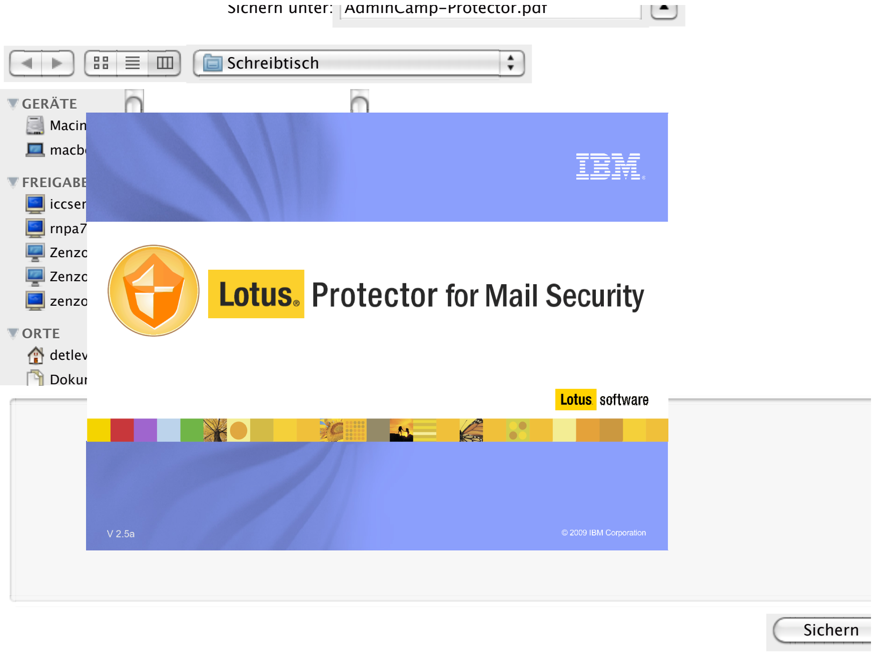
Mittwoch, 30. Sept. 2009
Track: 4 - Session: 8

Lotus Protector

Referenten:
Detlev Poettgen, http://www.netzgoetter.net
Andreas Schulte, IBM Deutschland GmbH

AdminCamp 2009

Gelsenkirchen, 28.-30. September 2009



Sichern unter: AdminCamp-Protector.pdf

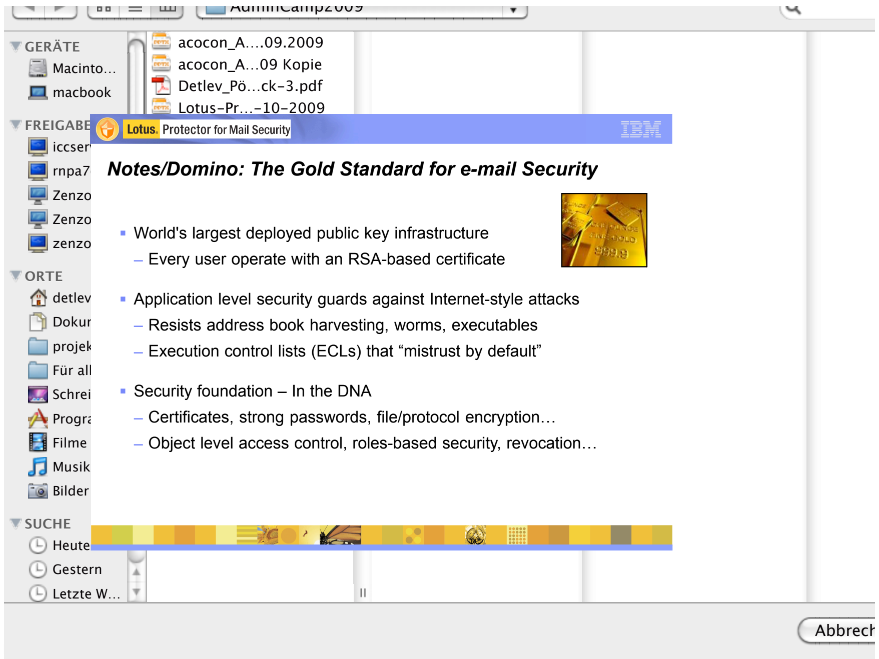
IBM

Lotus. Protector for Mail Security

Lotus software

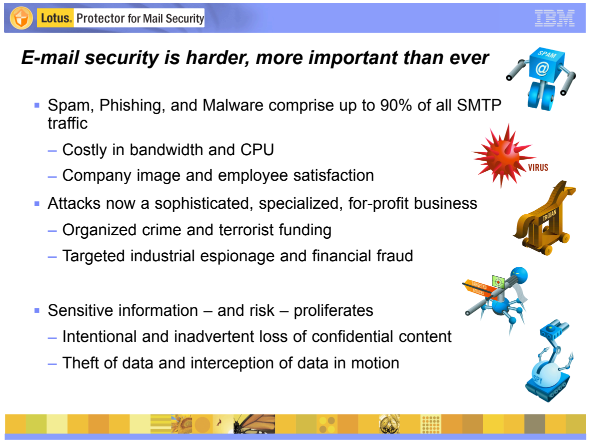
V 2.5a

© 2009 IBM Corporation



Notes/Domino: The Gold Standard for e-mail Security

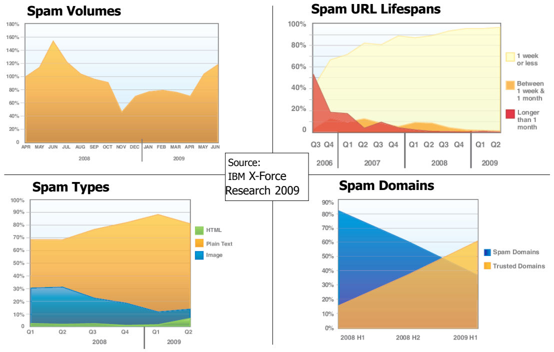
- World's largest deployed public key infrastructure
  - Every user operate with an RSA-based certificate
- Application level security guards against Internet-style attacks
  - Resists address book harvesting, worms, executables
  - Execution control lists (ECLs) that “mistrust by default”
- Security foundation – In the DNA
  - Certificates, strong passwords, file/protocol encryption…
  - Object level access control, roles-based security, revocation…



E-mail security is harder, more important than ever

- Spam, Phishing, and Malware comprise up to 90% of all SMTP traffic
  - Costly in bandwidth and CPU
  - Company image and employee satisfaction
- Attacks now a sophisticated, specialized, for-profit business
  - Organized crime and terrorist funding
  - Targeted industrial espionage and financial fraud
- Sensitive information – and risk – proliferates
  - Intentional and inadvertent loss of confidential content
  - Theft of data and interception of data in motion

E-mail-borne attacks change rapidly


Spam Volumes

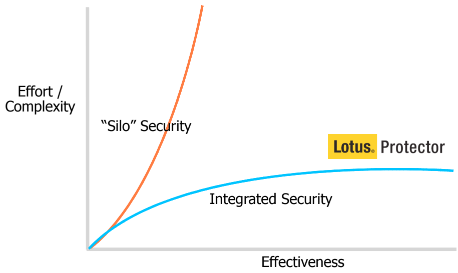
Spam URL Lifespans

Spam Types

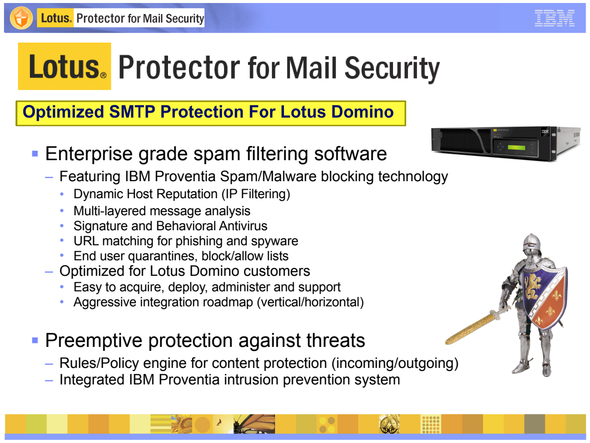
Spam Domains

Source:
IBM X-Force
Research 2009

Dynamics of Security Integration



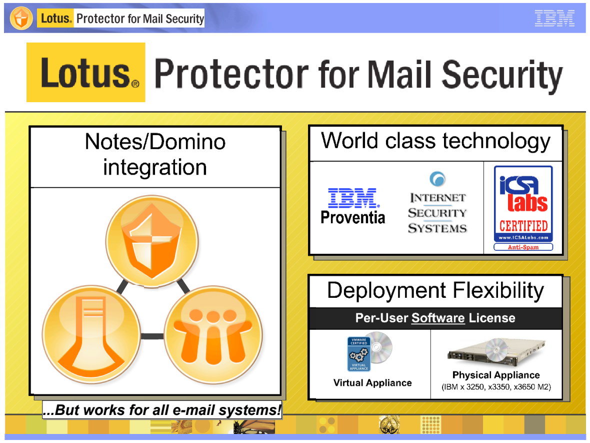
Lotus® Protector for Mail Security



Lotus® Protector for Mail Security

Optimized SMTP Protection For Lotus Domino

- Enterprise grade spam filtering software
  - Featuring IBM Proventia Spam/Malware blocking technology
    - Dynamic Host Reputation (IP Filtering)
    - Multi-layered message analysis
    - Signature and Behavioral Antivirus
    - URL matching for phishing and spyware
    - End user quarantines, block/allow lists
  - Optimized for Lotus Domino customers
    - Easy to acquire, deploy, administer and support
    - Aggressive integration roadmap (vertical/horizontal)
- Preemptive protection against threats
  - Rules/Policy engine for content protection (incoming/outgoing)
  - Integrated IBM Proventia intrusion prevention system



Lotus. Protector for Mail Security

Notes/Domino integration

...But works for all e-mail systems!

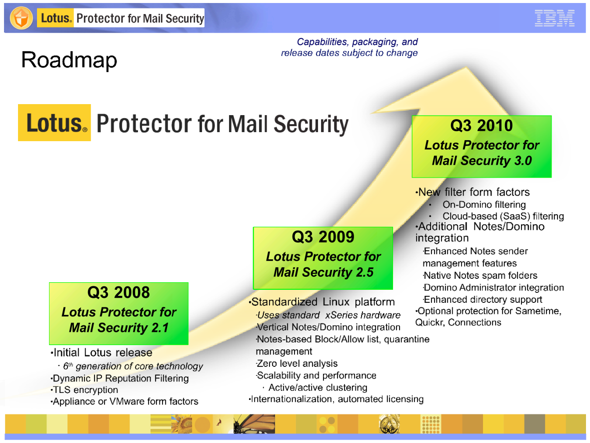
World class technology

IBM Proventia
Internet Security Systems
ICSA labs CERTIFIED
www.ICSALabs.com
Anti-Spam

Deployment Flexibility

Per-User Software License

Virtual Appliance	Physical Appliance (IBM x 3250, x3350, x3650 M2)



Roadmap

Capabilities, packaging, and release dates subject to change

Lotus. Protector for Mail Security

Q3 2008
Lotus Protector for Mail Security 2.1

- Initial Lotus release
  - *6th generation of core technology*
- Dynamic IP Reputation Filtering
- TLS encryption
- Appliance or VMware form factors

Q3 2009
Lotus Protector for Mail Security 2.5

- Standardized Linux platform
  - *Uses standard xSeries hardware*
  - Vertical Notes/Domino integration
  - Notes-based Block/Allow list, quarantine management
  - Zero level analysis
  - Scalability and performance
    - Active/active clustering
- Internationalization, automated licensing

Q3 2010
Lotus Protector for Mail Security 3.0

- New filter form factors
  - On-Domino filtering
  - Cloud-based (SaaS) filtering
- Additional Notes/Domino integration
  - Enhanced Notes sender management features
  - Native Notes spam folders
  - Domino Administrator integration
  - Enhanced directory support
- Optional protection for Sametime, Quickr, Connections

Notes Inbox Integration

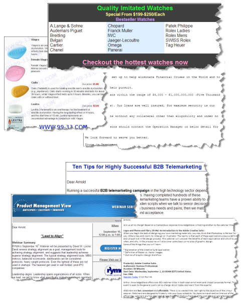
Gives end users complete control over ALL unwanted e-

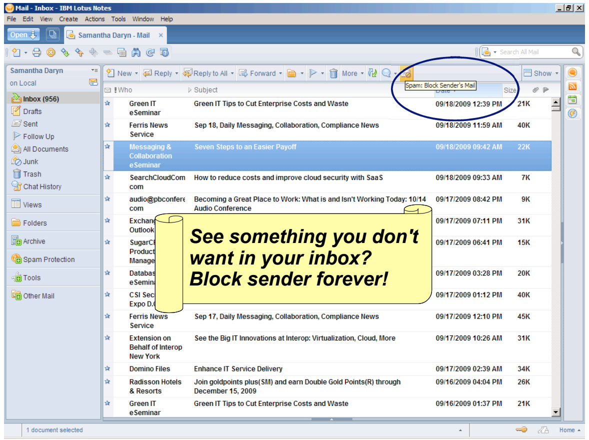
Objective Spam

- Pharma, sexual, stock scams etc.
  - *Protector for Mail Security stops objective spam cold at the gateway*

Subjective Spam

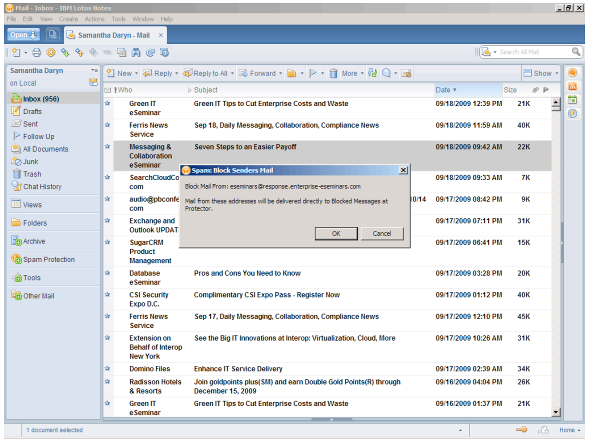
- Newsletters, mailing lists, event invitations etc.
  - *Notes integration lets users block subjective spam senders permanently*


Quality Imitated Watches
Checkout the hottest watches now
WWW.59-33.COM
Ten Tips for Highly Successful B2B Telemarketing
Product Management View



Who	Subject	Date	Size
Green IT eSeminar	Green IT Tips to Cut Enterprise Costs and Waste	09/18/2009 12:39 PM	21K
Ferris News Service	Sep 18, Daily Messaging, Collaboration, Compliance News	09/18/2009 11:59 AM	40K
Messaging & Collaboration eSeminar	Seven Steps to an Easier Payoff	09/18/2009 09:42 AM	22K
SearchCloudCom com	How to reduce costs and improve cloud security with SaaS	09/18/2009 09:33 AM	7K
audio@pbconfere com	Becoming a Great Place to Work: What is and Isn't Working Today: 10/14 Audio Conference	09/17/2009 08:42 PM	9K
Exchang Outlook		09/17/2009 07:11 PM	31K
SugarC Product Manage		09/17/2009 06:41 PM	15K
Databas eSemin		09/17/2009 03:28 PM	20K
CSI Sec Expo D.		09/17/2009 01:12 PM	40K
Ferris News Service	Sep 17, Daily Messaging, Collaboration, Compliance News	09/17/2009 12:10 PM	45K
Extension on Behalf of Interop New York	See the Big IT Innovations at Interop: Virtualization, Cloud, More	09/17/2009 10:26 AM	31K
Domino Files	Enhance IT Service Delivery	09/17/2009 02:39 AM	34K
Radisson Hotels & Resorts	Join goldpoints plus(SM) and earn Double Gold Points(R) through December 15, 2009	09/16/2009 04:04 PM	26K
Green IT eSeminar	Green IT Tips to Cut Enterprise Costs and Waste	09/16/2009 01:37 PM	21K

See something you don't want in your inbox? Block sender forever!



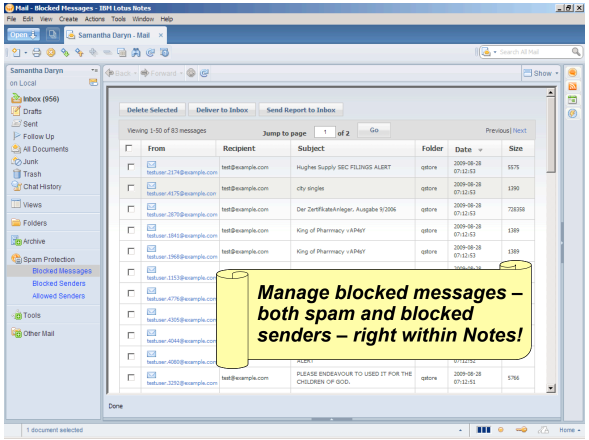
Mail - Inbox - IBM Lotus Notes

Who	Subject	Date	Size
Green IT eSeminar	Green IT Tips to Cut Enterprise Costs and Waste	09/18/2009 12:39 PM	21K
Ferris News Service	Sep 18, Daily Messaging, Collaboration, Compliance News	09/18/2009 11:59 AM	40K
Messaging & Collaboration eSeminar	Seven Steps to an Easier Payoff	09/18/2009 09:42 AM	22K
SearchCloudCo com		09/18/2009 09:33 AM	7K
audio@pbconfe com	0/14	09/17/2009 08:42 PM	9K
Exchange and Outlook UPDAT		09/17/2009 07:11 PM	31K
SugarCRM Product Management		09/17/2009 06:41 PM	15K
Database eSeminar	Pros and Cons You Need to Know	09/17/2009 03:28 PM	20K
CSI Security Expo D.C.	Complimentary CSI Expo Pass - Register Now	09/17/2009 01:12 PM	40K
Ferris News Service	Sep 17, Daily Messaging, Collaboration, Compliance News	09/17/2009 12:10 PM	45K
Extension on Behalf of Interop New York	See the Big IT Innovations at Interop: Virtualization, Cloud, More	09/17/2009 10:26 AM	31K
Domino Files	Enhance IT Service Delivery	09/17/2009 02:39 AM	34K
Radisson Hotels & Resorts	Join goldpoints plus(SM) and earn Double Gold Points(R) through December 15, 2009	09/16/2009 04:04 PM	26K
Green IT eSeminar	Green IT Tips to Cut Enterprise Costs and Waste	09/16/2009 01:37 PM	21K

Spam: Block Senders Mail

Block Mail From: eseminars@response.enterprise-eseminars.com

Mail from these addresses will be delivered directly to Blocked Messages at Protector.

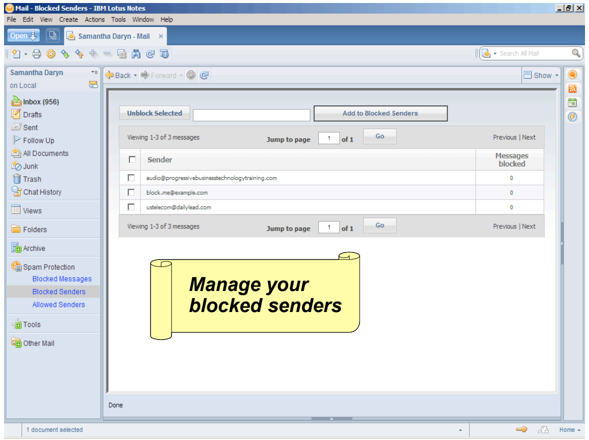


Mail - Blocked Messages - IBM Lotus Notes

Viewing 1-50 of 83 messages   Jump to page 1 of 2

□	From	Recipient	Subject	Folder	Date	Size
□	testuser.2174@example.com	test@example.com	Hughes Supply SEC FILINGS ALERT	qstore	2009-08-28 07:12:53	5575
□	testuser.4175@example.com	test@example.com	city singles	qstore	2009-08-28 07:12:53	1390
□	testuser.2870@example.com	test@example.com	Der ZertifikateAnleger, Ausgabe 9/2006	qstore	2009-08-28 07:12:53	728358
□	testuser.1841@example.com	test@example.com	King of Pharrmacy vAP4sY	qstore	2009-08-28 07:12:53	1389
□	testuser.1968@example.com	test@example.com	King of Pharrmacy vAP4sY	qstore	2009-08-28 07:12:53	1389
□	testuser.1153@example.com				2009-08-28	
□	testuser.4776@example.com					
□	testuser.4305@example.com					
□	testuser.4044@example.com					
□	testuser.4080@example.com		ALERT		07:12:52	
□	testuser.3292@example.com	test@example.com	PLEASE ENDEAVOUR TO USED IT FOR THE CHILDREN OF GOD.	qstore	2009-08-28 07:12:51	5766

Manage blocked messages – both spam and blocked senders – right within Notes!

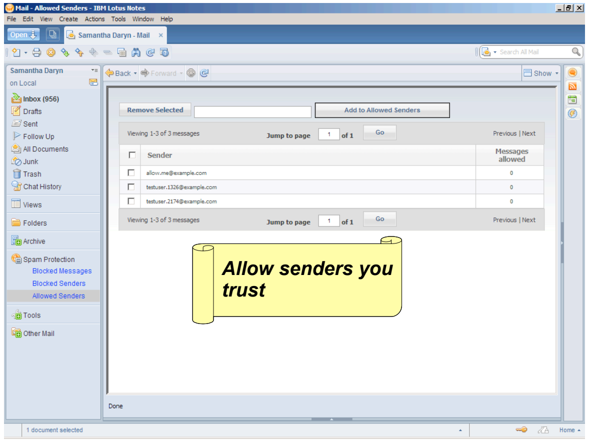


Viewing 1-3 of 3 messages **Jump to page** 1 **of 1** Go Previous | Next

□	Sender	Messages blocked
□	audio@progressivebusinesstechnologytraining.com	0
□	block.me@example.com	0
□	ustelecom@dailylead.com	0

Viewing 1-3 of 3 messages **Jump to page** 1 **of 1** Go Previous | Next

Manage your blocked senders

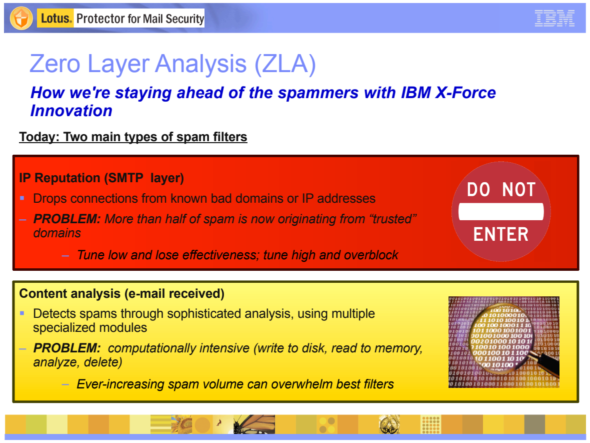


Viewing 1-3 of 3 messages **Jump to page** 1 **of 1** Go Previous | Next

□	Sender	Messages allowed
□	allow.me@example.com	0
□	testuser.1326@example.com	0
□	testuser.2174@example.com	0

Viewing 1-3 of 3 messages **Jump to page** 1 **of 1** Go Previous | Next

Allow senders you trust



Zero Layer Analysis (ZLA)

How we're staying ahead of the spammers with IBM X-Force Innovation

Today: Two main types of spam filters

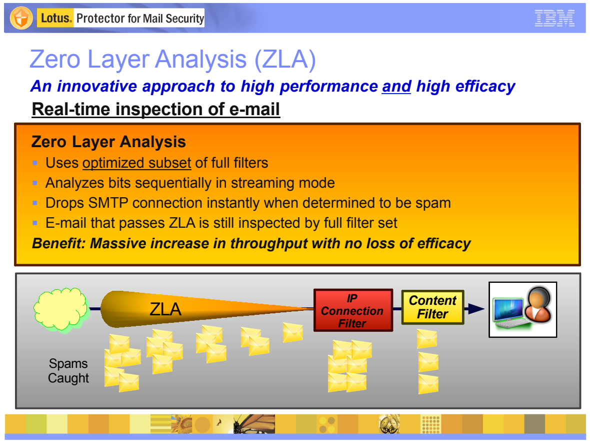
IP Reputation (SMTP layer)

- Drops connections from known bad domains or IP addresses
- ***PROBLEM:*** *More than half of spam is now originating from "trusted" domains*
  - *Tune low and lose effectiveness; tune high and overblock*

DO NOT ENTER

Content analysis (e-mail received)

- Detects spams through sophisticated analysis, using multiple specialized modules
- ***PROBLEM:*** *computationally intensive (write to disk, read to memory, analyze, delete)*
  - *Ever-increasing spam volume can overwhelm best filters*



Zero Layer Analysis (ZLA)

An innovative approach to high performance <u>and</u> high efficacy

Real-time inspection of e-mail

Zero Layer Analysis

- Uses optimized subset of full filters
- Analyzes bits sequentially in streaming mode
- Drops SMTP connection instantly when determined to be spam
- E-mail that passes ZLA is still inspected by full filter set

Benefit: Massive increase in throughput with no loss of efficacy

ZLA

IP Connection Filter

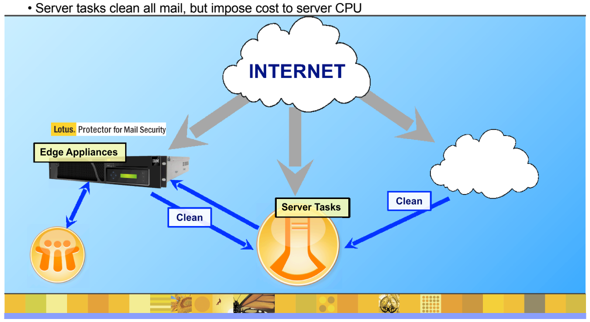
Content Filter

Spams Caught

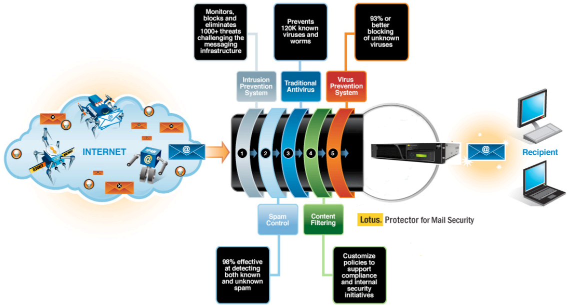
Popular Filter Deployment Options

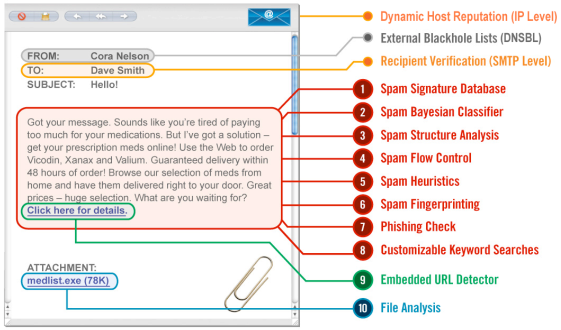
There are multiple approaches to spam and virus filtering, often with redundancy

- Edge appliances and cloud services filter SMTP, but don't see internal mail
- Cloud services allow less control by the customer and tends to have less filter efficacy
- Server tasks clean all mail, but impose cost to server CPU



Filter Process


Monitors, blocks and eliminates 1000+ threats challenging the messaging infrastructure
Prevents 120K known viruses and worms
93% or better blocking of unknown viruses
Intrusion Prevention System
Traditional Antivirus
Virus Prevention System
INTERNET
1
2
3
4
5
Recipient
Spam Control
Content Filtering
Lotus. Protector for Mail Security
98% effective at detecting both known and unknown spam
Customize policies to support compliance and internal security initiatives



FROM: Cora Nelson
TO: Dave Smith
SUBJECT: Hello!

Got your message. Sounds like you're tired of paying too much for your medications. But I've got a solution – get your prescription meds online! Use the Web to order Vicodin, Xanax and Valium. Guaranteed delivery within 48 hours of order! Browse our selection of meds from home and have them delivered right to your door. Great prices – huge selection. What are you waiting for?
Click here for details.

ATTACHMENT:
medlist.exe (78K)

- Dynamic Host Reputation (IP Level)
- External Blackhole Lists (DNSBL)
- Recipient Verification (SMTP Level)

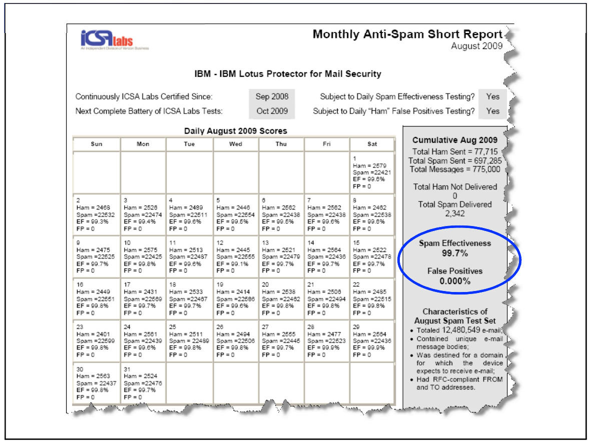
1. Spam Signature Database
2. Spam Bayesian Classifier
3. Spam Structure Analysis
4. Spam Flow Control
5. Spam Heuristics
6. Spam Fingerprinting
7. Phishing Check
8. Customizable Keyword Searches
9. Embedded URL Detector
10. File Analysis

IBM X-Force Research

- Proprietary Research
  - *Bayesian Filter, URL Checker, Meta Heuristics, Flow Control, Structure Analysis, Phishing detection, Fuzzy Fingerprints, Behavioral Antivirus…*

- URL Database
  - *9.3 billion evaluated web pages and images*
    - *150 million new pages each month*
    - *150,000 new categorized sites each day*
  - *100 million URL filter entries*
  - *68 categories of spam URLs*

- Spam/Phishing Database
  - *80 million spam signatures in the database*
    - *2 million new signatures per day*
  - *> 98% effective against spam*
  - *< 0.001% false-positives*



Monthly Anti-Spam Short Report
August 2009

IBM - IBM Lotus Protector for Mail Security

Continuously ICSA Labs Certified Since:	Sep 2008	Subject to Daily Spam Effectiveness Testing?	Yes
Next Complete Battery of ICSA Labs Tests:	Oct 2009	Subject to Daily "Ham" False Positives Testing?	Yes

Daily August 2009 Scores

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1 Ham = 2579 Spam =22421 EF = 99.6% FP = 0
2 Ham = 2468 Spam =22532 EF = 99.3% FP = 0	3 Ham = 2526 Spam =22474 EF = 99.4% FP = 0	4 Ham = 2489 Spam =22511 EF = 99.6% FP = 0	5 Ham = 2446 Spam =22554 EF = 99.5% FP = 0	6 Ham = 2562 Spam =22438 EF = 99.5% FP = 0	7 Ham = 2562 Spam =22438 EF = 99.6% FP = 0	8 Ham = 2462 Spam =22538 EF = 99.6% FP = 0
9 Ham = 2475 Spam =22525 EF = 99.7% FP = 0	10 Ham = 2575 Spam =22425 EF = 99.8% FP = 0	11 Ham = 2513 Spam =22487 EF = 99.6% FP = 0	12 Ham = 2445 Spam =22555 EF = 99.1% FP = 0	13 Ham = 2521 Spam =22479 EF = 99.7% FP = 0	14 Ham = 2564 Spam =22436 EF = 99.7% FP = 0	15 Ham = 2522 Spam =22478 EF = 99.7% FP = 0
16 Ham = 2449 Spam =22551 EF = 99.8% FP = 0	17 Ham = 2431 Spam =22569 EF = 99.7% FP = 0	18 Ham = 2533 Spam =22467 EF = 99.7% FP = 0	19 Ham = 2414 Spam =22586 EF = 99.6% FP = 0	20 Ham = 2538 Spam =22462 EF = 99.8% FP = 0	21 Ham = 2506 Spam =22494 EF = 99.8% FP = 0	22 Ham = 2485 Spam =22515 EF = 99.8% FP = 0
23 Ham = 2401 Spam =22599 EF = 99.8% FP = 0	24 Ham = 2561 Spam =22439 EF = 99.6% FP = 0	25 Ham = 2511 Spam = 22489 EF = 99.8% FP = 0	26 Ham = 2494 Spam =22506 EF = 99.8% FP = 0	27 Ham = 2555 Spam =22445 EF = 99.7% FP = 0	28 Ham = 2477 Spam =22523 EF = 99.9% FP = 0	29 Ham = 2564 Spam =22436 EF = 99.9% FP = 0
30 Ham = 2563 Spam = 22437 EF = 99.8% FP = 0	31 Ham = 2524 Spam =22476 EF = 99.7% FP = 0					

Cumulative Aug 2009

Total Ham Sent = 77,715
Total Spam Sent = 697,285
Total Messages = 775,000

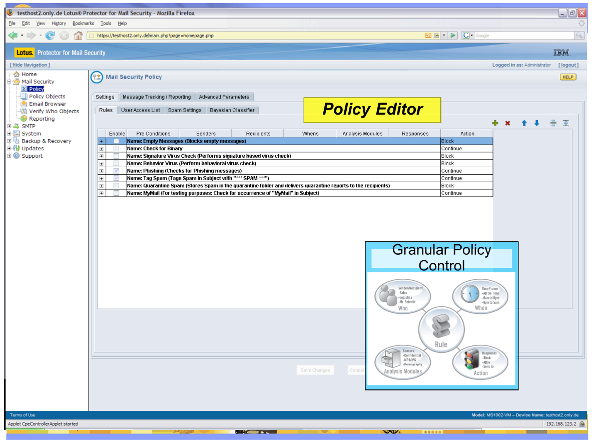
Total Ham Not Delivered
0
Total Spam Delivered
2,342

Spam Effectiveness
99.7%

False Positives
0.000%

Characteristics of August Spam Test Set

- Totaled 12,480,549 e-mail;
- Contained unique e-mail message bodies;
- Was destined for a domain for which the device expects to receive e-mail;
- Had RFC-compliant FROM and TO addresses.


testhost2.only.de Lotus® Protector for Mail Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://testhost2.only.de/main.php?page=homepage.php
Google
Lotus. Protector for Mail Security
IBM
[Hide Navigation]
Logged in as: Administrator [logout]
Home
Mail Security
Policy
Policy Objects
Email Browser
Verify Who Objects
Reporting
SMTP
System
Backup & Recovery
Updates
Support
Mail Security Policy
HELP
Settings
Message Tracking / Reporting
Advanced Parameters
Rules
User Access List
Spam Settings
Bayesian Classifier
Save Changes
Cancel
Terms of Use
Model: MS1002-VM – Device Name: testhost2.only.de
Applet CpeControllerApplet started
192.168.123.2

	Enable	Pre Conditions	Senders	Recipients	Whens	Analysis Modules	Responses	Action
⊞	□	**Name: Empty Messages (Blocks empty messages)**						Block
⊞	□	**Name: Check for Binary**						Continue
⊞	□	**Name: Signature Virus Check (Performs signature based virus check)**						Block
⊞	□	**Name: Behavior Virus (Perform behavioral virus check)**						Block
⊞	☑	**Name: Phishing (Checks for Phishing messages)**						Continue
⊞	☑	**Name: Tag Spam (Tags Spam in Subject with "*** SPAM ***")**						Continue
⊞	□	**Name: Quarantine Spam (Stores Spam in the quarantine folder and delivers quarantine reports to the recipients)**						Block
⊞	□	**Name: MyMail (For testing purposes: Check for occurrence of "MyMail" in Subject)**						Continue

Policy Editor

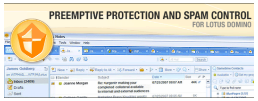
Granular Policy Control

IBM xSeries deployment options

	Economy	Value	Scale	Performance
IBM xSeries [1]	**x3250 M2**	**x3350**	**x3550 M2**	**x3650 M2**
Processor / speed / cache [2]	1x Intel® Xeon™ Processor X3330 / 2.66GHz / 6MB	1x Intel® Xeon™ Processor E3120 / 3.15GHz / 6MB	1x Intel® Xeon™ Processor E5502 2C / 1.86GHz / 4MB	2x Intel® Xeon™ Processor E5502 2C / 1.86GHz / 4MB
Total Memory / type [3]	3 GB / DDR2	4 GB / DDR2	4 GB / DDR3	4 GB / DDR3
Optical Device [4]	1x DVD/CD-RW Combo	1x DVD/CD-RW Combo	1x DVD/CD-RW Combo	1x DVD/CD-RW Combo
Controller [5]		1x ServeRAID-BR10il SAS/SATA	1x ServeRAID-MR10i SAS/SATA	1x ServeRAID-MR10i SAS/SATA
Storage [6]	1x 250GB 7.2k RPM 3.5" SATA	2x 300GB 10K 6Gbps SAS 2.5"	2x 300GB 10K 6Gbps SAS 2.5"	4x 73GB 15K 6Gbps SAS 2.5" 2x 300GB 10K 6Gbps SAS 2.5"
Redundancy [7]		1x 450w power supply	1x 675w power supply	1x 675w power supply
Network cards [8]	2x broadcom or Intel Network	2x broadcom or Intel Network	2x broadcom or Intel Network	2x broadcom or Intel Network
Rack Form factor	1U	1U	1U	2U
Limited Warranty [9]	One year parts and labor	One year parts and labor	Three year parts and labor	Three year parts and labor
Throughput: emails / hour [10]	**115k**	**180k**	**250k**	**360k**

1. No operating system needed. Lotus Protector software includes a Linux operating system
2. Different CPUs will work and may only change throughput results
3. Different memory sizes will work and may only change throughput results
4. Requires a DVD ROM minimum to install Lotus Protector
5. Controllers BR10i, MR10i, BR10il required for Raid. MR10i must be used with more than 2 Raid mirror sets
6. The 10k or 15k RPM disk speed is recommended. Different disk sizes and speeds will work and may only change throughput results.
   - Minimum storage size if you do not plan to retain blocked spam = 40GB.
   - If you plan to retain blocked spam, your approximate minimum storage per disk = 40GB + (emails/day x retention days x 0.000007 GB)
7. A redundant power supply is not required but provides more reliability
8. These network cards have been verified for this use.
9. Minimum warranty. Many other warranty and repair options can be selected
10. Measured filtering of incoming internet emails of average 19kB size with pre-filters turned off. IP pre-filtering and SMTP pre-filtering increase throughput.

Resources



www.ibm.com/lotus/protector/mailsecurity

- Feature Description
- Brochure
- Specifications
- White Papers
- Demo, Video
- ICSA Certification
- X-Force Statistics Graphs
- Support
- How to buy
- Product Documentation…

Questions?

Lotus® Protector

http://www.ibm.com/software/lotus/products/protector/

Vielen Dank

Legal Disclaimers

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC^2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.