

## PineApp Mail-SeCure vs. Barracuda Spam Firewall

**This comparison analysis describes the main differences between PineApp Mail-SeCure and Barracuda's Spam Firewall. This document will provide marketing tools in order to sharpen these differences and provide a better understanding of them.**

### Anti-Virus

PineApp Mail-SeCure includes five Anti-Virus engines:

- **Three F-Secure® Anti Virus engines** – these three award-winning engines: F-Secure Libra, F-Secure Orion and Kaspersky Labs provide a security suite for all heuristic and signature based Viruses.
- **CommTouch™ Zero-Hour Detection engine** – this engine identifies new-age Virus outbreaks within 2 minutes of the outbreak (even before Anti-Virus vendors release a signature to detect it) and blocks them at the perimeter.
- **PineApp Heuristic Anti-Virus engine** – this engine provides an additional protection layer by detecting and blocking all known and unknown vandals, malicious code and suspicious mail behavior.

Barracuda's Spam Firewall has only two Anti-Virus engines, based on open source (ClamAV). Furthermore, the second engine is an unknown propriety engine. This means that the Anti-Virus updates can sometimes be very late (in some cases – too late).

Barracuda's system does not feature zero hour detection. This means that the customer's organization is often left exposed and unprotected for a long period of time (in some cases - more than 18 hours), until a signature is released.

### Anti-Spam

Mail-SeCure integrates eleven different Anti-Spam layers, which provide overlapping detection to compensate some of the engines' disadvantages. This system has a 98.5% detection rate and a very low false positive ratio. This detection rate is achieved “out-of-the-box”, thus no ongoing maintenance of the engines is required.

Barracuda's Anti-Spam engines are mainly based on Heuristic and Bayesian engines. However, they require user or admin management to keep them in shape. Therefore, detection rate can vary from 80% to 95% - depending on the time of the system's update.

Image-based Spam – Mail-SeCure incorporates Commtouch RPD™ technology, which is very effective against Image-based Spam. For the last couple of months, Barracuda has been struggling with such Spam; Different solutions they have offered have turned out to be ineffective and resource consuming.

### **IP Reputation – a unique feature of PineApp Mail-SeCure**

This powerful additional layer blocks Zombies at the SMTP session level. IP Reputation saves bandwidth and lowers the load on the Mail-SeCure system. This mechanism is based on sniffers located all over the world, monitoring traffic of hundreds of millions of email messages daily. The IP Reputation center dynamically classifies IP's according to a profile built from parameters such as volume, percentage of Spam and Viruses and escalation.

### **Policy Management**

Mail-SeCure provides a Three-tier (global/group/user) policy management tool. This tool allows to customize the policy of incoming and outgoing **emails containing attachments**. One may block, delete, strip and park messages. Users may manage their quarantine and view, release or download their blocked mail.

Barracuda's Spam Firewall has only a very basic management tool.

### **Load Balancing and Scalability**

Load balancing, fault tolerance and high availability are features that are **integrated** in all Mail-SeCure systems. Businesses can share traffic load and grow and optimize their scanning power by stacking two or more Mail-SeCure appliances, adding additional systems instead of replacing existing ones.

Barracuda's Spam Firewall does not feature Load Balancing and Scalability.

	PineApp Mail-SeCure	Barracuda Spam Firewall
<b>Anti Virus</b>		
Number of Engines	5	2
Engine types	3 by F-Secure, Commtouch Zero-Hour™ and PineApp Heuristic	One open source and one propriety
Zero-Hour Protection	✓	✗
<b>Anti Spam</b>		
Proven detection ratio	98.5%	80-95%*
Proven Image-based Spam detection	✓	✗
IP Reputation technology	✓	✗
RPD™ Technology	✓	✗
Zombie detection (ZDS)	✓	✗
Bayesian engine	✓	✓
Heuristic engines	✓	✓
RBL	✓	✓
NextGen Greylisting	✓	✗
<b>Content filtering</b>	✗	Global Only
<b>Anti-Spoofing</b>	✓	✓
<b>Denial of Service protection</b>	✓	✓
<b>Anti-Phishing</b>	✓	✓
<b>Policy Management</b>		
3 Tier General Policy rules (Global/Group/User)	✓	Limited
3 Tier Policy Attachment rules (Global/Group/User)	✓	Global Only
3 Tier Footnotes rules (Global/Group/User)	✓	Global Only
3 Tier Spam score rules (Global/Group/User)	✓	Available for 600 model and above
Different policy for outgoing and incoming mail	✓	✗
LDAP Synchronization	✓	✓
End-user quarantine	✓	✓
End-user Black and white lists	✓	✓
<b>Mail Routing</b>	✓	✗
<b>Masquerading</b>	✓	✗
<b>Integrated load balancing</b>	✓	✗
<b>Optional mail server</b>	✓	✗
<b>Automatic Software updates</b>	✓	✓

\* Results may vary according to modifications by administrator