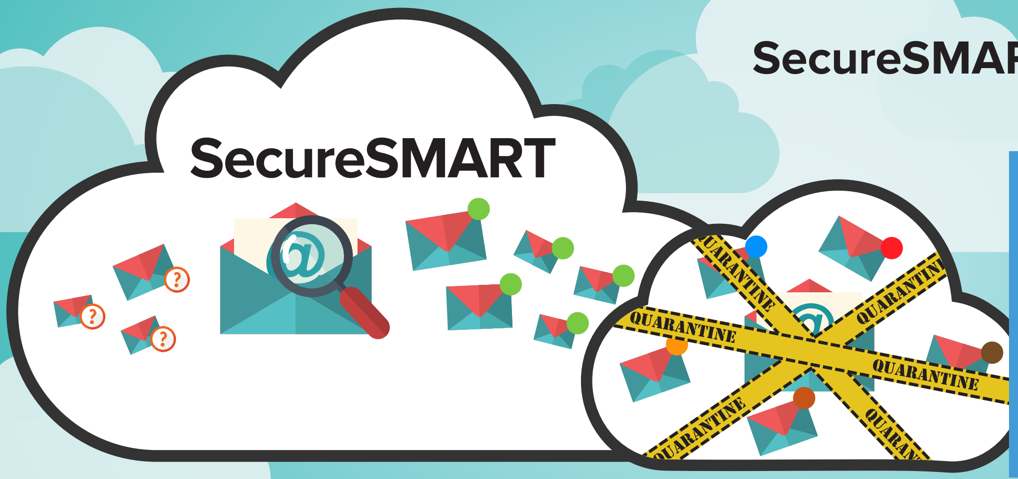


● Clean ● Virus ● Policy ● Spam ● Bulk ● Reject

SecureSMART advanced policies

Policy block examples

- “Friendly from” and “envelope from” mismatch
- New domain bulk mailing
- Spoofing
- Keyword flagged in message body

You Shouldn’t Have to Pay Extra for Advanced Threat Protection. *With SecureSMART, You Won’t.*

In today’s dangerous security landscape, we don’t believe that advanced threat protection is an optional extra you should have to pay for. We believe it’s mission critical for every business. That’s why we’ve made Advanced Threat Protection standard for all of our customers, keeping you safe from the new generation of targeted attacks.

By using SecureSMART, you can reduce your risk from this type of attack.

What do we do?

Once you sign up, you automatically get a standard set of policies to protect your business from certain attacks. This includes our industry leading spam and virus protection. You’ll also receive a customisable solution that protects against attacks targeted at your business.

According to the US Federal Bureau of Investigation, the international average business loss from successful social engineering email attacks like phishing and spear phishing is about $120,000 (c£82,000).* This is because organisations are often vulnerable to advanced threats that cloak themselves by using a variety of means and methods to escape detection.

* http://www.ic3.gov/media/2015/150827-1.aspx

What’s already set up?

Beyond our robust spam and virus protection, you are automatically set up to receive:

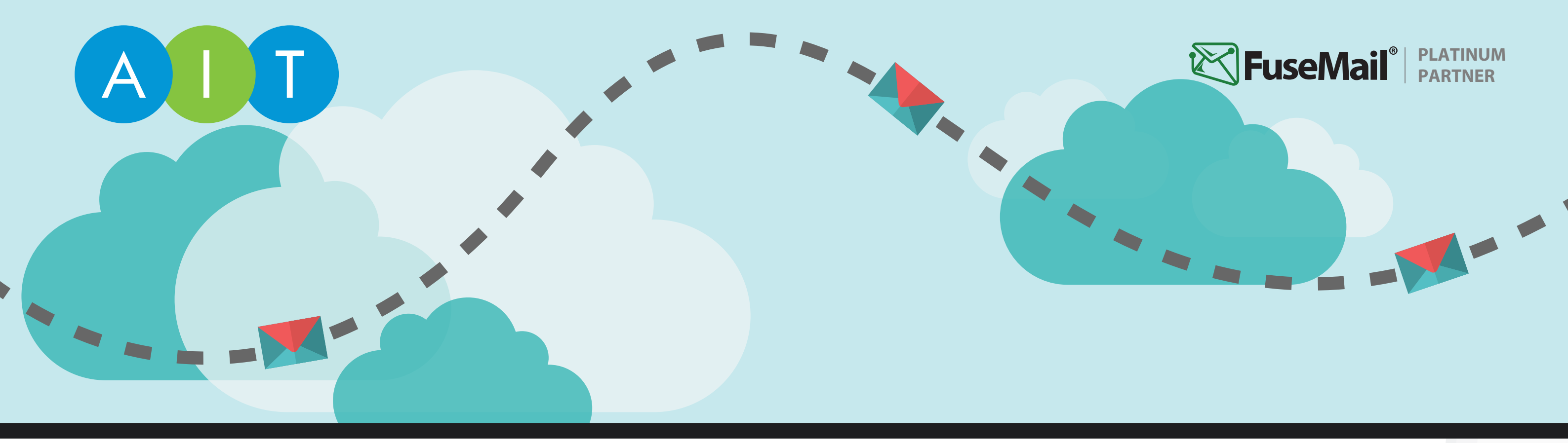
Email Spoofing Detection.
A check on every “friendly from” and “envelope from” email address. This ensures that all emails sent to you are aligned before they come through.

New domains checks.
The newer the domain, the more likely it is to be a threat. If we see a domain which jumps from sending zero or a small number of emails to thousands, we know this is suspicious and these emails are stopped..

Advanced VB Checker.
We stop known viruses contained within Office documents and PDFs, and also scan any seemingly innocent VB code to proactively identify “suspicious behaviour”.

AIT

AIT Ltd 2 Hawthorn Park, Coal Road, Leeds LS14 1PQ
0113 273 0300 • solutions@ait.co.uk
ait.co.uk



Start benefiting from these policies right away.

Call AIT today on 0113 273 0300.

What other types of policies can I set up for my organisation?

Other example policies you can set up free-of-charge within the SecureSMART portal:

Checks around your domain(s). We can quickly identify whether or not email coming from your domain is legitimate, to protect you from social engineering style attacks such as **phishing and spear phishing**.

Searches for keywords in emails coming from outside your domain. You can set up a policy to scan your emails for known **phishing keywords** such as BACS, wire transfer, bank transfer, credit card details and so on.

Regular expressions. It's simple to set up a series of regular expressions to detect how near a match your domain is to the sender's domain, which helps to protect your business from **social engineering attacks**.

Once an email is marked as suspicious, it is sent to quarantine and can easily be viewed in the administration portal under our smart email logs. Depending on how you have set up your end-user spam reports, you can opt to have these appear in the spam report or not. You can always give us a call, explain your needs, and we'll be happy to set it up for you or walk you through it.

Haven't set up SecureSMART, the industry leading email security platform?

Give us a call on 0113 273 0300 to book your demonstration or set up your free 14-day trial.