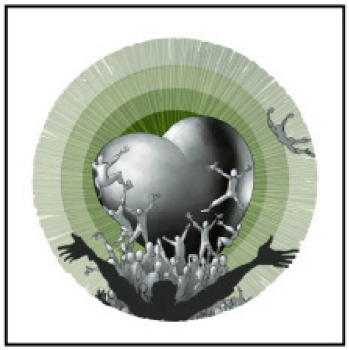
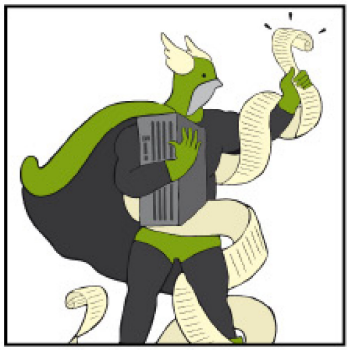
IBM SOFTWARELAND 2009.
SOLUZIONI INTELLIGENTI PER PROSPETTIVE CHE CAMBIANO.




Roberto Boccadoro
Lotus Protector

Compliance and Security secondo IBM

Protezione preventiva e controllo dello spam, virus e contenuto delle email per il tuo ambiente di posta Domino, con Lotus Protector

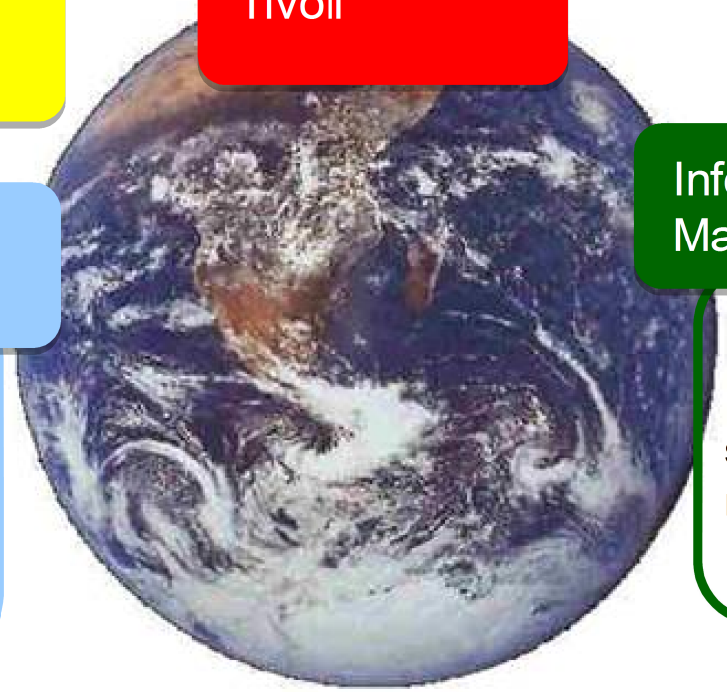
Lotus

Gestione del rischio, rispetto delle leggi e delle policy aziendali, report standard conformi alle normative

Tivoli

Gestione delle identità e controllo degli accessi alle risorse aziendali: le soluzioni TIVOLI

Tivoli



Rational

Le soluzioni Rational a garanzia della sicurezza delle applicazioni e il rispetto della compliance

Information Management

Il rispetto delle normative legali e di settore per la privacy dei dati e il records management

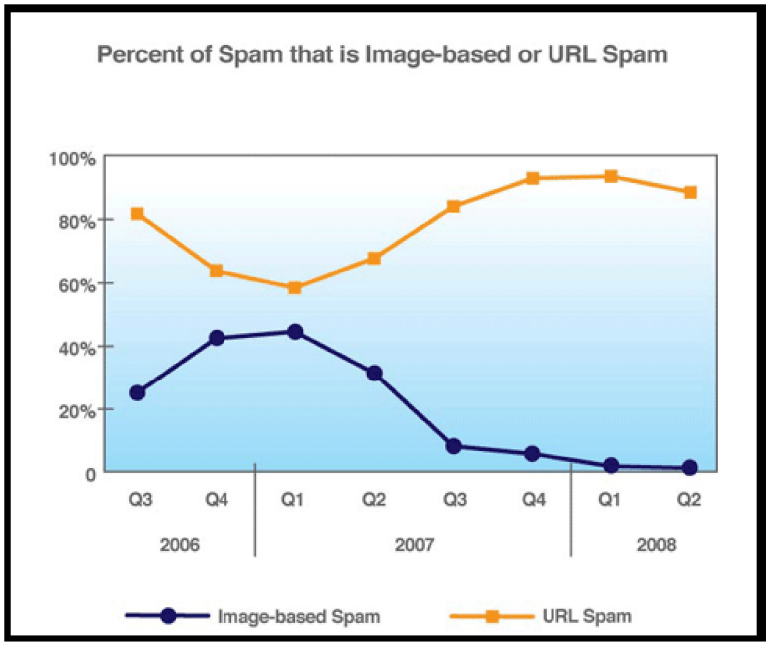
La sicurezza della posta è sempre più importante e difficile da ottenere

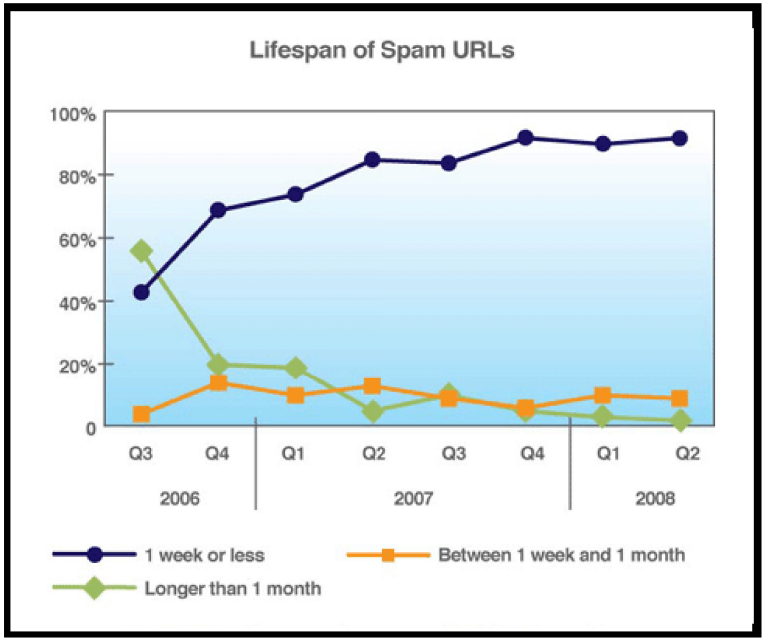
- Spam, Phishing, e Malware sono il 90% del traffico SMTP
  - Costo di banda e CPU
  - Danni all'immagine della società ed impatto sulla produttività dei dipendenti
  - Fuoriuscita di informazioni confidenziali



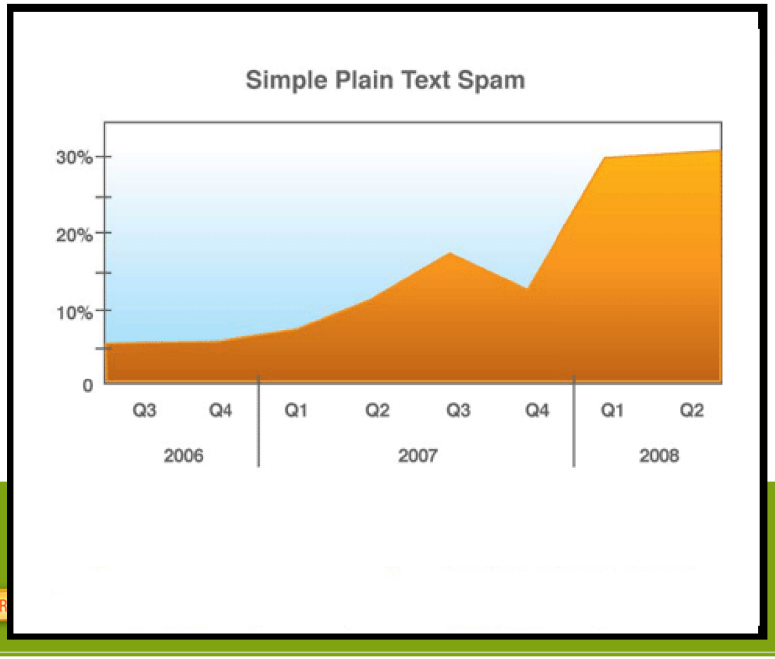


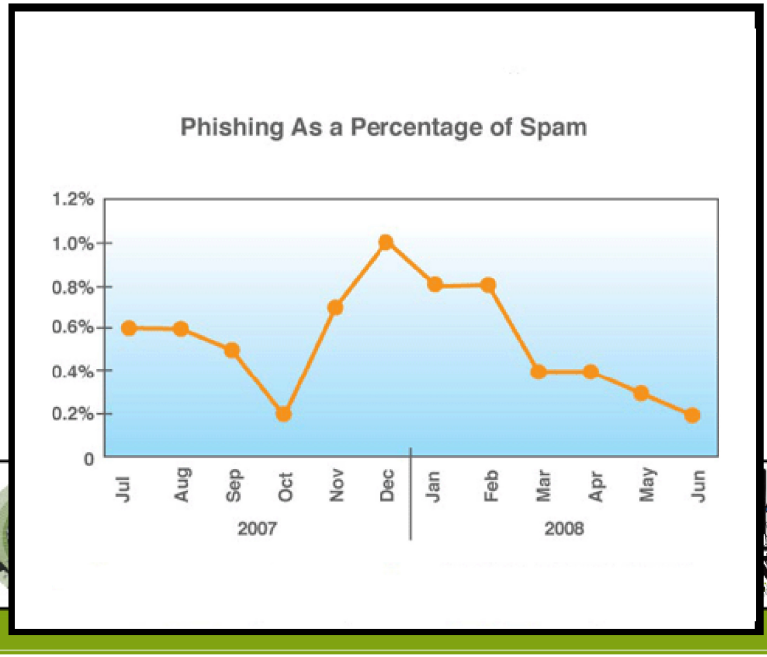
I tipi di attacco cambiano rapidamente



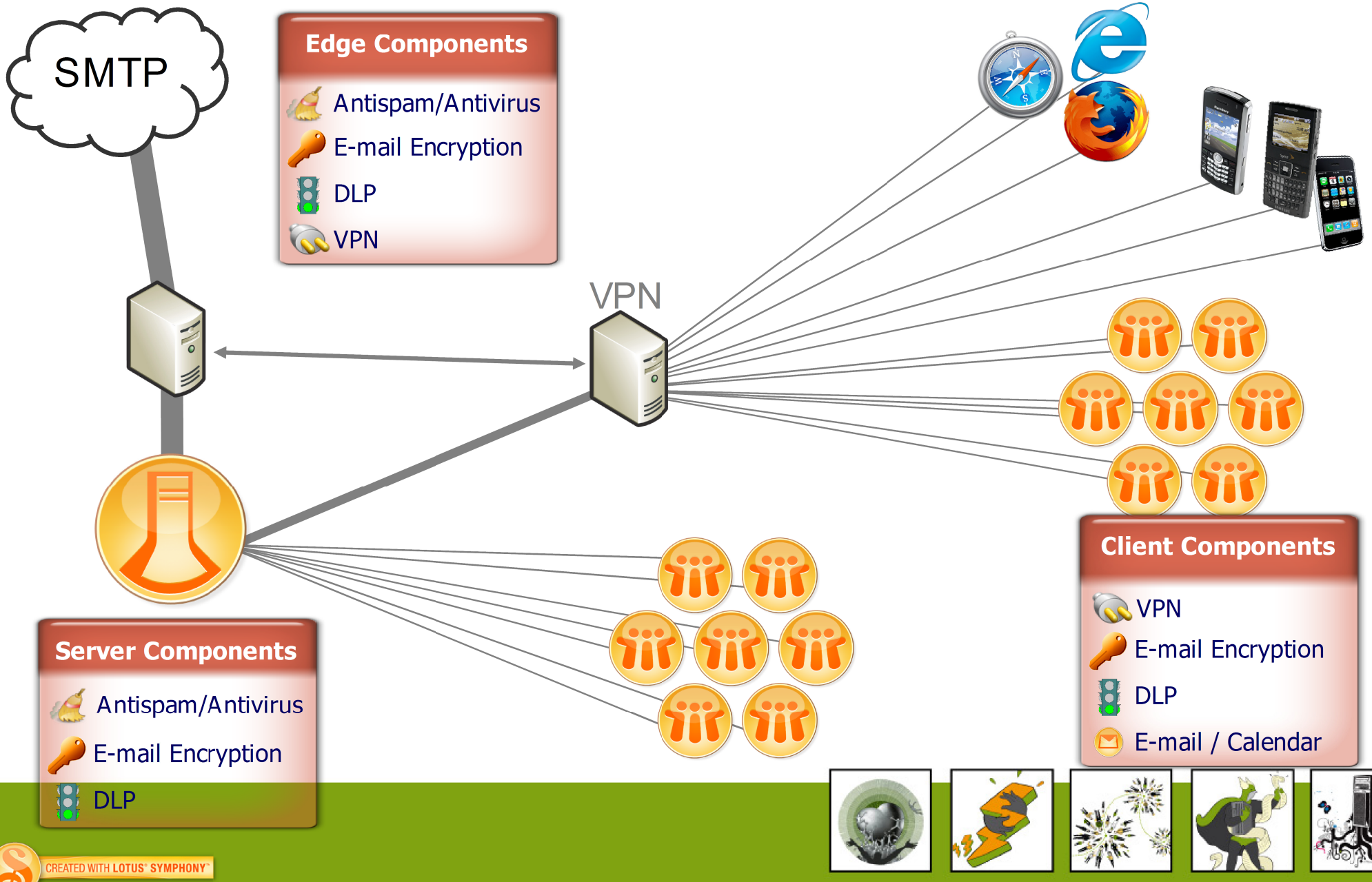


Source: IBM X-Force Research 2008





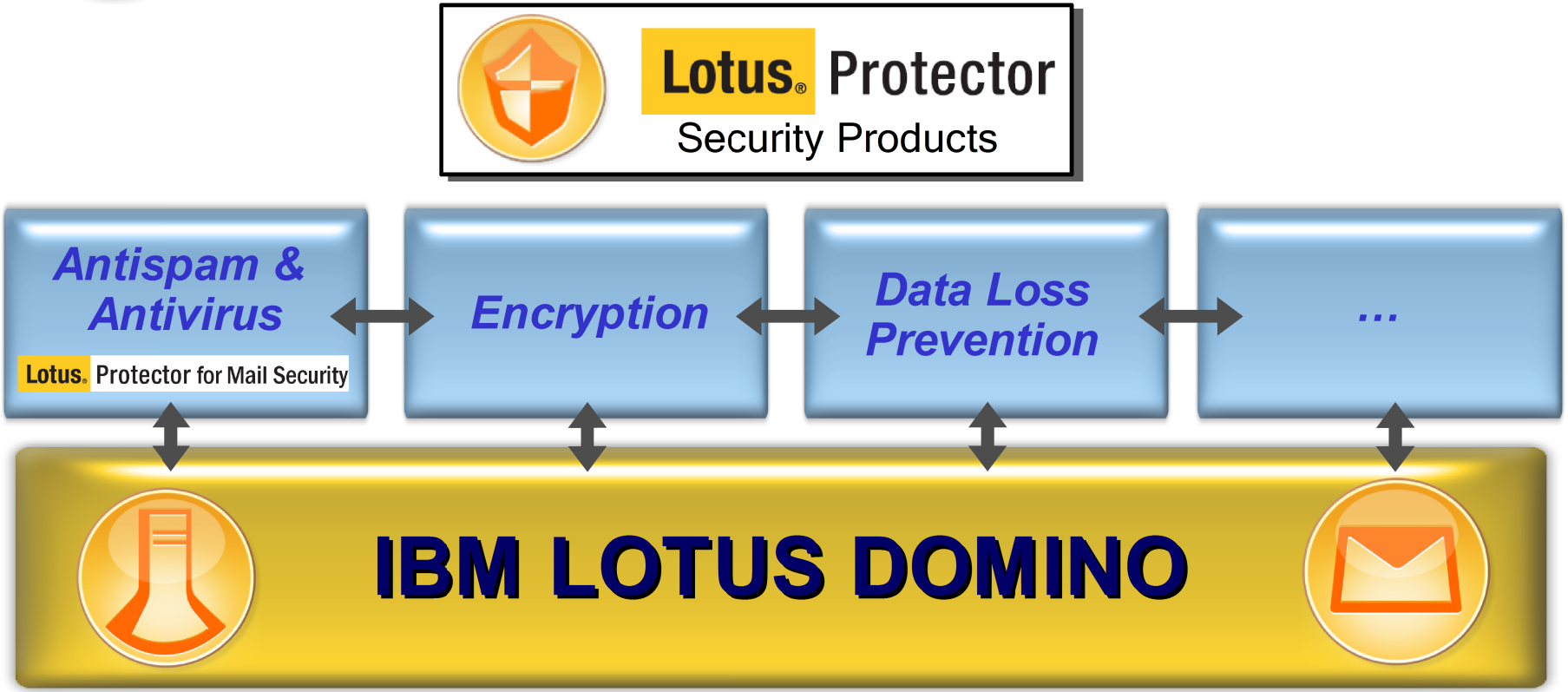
La sicurezza in una rete Domino



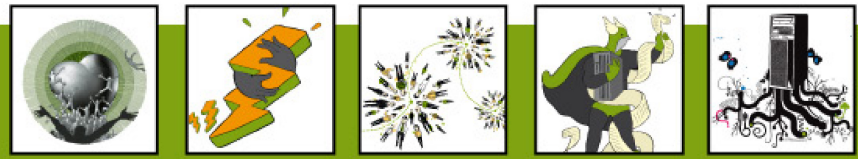
Notes/Domino: Lo Standard per la sicurezza della posta

- La più grande public key infrastructure installata al mondo
  - 145 milioni di licenze
  - Ogni utente ha un certificato tipo RSA
- 0 = numero di attacchi che hanno avuto successo contro Notes/Domino
  - Resiste a “address book harvesting”, worms, eseguibili,...
  - Execution control lists (ECLs) che “non consente nulla” per default
- La sicurezza nel DNA
  - Certificati, passwords forti, cifratura file e protocolli…
  - Controllo accessi a livello di oggetto, sicurezza basata su ruoli,…
- 36 Security Bulletin relativi all'email emessi dal 2000 ad oggi.
  - Molti non richiedono fix ma solo configurare bene il server o il client (ECL)
  - Altri sistemi di posta, quante security patch ogni mese ?

IBM Lotus Protector



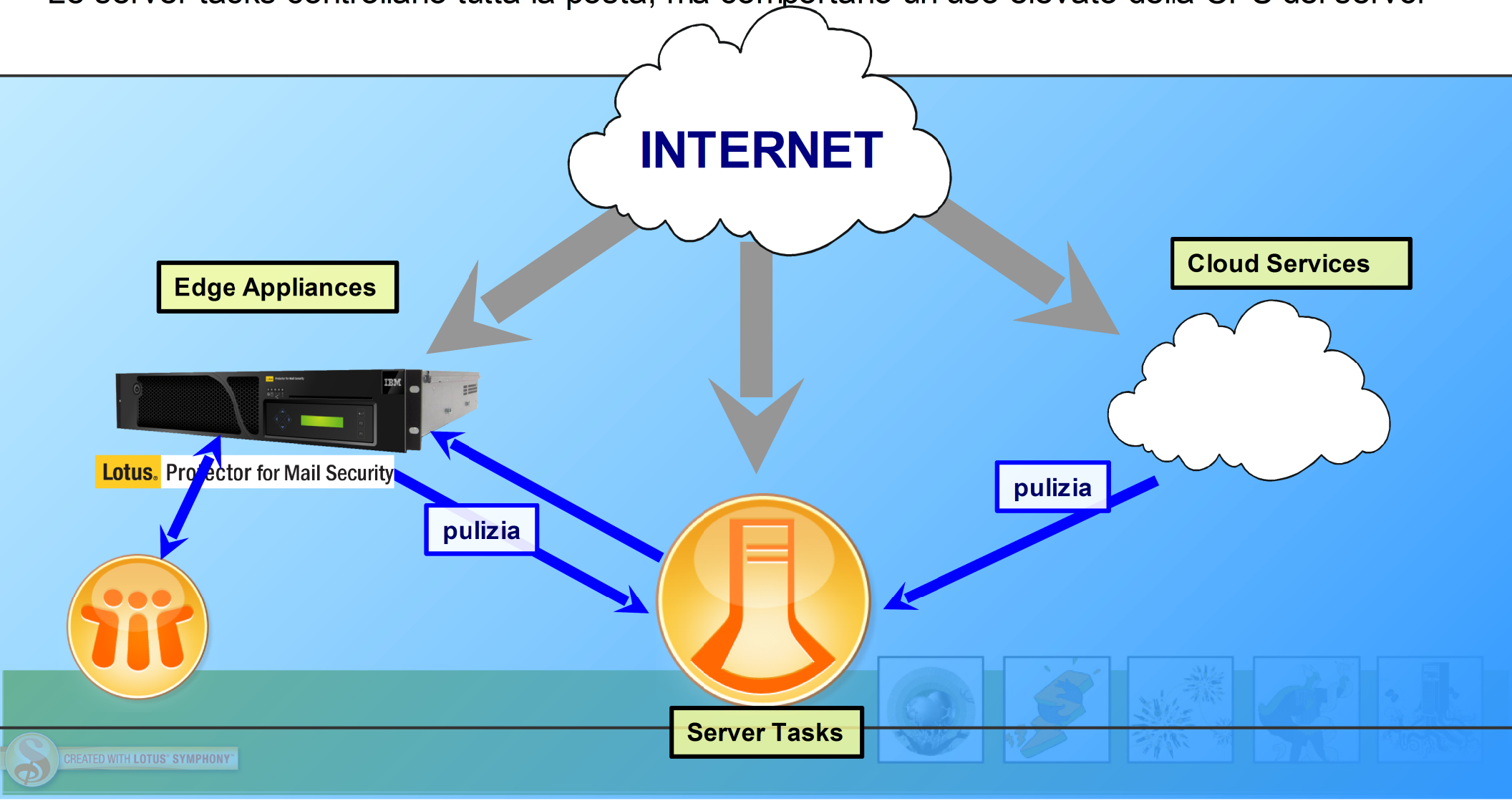
Lotus® Protector for Mail Security



Opzioni disponibili sul mercato

Ci sono vari approcci alla protezione da spam e virus

- Edge appliances e cloud services filtrano la posta SMTP, ma non quella interna
- Cloud services consentono minore controllo da parte del cliente
- Le server tasks controllano tutta la posta, ma comportano un uso elevato della CPU del server



Lotus® Protector for Mail Security

Protezione SMTP per Lotus Domino

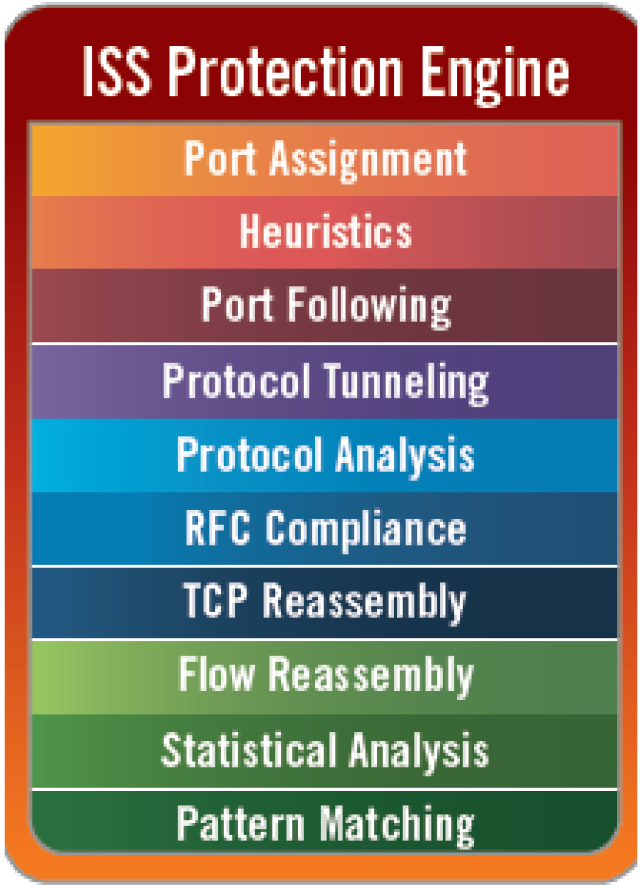
- Software di filtraggio spam
  - Basato su tecnologia IBM Proventia Spam/Malware blocking
    - Dynamic Host Reputation (IP Filtering)
    - Analidi dei messaggi multilivello
    - Antivirus basato su Signature e Behavioral Antivirus
    - Controllo URL per phishing e spyware
    - Possibilità per gli utenti di avere la quarantena e liste blocca/ consenti
  - Ottimizzato per clienti Domino
    - Facile da acquisire, installare, ed amministrare
    - Roadmap chiara di integrazione
- Protezione preventiva
  - Regole/Policy per protezione del contenuto (in entrata/in uscita)
  - IBM Proventia intrusion prevention system integrato

Intrusion Prevention System : cosa è

- *Intrusion Prevention System:* Hardware o software dotato delle seguenti caratteristiche:
  - L'*intelligenza* per analizzare le comunicazioni sulla rete e/o le attività del computer per individuare attività potenzialmente dannose
  - Abilità di bloccare automaticamente tali attività basandosi su analisi
  - Abilità di lavorare a più livelli (rete, applicazioni, trasporto, etc.)
  - Funzionamento real o near-real time

Intrusion Prevention System

- IPS per SMTP fa sì che la vostra infrastruttura di messaginng non sia mai compromessa



Lotus® Protector for Mail Security

Tecnologia avanzata

IBM Proventia

INTERNET SECURITY SYSTEMS

ICSA labs CERTIFIED www.ICSALabs.com Anti-Spam

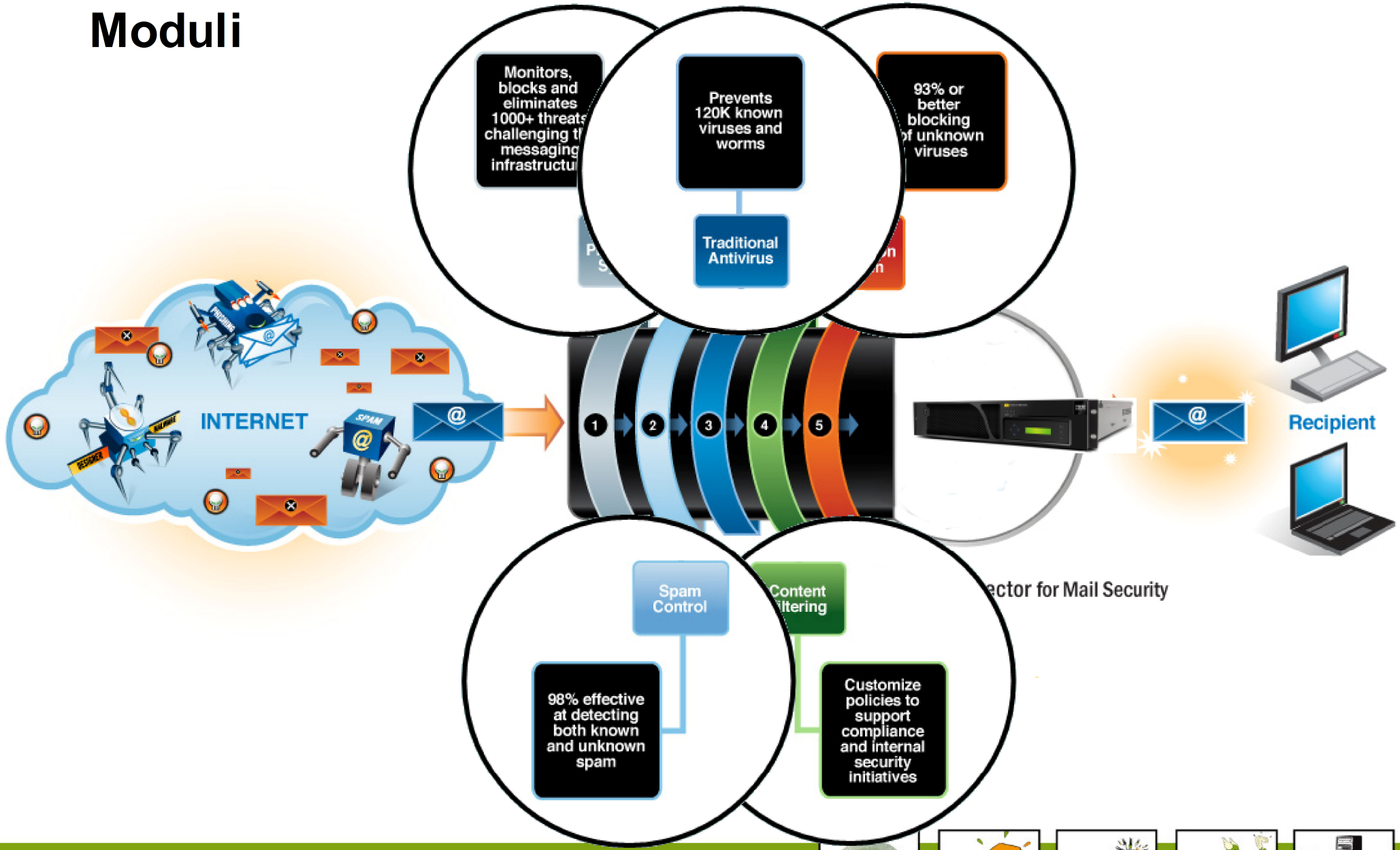
Deployment flessibile

Per-user software license

Software Appliance

Hardware Appliance

Moduli


Monitors, blocks and eliminates 1000+ threats challenging t messaging infrastructu
Prevents 120K known viruses and worms
Traditional Antivirus
93% or better blocking of unknown viruses
INTERNET
1
2
3
4
5
Recipient
ector for Mail Security
Spam Control
98% effective at detecting both known and unknown spam
Content iltering
Customize policies to support compliance and internal security initiatives

IBM SOFTWARELAND 2009.

IBM

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

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.

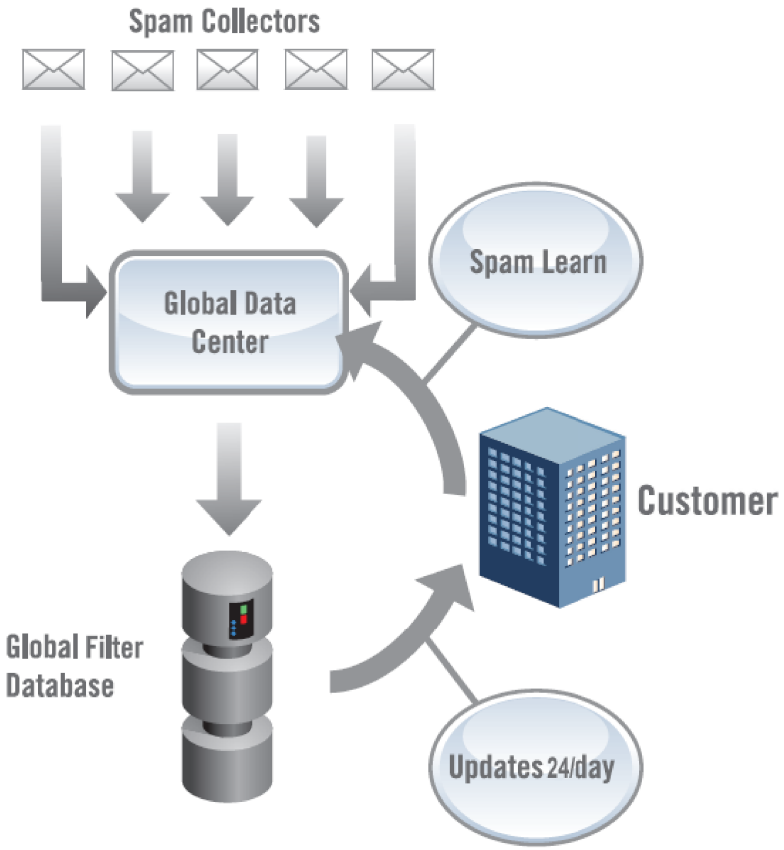
ATTACHMENT:
medlist.exe (78K)

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. Cus[illegible]

9. Embedded URL Detector
10. File Analysis

IBM ISS Filter Infrastructure

- Filter Database:
  - 2,000 Spam Collectors e Web Crawlers
  - 22 worldwide data centers
- Filter Analysis
  - 1,000 server database farm



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

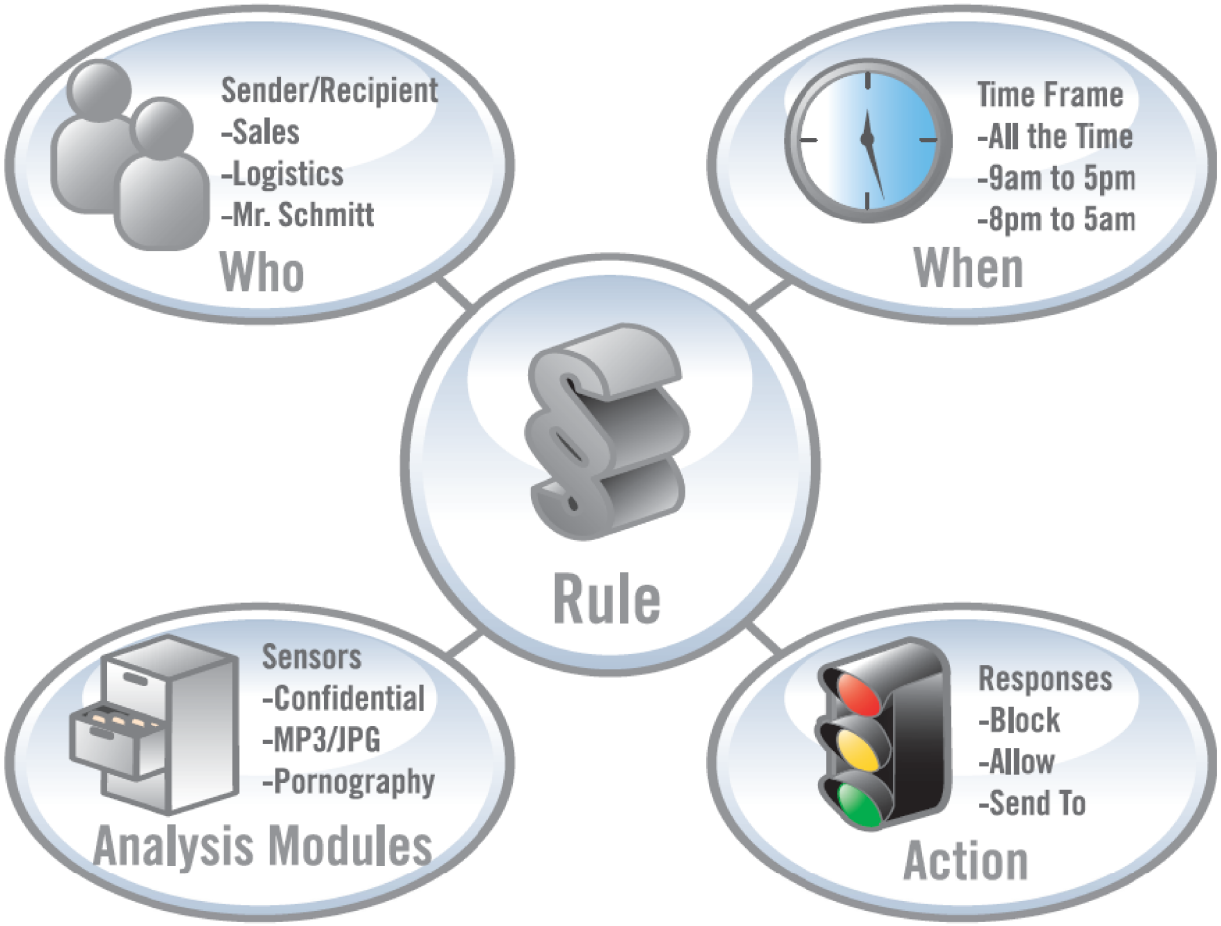
- 80 million spam signatures in the database
  - 2 million new signatures per day
- > 98% effective against spam
- < 0.001% false-positives
- 62 categories of spam URLs

Controllo granulare delle Policy

- Creazione di policy semplice, basata su regole
  - chi – cosa – quando – azione

SC MAGAZINE RATING	
Documentation	★★★★☆
Ease of use	★★★★★
Features	★★★★★
Performance	★★★★★
Support	★★★★☆
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Highly customizable and easy to use at a low cost of ownership.
Weaknesses Documentation could use a bit of simplification and organization.
Verdict A very strong product for any size organization. It is easy to set up and manage and loaded with features. For its policy engine and ease of use, we designate the Proventia Network Mail Security appliance our Recommended product.



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

Lotus. Protector for Mail Security

IBM

[Hide Navigation]

Logged in as: Administrator [logout]

Policy Editor

- Home
- Mail Security
  - Policy
  - Policy Objects
  - Email Browser
  - Verify Who Objects
  - Reporting
- SMTP
- System
- Backup & Recovery
- Updates
- Support

Mail Security Policy

HELP

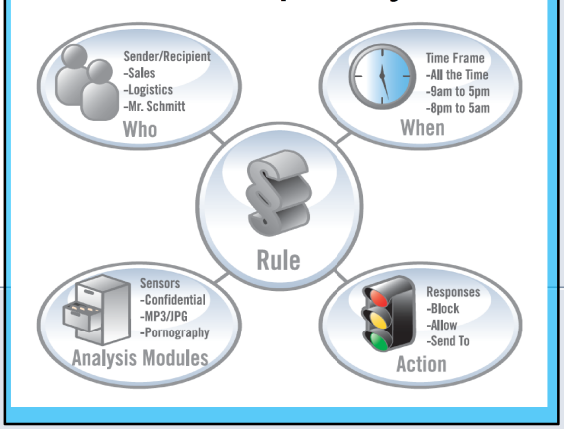
Settings | Message Tracking / Reporting | Advanced Parameters

Rules | User Access List | Spam Settings | Bayesian Classifier

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

Save Changes Cancel Changes

Controllo granulare delle policy



Roadmap

Lotus® Protector for Mail Security

Q3 2008
Lotus Protector for Mail Security 2.1

- Primo rilascio Lotus
  - *6° generazione della tecnologia*
- IP Reputation Filtering
- TLS encryption
- Appliance or VMware

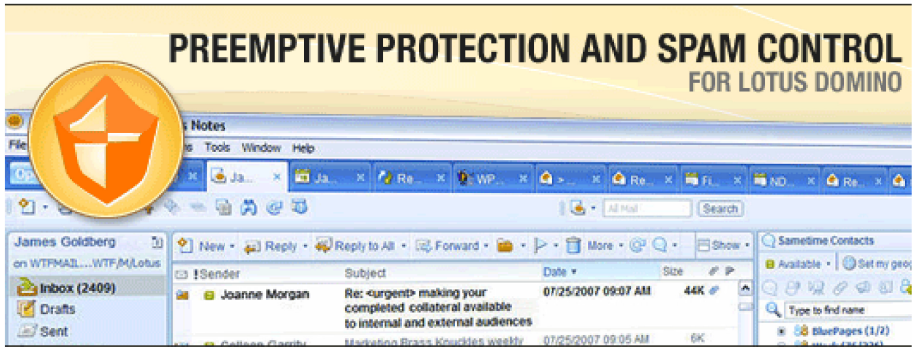
Q2 2009
Lotus Protector for Mail Security 2.5

- Standardized Linux platform
  - *Utilizzo hw standard xSeries*
- Integrazione Notes/Domino
  - Block/Allow list e gestione quarantena Notes-based
  - Gestione mail interne

Q1 2010
Lotus Protector for Mail Security 3.0

- Horizontal Protector integration
  - *Integrazione con encryption, DLP*
- Ulteriore integrazione Notes/Domino
  - APIs, Web services
- Protezione per Sametime, Quickr, Connections

Ulteriori informazioni



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…