

## intY MailDefender

### FAQ



#### **Q. Why is MailDefender going to stop spam better than my current solution?**

Because it's designed to work at the Internet level, it has many advantages that can only be found in a system that is trusted by hundreds of thousands of users. It uses multiple spam and virus filter engines, including a heuristic virus scanner to protect against new unknown threats, all of which are continually updated.

#### **Q. What's so good about a solution that works at the Internet level?**

Because MailDefender is hosted in intY's data centres, spam and viruses are removed well away from your network, which means you don't have to download lots of dangerous and unwanted emails. That means Internet connection is used more effectively and also means that malicious software is dealt with by us and not your mail server.

#### **Q. So what do I need to install?**

Absolutely nothing. No hardware and no software are required. The management portal for MailDefender is accessed via a web browser so all you need is a username and password.

#### **Q. Can I trust MailDefender to be reliable?**

Because we process mails for over half a million users, intY has built up a redundant infrastructure across multiple data centres. MailDefender has been designed on a fully resilient architecture so it can withstand the loss of individual scanner's, Internet links and so on, without disruption to your service.

#### **Q. How does MailDefender scan my mail?**

When you sign up for the service, your email domain records are changed to pass all your email traffic to MailDefender. We filter it and then pass on the resulting clean emails to your mail server.

#### **Q. What if I want to look at a 'spam' email: won't it be filtered out?**

Spam emails are placed in a searchable quarantine queue where they are held for 21 days. The quarantine management allows the mail to be viewed and released if required.

#### **Q. Our people haven't got the time to manage a complex system; isn't MailDefender**

**going to be an extra burden to look after?**

Not at all. We've made sure that MailDefender is simple to live with. In day to day operation, the majority of users simply get spam and virus free mail and never need to perform routine

management. In fact many users find they never even need to check their quarantine queues at all. Because we update MailDefender automatically 24/7, you never have to worry about being caught out by not applying the latest signatures.

**Q. I've used a spam filter before & still received lots of unwanted mails: why is your solution going to be any better?**

MailDefender uses multiple spam detection engines, including Cloudmark and SpamAssassin, plus address block lists, all of which are continually updated and adapted to combat emerging spam techniques.

Cloudmark's detection technology is unique, because unlike competitive solutions, it isn't based on software judgements of what constitutes spam. Its scanning signatures are based on real time feedback from over 100 million email users worldwide. Individuals spam reports are graded, analysed and compared in real time to produce unique fingerprints for every mail passing through the system. Reliable spam reporters are graded higher than new users without a proven track record. In this way the system gathers the most accurate decision making capability in the industry, which results in a spam free inbox for MailDefender users.

**Q. I already use a virus program; why do I need one for my email?**

For many years email has been the prime method hackers have used to distribute malicious software. There is wide agreement amongst security experts that a multi-layered approach to virus protection is the best approach. In other words, don't put all your eggs in one basket. Having antivirus protection in MailDefender doesn't mean you should get rid of desktop AV software, because there are still plenty of ways a PC can be infected besides email. However, by removing viruses from email outside your network, you are limiting the number of threats as a whole that your defence systems have to deal with.

**Q. Can MailDefender protect me if I get a virus infection other than by email?**

Yes. Because it scans outgoing mails for viruses as well as incoming, if a PC becomes infected and starts trying to replicate itself by external email, MailDefender will block the infected mails as they leave your network, so containing the damage until you can disinfect the systems involved.

**Q. So what antivirus does MailDefender use?**

On the basis that no one set of AV signatures will catch every piece of malicious software, MailDefender uses multiple systems. We use the Sophos, Clam, and Cloudmark detection engines plus our own heuristic scanner which checks for unknown threats. We check for updates every 5 minutes.

**Q. What if I have users that don't want the same spam filtering as everyone else?**

MailDefender can be tailored to the individual needs of each person in your organisation. We recognise that what is spam to one person might not be to another, so MailDefender gives you the tools to adjust the level of filtering so each user gets the email they need to be productive.

**Q. What about other threats than viruses?**



The scanning engines in MailDefender are routinely referred to as 'antivirus' signatures but also check for Trojans, worms and other malware.

Phishing emails are undergoing a rapid increase at the moment because most users now have better basic antivirus protection. As they contain no active content and look just like genuine emails, they are particularly hard to detect. The Cloudmark technology in MailDefender is exceptionally good at blocking this type of threat. In fact it is accredited by PayPal as a recommended means of blocking phishing scams.