

Anti-exploit for business

Innovative exploit mitigation delivers four layers of protection

WHAT IT DOES FOR YOU

- Protects browsers, including Internet Explorer, Firefox, Chrome, and Opera
- Protects browser components, including Java and Flash
- Defends against drive-by download attacks
- Shields vulnerable applications, including Microsoft Office, PDF readers, and media players
- Blocks unknown and known exploit kits

Stops unknown and known exploit attacks and protects application and browser vulnerabilities

Malwarebytes Anti-Exploit for Business protects your business from one of the most advanced cyber attacks: zero-day exploits targeting browser and application vulnerabilities. Its proprietary technology wraps vulnerable programs in four defensive layers that prevent an exploit from installing its payload, or even executing initial shellcode. And, unlike an antivirus solution, which is focused on what (signatures) is being delivered, Malwarebytes Anti-Exploit for Business examines how it is being delivered, providing a robust, specialized endpoint defense that prevents ransomware, Advanced Persistent Threats (APTs), financial malware, and corporate cyber-espionage attacks, which exploit software vulnerabilities.

Key Benefits

Offers your business the most complete exploit mitigation solution. No other endpoint exploit mitigation solution provides four layers of protection. These layers (operating system bypasses, malicious memory caller, application behavior, and application hardening) work together to block exploits instantly. In the first stage of the attack, they prevent shellcode execution. In the second stage, they protect against memory calls, sandbox escapes, and memory mitigation bypasses.



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 Anti-Exploit for Business technology doesn't use a signature database like traditional endpoint security, so it doesn't require frequent updates and conserves network bandwidth. Its small 3 MB footprint and lean client further minimizes use of system resources. And, unlike other exploit mitigation solutions, Malwarebytes Anti-Exploit for Business doesn't waste valuable CPU cycles employing virtual machines. This makes Malwarebytes Anti-Exploit for Business the perfect solution for older hardware and EOL operating systems like Microsoft Windows XP, which will no longer be supported with security updates.

Hands-free, maintenance-free

Malwarebytes Anti-Exploit for Business uses advanced technology that doesn't employ blacklisting/whitelisting or sandboxing, so it needs far less management by the IT department than traditional endpoint security. Malwarebytes Anti-Exploit for Business also requires minimal or no end-user interaction. Install it and forget it.

Four layers of exploit protection

Trigger vulnerability



Execute shellcode



Bypass OS & DEP



Execute payload



Execute malicious actions

Layer 1: Application hardening

Employs techniques that harden outdated or unpatched applications to be less susceptible to exploit attacks.

Layer 2: Protection against OS security bypass

Uses advanced memory techniques to prevent exploit shellcode from executing by detecting attempts to bypass Data Execution Prevention (DEP) or use ReturnOriented Programming (ROP) gadgets.

Layer 3: Malicious memory caller protection

Incorporates multiple 32- and 64-bit memory exploit mitigation techniques to prevent exploits from executing payload code from malicious memory areas.

Layer 4: Application behavior protection

Blocks sandbox escapes such as Java exploits, as well as exploits that abuse weak application design in Word, PowerPoint, and others. Last defense against exploits that bypass memory corruption mitigation.

TECH SPECS

Endpoint system requirements

Version: 1.08

Languages available: English

Supported operating systems:

Windows 10® (32/64-bit)

Windows 8.1® (32/64-bit)

Windows 8® (32/64-bit)

Windows 7® (32/64-bit)

Windows Vista® (32/64-bit)

Windows XP® (Service Pack 3 or later) (32/64-bit)

Windows Server 2012®/2012 R2® (64-bit)

Windows Server 2008®/2008 R2® (32/64-bit)

Windows Server 2003® (32/64-bit)

Additional requirements for managed mode:

Windows Installer 4.0 (Windows XP only, already included in other Windows versions)

.NET Framework 3.5

Hardware requirements:

2048 MB (64-bit/server OS), 1024 MB (32-bit OS, 256 MB or more for Windows XP)

800 MHz CPU minimum

10 MB of free hard disk space

800x600 or greater screen resolution

Management Console system requirements

(managed mode only)

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:

.NET Framework 3.5

Supported operating systems:

(excludes Server Core installation option)

Windows Server 2012 R2 (64-bit)

Windows Server 2012 (64-bit)

Windows Server 2008 (32/64-bit)

Windows Server 2008 R2 (32/64-bit)

Supported Microsoft SQL servers:

SQL Server 2014

SQL Server 2012

SQL Server 2008 (for larger installations)

SQL Express 2008 (shipped with product, subject to review, 10 GB maximum database size limitation)



malwarebytes.com/business



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes protects consumers and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware, the company's flagship product, has a highly advanced heuristic detection engine that removed more than five billion malicious threats from computers worldwide. More than 10,000 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.

Copyright © 2016, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.