
Messaging Assurance Gateway: The Next-Generation in Anti-Spam & Anti-Virus Solutions

The Problem: Spam is Growing, Unchecked

According to Ferris Research, spam and viruses now account more than 90% of all email. In addition spam continues to increase at alarming rates year over year. Why does it continue to grow? Profit driven hackers and spammers continue to invest in driving the quantity of spam and developing new techniques to bypass spam filters. Spam is no longer an advertising tool. It is used by criminals to hack into secure systems at universities, businesses, and retail outlets. Spammers can make tens of thousands of dollars per month preying on the public. Many innocent recipients still don't realize that they are sending information just by clicking on email documents.

Viruses, spam, and phishing schemes result in lost productivity, lost business, security violations, and increased capital drains to businesses every day. Despite the use of first and second generation anti-spam and anti-virus products by many businesses, the problem continues to grow. According to a Nucleus Research report, implementing some anti-spam products only result in a 26% increase in productivity, because spam continues.

The cost of spam is estimated to exceed \$50 billion in the U.S. alone. Businesses here spent \$1500-\$2000 per employee to fight spam and viruses. That is up significantly from the \$600-\$800 spent in previous years. Spam and other message-based threats are growing proportionally and have far reaching global effects and business implications.

The spam and virus problem is:

- Large and growing,
- Not just a security issue, but a productivity issue,
- A "real dollar" expense for all enterprises.

Red Condor Offers Multiple Solutions for Your Email Security

Depending on your organizations needs, you can get the power of Red Condor's breakthrough email security technology as either a hosted service or network appliance – both fully managed:

- **Hosted Services:** Let our technical experts do all the work. With Red Condor's hosted service you can get the benefits of our technology immediately, and you don't have to install any software or hardware. Nothing to install on servers, nothing to install on desktops. No manuals to read, no tech training to attend, no downtime. We do it all for you, and you reap the benefits of safe, secure email. Say goodbye to the distractions of spam and the dangers of viruses, phishing, identity theft, and other email-related hazards. With our hosted service, you can activate service in minutes.
- **Network Appliances:** Red Condor's Message Assurance Gateway (MAG) network appliances provide cost effective, localized protection of email systems for larger organizations and enterprises.

MAG-series network appliances are non-disruptive standalone devices compatible with all email servers, systems, and client software. And they work without the need for any software to be installed or updated on any servers or client computers. Red Condor's revolutionary Vx Technology™ provides fail-safe redundant operation of MAG-series network appliances – even if those devices are off-line due to overwhelming attacks, power failure, or other network issues.

Why Red Condor?

Thousands of businesses around the world already rely on Red Condor to safeguard their email. Now your organization can enjoy the same enterprise-class protection and managed security services that have made Red Condor the emerging leader in email protection technology.

- **Multi-Layer Protection from One Service:** In addition to spam filtering, Red Condor also filters viruses, spyware, phishing schemes, and Trojans. We also help protect your network systems from overwhelming attacks such as denial of service and directory harvest attacks.
- **Zero Tolerance for False Positives:** Red Condor has a strict policy that guides all its filtering processes: a filter rule will not be implemented if it results in even one good email being discarded. There is no probabilistic guessing or statistical heuristics in the Red Condor system, only absolute criteria that leads to a definitive action. Red Condor's proven technology tracks evolving spam campaigns in real-time with near-zero false-positive rates while achieving block rates over 99.99%.
- **Email Behavioral Profiling™:** In addition to filtering email based on content and keywords, Red Condor analyzes email's behavioral to further determine whether a message is legitimate mail or spam. Simply put, if email has the intent to deceive, defraud, or otherwise misrepresent itself, it is eliminated. With a single set of behavior-based filter rules, it meets the needs of a diverse set of customers – from pre-schools to fertility clinics – without making mistakes.
- **Unique Spam Filtering Technology:** Red Condor does not use unreliable heuristics, DNS blacklists, or Bayesian filters to identify spam. Instead, it investigates email messages, applying uniform standards before crafting the precise rules that block just the spam, not your important email correspondence.
- **Vx Technology™ for fail-safe operation:** All of our MAG-series network appliances use our revolutionary Vx Technology™ to provide fault-tolerant fail-safe operation. If your system goes down due to overwhelming attacks, power failure or other network issues, email protection is automatically re-directed to our back-up servers so you get uninterrupted protection and security.
- **Perimeter Defense System:** Instead of installing software and allowing threats into your network and desktops, Red Condor acts as a perimeter defense in front of your email server. We take and screen the emails before they get to you. This protects you and ensures that no malicious content corrupts your servers.

- **Email Disaster Recover for Up to 96 Hours** - Not only are our servers redundant, but we provide redundancy for your email server. If your mail server goes down, Red Condor will store inbound email for up to 96 hours. When your server comes back online, email is released in an orderly fashion to prevent overloading your server. This service can be used to perform scheduled maintenance as well as protect your business from outages.
- **Human in the Loop**:-Some companies rely only on software to detect new types of spam. At Red Condor, we utilize the skill of email experts in addition to our cutting-edge technology. We feel that the addition of human intelligence is one of the best ways to beat spammers at their own game. When spammers adopt a new technique, Red Condor is able to accurately and rapidly adapt.

Red Condor Offers Zero Administration

Red Condor is easy-to-use and self-configuring. There is absolutely nothing to install, upgrade, or maintain. And your existing mail user agents, such as Microsoft Outlook or Netscape Messenger, continue to send and receive mail without any changes. After creating an account at Red Condor, you will receive an email with instructions for configuring your mail exchanger (MX) records. Your IT administrator or ISP should be able to make these changes in a few minutes. If you have any questions, you can contact a Red Condor Technical Support Engineer.

Email Policy Management at Your Fingertips

Normally there is no need to administer the MAG service, but when you first signup, you may wish to visit your web dashboard to set your email policy to match your internal email policy or personal preferences.

Web Dashboard

The Red Condor Dashboard provides administrators and mailbox owners with an easy to use console for managing the Red Condor service. Administrators set email filtering policy and reporting frequency for the domain and mailbox level. Everything else is taken care of as part of the Red Condor Managed Service.

Spam Digest

A Spam Digest is an emailed version of the Quarantine page that allows each mailbox owner to review and release spam. The digest delivery frequency can be set to Daily, Weekly, Monthly, or Never. By default, the frequency is set to Never. Users do not need to report spam or develop rules to block it. Your spam problem simply disappears.

The Red Condor Difference – Compare Us to the “Other Guys”

The important difference in Red Condor’s approach to fighting spam and viruses is also in how we are different in our technology and techniques. The other market leaders frequently rely on the more common first and second generation of spam filtering and blocking techniques. Unfortunately, spammers have already bypassed many of these processes.

Open Source Software: We do not use open source filtering software, but we do run our proprietary technology on top of open source platforms, and we are definitely fans of the open source community. One of the main downsides to the most widely deployed open source spam filtering solution (spam assassin) is that it requires constant optimization and tuning from the operator to be effective. Also, spammers have full access to the source code, and can devise methods to circumvent open source spam blocking techniques easily and rapidly. Red Condor's managed service (for both our hosted and appliance solutions) requires zero administration or tuning – we do the work for the customer so they can just turn on our service and stop worrying about spam.

Fixed Keyword & Phrase Filtering: This technique can be ineffective because it relies on user configuration and training. The ease of scripting tools available to spammers makes unique message-by-message randomization prevalent for most spam. One well known technique relies on mixing certain characters on a random basis. Keyword blocking does little to keep up with these now simple techniques, letting the messages through unblocked.

Heuristic Scoring & Bayesian Filtering: Increasingly, message-by-message unique randomization techniques make both Bayesian and heuristic-based filtering techniques almost entirely ineffective. Attempts to leverage these filtering techniques push the administration of such solutions on to the end users. This not only wastes valuable time, but results in poor block rates or high false identification of good, valid messages (aka, false-positives).

DNS Real-Time Blacklists (RBLs): One of the most significant causes of false-positives, or good email that's accidentally discarded. Each day globally there are estimated to be 200,000 new Zombie and Bot ("robot") networks, (e.g., spammer corrupted and controlled Personal Computers that are sending out the latest spam campaigns). That means there are millions of such corrupted networked PCs at any given time. Because there are so many moving parts, fixed blacklist can quickly become ineffective. Systems that rely too heavily on this technique in their filtering can also have a high rate of false-positives.

The "Junk Mail Bin": There is sometimes a default folder inside enterprises email clients, the Junk Mail folder. This type of solution creates a stream of "unresolved" messages. These are messages that the spam filter couldn't make an absolute determination of the quality of the message. These messages instead of being blocked are forwarded on to the end users Junk Mail Bin for resolution. This forces the end users to continually check their Junk Mail Bin resulting in twice the work. Conservative estimates of the cost of such false-positives (mistaken categorizations of valid messages) are in the \$5 to \$10 range (depending on the cost of labor). Additionally, even one critical false-positive could literally cost a business thousands of dollars in lost revenue.

Conclusion: Red Condor's Messaging Assurance Gateway is Superior

Red Condor's state-of-the-art email security eliminates spam, and protects against viruses, spyware, phishing schemes, identity theft, and other dangerous or undesirable content. We ensure that important emails get through without being incorrectly blocked. Red Condor's sophisticated intrusion



detection and defense systems also protect email servers and networks from external threats such as denial of service and directory harvest attacks.

Exceptional Performance – Effortless Control

- Fully managed solution
- Next generation filter algorithms
- SMTP Session level defense against directory harvest and denial of service attacks
- Vx Technology™ with failover resiliency
- Email disaster recovery
- Human in the Loop review
- 24 x 7 x 365 customer support

We've developed the best technology to stop spam, viruses, spyware, phishing schemes, and other offensive content, while making sure that important emails get through.

We're easy to use, affordable and reliable.

We're Red Condor. We're the best at what we do. And we're ready to prove it to you with our 30-day free trial. Go to www.RedCondor.com now.

About Red Condor

Red Condor is revolutionizing spam fighting with its next generation technology. Red Condor's highly accurate email filter, hybrid architecture Vx Technology™, and fully [managed appliances](#) lead to a dramatic reduction in the cost of owning a premium [spam filter](#). With solutions for [small business](#), as well as ISPs with millions of email inboxes, Red Condor has a cost-effective, time-saving solution that is rapidly gaining market share. The system's design has built-in zero tolerance for lost email, and a near zero false-positive rate while achieving long-term spam block rates greater than 99%. This next-generation technology is backed by a 24x7 customer care center staffed by email security experts at Red Condor's headquarters. For more information, visit www.redcondor.com.

RedCondor

1300 Valley House Drive, Suite 115 Toll Free: 888-9NOSPAM
Rohnert Park, CA 94928 1-888-966-7726

www.RedCondor.com