



# stop spam and viruses – solutions designed specifically for service providers

## A Growing Problem

Today, spam can account for nearly 90% of the email consumers receive<sup>1</sup>, and the volume of abuse traffic continues to increase. The speed and sophistication of attacks is also growing with a rise in zombies, phishing and other fraudulent threats.

Service providers are being hit hardest, facing whopping bandwidth and storage costs, growing message filtering costs, a drain on customer support resources and subscriber churn — all caused by

## powerful, flexible solutions fit for service providers

While there are a number of anti-abuse tools on the market, almost all of them are designed for the enterprise whose needs differ dramatically from the service provider's. As a service provider, your user base is orders of magnitude larger than that of most enterprises. What's more, you face frequent denial-of-service and directory harvest attacks. Along with stopping inbound attacks, you must give equal attention to preventing abuse, ensuring that it never originates from your users.

Your top priority is to reduce abuse-related costs, including subscriber churn, so a highly scalable, low-cost solution is essential. Meanwhile, you'd also like to differentiate your premium services with added abuse protection, so the solution you choose must be flexible.

With years of experience developing messaging solutions for service providers, Critical Path offers a highly efficient, comprehensive, anti-abuse solution specifically designed for ISPs, telcos and mobile operators.





## The Anti-Abuse Solution

Offering a turnkey solution, *Anti-Abuse*, part of the Memova® suite of applications and services, is used by more than 25 leading service providers around the globe, protecting more than millions of users and blocking millions of unwanted, unsafe messages each day.

- Consistently stops 98% of abuse traffic and performs 6 to 10 times faster than comparable email security solutions which greatly improves the email experience
- Quashes up to 70% of abuse with first-line-of-defense traffic management, reducing the need for costly message content analysis and dramatically lowering overall costs
- Includes cutting-edge traffic management capabilities, such as sender verification, reputation checks, rate controls and tarpitting capabilities
- Provides administrators with full insight and control over abuse traffic
- Provides a basic level of anti-abuse protection for all users, while enabling the added protection needed to differentiate premium access bundles and business services, thereby driving customer upgrades
- Sits at the network gateway, stopping abuse before it enters or exits your mail system
- Works with any messaging system and allows you to deploy a solution in a matter of hours
- Built on Critical Path's SMTP Relay Server—industry-endorsed for its high performance and low total cost of ownership at scale

## Double Your Defenses, Strengthen Your Control



*Anti-Abuse* stops spam, viruses, mailbombs, denial-of-service, directory harvest and phishing attacks in the most cost-effective manner— at the gateway.

The solution provides two lines of defense, flexible options and customized controls.

### 1st Line of Defense—Advanced Traffic Management

*Anti-Abuse* blocks spam and viruses at your network gateway before they reach your messaging system. Advanced traffic management forms the first line of defense, reducing security threats and minimizing system loads, while ensuring the continuous availability of your messaging services. Sender validation and reputation techniques guard against phishing and spoofing tactics, dropping inbound traffic from known spammers, while enabling trusted senders to bypass secondary abuse checks. Sophisticated rate control capabilities automatically detect and block mail bombs, denial-of-service attacks and directory harvest attacks in real-time.





In addition, *Anti-Abuse* also offers new tarpitting capabilities slow the processing of messages from potential spam sources to the point where a spammer loses all economic productivity and will remove your domains from future attacks.

- 🔒 **Granular Controls:** While *Anti-Abuse* is effective out-of-the-box, a full range of granular controls, which allow administrators to fine-tune the solution, are available.
- 🔒 **Outbound Reputation Protection:** Sender authentication techniques, along with relay controls, ensure that only authorized users can send mail from your system. Advanced rate control capabilities stop outbound abuse by enforcing limits on traffic volumes within set time periods.
- 🔒 **Content Controls:** You can create custom whitelists, enabling trusted senders to efficiently bypass abuse checks. You can also use public blacklists or create custom blacklists, automatically dropping traffic from known sources of abuse. You can enforce policies and attachment rules to safeguard against the distribution of inappropriate content, and you can implement disclaimers to limit your liabilities.

## 2nd Line of Defense—Message Content Analysis

Traffic management, the first line of defense, detects up to 70% of abuse traffic. To take anti abuse protection a step further, consistently stopping more than 95%, *Anti-Abuse* provides a second line of defense—sophisticated message content analysis. *Anti-Abuse* uses a full range of message content analysis techniques, including deterministic techniques, such as signatures and spammer asset tracking, and predictive techniques, such as heuristic analysis, as well as feedback from subscribers and human editors. As a result, the solution has a proven ability to evolve along with or ahead of new abuse tactics and emerging threats.

Identified spam is dropped or conveniently tagged or filed for the subscriber. When *Anti-Abuse* is deployed with other solutions from the Memova suite, a full range of end-user controls at the mailbox level are available.

Traffic management stops up to 70% of abuse, minimizing the need for costly message content analysis.





## Flexible Options

With two options to choose from, you can balance your functionality needs with your budget. The Standard solution provides an advanced level of protection for consumer subscribers, while the Premium level enables you to go one step further—optimizing anti-abuse services by subscriber segment.

You can maximize your investment by choosing a configuration that meets your needs, which includes seamless integration, administration and management.

### Anti-Abuse Standard

This option combines cutting-edge traffic management capabilities, such as sender verification, reputation checks and rate controls, with anti-virus protection and comprehensive anti-spam and anti-phishing protection from Kaspersky.

The *Anti-Abuse Standard* solution cost-effectively stops 95% of abuse with less than one in 1,000,000 false positives. It provides effective protection for your full consumer subscriber base at a competitive price.

### Anti-Abuse Premium

Encompassing all of the capabilities of the Standard option, *Anti-Abuse Premium* provides the industry's most compelling abuse protection solution for service providers. It features anti-spam and anti-phishing protection from Cloudmark, including unique subscriber controls such as Personal Address Book-based safelists.

When deployed with other solutions from the Memova suite of applications, *Anti-Abuse* provides entitlement-based protection on a per-domain, per-user or class-of-service basis. This means you can effectively differentiate and drive upgrades to premium business services, as well as high-value access packages, by bundling in compelling subscriber controls and premium Cloudmark protection to block more than 98% of spam with near-zero false positives.

## Deployment

- 🔑 **Works with Your Existing Messaging System:** Based on the industry SMTP standard with support for subscriber authentication in a multiservice environment, *Anti-Abuse* seamlessly integrates with your existing mail system.
- 🔑 **Get Up and Running Now:** *Anti-Abuse* is a turn-key solution that can be deployed in a matter of hours, instantly protecting your mail system and subscribers. USB memory card back-up and restore capabilities enable a server to be cloned in no time.





## Administration

- ❶ **Legal Interception:** *Anti-Abuse* enables transparent mailbox monitoring of select subscriber accounts, in accordance with local legislation and as required by law-enforcement authorities.
- ❷ **Secure Channel Encryption:** The solution supports Secure Sockets Layer (SSL)/Transport Layer Security (TLS), providing comprehensive encryption of messages between gateways.
- ❸ **Powerful Administration:** Powerful administration enables you to seamlessly manage up to 40 servers. The rich, Web-based administrative interface provides real-time reporting and enables administrators to easily define Access Control Lists or other custom configurations. With *Anti-Abuse*, you can tailor the operation to meet your specific requirements.

## Performance

Proven, carrier-grade scale, *Anti-Abuse* is built on Critical Path's SMTP server. Industry-endorsed for its high performance, reliability and massive scalability at a low total cost of ownership, the server can routinely handle more than 4 million messages per hour and up to 10,000 simultaneous connections. This industry-leading performance means there is no humanly detectable mail latency and effectively no risk of denial-of-service attacks stopping the delivery of legitimate email.

## Flexible Options, Reliability You Can Count On

*Anti-Abuse* offers the scalability, reliability and the flexibility to meet your safety requirements. *Anti-Abuse* solutions are available in software or appliance options. Contact your local Critical Path representative, and learn how *Anti-Abuse* can meet and exceed your safety requirements.

### Sales and General Information

United States & Canada  
1 (877) 441 PATH  
[info@criticalpath.net](mailto:info@criticalpath.net)

United Kingdom  
+44 1 625 507300  
[info.uk@criticalpath.net](mailto:info.uk@criticalpath.net)

France  
+33 1 55 60 23 90  
[info.fr@criticalpath.net](mailto:info.fr@criticalpath.net)

Germany  
+49 30 89 66 0 0  
[info.de@criticalpath.net](mailto:info.de@criticalpath.net)

Italy  
+39 (011) 451 3811  
[info.it@criticalpath.net](mailto:info.it@criticalpath.net)

Spain  
+34 91 567 8467  
[info.es@criticalpath.net](mailto:info.es@criticalpath.net)

Sweden  
+46 7576 01200  
[info.se@criticalpath.net](mailto:info.se@criticalpath.net)

Switzerland  
+41 44 308 38 90  
[info.ch@criticalpath.net](mailto:info.ch@criticalpath.net)

Hong Kong  
852 2251 8116  
[asiapacific@criticalpath.net](mailto:asiapacific@criticalpath.net)

India  
9122 5656 1412  
[asiapacific@criticalpath.net](mailto:asiapacific@criticalpath.net)

Indonesia  
62 21 230 2141  
[asiapacific@criticalpath.net](mailto:asiapacific@criticalpath.net)

Singapore  
65 6 533 9553  
[asiapacific@criticalpath.net](mailto:asiapacific@criticalpath.net)

Latin America  
[sales.latinamerica@criticalpath.net](mailto:sales.latinamerica@criticalpath.net)

Contact the office nearest you  
for more information.

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

