



## Looking for that extra level of email security and filtering for your Office 365 package?

Then take a look at 11 reasons why you should choose SecureSMART to enhance Office 365's email security offering.

**1 Not one, not two but three**  
SecureSMART offers industry leading levels of email security. Offering three antivirus engines on the system, guarantees a 100% known virus detection rate. We also guarantee a 99% spam detection rate and a service availability of 99.999%.

**2 ContinuitySMART**  
Are your emails completely reliant on Office 365 uptime? Not anymore! Use any device with a web browser to access your emails. With ContinuitySMART you can add Always On email continuity to your package to ensure that your business doesn't stop in the event of downtime.

**3 Data leakage protection**  
With SecureSMART you can search email bodies, attachments and headers for complete peace of mind. Configure your policies to search for PCIDSS (Payment Card Industry Data Security Standard) compliance or even check for confidential business information or customer databases. You can configure this yourself from simple lists to complex RegEx strings.

**4 System customisation**  
Our system allows complete customisation at administrator level. You can create dynamic rules as you need them - these are active instantly allowing you to react quickly when you need to.

**5**

## Minimise day to day administration – you've got better things to do!

Our system empowers end users to handle their own quarantine and continuity. They have the option to use automated quarantine reports or an online portal where they can release, reject, maintain their own allow and deny lists etc.

**6**

## Advanced VB Checker

We already stop known viruses contained within Office Documents and pdfs, but now we also scan seemingly innocent VB code within them to proactively identify 'suspicious behaviour'. This means that even if a document doesn't contain a virus, we can still identify code that performs potentially harmful actions, such as accessing the internet to download a virus, or accessing your customer's hard drives to add, delete or amend files.

**7**

## Large file handling

To help you manage mailbox sizes we strip large incoming (and outgoing if you choose) file attachments from emails. The file is replaced with a link in the email which the recipient can choose to click on to download the file. This protects your bandwidth, helps keep mailbox sizes manageable and helps your end users to receive/send email which would not get through most file size restrictions.

**8**

## Message alerts (SMS and email)

SecureSMART alerts system admins via email and/or text message if your inbound message queues go over a certain threshold (set by you). They can also be set to alert you if we are unable to connect to your firewall or if a user tries to send a message which has a virus in it.

**9**

## Advanced Threat Protection – as standard

Our customers get ATP as standard because viruses and spammers don't attack you based on your package limitations. Using Advanced Policies, SecureSMART gives you advanced threat protection from the more sophisticated threats out there. This includes protection from phishing, spear phishing, spoofing and more.

**10**

## Single, unified interface for ALL messages

Our email logs are the best in the business. Whether your emails are clean, spam, (high, medium or low risk), rejected or anything else, you can view and manage them through one area in your administration portal. No need to check different things under different menus.

**11**

## Take your security with you

SecureSMART is platform independent, so if you ever moved away from Office 365, you can take your email security and backups (14 or 90 days) with you.

