

NORMAN®
EmailProtection

IN THIS PRODUCTSHEET:

- » Benefits
- » Highlights
- » Features
- » System requirements

Norman Email Protection provides your organization with the tools to effectively counter security threats such as spam, viruses, fraud, phishing, botnets and other unauthorized communication.

With the proprietary anti-spam engine Sequential Content Analyzer (SCATM) - spam simply cannot get through. Norman Email Protection's multiple predictive and deterministic filters, as well as its artificial intelligence-based content analyzer, provide zero-day threat protection. On top of that, add various protocols filters and our proprietary Sender Reputation System (SRS), and you have an unbeatable combination that blocks threats at the network and content levels.

Norman Email Protection Benefits

- » Microsoft® Exchange and Active Directory Integration
- » DirectQuarantine™ Outlook Add-on
- » Industry-leading performance
- » Consistent 99% catch rate
- » Less than 0.001% false-positives
- » Official Microsoft® Certified Gold Partner – Complete Windows® compliance for your data center
- » Industry-leading content management and intelligent pattern detection
- » Sequential Content Analyzer - SCA™ – predictive technology to thwart zero-day attacks
- » Sieve-based full featured scripting engine for restriction-free policy management
- » End-user security options and quarantine management
- » 3 levels of granularity for maximum customization of all user & administrative settings
- » Leverages standard email clients, such as Microsoft Outlook® – No end-user training required
- » Complete inbound & outbound email scanning
- » system optimization, monitoring, and online back-ups – administrators can reduce their task overhead and increase their productivity
- » Easy to install, configure and use



HIGHLIGHTS

- Easy to install and operate
- Seamlessly integrates with Microsoft® Exchange, Lotus® Domino® and other standards-based email servers
- End-user quarantine management directly from their Outlook client
- Email Policy Management enables organizations to control what content can and cannot leave or enter their local network through email
- Highly granular features with specific permissions and settings for users/domains
- Multi-level administration
- Backed by Norman's proprietary and centrally managed email filtering technology, providing
 - Complete email protection
 - Inbound/outbound filtering and monitoring
 - No spam training
 - Powerful scripting engine

Norman Email Protection Features

Antispam and antivirus

- » 99% catch-rate
- » Less than 0.001% false-positives
- » Leading perimeter defense
 - Sender reputation system (SRS)
 - Blacklisting, whitelisting & advanced greylisting
 - Attachment & language filtering
- » Intelligent scanning and content analysis
 - Multi-layered content filtering based on both predictive and deterministic methods
 - Encrypted and archived files
 - File extension spoofing detection
- » Image spam detection – industry leading catch rates
- » Automatic updates every 15 minutes
- » Integrated Norman anti-virus
- » Auto-trusted lists

Mail server protection

- » BATV to eliminate backscatter spam
- » SMTP authentication
- » DKIM verification and signature support
- » Spoofing protection with sender policy framework (SPF) and DKIM
- » Directory harvesting defense
- » Open relay protection
- » Mail server cloaking
- » Supports opportunistic TLS
- » Enhanced PDF scanning

Administration and reporting

- » Intuitive interface with a choice of access methods – Windows® management console and web-based monitor console
- » Incremental Norman anti-virus updates (bandwidth reduction)
- » Granular policy settings

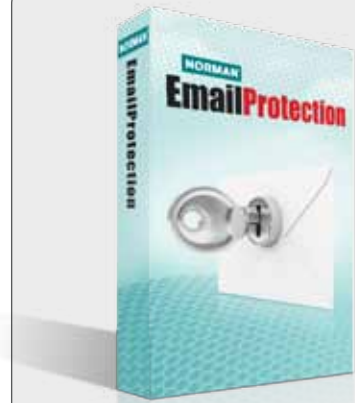
- » Separate controls for phishing policies
- » Real-time dashboard & system health report
- » System overview and security threats at a glance
- » Reports of server, domain and user statistics
- » Report scheduling
 - Automatically generate reports on a daily, weekly or monthly basis
- » Trend analysis and tracking of top issues

Policy management

- » Custom Sieve™ scripting – RFC-compliant for flexible policy implementation & foreign language support (UTF-8)
- » Full-message encryption with PGP® Universal Gateway Email
- » TLS and SSL support
- » Inbound, outbound and internal e-mail monitoring
- » Message audit logs

Quarantine management

- » Unique end-user interface – complete inbox control at the individual user level
- » Individual, customizable quarantine reports with one-click message release
- » Sort by security-threat level
- » Personalized filter settings
- » Phishing release capability
- » Permanently block individual senders



SYSTEM REQUIREMENTS

- Windows Server 2003, 2003R2, 2008 and 2008R2 (32-bit and 64-bit) and Windows Small Business Server (SBS) 2003 x86, 2008 x64 and 2011 x64
- Support for Microsoft SQL Server 2000 x86, 2005 x86/x64, 2008 x86/x64, 2008R2 x86/x64 Support for Microsoft SQL Server 2005 Express Edition x86
- 2.13GHz Dual Core with minimum 1024MB RAM
- 40GB IDE or SATA, 7200 RPM HD (mirrored is recommended)
- 100Mbit ethernet connection
- NTFS file system with Indexing disabled
- MDAC 2.8 SP1 or higher
- DNS servers accessible through the server
- IIS 6.0 or higher
- .NET Framework 3.5 SP1 or higher
- Internet Explorer 7+, Chrome or FireFox. Real-time reports require Adobe SVG Viewer



Microsoft Partner
Gold Independent Software Vendor (ISV)

Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services.

Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

www.norman.com

Norman SandBox® US Patent Number 7,356,736

NORMAN®