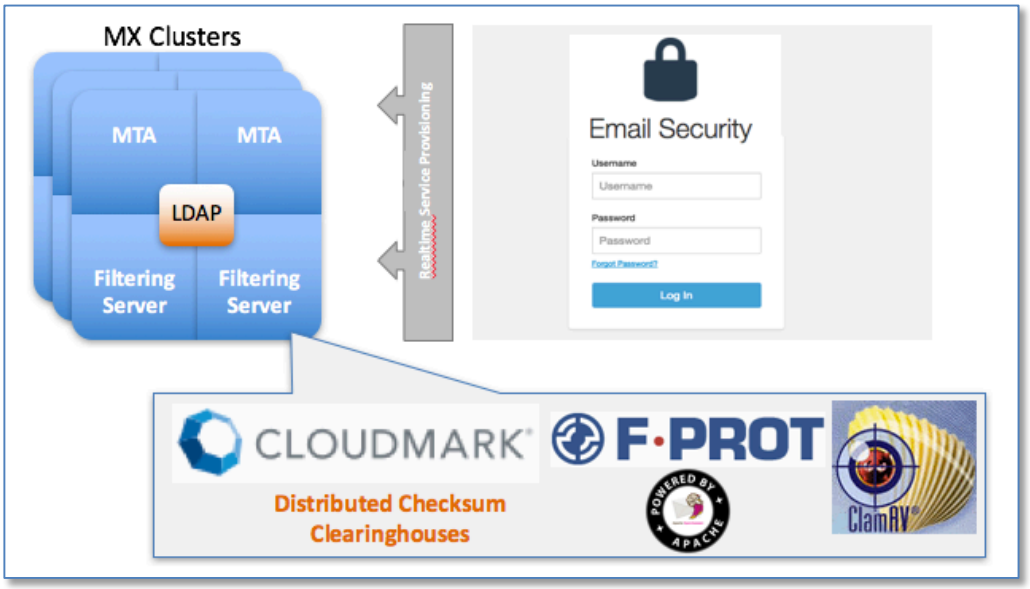
- Message logs
- Graphical Statistics
- Domain wide quarantine with administrator release. User level quarantine based on users' local junk folder.
- Create domain level administrator logins
- Easily pause mail delivery, automatically invoking the FailSafe queuing feature, allowing mail server maintenance to be performed without bouncing mail.
- Advanced mail routing controls – e.g. delivery to multiple servers
- Advanced spam filter controls
- Domain wide White and Black list management
- Attachment filtering controls
- 1 click addition of alias domains free of charge
- Support for sending outgoing email (smart host)

How it Works

Email Security with FailSafe is a fully managed 'Cloud' solution running on multiple servers in multiple different UK data centres for maximum possible reliability and speed.

In practice, the MX records for all of your email domains are adjusted so that all email is handled by Email Security where it is scanned and filtered before being forwarded on to your in-house server(s). Outbound email can also be sent via Email Security.

The system comprises 3 primary MX clusters. Each cluster contains multiple Message Transfer Agents and filtering servers and can handle many hundreds of thousands of emails per hour without introducing delays. Configuration information is stored in a distributed LDAP database which replicates between all MX clusters in near real time which means administrative changes take effect almost immediately, certainly within 1 minute at most. Additional capacity can easily be added without causing service disruption to ensure that we can keep abreast of increases in mail volumes.



System Architecture

Multiple layers of technology and techniques are employed:

Traffic Shaping and Policy Enforcement

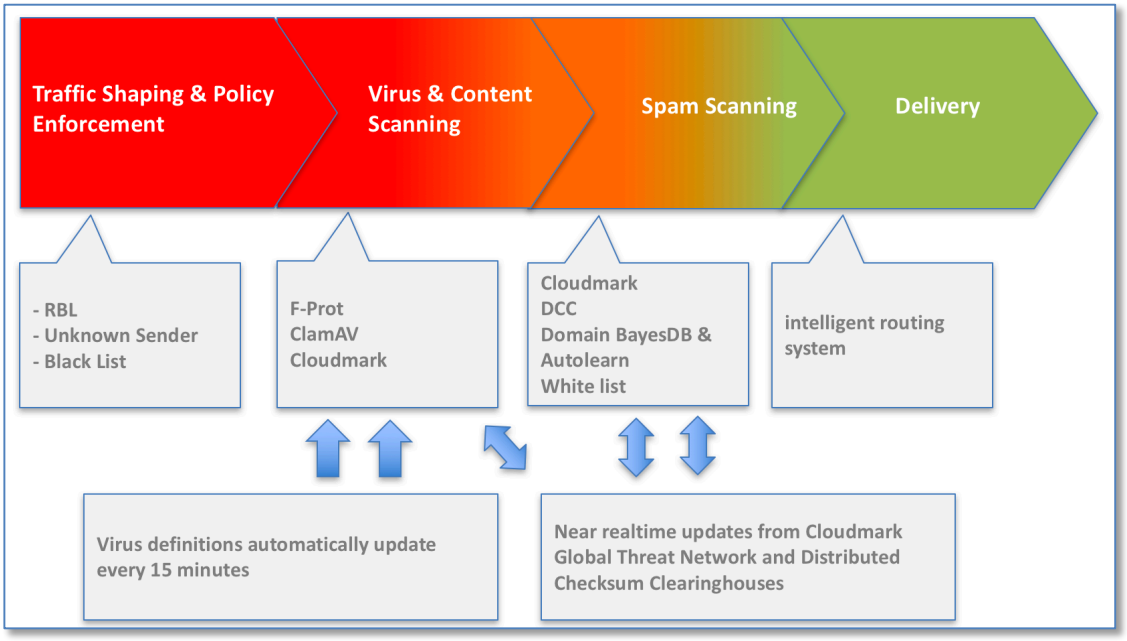
Incoming email connections are profiled and checked for compliance with protocol standards and for characteristics common amongst spammers – the results of these tests are logged into the systems own Realtime Black List (RBL) and we use this information later on during the processing of the email and for each subsequent new email. Blacklists are processed at this time also.

Virus and Content Scanning

We pass all mail through our primary virus scanner which is updated continuously and automatically throughout the day, if this is successful we repeat this process with a second, independent virus scanner. At this stage we also check whether the email contains any blocked attachments. If the email passes these checks and is whitelisted, the email is delivered to your server(s), otherwise it will be scanned further.

Spam Scanning

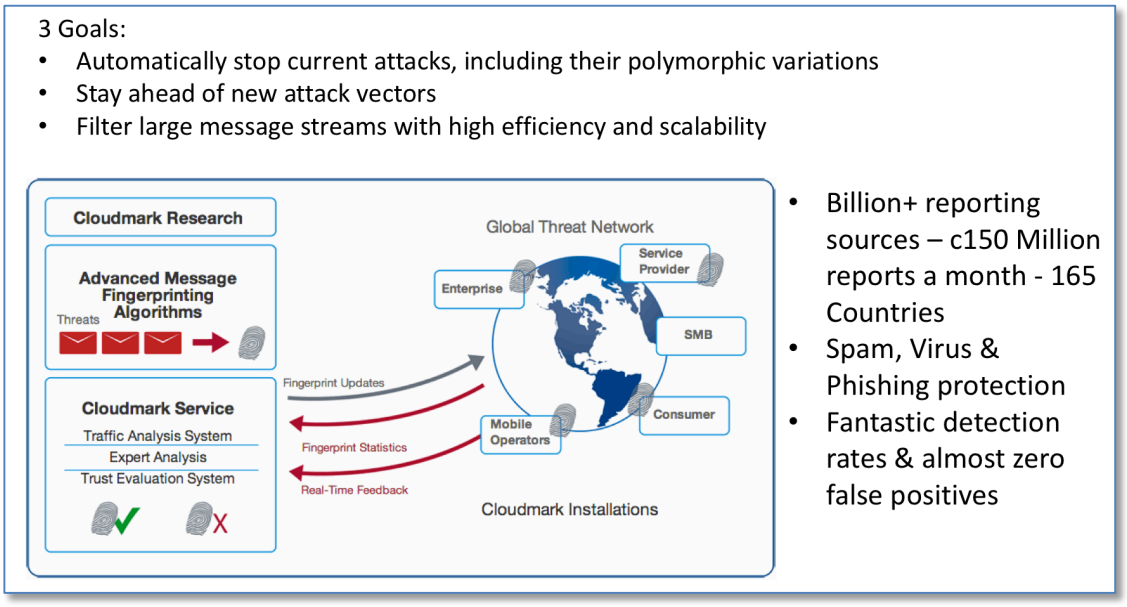
The core spam filtering engine contains multiple layers of checks, using various different technologies. Each check results in a 'score' – being the probability of whether the email is spam or not. The combined score is used in the configuration interface to adjust actions to perform. As well as Cloudmark, the real time threat network with over a billion reporting sources described below, the spam system also performs Bayesian analysis on every email and stores the Bayesian statistics for each domain in a separate database. This means that over time the system learns the email characteristics of each unique domain and becomes more and more accurate. This combination of Cloudmark's 'hive' mind approach and the domain specific Bayesian analysis, plus the various other layers of protection, creates a highly effective solution with very few false positives.



How It Works

Cloudmark

During the spam scanning stage, all emails are checked to see whether their fingerprint matches one in the Cloudmark database. Cloudmark receive real time reports – some 150 million a month from over 165 countries. These reports are aggregated and if enough matching fingerprints are corroborated, the data is entered into the next update which will be distributed to our systems within 30 seconds. This technique provides almost realtime visibility of threats globally and is extremely effective in catching new spam, phishing and virus content which has not yet been spotted and added to the virus definitions systems.



Cloudmark Authority Global Threat Reporting Network