

## **RassaiMail™** – Premium Web Mail Hosting Service

### **On-Demand Email Hosting**

- No software to install
- No hardware to manage
- No upgrades or patches to download
- 99.99% uptime guarantee

### **Secure Webmail Access**

- Anytime, anywhere access to email
- SSL-encryption for additional security

### **Large Mailboxes**

- 100MB or 1GB (1,024MB) mailboxes
- Storage is upgradeable per user, sold in 500MB blocks (max 2,047MB/user)

### **SSL-encrypted POP3 & IMAP4 email access**

- POP3, IMAP & SMTP access
- Compatible with Outlook, Thunderbird and others

### **Dual Scanning Virus Protection**

- Unique three-stage, dual virus scanning process for extra protection
- Prevents customers from sending and receiving computer viruses and threatening attachments

### **Spam Filtering**

- Utilizes thousands of constantly evolving tests
- Results combined using a methodical weighting system for maximum accuracy
- Safe listing capabilities to prevent false positives
- Exclusive lists allow customers to reject email from all random email addresses

### **SMTP Authentication, Clean Mail Servers**

- SMTP authentication is required for all sent emails
- Strict anti-spam policy is enforced to maintain network integrity

### **Large attachment size limits**

- Incoming and outgoing message size limits are set to 35 MB
- This allows a 25 MB file to be attached (MIME encoding adds 33% to size)

### **Secure control panel**

- Accessible at all times via the Web
- Add and delete mailboxes and aliases
- Change passwords
- Allocate storage space
- Download statistics
- Adjust Spam filtering settings
- Update account information

### **Unlimited email address aliases (domain-based email only)**

→ Ability to create as many email address aliases as needed, each of which can forward to a total of 50 email accounts. Up to four of those recipients can be sent to external email accounts.

→ For example, sales-1@example.com can forward emails to 46 employees and four of suppliers working for a different company. Alternatively, sales-1@example.com could forward to 50 employees.

#### **Unlimited domain name aliases (domain-based email only)**

→ Ability to create as many domain name aliases as needed. Domain name aliases can be set up to point mail from a user at the alias domain to the email account where the domain alias points.

→ For example, mike@example.com can be set up to point to mike@yourexample.com. This allows customers to receive emails sent to multiple domains without having to set up email accounts at each.

#### **Other features include:**

- 24x7 system monitoring
- Email forwarding
- Personal address book
- External POP3 access
- Vacation auto responder
- Custom signatures
- Printer-friendly emails

#### **Upgradeable Features**

- Private label **RassaiMail™** site
- Bcc Archiving for data backup and monitoring

## **RassaiMail™ Features**

### **Preview Pane**

The preview pane allows users to quickly navigate their email messages, while always maintaining a view of the rest of the inbox. The preview pane can be turned on and off per user, depending on individual desires.

### **Conversation View**

When the conversation view is turned on, it makes it easy for email users to quickly view all emails that were part of conversation strings. For example, if two business associates trade 20 emails over a week's period of time and each time they "Reply" to the previous email, turning on the conversation view will group all 20 of those messages together, as long as all of those messages are stored in a single folder, such as the inbox. This can make for easier navigation of specific conversations between two or more email users and especially for users that subscribe to list serves.

### **Folders and Sub-Folders**

Users can now create an unlimited hierarchical folder structure. For example, they could create one folder that has to do with a high level topic and then several sub folders within that main folder. They can even create sub-folders within sub-folders for more meticulous organization of their email data.

### **Message Action Items**

(Flag for Follow Up, Remove Flag, Mark as Read, Mark as Unread, Export to Zip)

With message action items, users can now organize their messages more efficiently. For example, if a user reads an email and needs to reply later, the user can flag the message for follow up. The user would then be able to sort messages based on those that are flagged for follow up. This would help the user to recognize that there are action items they need to take at a later point in time.

### **Message Priority**

Message priority flags are now shown in the message listing. When a user receives an email marked as "urgent," an exclamation icon will appear to the left of message.

### **Purge Trash**

Added links to main menu for purging the Trash, Spam and Sent Mail folders. Purge links can be manually added or removed from all other folders.

### **HTML Editor**

The HTML editor allows email users to compose messages in HTML, using features such as "Bold," "Underline" and "Italicize." Users can also format the style of the page using different fonts and color pallets. HTML composing can be turned on and off per user, allowing users to choose when they want to send emails in HTML verses plain text.

### **Microsoft Rich Text Format**

Added support for viewing and responding to emails that were sent in Microsoft Rich Text format (MS-TNEF).

### **Frequent Contacts**

When email users add contacts to their address book, they can now designate certain contacts as "Frequent Contacts." Frequent contacts will then be displayed on the "Compose Mail" page making it very simple to add contacts to the "To," "Cc" or "Bcc" address fields when writing emails.

### **Address Auto-complete**

When typing an address into the "To," "Cc" or "Bcc" address fields on the "Compose Mail" page, Webmail will attempt to match partially typed names against the user's address book. If a match is found, the user will be able to press the Tab key and have the rest of the address automatically filled in.

### **Attachment Sizes**

The compose page now shows the size of attachments that have been uploaded. This helps users know how large an email is before they send it.

### **Enhanced Search**

Email users can now search for emails within specific folders, rather than all folders. They can also search specific fields (body, subject, from, to, cc), rather than always searching all fields.

### **Enhanced Filtering**

New filtering options have been added to help users better organize their incoming email. Emails can be copied to folders, rather than moved. Filtering matches can use improved matching logic to identify very specific emails. Mail can also be forwarded to alternate addresses, such as cell phones, if it contains certain content or is from specific people. The filtering occurs immediately when each email message is received.

### **Settings**

Many new user customizable settings have been added to enhance the use of **RassaiMail™**. Settings include display options, folder list options, message formats, external mail delivery options, and more.

### **RSS Feeds in Your Inbox**

The **RassaiMail™** RSS reader allows email users to manage their favorite blogs and RSS feeds alongside their email. Users can view their feeds using **RassaiMail™**, or their desktop or wireless email client, like Microsoft Outlook or Thunderbird.

### **No Software to Install**

The RSS reader integrates seamlessly into the **RassaiMail™** email hosting platform—there's no software to install.

### **Works Just Like Email**

With the RSS reader, users can work with feeds the same way they work with email. Feeds will arrive in their Inbox, where they can then flag or file the feed, or forward it as an email message. Because it works just like email, it is easy to use—even for users who are unfamiliar with RSS technology.

### **Administrative Controls**

The RSS reader includes administrative-level features that allow email administrators to control how employees use the reader. Administrators can automatically subscribe users to specific feeds, and permit or restrict the users' ability to subscribe to feeds of their choice.



### Support for POP and IMAP

In the RSS reader, a user's feeds will be stored in the My Feeds folder. Users can also organize their feeds into folders that they create (e.g., Business Blogs, General Interest).

If your users use IMAP with their desktop or wireless email client, they can view their feeds as they arrive in their feed's folder. Or, if they use POP, their feeds can be automatically redirected into their Inbox. This makes it possible for users to view their feeds from virtually any location, using any email client.

### Subscribing and Unsubscribing

A significant benefit of RSS is the ability for users to subscribe to feeds they like—and unsubscribe from ones that no longer meets their needs. Because no personal information is required to subscribe to a feed, users can control the flow of information. With the **RassaiMail™** RSS reader, users can unsubscribe from a feed the same way they delete a folder—it's that easy.

## Spam Filtering

The **RassaiMail™** spam filtering system blocks more than 98% of email spam and directory harvest attacks. Accurate spam filtering is accomplished by evolving spam defenses on a daily basis as well as enhancing email administrator and end user customization options.

### Spam DNA and Weighted Tests

- Filters more than 98% of spam; filters are updated hourly
- Thousands of email characteristics ("DNA") are used to identify spam
- 25 third-party spam databases, several DNS checks, and message-formatting tests are also used when analyzing each email
- DNA and other data are used to perform more than 45 tests on every email
- Tests are combined into a weighting system and assigned a value
- When the total weight of an email is greater than a certain sensitivity threshold it will be flagged as Spam
- Integrates with Habeas and Bonded Sender to minimize false-positives

### Administrator and User Controls

- Sensitivity can be customized by administrators and end users
- There are several options for handling email once it is flagged as spam
- Safe lists allow users to accept email from blocked senders
- Exclusive setting allows users to block email from outside their safe list

## Spam Filtering: Spam Epidemic

### A Growing Problem

**RassaiMail™** estimates that as much as 85% of all email traffic on the Internet is spam. Spam is one of the fastest growing, most complex problems facing the Internet today. The problem has already led to millions of dollars in lost productivity and additional infrastructure costs for corporations and small businesses.

Businesses who maintain in-house email servers are fighting a losing battle to protect their systems from this epidemic because complexity of the problem is constantly evolving. Spammers are growing wiser on a daily basis, learning new methods to manipulate common Spam defenses and obtaining more sophisticated software to penetrate email in-boxes.

### Solving the Problem

The **RassaiMail™** spam filtering system accomplishes this by gathering real-time spam intelligence from a number of sources, and then actively using this intelligence to block unsolicited email. **RassaiMail™** tracks tens of thousands of live Spam email characteristics ("DNA"), which alone identify the majority of Spam. In addition, approximately 25 third-party Spam databases, several DNS checks, and several message-formatting tests are used when analyzing each email.

**RassaiMail™** incorporates this data into thousands of constantly evolving tests that are performed on every email that enters the hosted email environment. The results of these tests are combined using a methodical weighting system that successfully identifies over 95% of Spam with virtually zero false-positives.

### Weighted Tests

There are two important factors to consider when dealing with spam:



- No single test can identify all spam
- Some tests will falsely identify legitimate email as spam

Therefore, **RassaiMail™** allows no single test to cause an email to be flagged as spam. Instead, multiple tests are used in conjunction via a weighting system, where each test is assigned a point value. When an individual test fails, that point value is added to the overall weight. If the total weight of the email is greater than a certain threshold, the email is flagged as spam. Depending on the spam filtering sensitivity level set by each customer, it will take between two and five tests for the email to fail and be flagged as Spam. Point values also depend on the severity of each test.

## Spam Filtering: About Spammers

### Spam DNA

**RassaiMail™** collects tens of thousands of spam samples through the use of dummy mailboxes ("Spam traps") as well as data submitted by customers. Spam messages are then broken down into identifiable components, which are used to develop spam DNA. Spam DNA is similar to anti-virus "fingerprints", and can accurately identify most Spam based on specific content that would only be found in certain emails.

Advanced pattern recognition technology allows **RassaiMail™** to simultaneously apply thousands of heuristic algorithms to each email in search of parts of the email that are identifiable by the Spam DNA. When a match is found, the email fails this heavily weighted Spam test.

### Open Relays and Known Spam Sources

Open relays are the most common source of spam. These are improperly configured mail servers that allow outbound mail to be sent by just about anybody. Spammers use automated tools to search the Internet for vulnerable servers, and then hijack these servers to increase the amount of Spam they can send.

To combat this problem, there are several third-party organizations that maintain active databases that "blacklist" open relays. Databases also exist that blacklist other known spam sources such as proxies, insecure web forms, and dial-up IP addresses.

**RassaiMail™** tests each email against approximately 25 of these well-known blacklist databases, including those from Osirusoft, SpamCop, SpamHaus and "Not Just Another Black List" (NJABL). These databases are updated multiple times every day. Each blacklist test that an email fails adds an additional weight value to the email.

### DNS and RFC Violations

Spammers tend to be careless in how they send email. Therefore it is important to scrutinize each inbound email to see if it followed all of the rules defined by current RFC's. The following tests examine the mail server that delivered the email as well as the domain name used in the sender's return address:

- Did the mail server falsely identify itself in the "HELO/EHLO" data?
- Is the mail server missing its reverse DNS record?
- Is the domain missing "A" and "MX" DNS records or using illegitimate values?
- Is the domain missing "postmaster" and/or "abuse" addresses?
- Does the domain not accept delivery status notifications?
- Was the email sent from a mail server that is not authorized to send mail using the sender's domain name? (Such as @yahoo.com email sent from an Earthlink mail server)

The email message headers are also examined:

- Are message headers improperly formatted or missing required data?
- Are message headers in a format consistent with Spam?
- Is the return address in a format consistent with automated mailers?

Blocking based on any of these tests alone would block a large amount of legitimate email. However, when used in conjunction with a weighted filtering system, these tests are extremely effective.

### Elusive Spammers

Most Spammers are very aware of the filtering techniques used by top-tier email service providers such as **RassaiMail™**. This has led Spammers to develop creative tactics and advanced software in an attempt to bypass filtering systems.

For instance, many Spammers now use binary encoding to hide their text and HTML email from signature-based filters. **RassaiMail™** uses pre-processors to decode binary MIME segments, rendering this trick useless against the Spam DNA filters. Additionally, it is common for Spam to include invisible HTML code in an attempt to circumvent content filters. This tactic is also useless against the **RassaiMail™** spam filtering system. Since there is no legitimate reason why an email would contain such formatting styles other than to bypass Spam filters, the Spam DNA filters add weighting to emails that use various forms of trickery to obscure the email content.

Aggressive Spammers are also engaged in "Polymorphic Spam Attacks". These are attacks where many copies of the same email are sent, but with each email containing subtle differences in punctuation, spacing or wording designed to circumvent content filters. The Spam DNA Filtering® technology is designed to recognize similar pieces of content in these email mutations and flag them as Spam.

Spam is often times sent through several different mail servers before arriving at its final destination. This is done to disguise the original source of the email in an attempt to evade Spam blacklists. However, unlike most filtering systems, **RassaiMail™** traces the email back to its origin and scans each hop along the way. If any server that the email was routed through fails a blacklist or DNS test, additional weighting is added to that email.

### **Geographical Routing**

The geographical routing test analyzes the Internet route that an email travels, and searches for highly inefficient routing that is very common in Spam. For example, an email might fail this test if it is sent from an account in the U.S. to another account in the U.S., but is routed through a mail server in Korea.

A second geographical test uses Spam statistics to identify countries that have a high probability of sending Spam. If an email travels through one of these countries, a variable weight is added to the email based on the country's current Spam rate.

## **Spam Filtering: Weighted Tests**

### **Combining the Tests**

After rigorous testing, a final weighting is assigned to each email. A threshold is then used to determine if the email should be identified as spam. If the email weighting is lower-than the threshold, the email is deemed to be spam-free and is delivered unmodified. However, if the email's weighting is equal-to or greater-than the threshold, the email is identified as Spam and the appropriate action is taken.

Every email domain administrator using the spam filtering system can control the sensitivity used to determine if an email is spam, and can override that sensitivity for individual users. A high sensitivity causes a low threshold to be used and catches almost all spam. A low sensitivity causes a higher threshold to be used, and catches only the most obvious spam. Advanced false-positive prevention makes high sensitivity the optimal setting for most companies.

### **What To Do With Spam**

Once a spam email has been identified, there are several actions that can be taken. The following actions are available to every email domain administrator. These can also be overridden for specific users:

- Delete the email immediately. This is usually not advised, just in case a legitimate email is falsely identified as spam.
- Deliver to a spam folder. This will allow each user to review their spam in their own webmail folder. Emails inside this folder can be automatically deleted after a specified number of days or total emails.
- Deliver to an alternate email address. This is useful if a company wants to have a single administrator review all of the spam that their users receive.
- Add text to the beginning of the subject. This will allow each user to set up custom filtering rules inside of desktop email software clients such as Microsoft Outlook.

When the "Deliver to a spam folder" action is used, an additional feature becomes available. Automated spam folder cleanup can be scheduled in order to delete old spam from spam folders. The domain administrator can specify how many days to keep Spam in webmail folders, or how many total spam emails to keep before old emails are deleted. Each user can choose to use the domain's default setting or they can specify their own cleanup option.

## Spam Filtering: False Positives

### False Positive Prevention

Every effort is made to ensure that legitimate emails are not falsely identified as spam ("false-positives"). To prevent this, several filtering tests have been incorporated which are designed with the reverse approach of identifying characteristics found in legitimate email instead of identifying spam. These tests work in conjunction with the weighting system to help eliminate false-positives. Specific details of these tests cannot be provided, in order to keep this information out of the hands of spammers.

Every email domain administrator using the spam filtering system can control the sensitivity used to determine if an email is spam, and can override that sensitivity for individual users. A high sensitivity causes a low threshold to be used and catches almost all spam. A low sensitivity causes a higher threshold to be used, and catches only the most obvious spam. Advanced false-positive prevention makes high sensitivity the optimal setting for most companies.

Additional false-positive protection is also acquired from two third party tests that have been bundled into the spam filtering system. The Bonded Sender Program and the Habeas SENDER WARRANTED EMAIL (SWE) system have been fully integrated and are described in dedicated sections below.

If a legitimate email still ends up being falsely identified as spam, a final layer of false-positive prevention can be used. Safe Lists allow domain administrators and email users to specify email addresses and domains that should always bypass the filtering system. Further information on Safe Lists is provided in a dedicated section below.

### Bonded Sender

**RassaiMail™** has integrated the IronPort Bonded Sender™ Program into its spam filtering system. The Bonded Sender Program is aimed at eliminating the possibility of legitimate emails being flagged as spam by anti-Spam filtering systems. Bonded Sender ensures the integrity of email campaigns by requiring originators of legitimate email to adhere to email standards, undergo a qualification process and post a financial bond. With the guarantee of legitimacy, participating ISPs and corporations allow Bonded Sender email to circumvent spam filters. Email recipients who feel they have received an unsolicited email from a Bonded Sender can complain to **RassaiMail™**, their ISP, or IronPort. TRUSTe, the leader in Internet privacy certification, manages the complaints, which, if supported, result in charges against a sender's bond and potentially expulsion from the Bonded Sender program.

### Habeas SENDER WARRANTED EMAIL (SWE)

**RassaiMail™** has integrated technology from Habeas ([www.habeas.com](http://www.habeas.com)) to help ensure that legitimate email is not falsely identified as Spam. Habeas has created an enforcement system called SENDER WARRANTED EMAIL (SWE) that enables individuals and companies to warrant that the email they are sending is not Spam. The SWESM technology is based on existing trademark and copyright laws, which allows Habeas to obtain enforceable injunctions and judgments against spammers through the Courts.

What this means is that any email sent under the Habeas system is warranted (guaranteed) not to be spam and meets the exacting standards for a HABEAS COMPLIANT MESSAGE. Habeas has some of the strictest standards in the industry, including only permitting mailing lists that are verified opt-in. When a Habeas SENDER WARRANTED EMAIL arrives to the **RassaiMail™** system, it is delivered to the recipient with confidence that the email is legitimate.

## Spam Filtering: Filtering Options

### Safe Lists

While every effort is made to ensure that legitimate emails are not identified as spam, a small number of false positives are unavoidable. To solve this problem, domain administrators and email users can specify trusted email addresses that should always bypass the filtering system. This feature should be used when specific emails sometimes gets identified as spam, such as opt-in newsletters or emails from colleagues whose mail servers are blacklisted or miss-configured.



### **Exclusive Filtering**

For customers desiring maximum spam protection, the Exclusive filtering level can be used to block email from all email addresses not appearing on the Safe List (described above). This will cause email from all unknown senders to be flagged as spam and will allow the appropriate action to be taken.

### **Individual User Flexibility**

Email domain administrators define the default Spam filtering settings for email users. Users then have the option to customize their spam filtering level via their webmail account options panel, setting their protection level to High, Low, or Exclusive. Each user is also able to decide how they want their Spam handled. They can elect to use the default setting defined by the domain administrator, or they can change it to any of the seven options described in the "What To Do With Spam" section above. In addition, users are also given control of their own Safe List, which works in conjunction with the domain-wide Safe List. All user-level controls are also configurable by the domain administrator via the control panel.

### **Network-level Spam Security**

The **RassaiMail™** carrier-grade email network is guarded against intrusion at its border firewalls and is monitored 24x7 by Tier 1 Engineers. Global filtering rules block traffic from the most abusive Spam and virus sources on the Internet. A special protocol-level firewall was built by **RassaiMail™** to monitor SMTP, POP3 and IMAP4 usage patterns and provide real-time blocking of malicious traffic. This provides highly effective protection against Directory Harvest Attacks (also known as Dictionary Attacks), which greatly reduces the chances of customer email addresses ending up on bulk mailing lists. In addition, this security layer protects customers from mail bombs, mail loops, brute-force password hacks, buffer-overflows, and other malicious attacks.

### **Abuse and Blacklist Monitoring**

Great effort is taken to keep abusive users off of the **RassaiMail™** system and to keep the **RassaiMail™** system off of the anti-Spam blacklists. Acceptable Use Policy compliance is strongly enforced in order to maintain the integrity of the email service for the benefit of all customers. Spikes in outgoing email usage, or heavy outgoing spam filtering failures send real-time alerts to engineers in order to diagnose and stop abuse. **RassaiMail™** mail server IP addresses are constantly cross-listed against all known anti-spam blacklists in order to ensure that no mail server is ever blacklisted. If one is blacklisted, this will ensure that the proper action is taken to immediately remove the mail server from the blacklist.

## **Spam Filtering: Dictionary Attacks**

### **Network-level Spam Security**

The **RassaiMail™** carrier-grade email network is guarded against intrusion at its border firewalls and is monitored 24x7 by Tier 1 Engineers. Global filtering rules block traffic from the most abusive spam and virus sources on the Internet. A special protocol-level firewall was built by **RassaiMail™** to monitor SMTP, POP3 and IMAP4 usage patterns and provide real-time blocking of malicious traffic. This provides highly effective protection against Directory Harvest Attacks (also known as Dictionary Attacks), which greatly reduces the chances of customer email addresses ending up on bulk mailing lists. In addition, this security layer protects customers from mail bombs, mail loops, brute-force password hacks, buffer-overflows, and other malicious attacks.

## **Virus Scanning**

### **Dual Scanning Virus Protection**

The **RassaiMail™** virus scanning solution scans all inbound and outbound emails using a unique three-stage, dual scanner process.

#### Stage 1: Restricted Attachments

The first level of protection prevents the sending of certain types of attachments, which could contain dangerous code and are often used by malicious hackers to spread viruses. These files either contain executable code themselves or may contain links to other files that contain executable code. Restricted file types include, but are not limited to program files (.exe, .com), script modules and files (.bas, .vbs, .js), Internet links (.url, .ins), and shortcuts to files (.lnk, .pif).

When an email is sent that contains a restricted file attachment, the sender receives a rejection notice informing them of the restriction.



### Stage 2: The Dual Virus Scan

Any portion of an email that has the possibility to contain a virus is scanned during Stage 2. This includes almost every type of file attachment as well as HTML messages and embedded scripts. Redundant, industry leading virus scanners are put to use, rooting out malicious worms, Trojan horses, and macros before they have a chance to do any harm.

Each portion of an email is passed through two, independent virus scanners to ensure maximum protection against new email born viruses. Clam AntiVirus ([clamav.net](http://clamav.net)) and F-Prot ([frisk-software.com](http://frisk-software.com)) are the current scanners of choice. Both companies maintain 24-hour dedicated virus researchers who respond to new and emerging threats, doubling the chances of blocking new virus outbreaks. Updated virus definitions are automatically pushed to the email system by the two vendors immediately as they are released.

The **RassaiMail™** system was built from the ground up with the ability to "plug-in" virtually any virus scanner on the market. This protects Stage 2 of the **RassaiMail™** system from depending on any one company, and allows for seamless upgrades to the latest "best-of-breed" virus protection as the market evolves.

If a virus is found, the email is quarantined and the sender is notified (see Virus Notifications).

### Stage 3: The Pre-scan

The third stage serves two functions. First, it searches for email vulnerabilities. It then searches for MIME segments that have the potential to carry a virus.

By searching for email vulnerabilities, the scanner is able to block emails that are dangerously formatted and which could execute code without user intervention. This includes protection against all known Microsoft Outlook security threats such as MIME headers exploits, fragmented message segments and file extension obscuring. This most notably provides protection against worm viruses that can replicate themselves by using the Microsoft Outlook address book.

If vulnerabilities are found, the email is quarantined and the sender is notified (see Virus Notifications).

The system then checks for any portion of the email that could possibly contain a virus. If all MIME segments are guaranteed to be safe, then scanning stops at Stage 1. However, if any MIME segment is found that is not guaranteed to be safe, the email continues to Stage 2. This eliminates unnecessary scanning of plain-text emails and safe attachments such as images, keeping email delivery ultra-efficient without compromising email security.

### **Virus Notifications**

When a virus or email vulnerability is found, the email is quarantined within the network. Since viruses forge the sender address on the email, the sender is only notified if the virus was sent by one of our users using Webmail or SMTP Authentication. This protects innocent people from receiving erroneous bounce messages when the virus uses their forged email address in the message's "From" field.

### **Zero Added Points of Failure**

Redundancy and fail-over support are built into every aspect of the **RassaiMail™** system. Should any portion of this three-stage process fail, safeguards are in place to ensure that the remaining stages execute and email traffic continues without interruption.

### **Effectiveness**

**Thousands of virus-infected emails arrive at the RassaiMail™ system each day. To date, not a single infected email is known to have made it through successfully. Even newborn viruses that have not yet been added to the virus definitions are stopped at the door.**

## Security

Network security vulnerabilities pose multi-billion dollar threats to corporations. **RassaiMail™**, in partnership with Rackspace Managed Hosting, protects you with the industry's most potent security tools and techniques that are designed, built and maintained specifically for enterprise-class Web operations.

### Infrastructure

Security starts at the data center and includes physical locks, access controls and biometric surveillance systems. Robust fire suppression, HVAC, power feeds, hot-swappable servers and routers are available in the event of an outage. Background checks and certifications ensure the integrity of all personnel.

### Network

The **RassaiMail™** network is 100% Cisco Powered, built on hardened routers and audited by Cisco. This ensures maximum-security protection at every level. The **RassaiMail™** network incorporates a Rackspace-patented Intrusion Detection System to protect against external threats.

Firewalls are managed by security specialists and deployed in a "private IP" space, which isolates the **RassaiMail™** network from outside threats. Network security features also include multi-level privileges, OS lockdowns, centralized authentication and device change logs.

### Hardware

The **RassaiMail™** OS is loaded, hardened and aggressively patched to ensure proper security. By maintaining on-site hardware inventories, laboratories and automated deployment systems, in addition to close relationships with key hardware vendors, Rackspace is able to guarantee **RassaiMail™** hardware availability and smooth scaling.

### Applications

Rackspace monitors the availability of **RassaiMail™** hardware and network services 24 hours a day. **RassaiMail™** engineers monitor the operation of the OS, critical applications and other data points via a centralized monitoring environment. **RassaiMail™** engineers are immediately alerted to potential problems and have tools at their disposal to diagnose problems on individual servers in real time.

### Security Patching

By constantly updating security systems, Rackspace ensures optimum protection for our customers. They monitor and address emerging threats, and quickly process and apply new security patches.

### Threat Analysis

Rackspace employs advanced technologies to identify and address security weaknesses in servers, applications and network activities. They constantly examine all firewalls, load-balancers, SSL accelerators and switches, as well as external developments, for any potential security events.

### Forensics

Should a security event occur, **RassaiMail™** can conduct a comprehensive post-incident examination designed to reduce the risk of future threats. By documenting dollar losses, if any, **RassaiMail™** can help justify the involvement of the FBI or other law enforcement agencies.

### Security Testing Laboratory

Rackspace subjects all devices to full security testing before they are deployed — including the installation and configuration of the Operating System, the disabling of vulnerable or unneeded services, and advanced vulnerability tests.

## Abuse Monitoring

### Maintaining Email Network Integrity

Blacklist Protection Through Abuse Prevention

Preventing internal email system abuse is often an overlooked component of a successful email hosting system. Preventing internal email abuse helps to maintain the integrity of the network where the email platform is hosted, regardless of whether

that system is maintained in-house or managed by a third party provider. With the amount of Spam being sent through email today, maintaining network integrity is as important as ever, and as challenging. Businesses and service providers that do not prevent internal email system abuse run the risk of outbound emails ending up in junk mail folders across the Internet.

#### Blacklist Protection

Several organizations have formed over the past few years to combat the growing Spam epidemic. Many of these organizations publish blacklists of mail servers that are known to send Spam. Blacklists are used by thousands of ISPs as part of their Spam defense. In an unprotected environment, an email system can easily find itself on one of these industry blacklists, resulting in mail delivery problems and immeasurable costs in lost business.

**RassaiMail™** has years of experience in this area and actively protects its customers from blacklisting. Many times blacklisting can occur simply as a result of an unknowing employee sending out a bulk email without realizing the potential consequences. In order to effectively protect the **RassaiMail™** network from abuse, **RassaiMail** identifies and prevents abnormally large amounts of email from being sent within a short time period from its hosted email system. The software identifies spikes in outbound mail rates and automatically delays potentially disastrous bulk mailings. Emails that enter the delay queue are delivered 10 minutes later if the next highest threshold is not reached. If the next highest threshold is reached, the delayed emails and all new emails are placed in a hold queue and administrators are alerted. **RassaiMail™** works with customers to jointly decide what action should be taken on the bulk mailing, while it sits in a hold queue.

This anti-abuse software prevents potentially detrimental bulk email from leaving the email system, violating anti-Spam laws and exposing it to blacklists maintained throughout the world.

#### Blacklist Detection and Removal

In the unlikely event that a mail server IP address becomes temporarily blacklisted, **RassaiMail™** has two methods to work around the issue while it is being resolved. First, **RassaiMail™** uses "fallback routing" to automatically redirect mail through alternate SMTP servers if delivery is not possible through the primary outgoing server cluster. Second, **RassaiMail™** maintains a pool of spare "clean" IP addresses within multiple Class C subnets. If blacklisting occurs, a quick firewall reconfiguration is all that is needed to reroute outgoing mail through a new set of IP addresses.

**RassaiMail™** performs a daily lookup of all mail server IP addresses in approximately 150 anti-Spam blacklists. **RassaiMail™** maintains up-to-date contact information for all blacklist providers. If blacklisting occurs, **RassaiMail™** is well prepared to reconcile the problem.

## Statistics

**RassaiMail™** provides customers with a multitude of statistics measuring activities pertaining to overall email system functionality. Statistics include:

- Domain, alias and user counts
- Login activity
- Daily POP3/IMAP4/SMTP usage
- Daily Webmail usage
- Number of emails scanned and viruses detected
- Number of emails scanned and filtered as spam
- The most frequent viruses
- The number of emails rejected due to a full mailbox

## Monitoring

In addition to the dedicated Network Operation Center (NOC) personnel who continuously monitor network and server health, displays are strategically placed throughout the Rackspace data center, allowing all employees to monitor "at-a-glance" status of critical systems.

In an effort to detect potential problems before they impact **RassaiMail™**, email hosting services, **RassaiMail™**, also monitors the status of the platform, including routine checks on hardware, processes and mail queues, using both automated and manual tools and testing procedures.

Monitoring includes:

- Overall service availability
- Mail server availability on all mail ports
- Disk space usage
- Database connectivity
- DNS availability
- Load balancing
- Network status

## Partners: Open Source



### Red Hat Enterprise Linux

[www.redhat.com](http://www.redhat.com)

Founded in 1993, Red Hat is the most recognized Linux brand in the world, serving global enterprises through technology and services made possible by the open source model. Red Hat's Enterprise Linux family of operating systems provides extreme stability, performance and scalability for mission-critical systems. The operating systems have a 12-18 month release cycle and are backed by seven years of technical support for every version.



### Postfix

[www.postfix.org](http://www.postfix.org)

Postfix was originally developed as an alternative to the widely-used Unix SMTP program called Sendmail. It has since become arguably the most powerful SMTP server on the planet. The software is developed and maintained by Wietse Venema, who along with the open source community, continue to build tremendous functionality and performance enhancements into the software.



### Courier-IMAP

[www.courier-mta.org](http://www.courier-mta.org)

Courier-IMAP is an open source server developed by Double Precision, Inc. to provide IMAP and POP3 access to Unix mailboxes stored in "Maildir" format. "Maildir" is a directory-based mail storage format originally introduced in the Qmail mail server, and adopted as an alternative mail storage format for Postfix. It is a faster and more efficient way to store mail.



INNOVATIVE WEB STRATEGIES



#### **SquirrelMail**

[www.squirrelmail.org](http://www.squirrelmail.org)

SquirrelMail is a standards-based webmail package written in PHP. It includes built-in pure PHP support for the IMAP and SMTP protocols, designed for maximum compatibility across browsers. The software is designed to be robust and extremely flexible, providing a plug-in API that allows organizations to add extended functionality. This open source project is lead by Rick Castello, and is the foundation for the **RassaiMail™** webmail platform.



#### **ClamAV**

[www.clamav.net](http://www.clamav.net)

ClamAV is an open source anti-virus toolkit for UNIX. The primary purpose of this software is mail server virus scanning. The package provides a fast and scalable multi-threaded daemon and a tool for automatic updating via Internet. The virus database is kept extremely up to date through the combined efforts of the organizations that use the software.



#### **SpamAssassin**

[spamassassin.apache.org](http://spamassassin.apache.org)

SpamAssassin is an engine for deploying a wide-spectrum of mail filtering tests that can identify spam. This open source software provides extreme flexibility through an API, allowing it to be used in a wide variety of email systems, including Postfix.

amavisd-new

#### **amavisd-new**

[www.ijs.si/software/amavisd/](http://www.ijs.si/software/amavisd/)

amavisd-new is a high-performance interface between mail servers (MTAs) and content checkers: virus scanners and SpamAssassin. Mark Martinec maintains this open source software, with contribution of ideas, patches and reports from the amavis-user mailing list community.



#### **OpenLDAP**

[www.openldap.org](http://www.openldap.org)

OpenLDAP is an open source implementation of the Lightweight Directory Access Protocol ("LDAP"). The software is actively developed by a worldwide community of volunteers whose collaborative efforts produce a robust, commercial-grade, fully featured, and open source LDAP suite of applications and development tools.



#### **Apache HTTP Server**

[www.apache.org](http://www.apache.org)

Apache has been the most popular web server on the Internet since April of 1996, with more than 67% of web sites on the Internet using it as of October 2004. The Apache HTTP Server is a project of the Apache Software Foundation. The Apache Software Foundation is a non-profit corporation that aids open, collaborative software development projects by supplying hardware, communication, and business infrastructure.



INNOVATIVE WEB STRATEGIES



#### PHP

[www.php.net](http://www.php.net)

PHP is an HTML-embedded scripting language. Much of its syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow web developers to write dynamically generated pages quickly. Andi Gutmans, Rasmus Lerdorf, Zeev Suraski and a number of other contributors are actively enhancing the PHP language.



#### MySQL

[www.mysql.com](http://www.mysql.com)

MySQL, Inc. develops and markets a family of high performance, affordable database servers and tools. MySQL is the world's most popular open source database, with more than 5 million active installations. With superior speed, reliability, and ease of use, MySQL has become the preferred choice of corporate IT Managers because it eliminates the major problems associated with downtime, maintenance, administration and support.

#### BIND

#### BIND

[www.isc.org/sw/bind/](http://www.isc.org/sw/bind/)

BIND (Berkeley Internet Name Domain) is an open source implementation of the Domain Name System (DNS) protocol. The BIND software is used on the vast majority of DNS Servers on the Internet, making it an essential component of the Internet's infrastructure. The Internet Systems Consortium, which was co-founded in 1994 by BIND's primary author, Paul Vixie, maintains the software.

## Partners: Infrastructure



#### Rackspace Managed Hosting

[www.rackspace.com](http://www.rackspace.com)

Rackspace runs four state-of-the-art, secure data centers - two in San Antonio, Texas, one in Herndon, Virginia, and one in London, England. This fast, reliable network is powered by UUNET, AT&T, Sprint, Qwest and SBC to ensure maximum network uptime - and has been running at 100% for the last two years.



#### Biz Net Technologies

[www.bnt.com](http://www.bnt.com)

**RassaiMail™** maintains a secondary data center in the Corporate Research Center at Virginia Tech (VTCRC) in Blacksburg, Virginia.

## Partners: Data Storage

### Data Storage

Data is the most critical component of an email system. Data must be rapidly accessible, the storage architecture must be extremely scalable, and lost data is unacceptable. The **RassaiMail™** system architecture has been designed to scale its load effectively, without experiencing data I/O bottlenecks that would slow user response time and constrain email throughput. All **RassaiMail™** solutions benefit from disk mirroring, offsite data replication, and tape backups for Disaster Recovery.



**Veritas**

[www.veritas.com](http://www.veritas.com)

**RassaiMail™** uses Veritas Netbackup software on a dedicated backup network, with no cross-server communication other than appropriate transmission of information from backup client to the Netbackup master server. Tape backups are performed 100% out of band.



**EMC**

[www.emc.com](http://www.emc.com)

## Partners: Monitoring

### Monitoring

The **RassaiMail™** internal monitoring systems run a variety of commercial and public domain software, as well as software developed in-house. These systems were designed to be modular, so that as new applications or information need to be monitored, they can be incorporated easily. Monitoring includes: bandwidth utilization, interface errors, environmental alarms, chassis info (disk, CPU, memory, temperature), intrusion detection, application performance, and more.



**BMC Software – PATROL Express**

[www.bmc.com](http://www.bmc.com)



**Quest Software – Big Brother**

[www.quest.com/bigbrother](http://www.quest.com/bigbrother)

## Partners: Security

### Security

The firewall solution in use at **RassaiMail™** is based on open-source initiatives developed for the OpenBSD operating environment. All servers run security hardened operating systems, undergo scheduled vulnerability scans, strict patch control, and include multiple layer Intrusion Detection Systems (IDS) and packet filtering. Our IDS will detect any known attacks or attempted hacks and report them to our engineers for immediate action. Every solution receives early warning detection, industry leading security analysis and incident response to keep your critical information safe.



**GeoTrust**

[www.geotrust.com](http://www.geotrust.com)

**RassaiMail™** has teamed with GeoTrust for its digital certificate needs. GeoTrust provides **RassaiMail™** administrators with immediate certificate issuance capabilities, removing the delays that are commonly associated with obtaining SSL certificates. **RassaiMail™** applications use 128-bit strong SSL encryption.

**OpenSSL**

[www.openssl.org](http://www.openssl.org)

## Partners: Anti-Virus

## Anti-virus

**RassaiMail™** scans for email borne viruses using a unique three-stage anti-virus process. Stage one identifies formatting vulnerabilities: email formatting "trickery" that can be used to hide attachments from anti-virus scanners. Stage two performs the anti-virus using dual, independent virus scanners with hourly updated virus definitions. Stage three blocks potentially unsafe attachments, which could carry malicious executable code. Should any portion of this three-stage anti-virus process fail, safeguards are in place to ensure that the remaining stages execute and email traffic continues without interruption.



### ClamAV

[www.clamav.net](http://www.clamav.net)

ClamAV is an open source anti-virus toolkit for UNIX. The primary purpose of this software is mail server virus scanning. The package provides a fast and scalable multi-threaded daemon and a tool for automatic updating via Internet. The virus database is kept extremely up to date through the combined efforts of the organizations that use the software.



### FRISK Software

[www.frisk-software.com](http://www.frisk-software.com)

FRISK builds one of the industry's top OEM anti-virus products in terms of reliability and speed of scanning. Their anti-virus products include advanced neural network and heuristic detection capabilities. The FRISK anti-virus team provides swift reaction to new and emerging virus threats.

## Partners: Anti-spam

### Anti-Spam

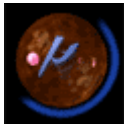
**RassaiMail™** has teamed up with several key players in the anti-spam arena and actively participates in ongoing research to combat the spam problem. New methods of identifying Spam and reducing false-positives are constantly being engineered. **RassaiMail™** has built its anti-Spam solution so that emerging technologies can be easily integrated.



### SpamAssassin

[spamassassin.apache.org](http://spamassassin.apache.org)

SpamAssassin is an engine for deploying a wide-spectrum of mail filtering tests that can identify spam. This open source software provides extreme flexibility through an API, allowing it to be used in a wide variety of email systems, including Postfix.



### Microneil Research Corporation

[www.microneil.com](http://www.microneil.com)

Based in Sterling, Virginia, MicroNeil's advanced anti-Spam pattern recognition technologies allow **RassaiMail™** anti-Spam filters to simultaneously apply thousands of heuristic algorithms to each email in search of identifiable Spam traits ("Spam DNA"). The efficiency, speed and depth of this technology make identifying "Polymorphic Spam" a reality. Polymorphic Spam is where many copies of the same email is sent, but with each email containing subtle differences in punctuation or spacing designed to circumvent content filters.



### SpamHaus

[www.spamhaus.org](http://www.spamhaus.org)

Spamhaus tracks the Internet's worst spammers, known Spam Gangs and Spam Support Services, and works with ISPs and Law Enforcement Agencies to identify and remove persistent Spammers from the Internet. The spamhaus Block List (SBL) is a free real time DNS-based database of IP addresses of verified Spammers. This is one of over twenty anti-Spam databases integrated into the **RassaiMail™** system.



### SpamCop

[www.spamcop.net](http://www.spamcop.net)



INNOVATIVE WEB STRATEGIES

Founded in 1998, SpamCop remains the premier Spam reporting service on the Internet. **RassaiMail™** aggressively reports Spammers to SpamCop, where the reports are then channeled to the appropriate network administrators. SpamCop's database of known Spammers is one of over twenty anti-Spam databases used by the **RassaiMail™** system.



#### **Bonded Sender**

[www.bondedsender.com](http://www.bondedsender.com)

The Bonded Sender Program allows legitimate email senders to bond their email financially to avoid being accidentally blocked by anti-Spam filters. **RassaiMail™** has integrated the Bonded Sender Program into its suite of anti-Spam tools to avoid falsely identifying legitimate email as Spam ("false-positives").



#### **CAUCE**

[www.cauce.org](http://www.cauce.org)

The Coalition Against Unsolicited Commercial Email (CAUCE) is an organization created to advocate for a legislative solution to the problem of Unsolicited Commercial Email. CAUCE has become the preeminent voice for the anti-Spam community in the US and has spawned the formation of similar organizations in Europe, Canada, India and Australia.



#### **Digital Phishnet**

[www.digitalphishnet.org](http://www.digitalphishnet.org)

The Digital PhishNet is a joint enforcement operation between industry and law enforcement designed to ensnare those who perpetrate phishing attacks. Its goals are simple: to identify, arrest and hold accountable, those that are involved in all levels of phishing attacks to include spammers, phishers, credit card peddlers, re-shippers and anyone involved in the further abuse of consumers' personal information. Members include ISPs, online auctions, financial institutions and law enforcement to include the FBI, Secret Service, US Postal Inspection Service, Federal Trade Commission, a number of Electronic Task Forces around the nation, and others.

#### **Anti-Spam Research Group**

[www.irtf.org/charters/asrg.html](http://www.irtf.org/charters/asrg.html)

ASRG, chartered by the Internet Research Task Force, is a group made up of deeply knowledgeable experts in the area of anti-Spam, Internet messaging, networking, and security. The purpose of this organization is to investigate the Spam epidemic as a large-scale network problem, and to openly discuss proposed solutions, evaluation techniques and implementation costs.

## **Partners: Domains**

### **Domain Registration**

**RassaiMail™** provides multi-year domain registration for 17 top-level domain extensions (.com, .net, .us, etc). DNS management is provided with all registrations at no additional cost.



#### **eNom**

[www.enom.com](http://www.enom.com)

eNom is an ICANN accredited domain registrar. **RassaiMail™** has integrated its domain registration system with eNom's application programming interface (API). This allows real-time domain registration and domain management to be completed through the **RassaiMail™** system.

