Malwarebytes ANTI-EXPLOIT FOR BUSINESS

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.

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

Features
Four layers of exploit protection

1. Protection against Operating System (OS) security bypasses

Employs multiple advanced memory protection techniques to detect exploit attempts which try to bypass the native Operating System protections such Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR)

2. Memory caller protection

Incorporates multiple memory techniques to prevent exploit code from executing from memory, such as from specific or special memory areas

3. 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

4. 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.

Innovative exploit mitigation delivers four layers of protection

Additional Features
• 100% instant, proactive technology does not rely on blacklisting (signatures), white-listing, 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

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, Application Hardening) work together to block exploits instantly, both in the first stage of the attack, preventing shellcode execution, and in the second stage, memory calls and sandbox escapes and memory mitigation bypasses.

Smaller, lighter, and easier to use
Malwarebytes Anti-Exploit for Business technology doesn't use a signature database like traditional endpoint security, so it doesn't require frequent updates, conserving 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 relies on 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.
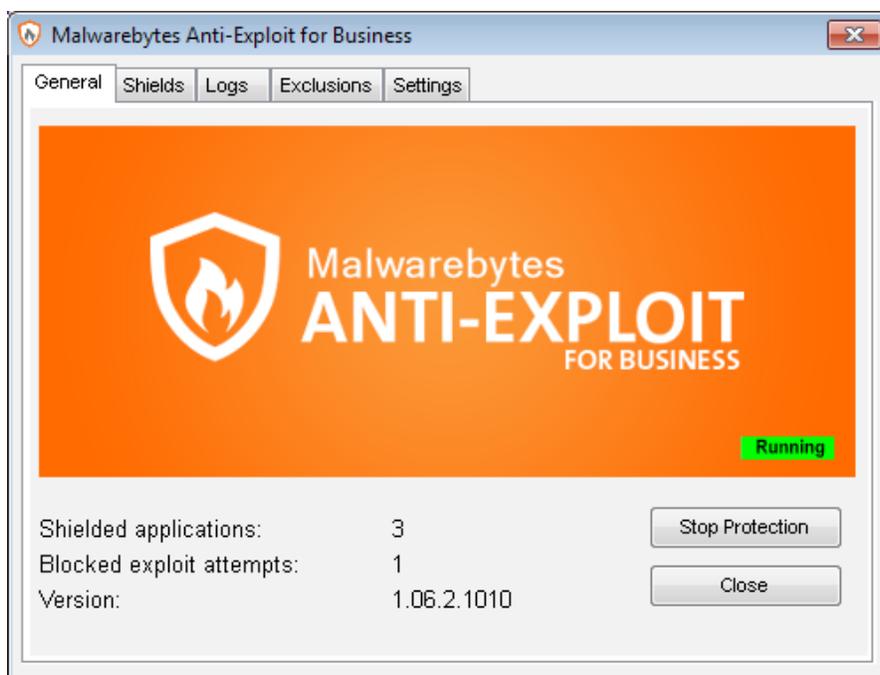
Malwarebytes ANTI-EXPLOIT

FOR BUSINESS

Innovative exploit mitigation delivers four layers of protection

Protected browsers and applications

Browsers
Internet Explorer
Mozilla Firefox
Google Chrome
Opera
And Others

Browser components
Java
Adobe Reader
Flash
Shockwave
Any other browser add-on the
runs in the browser process space

PDF readers
Adobe Acrobat Reader
Adobe Acrobat PRO
Foxit Reader

Applications
Microsoft Word
Microsoft Excel
Microsoft PowerPoint

Media players
Windows Media Player
(wmplayer)
Windows Media Player
(wmplayer2)
QuickTime
VLC Player
Winamp

Tech Specs

Endpoint System Requirements

Version: 1.06

Languages Available:
English

Supported Operating Systems:
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 2008®/2008 R2® (32/64-bit)
Windows Server 2003® (32/64-bit)
Windows Server 2012®/2012 R2® (64-bit)

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)

Hardware Requirements:
1024 MB (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: 1.5
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
.NET Framework 4.0

Supported Operating Systems:
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 Express 2008 (shipped with product, subject to review, 10 GB
maximum database size limitation)
SQL Server 2008 (for larger installations)