Lotus® software

Proactively protecting your messaging infrastructure with the IBM Lotus Protector for Mail Security solution.

Preemptive protection
and spam control
for your messaging infrastructure

Distributed workforces, virtual teams, road warriors and corporate globalization continue to make e-mail your organization's most indispensable application. In fact, employee productivity and customer satisfaction rely on it. That's why protecting your messaging infrastructure is vital to your day-to-day operations. However, in many organizations, e-mail continues to be plagued not only by spam but also by phishing, denial-of-service attacks, directory harvest attacks, viruses, worms and other types of malicious code. What's more, regulatory requirements and other standards for managing information are rapidly becoming more stringent. Therefore, your mail security solution must combine antispam technologies with comprehensive, preemptive antivirus and mail server protection.

As an IBM Lotus® Domino® administrator, you know that IBM Lotus Domino software is one of the most security-rich platforms available. However, there are security risks that originate on the Internet, outside of the Lotus Domino environment, that you can't necessarily control. Now there's a solution that can not only give you the protection you need, but also simplify your administration processes. The first product in a comprehensive new line of security offerings currently planned for Lotus Domino software,[1] the IBM Lotus Protector for Mail Security solution provides preemptive protection and spam control for your messaging infrastructure—while simplifying administration through seamless integration with your existing IBM Lotus Notes® and Lotus Domino platform. The solution helps to enforce outbound content compliance and acceptable use policies with customizable analysis modules designed to be easily adaptable to varying company needs. Plus, Lotus Protector for Mail Security technology is a key element in the Lotus Protector suite of products, which is designed to help you address the security risks that can affect the Lotus Domino environment.
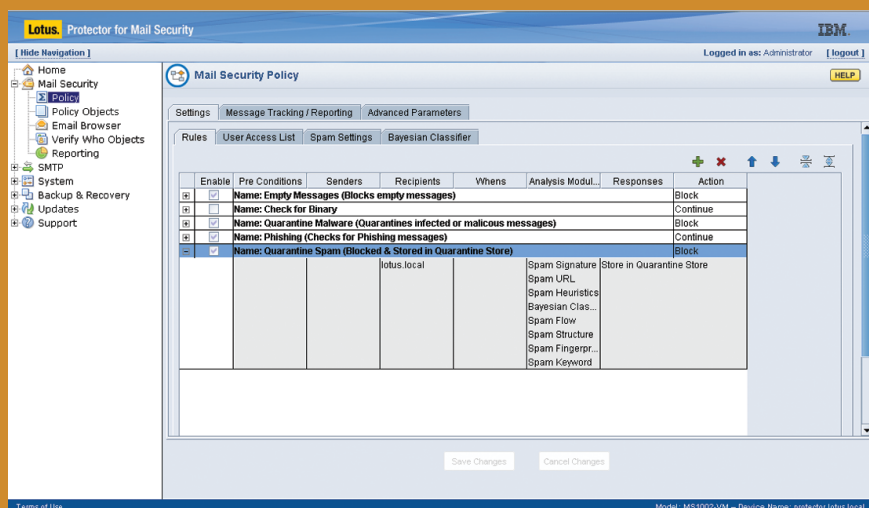
The Lotus Protector for Mail Security solution can download updates from the IBM Internet Security Systems™ (ISS) Global Data Center every 60 minutes to help you respond to changing spam tactics and threats.

Spam control and more

Spam continues to find its way to in-boxes daily, sometimes outnumbering legitimate e-mail. The fight against spam can negatively impact productivity and strain network and server capacities, affecting your end users as well as your system administrators.

Optimized for the Lotus Notes and Domino platform, the Lotus Protector for Mail Security solution lightens the spam burden in several ways. First, it can be quickly configured to block spam using either default or custom content filtering policies. Content filtering innovation is provided by the IBM ISS X-Force® research and development team. The X-Force team routinely monitors new spam techniques and distribution methods. By default, the Lotus Protector for Mail Security solution checks each hour for updates from IBM that include new spam signatures and potentially dangerous URLs. As a result, Lotus Protector for Mail Security technology helps you keep ahead of the latest spam trends, including social penny stock schemes and image-based spam.

In addition, the solution includes dynamic host reputation filtering technology—which leverages sophisticated IBM research on where spam is likely to originate—to help stop spam before it even reaches your system. By analyzing the source IP address on each incoming e-mail, it can make a mathematical judgment about whether or not the source of the e-mail is reliable. When an e-mail is deemed to be coming from an unreliable source, the connection is dropped—before the e-mail is delivered. As a result, you can help reduce the system load associated with managing spam by preventing spam from reaching your filter in the first place.

At the IBM ISS Global Data Center, IBM maintains a security database containing more than 95 million Web pages and relevant spam signatures to date. IBM operates spam collectors worldwide using e-mail accounts known as "honey pots," which receive hundreds of thousands of confirmed spam e-mails every day. Data gathered from these messages is fed into the Global Data Center. In addition, IBM has established a network of trusted IBM Business Partners and IBM corporate users that contribute spam data to the database. IBM spam protection technologies leverage data gathered from all of these sources to increase the efficiency of their spam filtering. Plus, with the optional Spam Learn feature, IBM offers anonymous, automated reporting of new spam back to the Global Data Center to be included in the database.
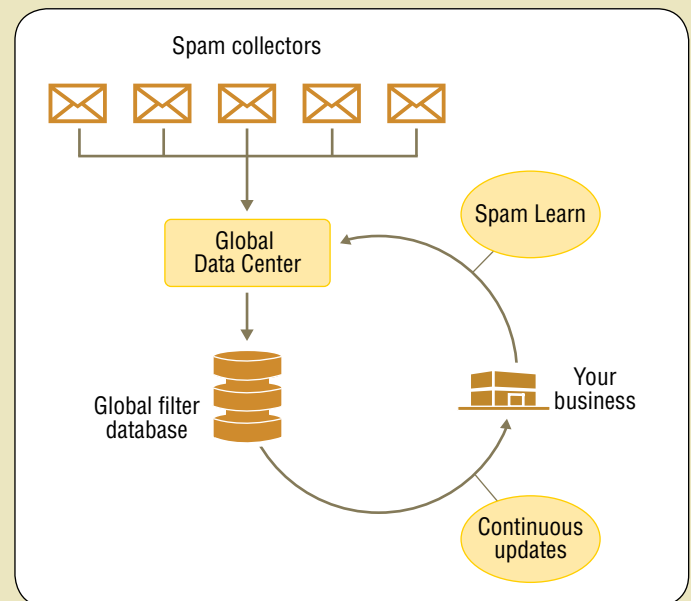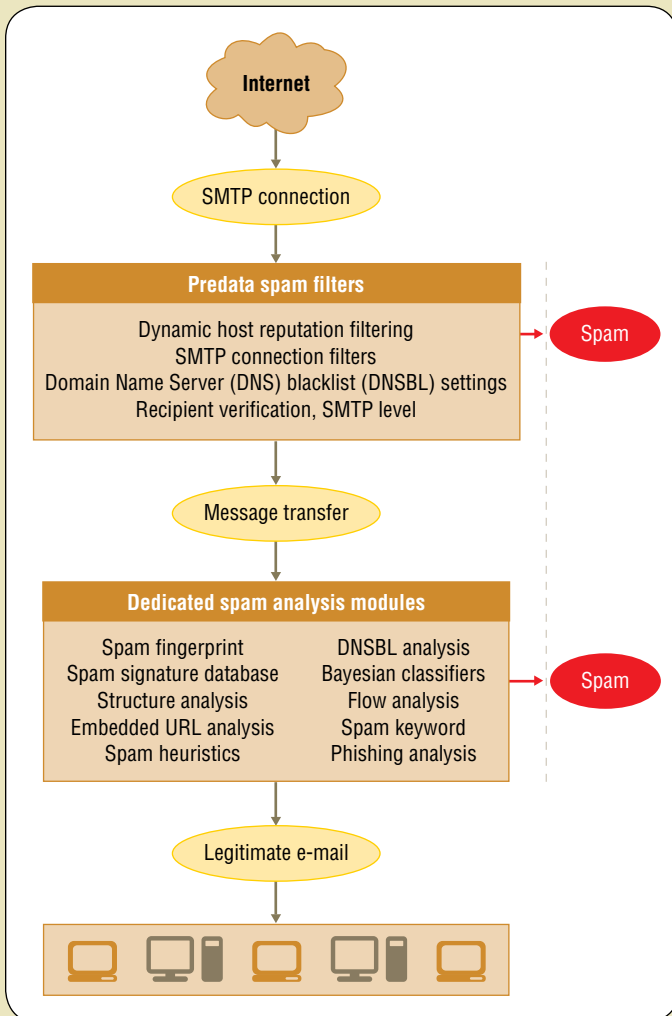

The Lotus Protector for Mail Security solution receives updates from the IBM ISS Global Data Center eight times per day to help you respond to changing spam tactics and threats.
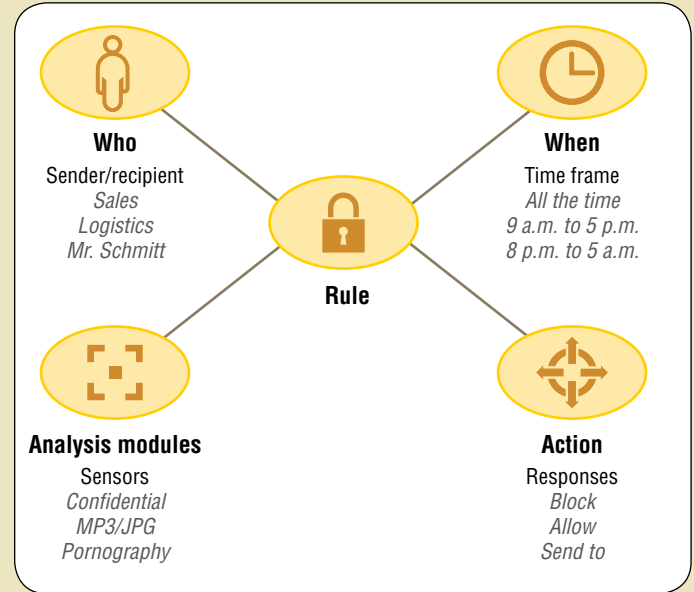
*More than 20 customizable analysis modules to help meet your
unique needs*

Lotus Protector for Mail Security technology combines multiple
analysis modules for greater customization, enabling you to
define policies or tailor modules to help meet legal and regula-
tory compliance requirements for data. Messages can also
be scanned for offensive words, customizable keywords and
attachment types—and specialized analysis capabilities help
prevent sensitive information such as Social Security and credit
card numbers from leaving your network. In addition, the phish-
ing module provides a separate analysis technique to protect
your employees against e-mail messages that target their
personal information.

Who
Sender/recipient
Sales
Logistics
Mr. Schmitt

When
Time frame
All the time
9 a.m. to 5 p.m.
8 p.m. to 5 a.m.

Rule

Analysis modules
Sensors
Confidential
MP3/JPG
Pornography

Action
Responses
Block
Allow
Send to

*You can develop spam filtering rules that fit your organization's policies and
tailor those rules to specific users.*

*Rules configuration helps improve ease of use, lessening the burden
on administrative staff*

Granular policy control includes simple rules-based policy
creation—enabling you to take action based on factors such
as who, what and when—and more than 10 different custom-
izable action types, such as modifications and notifications.
Policies can be applied globally, by user group or by indi-
vidual user. Plus, the Lotus Protector for Mail Security solution
supports Lightweight Directory Access Protocol (LDAP), including
Lotus Domino and Microsoft® Active Directory technologies. End
users can control their own allow and block lists, giving them per-
sonalized control over their own spam preferences. They can also
view and control their quarantined messages if granted permis-
sion by an administrator.

Internet

SMTP connection

Predata spam filters

Dynamic host reputation filtering
SMTP connection filters
Domain Name Server (DNS) blacklist (DNSBL) settings
Recipient verification, SMTP level

Spam

Message transfer

Dedicated spam analysis modules

Spam fingerprint
Spam signature database
Structure analysis
Embedded URL analysis
Spam heuristics

DNSBL analysis
Bayesian classifiers
Flow analysis
Spam keyword
Phishing analysis

Spam

Legitimate e-mail

*The Lotus Protector for Mail Security solution filters out spam before it even
reaches your network, helping save valuable bandwidth.*

Preemptively stop threats to messaging systems

Beyond spam control, the Lotus Protector for Mail Security solution is equipped with advanced protection technologies to provide security features that are ahead of the threat. With the award-winning IBM Proventia® Network Intrusion Prevention System (IPS) engine and IBM Virtual Patch® technology, the application supports the vital security necessary in today's IT environments.

Transport layer security provides an extra level of protection between your company and its partners or suppliers
Support for the Transport Layer Security (TLS) protocol enables you to automatically encrypt all e-mails between your company and trusted partners and suppliers. By establishing mutual public certificates on your server, you can make sure that communication between your company and these organizations is protected. The message transport agent at the edge of your network automatically encrypts all e-mails to and from such organizations—providing a seamless user experience.

Recipient verification technology and the queuing mechanism help ensure that your messaging infrastructure is protected from compromise
The solution's recipient verification technology and queuing mechanism helps protect your mail server from zero-day attacks, including denial-of-service and directory harvest attacks.

Many spammers direct spam at a particular domain simply by guessing at user names or naming conventions. Recipient verification technology helps minimize the effects of this practice by confirming that the specific user name to which each e-mail is addressed actually exists—before accepting the message. Any message that is addressed to an unknown recipient is rejected before the connection is accepted, helping to save valuable bandwidth.

The queuing mechanism is designed to provide multiple levels of protection against spam-based denial-of-service attacks. The application has two predefined thresholds for its unchecked queue, which begins to grow during a denial-of-service attack. When the total number of messages in the unchecked queue reaches the first threshold, the application begins throttling new Simple Mail Transfer Protocol (SMTP) connections based on a predefined period of time. When the number of messages in the unchecked queue reaches the second threshold, all new SMTP connections are answered with a "temporarily not available" message and a request to try again later, based on SMTP standards. Typical spam bots can't handle this type of rejection and will fail at this point, whereas valid SMTP servers will try again after a predefined period of time.

Multilayered antivirus protection helps block new zero-day virus threats in realtime
The Lotus Protector for Mail Security solution includes remote malware detection, which is automatically distributed to your application via signature updates to the filter database. In addition, behavioral genotype and signature antivirus technologies take action against suspicious code for known and unknown viruses. This technology analyzes both incoming and outgoing e-mail in parallel with the application's antispam features.

All Lotus Protector offerings are planned to easily integrate with your existing Lotus Domino user and security frameworks, presenting a seamless experience for users—and simplifying overall administration for you.[1]

Intelligent management features for ease of use

The Lotus Protector for Mail Security solution provides a number of intelligent management features that can be tailored to your organization's unique network environment. It includes:

- A stand-alone, security-rich, Web-based local management interface. The interface provides easy access to security and antispam policies.
- Standard or customized reports. Standard, centralized reports provide valuable insights, such as identifying which spammers present the biggest challenge to the messaging infrastructure. You can also create customized reports for additional flexibility.
- An exceptional clustering feature.[2] Because a separate management console isn't required, you can easily manage multiple servers through one appliance. In fact, Lotus Protector for Mail Security technology provides access to all quarantined messages and tracking information through the appliance you designate as the central appliance, regardless of where the traffic initially entered the network.

IBM Lotus Protector for Mail Security solution delivers

Designed to provide protection for organizations of all sizes, the application is available as both a hardware appliance and a virtual appliance. In either form, it receives automatic updates to keep spam, viruses and other malicious traffic at bay. If you're migrating toward virtualization within your enterprise to take advantage of today's superior processor technology, Lotus Protector for Mail Security technology running within a virtualized environment offers an attractive total cost of ownership, fast deployment, and simple backup and recovery operations.

A unified platform to address your security challenges

Create a unified platform to mitigate your security challenges. Find out more about how the Lotus Protector for Mail Security solution can help resolve messaging security headaches and improve your security posture against tomorrow's threats, as part of the dynamic Lotus Protector platform. Designed specifically for the Lotus Domino environment, the application tightly integrates with the Lotus Domino platform, simplifying administration of your messaging environment.

Technical specifications for the MS3004LP appliance

Rack units	2U
Scalability	Clustering support for large deployments
Maximum throughput	See ibm.com/software/lotus/protector for the most current data
Storage	4x80GB + 2x250GB (RAID1)
Redundancy	Hard disk, power supply, fans
Dimensions	• Height (in/mm): 3.40/86.36 • Width (in/mm): 19/482.6 • Depth (in/mm): 24/609.6 • Weight (lb/kg): 60/27
Power dissipation	• Units: AC • Voltage (V): 115/220 • Input range (V): 100–127/200–240
Operating temperature	+50˚F to +95˚F (+10˚C to +35˚C)
Nonoperating temperature	-40˚F to +158˚F (-40˚C to +70˚C)
Relative humidity (non-operating)	95% @ 90˚F (30˚C)
Emissions	FCC Class A

Technical specifications for the virtual appliance

Scalability	Ideally suited for small to midsize businesses with fewer than 1,000 users, and scalable to more strategic operating specifications as required, depending on the hardware base

System requirements	The following are the minimum available system resources required for VMware virtual installations.
	
	One of the following:
	
	• VMware Server 1.0.2 or later
	• VMware Workstation 5.5 or later
	• VMware Player 1.0.3 or later
	• VMware ESX 3.x or later
	
	Host hardware:
	
	• 2GB RAM (512MB required for each virtual instance)
	• 100GB hard disk space (30GB dedicated for each virtual instance)
	• Two network interfaces:
	  – One host-only interface
	  – One bridged network interface
	
	Virtual hardware requirements (per virtual installation):
	
	• 512MB RAM (minimum)
	• 30GB disk space

For more information

For more information about services that support Lotus and IBM WebSphere® Portal products, go to:

ibm.com/software/lotus/services

For more information about the IBM Lotus Protector for Mail Security solution, contact your IBM sales representative or visit:

ibm.com/software/lotus/protector

1 These statements represent current IBM plans and directions, which are subject to change without notice.

2 Available only in the MS3004LP. Clustering does not imply high availability.