



Sophos Protection for SharePoint

Antivirus protection for SharePoint shared data servers

Sophos Protection for SharePoint provides you with protection for your business data and collaborative environment. We stop viruses, spyware, adware, suspicious files and potentially unwanted applications (PUAs). Our sophisticated content-filtering capabilities control the distribution of inappropriate or sensitive content in your environment.

Key benefits

- Secures your mission-critical business data from viruses, spyware, adware, suspicious files and potentially unwanted applications
- Identifies unknown malware, suspicious files and behaviors through built-in pre-execution intrusion prevention technologies
- Controls the distribution of inappropriate or sensitive content through sophisticated content-filtering policy controls
- Simplified administration of single servers or multi-server farms with our unique three-clicks-to-anywhere task based management console
- Rich actionable reporting provides immediate insights into threat activity, content filtering performance and quarantine status
- Detailed searchable logging provides deep forensic capabilities
- Includes an integrated quarantine manager for deleting, disinfecting or authorizing files
- Updates automatically with the latest protection from SophosLabs—a global network of threat analysis centers
- Scans on-access, on-demand and at scheduled times, affording maximum protection and flexibility
- Includes 24/7 **certified expert support**. Contact us anytime for one-to-one assistance

All-in-one threat protection and content control

Block malware Our integrated quarantine manager allows you to authorize, delete or disinfect malware, potentially unwanted applications, suspicious files and controlled content.

Zero-day threat protection Our software uses a built-in host intrusion prevention system (HIPS) to stop zero-day threats. Pre-execution detection identifies unknown malware, suspicious files and behavior.

Content filtering A sophisticated content filtering policy engine blocks the distribution of inappropriate or sensitive content. Our engine identifies content using file names, types or phrases and keywords contained within a file.

Up-to-date scanning On-access, scheduled and on-demand content scans protect your data from the latest threats, minimize overhead and provide a transparent end-user experience.

Simplified and automated management

Easy to manage With our web-based management console, it's simple to secure your SharePoint environment. The real-time dashboard offers point-and-click policy customization, efficient quarantine management and relevant, actionable reporting.

Staying informed Our rich, customizable reporting provides immediate insights into threat activity, content filtering performance and quarantine status. And our detailed searchable logs provide deep forensic capabilities.

Try it now for free

Register for a free 30-day evaluation at sophos.com/products.

Faster, better proactive protection using innovative technologies

Block viruses Genotype virus detection technology proactively blocks families of viruses even before specific virus signatures are available.

Identify threats early Our HIPS technology uses the antivirus engine to identify suspect programs and potential malware before they execute.

Rule verification We constantly validate our behavioral rule sets against an extensive library of legitimate applications to ensure accurate detection.

Not wanted, not allowed The scanning engine blocks potentially unwanted applications (PUAs). These are files known or suspected of being malicious, containing adware or consuming resources (such as utilities, toolbars and other suspicious applications).

Always up to date Small updates are released as frequently as every ten minutes—an advantage for companies wanting fast protection with low impact on network resources. We deliver more protection with less impact on your users—our scanning is now 15% faster than our last major upgrade. See how [AV-Comparatives rates our performance](#).

Content filtering and data loss prevention simplifies compliance

Policies to keep you optimized Prevent data loss, guard against legal liability and ensure productive use of your infrastructure. Our policies control a wide variety of file types including executables, media files and archives. We also control sensitive data such as binaries, source code, databases, contact lists and XML files.

Anti-spoofing technology Eliminate masquerading file types with true file type anti-spoofing technology (e.g., renaming an MP3 as a DOC).

Controls information Make corporate compliance easy with point-and-click content policies. Policies are based on administrator-defined keywords, phrases or regular expressions contained within popular file types. This allows for controlling the distribution of sensitive or confidential information.

Manages violations Quarantine, block and/or replace file violations with placeholder text.

Trusted support from the experts

Expert analysis Highly-skilled analysts in SophosLabs provide proactive rapid protection against known and unknown threats.

Around-the-clock threat scrutiny Through technology, global visibility of emerging threats, and integrated threat expertise, SophosLabs provides 24/7 research. Our fast global response allows your organization to protect itself from increasingly complex threats.

Always supported Only Sophos delivers around-the-clock, in-house, expert customer support that is [certified](#) and comes standard with every license.

Licensing

Sophos Protection for SharePoint is included in our Endpoint Protection—Enterprise license or can be purchased separately. [Compare](#)

Rich actionable reporting provides immediate insights into threat activity, content filtering performance and quarantine status





System requirements

Platforms supported

- ▶ SharePoint
- ▶ Microsoft SharePoint Services 3.0—32 bit and 64 bit, SP1 and SP2
- ▶ Microsoft SharePoint Server 2007—32 bit and 64 bit, SP1 and SP2
- ▶ Microsoft SharePoint Foundation 2010
- ▶ Microsoft SharePoint Server 2010 (all editions)
- ▶ Microsoft Search Server 2008
- ▶ Microsoft Search Server 2008 Express Edition
- ▶ Microsoft Office Project Server 2007

Operating system

- ▶ Windows Server 2003—32 bit and 64 bit, SP2 (all editions)
- ▶ Windows Server 2003 R2—32 bit and 64 bit, SP2 (all editions)
- ▶ Windows Small Business Server 2003—SP2
- ▶ Windows Small Business Server 2003 R2—SP2
- ▶ Windows Server 2008—32 bit and 64 bit, SP1 and SP2 (all editions)
- ▶ Windows Small Business Server (SBS) 2008—SP1 and SP2
- ▶ Windows Server 2008 R2, SP0 and SP1 (all editions*)
- ▶ Windows Small Business Server 2011
- ▶ SQL Server
- ▶ Microsoft SQL Server 2005 (all editions)—SP3
- ▶ Microsoft SQL Server 2008 (all editions)—SP1 and SP2
- ▶ Microsoft SQL Server 2008 R2 (all editions)

Hardware

- ▶ Disk space—1 GB minimum
- ▶ Memory—1 GB minimum (2 GB or higher recommended)
- ▶ CPU—1.5 GHz minimum (2 GHz or higher recommended)

*Server core editions are not supported (because they are not supported by SharePoint).

Try it now for free

Register for a free 30-day evaluation at sophos.com/products.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK
© Copyright 2011. Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.

Sophos Data Sheet 11.11v1.dNA

SOPHOS