



Eliminate Viruses. Curb Spam. Enforce policies. Regain control.

Introduction

Viruses, spam and unsolicited use are the plagues of modern email systems. Each year companies lose a sizable portion of their budgets recovering from these effects. Xamime is an integrated solution for resolving all these issues and allowing you to regain the reins of control over your most critical communication resource.

Xamime does a lot more than just handle spam and viruses, Xamime gives you the power to lock out resource abuse by giving you the ability to enforce your corporate email rules. Xamime provides fine grained control without sacrificing ease of use and is hailed as having one of the most intuitive web interfaces, giving management the facility to quickly understand while providing powerful controls for the administrator.

If you are looking for a solution which will allow you to control the contents your email systems with ease and power both currently and into the future, Xamime is the choice to make.

Quick Points

- Xamime can integrate into your existing networks without requiring the purchase of new hardware¹
- Xamime protects your data from viruses² and your users from spam³
- Xamime can enforce corporate email policies and procedures for multiple users, divisions and locations

¹Providing the existing mail server meets the minimal requirements of Xamime. Xamime may be alternatively installed on a separate prefilter system for handling systems such as Exchange servers.

²Anti-Virus capabilities are provided via 3rd party Anti-Virus programs such as Command Anti-Virus, NOD32 and Sophos

³Anti-Spam capabilities are provided via 3rd party Anti-Spam programs such as SpamAssasin and Vipuls Razor

- Xamime provides administrative power yet still is very intuitive to use
- Xamime uses a simple to use yet powerful Access Control Language to allow you to define processing rules
- Xamime can stop uncontrolled outbreaks of worms and viruses spreading within your network
- Xamime is sold on a per-server basis, no need to worry about per-user licenses
- Xamime is transparent to your users, no installation required on workstations
- Xamime can retain email for further analysis or storage
- Xamime can be used to monitor employees email against unsolicited use
- Xamime, once installed will provide immediate protective effect to all machines⁴
- Xamime is available in four (4) different feature levels to best suit your requirements⁵
- Xamime has proven to be an invaluable addition to your email server, drastically reducing end user infection rates from viruses as well as reducing your running costs in line fees⁶ and end user support calls. With Xamime, your email becomes one less item to worry about.

Summary of Features

- Installation
 - Rapid installation

⁴Xamime will filter based on the rule sets created by the administrator, by default Xamime does not imply any rules.

⁵Xamime Level 1, 2, 3 and 4

⁶Xamime reduces line utilization by not relaying denial of spam messages or spreading viruses across expensive WAN links

- Integrates with existing Sendmail installation
- Installation removal capable in a matter of seconds
- Requires less than 10Mb of space to install (Xamime may however keep track of several gigabytes of retained email)
- Scanning Methods
 - Zip-Bomb detection
 - Scans both in-bound and out-bound email
 - File type scan (ie, JPEG, MPEG, AVI, DOC)
 - File name scan (ie, prettypark.exe, I-LOVE-YOU.VBS.TXT)
 - File text contents (ie, ">>>> This is a chain letter")
 - SpamAssassin tests
 - Mailpack size
 - Sender address
 - Receiver address
 - Virus content
 - External tests (as created by the administrator)
 - Password Protected ZIP detection
 - Malformed MIME headers
- Access Control Lists
 - Global, domain, group and user level selectivity
 - In-bound, out-bound and bidirectional mail vector selection
 - Address matching selection uses POSIX compliant regular expression syntax
- Processing Options
 - Groups, allows application of ACL's to multiple email addresses (ideal for white/black lists)
 - Explicit address blocking (prevent internal users from emailing corporate secrets to competitors)
 - X-header inclusion for unique marking
 - Disclaimer amendment (something administrators have desired)
 - Out-bound attachment compression.
- External application hooks
 - Xamime supports the use of external programs at particular stages of the filtering process,
 - *Prefilter* Used to typically invoke spam filtering with SpamAssassin. The prefilter gives access to the email mailpack prior to it being decoded by Xamime, this allows the administrator to examine and modify the mailpack in an untouched state.
 - *External* Within an ACL test, Xamime can call on an external program to perform various tasks applied to the unpacked email.
 - *Postfilter* On completion of all testing, the Postfilter provides a facility in which the administrator can update external databases or other information resources based on the results of the Xamime filtering outcome.
- Retained email
 - View blocked, passed or in-process email which has been retained
 - Date/Time range searching
 - Delete email
 - Inspect attachments in email
 - Sender, receiver and block comment searching
 - Redeliver email to intended recipient
 - Redirect email to new recipient
 - Inspect the ACL causing the retention
 - Spanning storage; permits retaining of email across multiple drives, partitions and even servers⁷
- Administration
 - All administration via WWW interface
 - Supported in all Javascript capable browsers (Netscape 4.x+, Mozilla, Opera and IE 4.x+)
 - Low link speed requirements, making administration over WAN/MODEM feasible
 - Simple, clean and intuitive interface

⁷Xamime Level 4 only

- Self contained application, no HTTP server required
- Multiple Administrator capable⁸
- Per Administrator access rights⁹
- Main configuration parameters
- Access Control Lists (ACLs)
- Blocked Email filtering / searching
- Administrator Access Controls (to create, edit, delete administrators)
- Administrator extendible file type definitions, allowing for specific exploit detection
- Others...
 - Xamime has a minimal memory footprint, the binary itself is less than 900K
 - Xamime is orders of magnitude faster than script-based¹⁰ email sanitation systems
 - Xamime has open standards, permitting 3rd party developers to produce support software as additional packages (ie, alternative reporting engines)¹¹
 - Xamime uses POSIX compliant regular-expression syntax for its email and text searching

addresses in a corporation into a per division group set. With each group thus permitting the administrator of Xamime to then apply unique rules to each corporate division.

- *Multiple administrators*; Having multiple administrators allows for more than a single administrator to control various aspects of Xamime. The main administrator can create/modify/remove other administrators and their rights, even creating other main like administrators if required.
- *Maximum ACLs*; The maximum number of ACLs dictates the degree of complexity of the site's filtering rule sets. Typically a single ACL is used per domain/group or set of filtering restraints.
- *Maximum ACL items*; The maximum ACL items refers to the number of individual rules which may be contained within a given ACL.
- *Maximum Users*;The maximum number of email users permitted with the supplied license of Xamime
- *Lexical Scanning*; The ability to scan within an email and its respective attachments for words and phrases of interest.
- *Prefilter*; Xamime provides a method/hook for administrators to gain access to the mailpack which is about to be processed (with envelope). This facility is typically used for operations such as integrating with SpamAssassin and Black/White list marking
- *Postfilter*; Xamime provides a method/hook for administrators to gain access to the mailpack after all Xamime filtering operations have been performed. The Postfilter also supplies all filtering results and statistics using the standard URI format to the executed method. The Postfilter is frequently used to collect information from Xamime to populate reporting systems.
- *Spanning Storage*; For large and/or long term email storage (as is required by several countries) Xamime now provides a spanning storage solution. Rather than storing all email in one location Xamime now can spread the storage across a span of partitions, disks and even computers¹². Using the unique storage destination specification system it's possible to load

Version comparison

Facility	Level 1	Level 2	Level 3	Level 4
Groups	-	Y	Y	Y
Multiple administrators	-	-	Y	Y
Maximum ACLs	3	5	∞	∞
Maximum ACL items	∞	∞	∞	∞
Maximum users	100	∞	∞	∞
Lexical Scanning	Y	Y	Y	Y
Prefilter	Y	Y	Y	Y
Postfilter	Y	Y	Y	Y
External Scan Support	Y	Y	Y	Y
SpamAssassin support	Y	Y	Y	Y
Sendmail Support	Y	Y	Y	Y
Postfix Support	Y	Y	Y	Y
Spanning Storage	-	-	-	Y

- *Groups*; The groups facility allows the conglomeration of an array of dissimilar email addresses (not able to be compactly described using regular expression patterns) for the use as an ACL and/or test selector. A typical example of use would be the segregation of all the email

⁸Xamime Level 3 and 4 only

⁹Xamime Level 3 and 4 only

¹⁰Compared to Perl, Python and Bash Shell script

¹¹All Xamime interfaces are openly documented, there are no legal or license requirements for use.

¹²Spanning computer storage via NFS, AFS or other network storage solutions

balance email storage to bias larger drives or even move storage to an entirely different location and still be able to search previous existing email, all this while your system is live. No more will you be cornered when your existing drive space runs out.

Links

- PLD Software
 - Web: <http://www.pldaniels.com>
 - Email: pldaniels@pldaniels.com
- Xamime
 - Web: <http://www.xamime.com>
 - Email: xamime@xamime.com

Your Xamime distributor



Xamime requirements

- Operating System Support
 - Linux glibc2.4+
 - FreeBSD 4+
- Memory
 - minimum, 512Mb suggested
- Drive space
 - 10Mb minimum (no retained email support), 10Gb suggested
- CPU
 - 1GHz Pentium class or greater suggested
- Mail Transport Agent Support
 - Sendmail
 - Postfix

- Supported Anti-virus applications
 - BitDefender <http://www.bitdefender.com>
 - Command <http://www.command.co.uk>
 - FProt <http://www.fprot.com>
 - Kaspersky <http://www.kaspersky.com>
 - McAfee <http://www.mcafee.com>
 - NOD32 <http://www.nod32.com>
 - Sophos <http://www.sophos.com>
 - Other Anti-virus applications can be supported using the Generic AV interface.
- Supported Anti-spam applications
 - SpamAssassin <http://www.spamassassin.org>
 - Other anti-spam applications can be supported using the Xamime prefilter facility