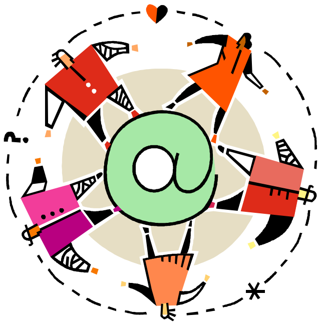
©Copyright 2005 by i-Guard.Net

i-Guard Enterprise

A comprehensive email content security solution for enterprise and service provider

White Paper



i-Guard.Net
Content Security Solution

The Problems

As Internet email system grows into a convenient and cost-effective infrastructure for global business communication, the lack of security in the present Internet email system also invites exploitation and exposes a new channel for attacks. Worst, unlike web application which is reactive in nature, the pro-active nature of email application allows viruses to reach any users even without user initiation. For this reason, email represents the greatest security threat to Internet users to date.

Spam, Email-borne Virus, Phishing …

Today, email-borne viruses are far more reaching and damaging than ever before. With the aid of widely-deployed, speedy, insecure email infrastructure and the pro-active nature of email application, spam and email-borne virus can reach anyone with a mailbox at the speed of the Internet. Traditional reactive anti-virus mechanism is not prepared for dealing with such aggressive fast-spreading email-borne virus. Adding to the problem is a clear sign of spam and virus convergence and this trend is on the rise as the law on spam is enforced. Together, spam and email-borne virus problems could easily cost an enterprise millions of dollars annually due to loss of productivity; wiping out, probably even exceeding, the benefits of email. FBI estimates that the spam and virus problems cause a world-wide damage of 200 billion dollars due to loss of productivity in 2003 alone (See Ref 1). Most damaging of all is the public trust on an economic infrastructure of growing significant.

Non-compliant Use of Email

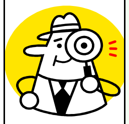
Unwise non-compliant use of email by employees also adds another threat dimension to the email security problem. Adding to that is the threat of sensitive confidential document leakage. Such threats could create legal liability and publicity disaster for the enterprise and impose substantial damages that have never been accounted for.

Insecure Email Communication

It has also been widely known that email communication can be easily and legally exposed to unintended viewers in many ways for various reasons (see Ref 2). Needless to say, such exposures could cause embarrassment, legal liability, sensitive corporate data leakage as well as privacy invasion and confidentiality concerns.

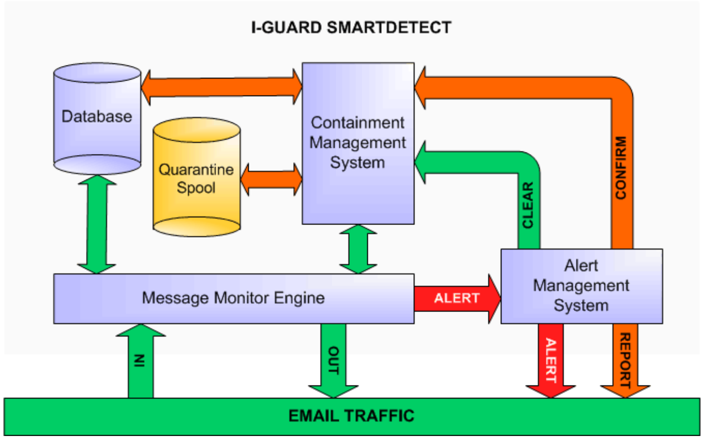
i-Guard.Net Solution

Spam and email-borne virus are dynamic and multi-facet problems. There will be no one-size-fit-all solution for problems of such fluidity. At i-Guard.Net, we believe that the only effective defense is a multi-layer defense strategy that combines both state-of-the-art detection technologies and effective prevention measures. i-Guard solution reflects such a comprehensive strategy to give the best possible protection as described below:

	Layer 1 – Early Alert A collaborative community-based early alert network system that helps to raise early alert of spam and email-borne virus attacks as they are occurring on the network; effectively, negating the attacks before they even become a threat to the community.
	Layer 2 – SmartDetect A unique patent-pending auto-detect, early-alert and pro-active containment technology used to suppress spam and email-borne virus attacks at the source of attacks rather than on message arrival with up to 100% catch rate in most cases.
	Layer 3 – SmartScreen A multi-layer high performance message screening technology that helps to identify spam and email-borne viruses arrived in dispersed traffic and quarantine them outside of the corporate perimeter, with close to 100% catch rate.
	Layer 4 – SafeDelivery A policy for secure message delivery designed to prevent recipient's exposure to dangerous message content and thus, minimize the opportunity for an unknown virus to infect and spread.

SmartDetect - Traffic Analysis

SmartDetect technology is a unique patent-pending auto-detection and pro-active containment sub-system designed to block unknown spam and virus attacks from overwhelming the corporate mail server and causing business disruption. i-Guard SmartDetect technology is capable of proactively blocking such attacks at the source of attacks with 100% of catch rate in most cases. The cornerstone of the SmartDetect sub-system is an efficient and intelligent email traffic monitor module responsible for detecting virus and spam attacks based on message traffic analysis. Using a combination of traffic analysis and cloaking-proof fingerprint message identification technologies, SmartDetect is not only highly accurate but capable of defeating many cloaking and disguise techniques often used by spammers and virus writers to avoid detection. Early detection enables SmartDetect to pro-actively suppress an attack at the early stage of the attack by containing such an attack at the source of attack as soon as it occurs. Such aggressive measure prevents precious mail server's resources and network bandwidth from being consumed by the attack and subsequently avoids costly business disruption.



SmartScreen – Message Filter Engine

Another icon of i-Guard virus and spam defense system is a state-of-the-art high performance multi-layer message screening engine, namely SmartScreen. SmartScreen is responsible for screening, identifying and filtering spam and email-borne virus-infected messages arriving in dispersed email traffic. SmartScreen combines several proven anti-spam technologies to improve processing performance as well as detection effectiveness against all kinds of known cloaking and disguise techniques employed by spammers and virus writers to bypass detection. Among them are:

Message Header Analysis

Many spam messages leave their signatures in the message header. Careful analysis of the message header helps to eliminate them quickly and efficiently before any more expensive spam detection mechanism is needed.

Permission-based Heuristics

Unlike the challenge-and-response (C&R) method that suffers from a number of drawbacks such as imposing the burden of proof on legitimate senders and unnecessary message delivery delay due to the sender's confirmation process, SmartScreen permission-based heuristics combines the use of a collective white list of legitimate senders that it automatically learned from the users and message traffic and other spam detection technologies to evaluate messages from unknown senders for acceptance or rejection prior to the invocation of the confirmation process. As a result, SmartScreen operates more intelligently, often results in faster message delivery and optimizes the burden of proof on legitimate senders while maintaining a high catch rate known to enjoy through C&R technique.

Content Analysis and Control

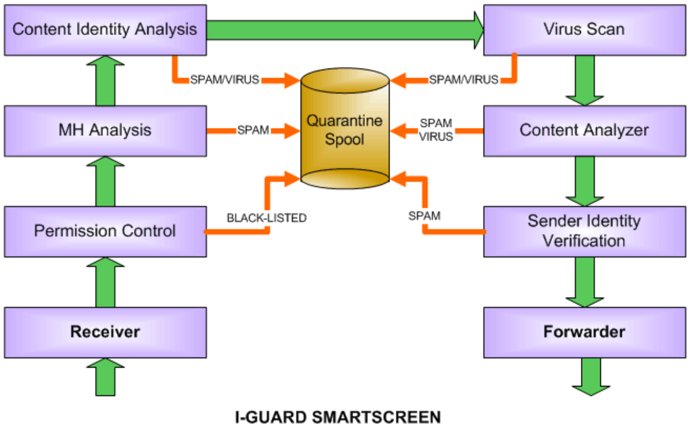
Also included in SmartScreen is a high performance content analyzer for identifying messages with undesirable or dangerous content based on a scored and categorized dictionary of keywords, phrases and URLs. Due to the high cost of content scanning, SmartScreen intelligently stages content analysis for optimized performance. This results in significant reduction in CPU usage and faster delivery. The supported content categories are: Adultery, Gambling, Fraud, Phishing, Violence, Radicals, Drugs, Tobacco, Spam and Virus.

Content Identification

Using signature-based technology, SmartScreen also implements a sophisticated high performance message content identifier for identifying messages known as spam or carrying virus. The content identifier is carefully crafted to avoid all known cloaking and disguise string pattern techniques often used by spammers and virus writers to avoid detection

Adaptive - Self-learning

Furthermore, SmartScreen is capable of automatically learning from various user activities, message traffic patterns and per-mailbox spam level and self-adjusting to improve its catch rate and overall message processing performance as well as to lower false positives. Thus, the longer SmartScreen operates, the smarter and more efficient it becomes.



SafeDelivery – Message Delivery Policy

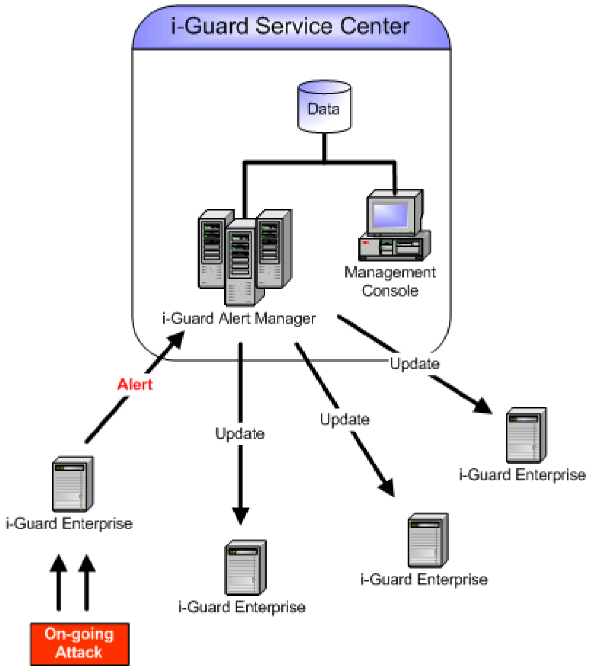
i-Guard solution also allows the users and administrator to establish personalized or centralized policy for enforcing a safe message handling policy designed to prevent users from falling into virus tricks as well as to raise the level of awareness and accustom users on safe message handling practices such as:

- ☑ Warning the user of messages with unsafe content,
- ☑ Securing messages with unsafe content from auto-execution prior to delivering them to the users or
- ☑ Isolating unsafe messages for audit and acceptance.

Community-based Early Alert System

The success of email-borne viruses in creating crisis in recent years is largely due to their ability to quick propagate themselves on the network and the large window of opportunity created by the slow virus identity update process. i-Guard Early Alert Network is designed to minimize this window of opportunity and to defeat email-borne virus at their own game, *speed*.

Both SmartDetect and SmartScreen are capable of detecting unknown spamming and email-borne virus and establish dynamic blocking rules upon such detection. Furthermore, an alert is generated to gain the administrator's attention to the attack. To enable the entire i-Guard community to capitalize on such dynamic detections, i-Guard offers a high performance community-based feedback and update system where dynamic blocking rules are automatically propagated to other i-Guard Enterprise installations within a short period of time, a few minutes, rather than days or hours as traditional anti-virus measure does it. Such quick alert delivery, in effect, negates the new attacks even before they become a threat to other member sites within the i-Guard community.



i-Guard SecureMail – Email Encryption

The globalization of the high-tech work force and business has fueled the use of email as a business conduit and document delivery vehicle due to the advantages of convenience, fast delivery, and cost-effectiveness that email offers. This trend creates a need for securing documents communicated via email that goes beyond the corporate VPN boundary. To meet this emerging need as well as to enable privacy protection for the mass, i-Guard.Net introduces a patent-pending email encryption technology offering several advantages over existing technologies in terms of ease of use, security, and flexibility.

Highly-Secure Encryption Technology

Unlike public-private two-key encryption system, i-Guard patent-pending i-Guard SecureMail technology encrypts outbound message using a unique per-message encryption key dynamically generated from a message characteristic and a sender's secret key. The sender's secret key is stored on a designated system where the message receiving system will later contact for a decryption key to decrypt the message. Similar to SSL technology, i-Guard SecureMail technology makes it extremely difficult for an intruder to break into an email conversation exchanged between two parties due to the dynamic nature of the encryption key. However, unlike SSL technology which protects messages on transit only, i-Guard SecureMail technology offers end-to-end security benefit, whether the protected messages are on transit or stored on a relay mail server along the delivery path.

No Key Management Burden

As a result of i-Guard unique encryption technology, i-Guard SecureMail eliminates the need for maintaining a list of public keys from the user. All message encryption and decryption tasks occur transparently from both the sender and the recipient.

Sender and Recipient Identity Verification

A side benefit of i-Guard SecureMail technology is that its algorithm automatically enforces sender's identity verification as the sender's identity must be valid for the decryption key to be correctly generated. With such capability, i-Guard solution can also serve as an alternative next generation sender identity verification-based spam, fraud and phishing prevention solution (the others are Yahoo DomainKey and Microsoft SenderID). Unlike other spam prevention solutions, i-Guard SecureMail technology does not require any changes to any Internet protocols.

Centralized and Distributed Encryption Engine

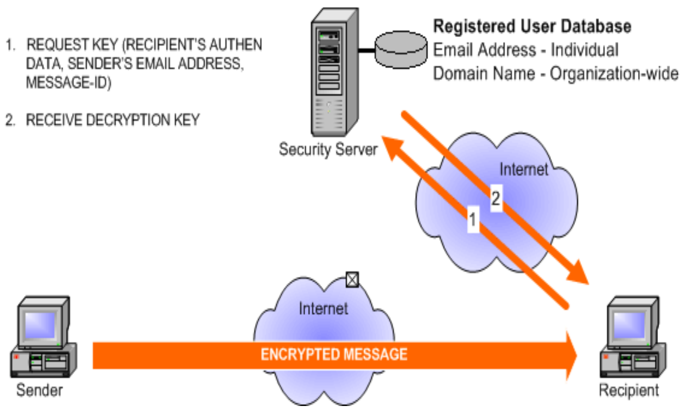
i-Guard Enterprise provides support for both centralized gateway-based and distributed agent-based encryption. While gateway-based encryption removes the administrator from the burden of per-system software installation and associated support, the agent-based encryption solution helps to cost-effectively avoid performance bottleneck on the message processing gateway. In either configuration, the administrator can always centrally enforce enterprise-wide message encryption policy.

Scalability, Ease of Management and Lower TCO

The integration of i-Guard SecureMail into i-Guard Enterprise offers many benefits. First, it simplifies setup as message encryption is now simply an option in the user's profile.

Secondly, message throughput is improved as messages can be efficiently processed in a single pass through i-Guard Enterprise system rather than multiple passes through multiple devices. When an i-Guard Agent desktop software is installed on the user's system, CPU-intensive encryption/decryption tasks can be distributed on today powerful client systems to improve scalability.

Obviously, such benefits will also lead to lower management, operation and maintenance costs.


1. REQUEST KEY (RECIPIENT'S AUTHEN DATA, SENDER'S EMAIL ADDRESS, MESSAGE-ID)
2. RECEIVE DECRYPTION KEY
Registered User Database
Email Address - Individual
Domain Name - Organization-wide
Security Server
Internet
2
1
Internet
ENCRYPTED MESSAGE
Sender
Recipient

Corporate Email Policy Enforcement

In today network computing environment, organizations face not only external security threats but also those from within. For example, a spyware can infect a local system and send sensitive corporate data to unknown Internet destinations. Additionally, unwise use of email by employees can create costly liability, publicity disasters or loss of competitive advantages. To tackle these problems, i-Guard Enterprise allows the administrator to establish and enforce outbound message control policies. Violating outbound messages are subject to specified control actions which could be bounced back to the sender, quarantined for audit or redirected to an audit mailbox. For example, using i-Guard Enterprise outbound message control policy, the administrator can establish rules for controlling the following types of outbound message:

☑ Message with obscene or offensive languages
☑ Message with confidential content
☑ Message with attachments classified as confidential
☑ Message matching keywords, phrases or URLs
☑ Forwarded message originating from a list of senders

Other Highlight Features

High Performance Message Processing Engine

i-Guard Enterprise filter engine implements a unique high-performance and scalable store-and-forward message processing architecture. SMTP message reception and forwarding engines implement state-of-the-art server design to optimize system overhead. As a result, i-Guard Enterprise filter engine is capable of serving thousands of concurrent MTA sessions even on a commodity Pentinum class hardware, while offers a high scanning and forwarding rate at the same time.

Safe Policy-based Message Management

i-Guard Enterprise never drops any messages without user's knowledge. Messages subject to control are classified and handled in accordance to user- and/or administrator-specified message handling policy, which could be label-and-forward, delete, quarantine, bounce-back to sender, etc.

Quarantine messages can be safely audited by the user or administrator for further delivery using an intuitive Explorer-like web-based Email Control Manager (ECM) application that can be conveniently accessible from anywhere.

Comprehensive Management System

i-Guard Enterprise comes with a comprehensive web-based administration system that enables the administrator to centrally and remotely manage all aspects of i-Guard Enterprise secure messaging operations: database management, user's profile management, quarantine message management, (attack) alert management and system/service management. Furthermore, system and service status are automatically monitored and graphically reported in real-time to the management system.

Personal and Central Security Policy

i-Guard Enterprise system can operate in pass-through mode or managed mode. In pass-through mode, messages are filtered based on an admin-established message control policy. Messages subject to control are appropriately labeled and forwarded to destined mail servers. In managed mode, each user can set up personal message control and handling policies, white/black list, etc. Messages subject to control will be handled by the user-specified message handling policy. In either mode, the administrator has full control in enforcing a high-precedent central security policy and black/white lists. Moreover, the administrator can even determine whether a message control policy should be made available for personalization or not.

High Granularity and Flexibility

Yet, in managed mode, the administrator has greater flexibility in accommodating individual needs with high granularity. Such high granularity results a high degree of message traffic accounting precision and therefore, can be used for tuning the system for better efficiency and security. To ease the administrator from the burden of user management, i-Guard Enterprise provides support for an optional automatic user registration procedure.

Virtual Message Control Engine

With such high granularity and flexibility in user management, i-Guard Enterprise allows the administrator to set up multiple virtual message control engines per hardware platform using a web-based customer management system. Just as virtual web hosting, when multiple customers can share the same server system, the acquisition and operational costs can be significantly reduced resulting both higher profit margin for service providers.

Spam Sensitivity Control

Another useful personalization feature of i-Guard SmartScreen is its per-user spam sensitivity control capability. Since each user may have a different definition of spam, enabling the user to adjust the spam sensitivity level will result in lower false positives and higher catch rate.

Automatic Contact List Synchronization

With an optional i-Guard Agent for Windows desktop, user's contact list on the desktop can be conveniently synchronized with the user's white list on i-Guard Enterprise system. Automatic synchronization of user's contact list helps to facilitate message acceptance from known correspondences and legitimate email users and therefore, optimize message processing. Contact and white list synchronization optionally works in both directions, i.e. auto-detected correspondences will be automatically imported to the user's contact list. Another side benefit of this feature is that the user can always conveniently access his/her contact list from anywhere at anytime using a web-based ECM application.

Per-mailbox Message Traffic Monitor and Report

i-Guard Enterprise keeps track of all inbound and outbound message statistics on a per-mailbox basis. This information can be used to inform the users of the level of spamming exposure of their mailbox. Using this information, the user can take appropriate action such as to abandon a severely-exposed mailbox. i-Guard Enterprise also uses this information to detect mass mailing activities and raises alert event on the administration console.

Cost-effective Message Store

Although i-Guard Enterprise can be configured for centralized quarantine message store, i-Guard Enterprise also allows the administrator to configure the system for storing quarantine messages right on the message processing (or filter) engines that process them. This, in effect, distributes the message store among the filtering engines and therefore, is more cost-effective than the centralized message store architecture.

Scalability and High Availability

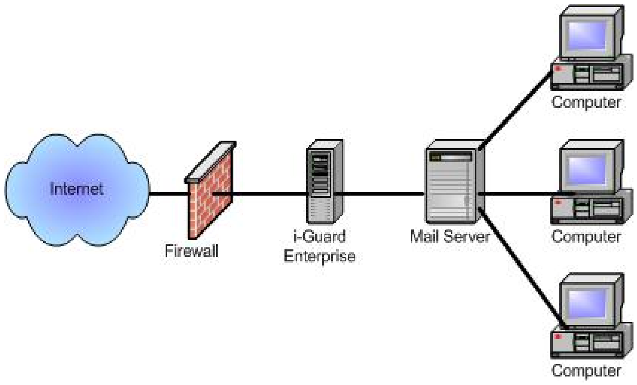
i-Guard Enterprise system design is highly modular. As a result, i-Guard message filter engine can be easily duplicated for scalability and high-availability. Adding more processing capacity to accommodate a growing user base or to improve performance and service availability is just a matter of plug-and-play.

Deployment Schemes

Intended for service provider and enterprise market with large user base, the design of i-Guard Enterprise system is the result of years of research and development to address ease of use, thorough protection, performance, scalability and high availability concerns. In addition, it must be extremely flexible to cope with various deployment preferences. Some customers prefer centralized approach for easy management and support, while others prefer client-based distributed approach to minimize capital equipment investment, low TCO (total cost of ownership) and scalability. Understanding such diversified demands, i-Guard Enterprise offers three customized editions designed for three different deployment plans as described below.

Gateway Deployment (IE Gateway Edition)

In this deployment configuration, i-Guard Enterprise Gateway Edition is deployed at network access point behind a firewall but in front of the local mail server. Inbound and outbound messages travel through i-Guard Enterprise for security processing and then moved on to destination once qualified. Messages subject to quarantine are stored on i-Guard Enterprise for audit by the local sender or recipient using web-based ECM application. Local spam and virus reported by the users or auto-detection mechanism will be automatically or manually reported to i-Guard service center for analysis. i-Guard Enterprise periodically communicates with i-Guard central service system to receive updates of new spam and virus identities.



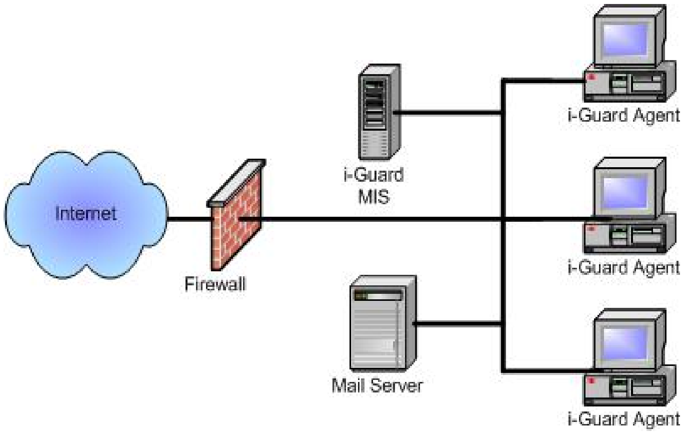
Gateway deployment plan is suitable to organizations with in-house expertise and having the desire to control email traffic and storage for privacy and confidentiality concerns.

Distributed Client Deployment (IE Client Edition)

In this deployment configuration, an i-Guard agent will be installed on every local user system. The agent performs all CPU-intensive message processing tasks and maintains its own copy of spam/virus identity database and personal black/white lists. It communicates with i-Guard Enterprise Client Edition for the purposes of reporting unknown spam and virus and receiving periodic updates of the spam/virus identity database. Report of spam and virus messages are either automatically or manually published to the local spam/virus identity database on i-Guard

Enterprise system for sharing among local users. In addition, i-Guard Enterprise also periodically receives updates of new known attacks from i-Guard central service center and makes them available for update to all local i-Guard agents. The administrator can establish a central security policy and disallow users from altering the pre-set central policy.

Among all deployment plans, this plan is the most attractive deployment plan in terms of low TCO and scalability. However, many service providers have shied away this deployment plan due to expensive agent software development and unpredictable support costs. Large ISPs such as AOL and SBC use this deployment plan to serve their huge customer base.



Managed Service Deployment (IE ISP Edition)

Originally designed as a service delivery platform for ISP market, i-Guard Enterprise offers a complete management solution for ISP to launch i-Guard managed-service serving own customer base. In this deployment plan, i-Guard Enterprise ISP Edition will be deployed on ISP premise which consists of a cluster of i-Guard message filter engines and a management system.

Using an intuitive web-based customer management system, the service provider signs up individual or group (business customer) accounts. For each group account, i-Guard Enterprise management system automatically creates a virtual message control (or i-Guard, for short) engine of which operating parameters can be tailored to specific customer's needs, either by the service provider or by the customer. Using a web-based administrative console, a group account administrator can:

☑ Setup operating parameters,

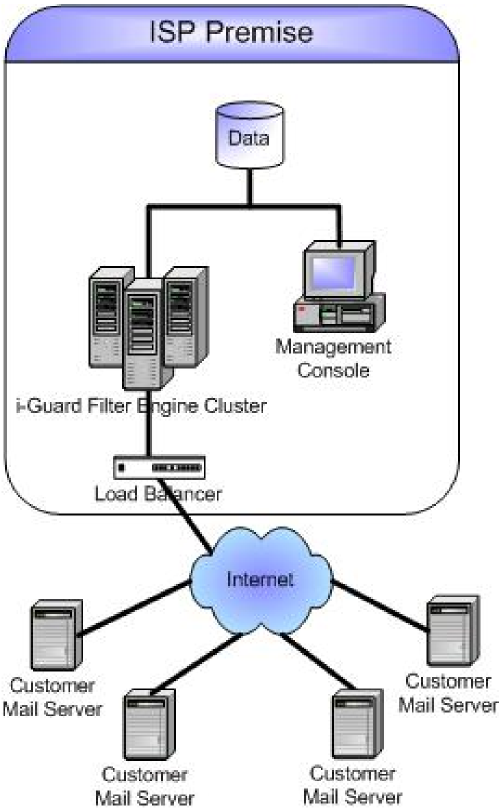
☑ Manage per-user personal security profiles,

☑ Establish a central message security policy,

☑ Configure one or more mail servers subject to message security control and

☑ View corporate-wide/per-user message traffic report.

As such, virtual i-Guard customers can be managed very much the same way as virtual web hosting that most ISPs and web hosting service providers are already familiar with.



Message to or from the customer's mail server are redirected to designated virtual filter engine for processing before forwarding to destination if qualified. Quarantine messages will be stored on the customer's virtual machine for audit either by the customer's administrator or by the users using the user-friendly web-based ECM application. Furthermore, to remove the customer from the burden of user management task, i-Guard Enterprise comes with an innovative auto-registration process that automatically sets up user accounts and associated message security policy as well as other management tools that allow the ISP to:

☑ Remotely monitor and manage the entire i-Guard Enterprise systems and services, including database management, message traffic report generation and trouble shooting

☑ Manage local spam/virus submission and alert events.

The key advantage of this deployment plan is that, from the service provider's perspective, it helps to:

☑ Centralize management and control to control the cost of customer support

☑ Allow many customers to share a hardware system to minimize capital equipment investment and maximize profit margin and

☑ Be able to serve customers with diversified computing environment.

Conclusion

As a result of several years of research and development, i-Guard Enterprise is the most powerful email security solution that offers many user benefits including: comprehensive and highly effective security protection, high performance, great deployment flexibility, ease of use and management and lowest TCO.

Thorough Protection

i-Guard Enterprise effectively protects its users against all email pitfalls such as spam, virus, fraud, scam and phishing through a pro-active message traffic monitoring and detection mechanism for dealing with unknown spam and virus attacks, a comprehensive multi-layer message screening technology and a deep attachment virus scanner, a safe message delivery policy and an aggressive community-based alert management system facilitating quick alert on on-going attacks. Furthermore, email privacy and confidentiality are protected through i-Guard SecureMail technology.

Performance

Careful engineering design in combination with intelligent processing heuristics helps i-Guard system to optimize overhead and maximize performance. As a result, i-Guard message control engine can operate reliably under high receive load from MTAs, while maintaining a high message throughput at the same time. Below is some performance data taken from our laboratories:

PERFORMANCE DATA

Message Size		Messages / Second
Body	**Attachment**	
1K (Text / HTML)	**None**	118 / 92
5K (Text / HTML)	**None**	85 / 73
10K (Text / HTML)	**None**	80 / 69
1K (Text)	**10K (Text / Zip)**	70 / 79

Server: i-Guard Enterprise Email Control Gateway (ECG)
Operating System: Redhat Linux 9.0
CPU: Pentinum 4 2.4 GHz (no hyper-threading)
Memory: 512MB
Hard Drive: Seagate 40GB
Network Card: 100Mbps
Load: 20,000 messages at the arrival rate of 667 msgs/s
Method of Measurement: message arrival rate
Performance Note: The same test was conducted on other systems with varying CPU speeds indicating that the message processing performance is linearly increased or decreased with faster or slower performance system, respectively.

For service providers, such performance characteristics mean each server can provide support for more customers or fewer servers to invest, resulting either higher profit margin or lower acquisition and operational costs.

Flexibility

Designed with high modularity, i-Guard Enterprise is a collection of several system components such as filter engine, system management system, database management system, etc. Such modularity allows the user to have great flexibility in managing i-Guard Enterprise deployment for meeting performance, manageability and cost-effectiveness requirements. For example, i-Guard Enterprise system components can be either centrally installed on a high performance server for centralized management or separately installed on multiple commodity less-powerful PC systems for distributed processing deployment. Moreover, the availability of i-Guard Enterprise on both Windows and Linux operating systems as well as the support for various deployment plans give the administrator even greater flexibility to provide support for a diversified operating environment in a large enterprise.

Ease of Use and Management

Recognizing that the management of large volume of email messages is a highly time consuming task, i-Guard Enterprise is highly automated so that time can be productively spent on business and security management tasks rather than on time-consuming system and message management tasks. Using i-Guard Enterprise management system, the administrator can easily manage i-Guard system components and monitor their status, manage database, review alert events and take actions. Often, these tasks can be done with a few mouse clicks.

Cost Effectiveness

i-Guard Enterprise is designed for both small and large enterprises as well as service providers. Therefore, cost effectiveness is one of the key design criteria and is reflected in i-Guard Enterprise system architecture. For example, the distributed message store design allows i-Guard Enterprise to achieve high availability, avoid single point of failure and good message retrieval response time without the need for an expensive back-end SAN system as a centralized quarantine message store.

Furthermore, for service providers, i-Guard Enterprise virtual i-Guard engine helps to minimize capital equipment investment and maximize profit margin.

REFERENCES

1. Report: Rise in virus attacks cost firms dearly (http://news.com.com/Report%3A+Rise+in+virus+attacks+costs+firms+dearly/2100-7349_3-5176420.html)

2. The privacy of your Email is not protected by law (Gartner, research ID No.: FT-23-3793)

3. Customer squeeze, as ISPs close in on virus (http://news.com.com/Customers+squeezed%2C+as+ISPs+close+in+on+viruses/2100-1038_3-5174061.html)

FILTER TECHNOLOGY COMPARISON

METHOD	Objects Filtered	Catch Rate	Training Required	Require Database Update	Message Throughput	Fooled by Cloaking	Others
Keyword Filter	Spam	80% - 90%	No	Yes	Low	Yes	Not scalable due to unpredictable CPU-intensive processing
Intention-based Filtering	Spam	90% - 95%	Yes	No	Low	Yes	Not scalable due to unpredictable CPU-intensive processing
Bayesian Filter	Spam	90% - 95%	Yes	No	Low	Yes	Not scalable due to unpredictable CPU-intensive processing
Challenge and Response	Spam	~100%	No	No	High	No	• Cause loss of unconfirmed messages and message delivery delay (wait for confirmation from sender). • No protection against spam and email-borne virus launched from an infected buddy system. • Fooled by a message sent by a virus from a buddy system.
Signature or Finger-print or DNA	Spam & Virus	90% - 95%	No	Yes	Med	Yes	No protection against unknown spam and virus and messages with objectionable content.
SmartScreen	Spam & Virus	~100%	No	Optional Required only when early alert service is desired	Med-to-High	No	SmartScreen shares many advantages as those of C&R. However, it eliminates all drawbacks associated with C&R and offers more thorough protection. For example, it is capable of: • dealing with known and unknown email-borne virus. • detecting spam or email-borne virus launched from an infected friendly system.

EMAIL ENCRYPTION TECHNOLOGY COMPARISON

FEATURES	SecureMail	PGP	SSL
Encryption Technology	Dynamic, Single Key	Static, Two-key	Dynamic, Single Key
Identity Verification	Sender and Recipient	Sender and Recipient	Sender and Recipient
Encryption Key Management	Simple user's registration	Time-consuming self-management	Complicated security certificate setup
Encryption Performance	Single-key - Good	Two-key - Slow	Good
Security Configuration	End-to-End Gateway-to-Gateway	End-to-End Gateway-to-Gateway	Gateway-to-Gateway
Security Protection	On transit and storage along the delivery path	On transit and on storage along the delivery path	Only on transit between end-user's system and mail server

KEY FEATURES

Spam/Phishing Protection

- Message Header Analysis
- Message Content Analysis / Identification
  - Categorized and Scored Keyword/Phrase/URL List
  - Dynamically-generated Known Spam Database
- Permission-based Heuristics
  - Personal White List
  - System-wide Buddy/Black List
  - Sender's Identity Validation
- Adaptive (self-learning) heuristics

Virus Protection

- Message Content Analysis / Identification
  - Categorized and Scored Keyword/Phrase/URL List
  - Known Email-borne Virus Database
  - Secure messages with dangerous contents (attachments, images, scripts, …)
- 3rd party virus scanner with deep compressed archive scanning (RAR v2.0, Zip, Gzip, Bz2, Tar, MS OLE2, Cab, CHM & SZDD)

Spam Prevention

- Sender Authentication
- Relay Control
  - Allow / Deny message relay
  - Allow / Deny relay from specific hosts and/or networks

Auto-Detection - Early Alert and Containment

- Auto-detection
  - Unknown Spam/Virus
  - 100% catch rate in most cases
- Alert Targets
  - Administrative Console
  - Specified Email Address(es)
  - i-Guard Early Alert Network (IEAN)
- Contain/Release messages associated with pending alerts
- Dynamic Rule Generation
  - Temporary or Permanent Message-blocking rules
  - Temporary or Permanent Sender-blocking rules

Quarantine Message Management

- Never drop any user's messages
- Personalized / system-wide message handlers
  - Redirect
  - Label and Forward
  - Delete
  - Bounce-back
  - Quarantine
- Messages are optimally stored for quick retrieval
- Per-user storage quota with auto-cleanup

Corporate Email Policy Compliance

- Block outbound messages with
  - Over-size
  - Obscene language
  - Matched specified keywords
  - Controlled materials
  - Encrypted content
  - Black-listed destination (domain or email address)
- Append specified text to outbound messages

Email Encryption / Secure Document Delivery

- Security protection configuration
  - End-to-end (required i-Guard Enterprise Agent software)
  - Gateway-to-gateway
- Simple setup
- Highly-secure per-message dynamic encryption key
- Secure encryption algorithm (128- or 256-bit AES)

Comprehensive Web-based Administration GUI

- System / Service Manager
  - Configuration and setup
  - Automatic status monitor and display (in LED)
  - System / service control (Start/Stop)
  - Remote system restart
- Database Manager
  - Manage database (backup and restore)
  - Customize local keyword / phrase / URLs list
  - Setup organization-wide buddy/black list
- Alert Manager
  - Manage messages quarantined due to alerts
  - Establish blocking rules on specific clients (IP address) and messages
  - Release messages quarantined due to a false alert
- Log Manager
  - Setup system log configuration
  - Manage log files
  - View and search the content of log files
- Message Submission & Database Publication Manager
- Account Manager
  - Virtual Filter Engine Setup
  - User Management
  - Message Traffic Report Manager
- User Management
  - Automatic User Registration
  - Personal Black/White List
  - Personal Email Control and Handling Policy
  - Personal Spam Sensitivity Control
  - Personal Quarantine Message Store

Quarantine Message Manager

- User-friendly Web-based Explorer-like GUI
- Allow user to view and manage personal quarantine messages
- Allow user to setup remote mailbox(es) for secure retrieval
- Support multiple remote mailboxes per user
- Support multiple local mailboxes per user

i-Guard Desktop Agent – for distributed processing

- Buddy list synchronization
- End-to-end encryption security
- Client-based encryption and compression
- Alert user on quarantine messages

Other Key Features

- High-availability configuration available
- Hot plug-in scalability
- Per-day throughput : ~7 million messages on Pentinum 2.4GHz (assuming an average message contains 10K of text data)
- Optional database update
- Temporary spool for inbound messages
- Support multiple mail servers on the same or different sites
- Support multiple mail domains per mail server
- Email address harvest attack protection
- Message traffic analysis and report
- Email DOS prevention

Compatibility

- Microsoft Exchange 2000 / 2003
- Oracle Mail Server
- Lotus Domino Server
- Novell GroupWise
- Sendmail
- Any SMTP/POP3 mail servers

Operating System

- Windows NT/2000/XP (Professional or Server)
- Linux