Malwarebytes

ENDPOINT SECURITY

OPSWAT PARTNER CERTIFIED

OPSWAT GOLD CERTIFIED Anti-malware

OPSWAT BRONZE CERTIFIED Antiphishing

Advanced threat prevention

Malwarebytes Endpoint Security is an innovative platform that delivers powerful multi-layered defense for smart endpoint protection. Malwarebytes Endpoint Security enables small and large enterprise businesses to thoroughly protect against the latest malware and advanced threats—including stopping known and unknown exploit attacks.

Key Benefits

Blocks zero-hour malware

Reduces the chances of data exfiltration and saves on IT resources by protecting against zero-hour malware that traditional security solutions can miss.

Saves legacy systems

Protects unsupported programs by armoring vulnerabilities against exploits.

Increases productivity

Maintains end-user productivity by preserving system performance and keeping staff on revenue-positive projects.

Easy management

Simplifies endpoint security management and identifies vulnerable endpoints. Streamlines endpoint security deployment and maximizes IT management resources.

Scalable threat prevention

Deploys protection for every endpoint and scales as your company grows.

Detects unprotected systems

Discovers all endpoints and installed software on your network. Systems without Malwarebytes that are vulnerable to cyber attacks can be easily secured.

Core Technologies and Technical Features

Anti-Malware

Proactive anti-malware/anti-spyware scanning engine

Detects and eliminates zero-hour and known viruses, Trojans, worms, rootkits, adware, and spyware in real time to ensure data security and network integrity. Extends its protection to Windows Server operating systems.

Three system scan modes (Quick, Flash, Full)

Enables selection of the most efficient system scan based on endpoint security requirements and available system resources.

Malwarebytes ENDPOINT SECURITY

Advanced threat prevention

Malicious website blocking

Prevents access to known malicious IP addresses so that end users are proactively protected from downloading malware, hacking attempts, redirects to malicious websites, and malvertising.

File execution blocking

Prevents malicious threats from executing code and quarantines them to prevent malware attacks.

Malwarebytes Chameleon technology

Prevents malware from blocking the installation of Malwarebytes Anti-Malware for Business on an infected endpoint so the infection can be remediated.

Advanced malware remediation

Employs delete-on-reboot to remove persistent or deeply embedded malware.

Command-Line interface

Offers an alternative to the Malwarebytes GUI for control and flexibility, and enables importation and exportation of client settings for faster configuration.

XML logging

Provides reporting in a convenient human- and machine-readable format to simplify use by log analysis tools and data management.

MSI package

Ensures flexible installation.

Anti-Exploit

Four layers of exploit protection

Protection against Operating System (OS) security bypasses
Employs multiple advanced memory protection techniques to detect exploit attempts that try to bypass the native Operating System protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).

Memory caller protection
Incorporates multiple memory techniques to prevent exploit code from executing from specific or special memory areas.

Application behavior protection
Prevents protected applications from being exploited by sandbox escapes and memory mitigation bypasses by preventing the exploit from executing its malicious payload.

Application hardening
Uses proven techniques, including mandatory Data Execution Prevention (DEP) Enforcement, Bottom-Up ASLR Enforcement, and Anti-Heap Spraying, to generically harden applications to be less susceptible to vulnerability exploit attacks, even if patches and updates have not been applied.

Additional features

- 100% instant, proactive technology does not rely on blacklisting (signatures), whitelisting, sandboxing, or virtual machines
- No signature database—no need for daily updates
- Extremely light 3 MB footprint
- Compatible with anti-malware and antivirus products
- Compatible with old and end-of-life Windows operating systems, including Windows XP
- Install and forget—no management necessary, almost no end-user interaction required

Malwarebytes ENDPOINT SECURITY

Management Console

Multiple client management
Centrally manages thousands of clients from a single console and automatically updates signature databases on distributed clients to ensure viable protection.

Push install functionality
Enables push install of Malwarebytes products to distributed clients from a single console for easier deployment.

Comprehensive policy rules
Create customized policies and access for different user groups

Flexible scan scheduling
Enables scheduling of endpoint scans and automatic client installs for off-peak hours to conserve network bandwidth and resources.

Endpoint identification
Detects all endpoints and their software on the network so vulnerable endpoints without Malwarebytes can be secured.

Virtual deployment simulator
Enables simulated deployment on an endpoint before installation so potential issues can be addressed in advance.

Email notifications
Sends email notifications to specified administrators/users based upon detected threats and/or multiple system performance criteria.

Active Directory integration
Easily integrates and synchronizes with Microsoft Active Directory.

Unobtrusive end-user experience
Offers different end-user visibility settings to ensure the optimal balance between notification, end-user security awareness, and productivity.

Central reporting
Create system reports (with printable logs) to enable enhanced security management and sends security events to Syslog server (JSON format).

Threat View
Aggregates necessary data to evaluate potentially malicious threats on the distributed clients, and tracks user access to potentially malicious websites. Threat View also tracks activity by both IP address and user login while displaying the aggregated data in a convenient chart format for more efficient analysis.

Malwarebytes
ENDPOINT SECURITY

Tech Specs

Malwarebytes Anti-Malware for Business

Version: 1.80

Languages Available:
English, Bosnian, Bulgarian, Catalan, Chinese Simplified, Chinese Traditional, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Latvian, Lithuanian, Macedonian, Norwegian, Polish, Portuguese (Brazil), Portuguese (Portugal), Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Vietnamese.

Hardware Requirements
CPU: 800Mhz
RAM: 2 GB (Windows Server), 1 GB (Windows), 256+ MB (Windows XP)
Available disk space: 25 MB
Screen resolution: 800x600 or greater
Active internet connection for database and product updates

Software
Microsoft Internet Explorer 6 (or newer), Firefox, Chrome or Opera browser

Supported Operating Systems
Windows 10 ® (32-bit, 64-bit)
Windows 8.1® (32-bit, 64-bit)
Windows 8® (32-bit, 64-bit)
Windows 7® (32-bit, 64-bit)
Windows Vista® (32-bit, 64-bit)
Windows XP® (Service Pack 3 or later)
(32-bit only)
Windows Server 2012®/2012 R2® (32-bit, 64-bit) - excludes Server Core installation option
Windows Server 2008®/2008 R2® (32-bit, 64-bit) - excludes Server Core installation option)
Windows Server 2003® (32-bit only)

Additional Requirements for Managed Mode
Windows Installer 4.0 (Windows XP only, already included in other Windows versions)
.NET Framework 3.5 (Windows XP only)
.NET Framework 4.0 (Windows Vista, Windows 7, Windows 8)

Malwarebytes Anti-Exploit for Business

Version: 1.08

Languages Available:
English

Hardware Requirements:
CPU: 800MHz CPU
RAM: 2 GB (Windows Server and 64-bit systems), 1 GB (32-bit systems), 512+ MB (recommended for Windows XP)
Available disk space: 10 MB
Screen resolution: 800x600 or greater

Supported Operating Systems
Windows 10 ® (32-bit, 64-bit)
Windows 8.1® (32-bit, 64-bit)
Windows 8® (32-bit, 64-bit)
Windows 7® (32-bit, 64-bit)
Windows Vista® (32-bit, 64-bit)
Windows XP® (32-bit, 64-bit, Service Pack 3 or later)
Windows Server 2012®/2012 R2® (32-bit, 64-bit)
Windows Server 2008®/2008 R2® (32-bit, 64-bit)
Windows Server 2003®/2003 R2® (32-bit, 64-bit)

Additional Requirements for Managed Mode
Windows Installer 4.0 (Windows XP only, already included in other Windows versions)
.NET Framework 3.5

Malwarebytes
ENDPOINT SECURITY

Malwarebytes Management Console

Version: 1.6

Languages Available:
English

Hardware
CPU: 2 GHz (dual-core 2.6 GHZ or higher recommended)
RAM: 2 GB (4 GB recommended)
Available Disk Space: 10 GB (20 GB recommended)
Screen Resolution: 1024x768 or greater
Active Internet connection for database and product updates

Software
Microsoft Internet Explorer 6 (or newer), Firefox, Chrome or Opera browser
.NET Framework 3.5
.NET Framework 4.0

Supported Operating Systems
(Excludes Server Core installation option)
Windows Server 2012®/2012 R2® (64-bit)
Windows Server 2008®/2008 R2® (32-bit, 64-bit)

Supported Microsoft SQL Servers
SQL Server 2014
SQL Server 2012
SQL Server 2008 (for larger installations)

Included Microsoft SQL Server
SQL Server 2008 Express (shipped with product, 10 GB maximum database size limitation)

About Malwarebytes
Malwarebytes protects consumers and businesses against malicious threats that escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware, the company's flagship product, has a highly advanced heuristic detection engine that has removed more than five billion malicious threats from computers worldwide. More than 70,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the company is headquartered in California with offices in Europe, and a global team of researchers and experts. For more information, please visit us at www.malwarebytes.com.