



Webroot from Modern Communications offers up to date and comprehensive protection in the cloud against malware threats associated with both email and web connectivity. Their comprehensive portfolio of services is feature rich and outperforms and offers greater functionality than that offered by the competition.

Key Reasons:

1. Webroot content control rules are applied instantly with a 30 second SLA. Webroot rules are easily edited and instantly applied.
2. Quarantine and searchable logs Webroot's Guarantee is that audit logs will be updated within 30 seconds of message reception for 99.9% of the time. If you have the Webroot system, you can respond immediately with all the necessary information at your finger tips, including SMTP receipts proving delivery, confirming as to whether an email has been accepted by the receiving server. This is an invaluable tool when people, both internal and external to your organization, claim not to have received an email, or to have sent one. This probably constitutes the majority of your support calls about email.
3. Webroot's Standard Spam Quarantine is 28 days as standard. This means that if someone is away for a fortnight and on day one they have a false positive, i.e. a legitimate email is designated as spam; there will be plenty of time to retrieve it from the quarantine area. False positives are 1:300 000.
4. Webroot scans with 5 x leading AV engines, thus you gain a higher level of protection for your users. This included protection against backscatter, a growing problem.
5. Advanced deep content scanning (meaning our rules engine can also look inside 300 different document types).
6. Webroot includes email content filtering (easy to use and very flexible rules engine) and TLS (Transport Layer Security) encryption as standard functions in the service.
7. End user portal – Webroot include 2 end user interfaces at no extra cost. The daily email report can be sent to end users worried about false positives, from which they can populate their own 'Allow list' and 'Deny list'. Alternatively, you can provide selected people an individual login for end users to have visibility of and check their own spam via a portal. These are optional as many prefer not to let end users choose their own allow lists.
8. Webroot has full LDAP integration included if you wish to utilise this function. This requires no plug-in locally on your network.
9. Webroot does not charge for adding additional domains
10. You are able to save and schedule any report configuration to suit your requirements. Thus, before a monthly (or daily/weekly) IT or management meeting you can have a PDF report combining all chosen reports sent to yourself for distribution or to a distribution list.

Reasons to Choose Webroot

Services provided:

- **Email filtering** – AV, anti-spam, content control via a comprehensive rules engine instantly applied, inappropriate imagery identified and stopped, scheduled reporting, logs of all activity/traffic available immediately, etc.
- **Email Archiving** – secure, unlimited storage archiving in mirrored data centers whilst allowing end users access to their own archive, thus removing the need for duplication on email servers and back-ups and enormous mailboxes. Speed of relay is reclaimed when email servers stop being used for storage. Compliant with Data Protection Act, etc
- **Email Encryption** – whilst TLS is a standard non-charged feature, desk top to desk top encrypted emails can also be mandated or selected for email with confidential content or attachment. Easy for end users and recipients alike.
- **Business continuity** – for when your server goes offline end users can access their email in a virtual mailbox via a web browser.
- **Deep Content Scanning** – ability to check into over 300 file types which is not possible to do with other services
- **Web Filtering** - web protection against malware and inappropriate web usage for office based and roaming users. Easy to use and very powerful.

For a free trial or demo please contact Julian Kirkpatrick on 0800 088 4008 or email webroot@modcomms.com