

Anti-Malware Security Features Checklist

Core Security Functionality

Rootkit Detection
 Virus and Worm Detection
 Trojan Horse Removal
 Adware and Spyware
 Detection
 Dual Use Software
 Detection or Containment
 Database Updates
 Behaviour-based Recognition
 Scanning Options
 Static Signature Detection
 Digital Signatures

Conformance to Protocol Standards

Scanning Incoming Traffic

Authentication

Password Management
 Password Compatibility
 Password Lockout

Cryptographic Standards

Encryption Algorithms

Advanced Encryption Standard
 (AES)
 Triple- Data Encryption
 Standard (3DES)

Key Establishment Algorithms

Rivest, Shamir, Adleman (RSA)
 Other algorithms based on
 exponentiation of finite fields
 Key Exchange Algorithm (KEA)
 Elliptic Curve algorithms

Digital Signature Algorithms

RSA
 Digital Signature Algorithm
 (DSA)
 Other algorithms based on
 exponentiation of finite
 fields
 Elliptic Curve Digital
 Signature Algorithm
 (ECDSA)

Hashing Algorithms

SHA-1
 SHA-224
 SHA-256
 SHA-384
 SHA-512

Cryptoperiod

Should be appropriate for
 the algorithm in use

Assurance Standards

Major Antivirus
 Certifications

Configurability

Changeable Default
 Values
 Logging

Usability

Configuration by Users
 Authentication by Users
 Maintenance by
 Administrators
 Failed logins
 Reconfiguration by
 Administrators
 False alarm
 Product compatibility
 Processing time

Manageability

Central Management
 Remote Management
 Authentication of
 Management Traffic
 Encryption of Management
 Traffic
 Product Removal

Scalability

Degree of Scalability