



Malwarebytes ENDPOINT SECURITY



Eine leistungsstarke mehrstufige Verteidigung schützt Endpunkte auf intelligente Weise.

Schützt vor neuer und Exploit-basierter Schadsoftware

Sichern Sie sich Malwarebytes Anti-Malware for Business und Malwarebytes Anti-Exploit for Business zusammen in einem leistungsstarken und kosteneffektiven Paket. Schützen Sie Ihre Endpunkte mit einer mehrstufigen Verteidigung von Malwarebytes. Diese bekämpft die aktuellsten und gefährlichsten Formen von Schadsoftware. Wir bieten Ihnen eine intelligente Lösung für Ihre Sicherheitsherausforderungen.

Malwarebytes Anti-Malware for Business

Antischadsoftware/Anti-Spyware

Erkennt und entfernt bekannte und unbekannte Viren, Trojaner, Würmer, Rootkits, Adware und Spyware in Echtzeit, um die Datensicherheit und Netzwerkintegrität sicherzustellen. Erweitert den Schutz auf Windows-Server-Betriebssysteme.

Blockierung bössartiger Websites

Verhindert den Zugang zu bekannten bössartigen IP-Adressen, sodass Endnutzer proaktiv vor dem Herunterladen von Schadsoftware, Hacker-Angriffen, Umleitungen auf bössartige Websites und „Malvertising“ geschützt werden.

Blockierung der Dateiausführung

Hindert bössartige Bedrohungen daran, Code auszuführen, und verschiebt diese in Quarantäne, um Schadsoftwareangriffe zu verhindern.

Chameleon-Technologie von Malwarebytes

Hindert Schadsoftware daran, die Installation von Malwarebytes Anti-Malware for Business auf einem infizierten Endpunkt zu blockieren, sodass die Infektion beseitigt werden kann.

Drei Modi für den System-Scan (Quick, Flash, Full)

Ermöglicht die Auswahl des effizientesten System-Scans je nach den Anforderungen für die Endpunktsicherheit und den verfügbaren Systemressourcen.

Fortschrittliche Beseitigung von Schadsoftware

Löscht Dateien beim Neustart, um hartnäckige oder tief eingebettete Schadsoftware zu entfernen.

Befehlszeilenschnittstelle

Stellt eine Alternative zur grafischen Benutzeroberfläche von Malwarebytes dar und bietet ein hohes Maß an Kontrolle und Flexibilität. Durch die Möglichkeit des Imports und Exports von Client-Einstellungen wird die Konfiguration beschleunigt.

XML-Protokollierung

Unterstützt die Erstellung von Berichten in einem praktischen visuell und maschinell lesbaren Format, um deren Verwendung durch Tools zur Protokollanalyse und für die Datenverwaltung zu vereinfachen.

MSI-Paket

Stellt eine flexible Installation sicher.



Malwarebytes Anti-Exploit For Business

Exploit-Schutz auf vier Ebenen

1. Schutz vor der Umgehung von Sicherheitsfunktionen des Betriebssystems

Erkennt mithilfe verschiedener fortschrittlicher Technologien zum Speicherschutz Exploit-Angriffe, über die versucht wird, die systemeigenen Sicherheitsfunktionen des Betriebssystems wie die Datenausführungsverhinderung und die zufällige Anordnung des Layouts des Adressraums zu umgehen.

2. Schutz vor Speicheraufrufen

Bezieht verschiedene Speichertechnologien ein, um Exploit-Code an der Ausführung aus bestimmten oder speziellen Speicherbereichen zu hindern.

3. Schutz des Anwendungsverhaltens

Schützt Anwendungen vor Sandkastenausbrüchen und Speicherausgleichsumgehungen. Das Tool hindert Exploits daran, ihre bösartigen Inhalte auszuführen.

4. Anwendungshärtung

Verwendet bewährte Technologien wie die Erzwingung der Datenausführungsverhinderung, die Erzwingung der zufälligen Anordnung des Layouts des Adressraums und die Bekämpfung des Heap-Sprayings. Auf diese Weise werden Anwendungen gehärtet, sodass sie generell weniger anfällig für Exploit-Angriffe auf Schwachstellen sind. Dies gilt selbst dann, wenn keine Patches und Aktualisierungen angewendet wurden.

Weitere Merkmale

- Zu 100 % sofort wirksame und proaktive Technologie – keine Abhängigkeit von schwarzen Listen (Signaturen), weißen Listen, Sandkästen oder virtuellen Computern
- Keine Signaturdatenbank – kein Erfordernis täglicher Aktualisierungen
- Extrem geringer Platzbedarf von nur 3 MB
- Kompatibilität mit Antischadsoftware und Antivirenprogrammen
- Kompatibilität mit alten und nicht mehr aktualisierten Windows-Betriebssystemen wie Windows XP
- Installieren und vergessen – keine Verwaltung und nahezu keine Endnutzereingriffe erforderlich

Vorteile

Bietet Ihrem Unternehmen die umfassendste Lösung zur Exploit-Abwehr

Keine andere Lösung zur Exploit-Abwehr für Endpunkte bietet vier Schutzebenen. Diese Ebenen (Schutz vor der Umgehung von Sicherheitsfunktionen des Betriebssystems, Schutz des Anwendungsverhaltens, Anwendungshärtung) arbeiten zusammen, um Exploits sofort zu blockieren. In der ersten Phase des Angriffs wird die Shellcode-Ausführung blockiert. In der zweiten Phase werden Speicheraufrufe, Sandkastenausbrüche und Speicherausgleichsumgehungen verhindert.

Kleiner, leichter und benutzerfreundlicher

Im Gegensatz zu herkömmlichen Endpunktsicherheitsprogrammen stützt sich die Technologie von Malwarebytes Anti-Exploit for Business auf keine Signaturdatenbank. Dadurch entfällt das Erfordernis häufiger Aktualisierungen und die Netzwerkbandbreite wird geschont. Durch den geringen Platzbedarf von nur 3 MB und den schlanken Client wird die Auslastung der Systemressourcen weiter minimiert. Im Gegensatz zu anderen Lösungen zur Exploit-Abwehr verschwendet Malwarebytes Anti-Exploit for Business außerdem keine wertvollen CPU-Zyklen durch den Einsatz virtueller Computer. Damit ist Malwarebytes Anti-Exploit for Business die ideale Lösung für ältere Hardware und Betriebssysteme wie Microsoft Windows XP, die nicht mehr durch Sicherheitsaktualisierungen unterstützt werden.

Geringer Arbeitsaufwand, wartungsfrei

Die fortschrittliche Technologie von Malwarebytes Anti-Exploit for Business stützt sich nicht auf weiße/schwarze Listen oder Sandkästen. Dadurch muss die IT-Abteilung weit weniger Verwaltungsaufgaben ausführen als bei herkömmlichen Endpunktsicherheitsprogrammen. Bei Malwarebytes Anti-Exploit for Business sind außerdem nur minimale oder keine Endnutzereingriffe erforderlich. Nach der Installation müssen Sie sich um nichts mehr kümmern.



Malwarebytes Management Console

Merkmale und Vorteile

- Ermöglicht die Push-Installation von Malwarebytes-Produkten auf verteilten Clients über eine einzige Konsole. Dies vereinfacht die Bereitstellung.
- Ermöglicht die Planung von Endpunkt-Scans und automatische Client-Installationen in Zeiträumen mit geringerer Auslastung. Hierdurch werden Netzwerkbandbreite und Ressourcen geschont.
- Erkennt alle Endpunkte und deren Software im Netzwerk. Endpunkte ohne Malwarebytes, die für Cyberangriffe anfällig sind, können so gesichert werden.
- Ermöglicht die simulierte Bereitstellung auf einem Endpunkt vor der Installation. Dadurch können potenzielle Probleme im Vorfeld geklärt werden.
- Sendet E-Mail-Benachrichtigungen an ausgewählte Administratoren/Nutzer – je nach den erkannten Bedrohungen und/oder ausgehend von verschiedenen Kriterien für die Systemleistung.
- Arbeitet parallel zu den Verwaltungskonsolen anderer Sicherheitsanbieter, ohne dass Konflikte auftreten oder vorhandene Endpunktsicherheits-Clients ersetzt werden müssen.
- Aktualisiert Signaturdatenbanken auf verteilten Clients automatisch, um einen durchgängigen Schutz sicherzustellen.
- Unterstützt individuelle Richtlinien und den Zugriff auf verschiedene Nutzergruppen.
- Bietet unterschiedliche Einstellungen für die Endnutzeranzeige, um einen optimalen Ausgleich zwischen Benachrichtigung, Sicherheitsbewusstsein der Endnutzer und Produktivität sicherzustellen.
- Stellt eine robuste Systemberichterstellung (mit druckbaren Protokollen) für eine erweiterte Sicherheitsverwaltung bereit.
- Sendet Sicherheitsereignisse an den Syslog-Server (im JSON-Format).

Threat View

Aggregiert die erforderlichen Daten, um potenziell bösartige Bedrohungen auf den verteilten Clients auszuwerten, und verfolgt den Nutzerzugriff auf potenziell bösartige Websites. Threat View verfolgt außerdem die Aktivitäten im Zusammenhang mit der IP-Adresse und der Nutzeranmeldung. Die aggregierten Daten werden zur effizienteren Analyse in einem praktischen Tabellenformat angezeigt.



Malwarebytes ENDPOINT SECURITY

Technische Spezifikationen Malwarebytes Anti-Malware for Business

Version: 1.80

Verfügbare Sprachen:

Englisch, Bosnisch, Bulgarisch, Katalanisch, Chinesisch (vereinfacht), Chinesisch (traditionell), Kroatisch, Tschechisch, Dänisch, Niederländisch, Estnisch, Finnisch, Französisch, Deutsch, Griechisch, Hebräisch, Ungarisch, Italienisch, Lettisch, Litauisch, Mazedonisch, Norwegisch, Polnisch, Portugiesisch (Brasilien), Portugiesisch (Portugal), Rumänisch, Russisch, Serbisch, Slowakisch, Slowenisch, Spanisch, Schwedisch, Thai, Türkisch, Vietnamesisch.

Hardwareanforderungen

CPU: 800 MHz
RAM: 1 GB Client; 2 GB Server
Speicherplatz: 25 MB
Bildschirmauflösung: Min. 800 x 600
Aktive Internetverbindung für Datenbank- und Produktaktualisierungen

.NET Framework 4.0 (Windows Vista, Windows 7, Windows 8)

Malwarebytes Anti-Exploit for Business

Version: 1.07

Verfügbare Sprachen:

Englisch

Hardwareanforderungen:

CPU: 800 MHz
RAM: 1024 MB (512 MB oder mehr empfohlen)
Speicherplatz: 10 MB
Bildschirmauflösung: Min. 800 x 600

Software

Browser Microsoft Internet Explorer (ab Version 6), Firefox, Chrome oder Opera

Unterstützte Betriebssysteme

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[®] (ab Service Pack 3)
(nur 32 Bit)
Windows Server 2012/2012 R2
(ohne Serverkerninstallationsoption)
Windows Server 2008/2008 R2
(ohne Serverkerninstallationsoption)
Windows Server 2003 (nur 32 Bit)

Zusätzliche Anforderungen für den verwalteten Modus

Windows Installer 4.0 (nur Windows XP, in anderen Windows-Versionen bereits enthalten)
.NET Framework 3.5
.NET Framework 4.0 (Windows Vista, Windows 7, Windows 8)

Unterstützte Betriebssysteme

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, ab Service Pack 3)
Windows Server 2008[®]/2008 R2[®] (32 Bit, 64 Bit)
Windows Server 2012[®]/2012 R2[®] (64 Bit)
Windows Server 2003 (nur 32 Bit)

Zusätzliche Anforderungen für den verwalteten Modus

Windows Installer 4.0 (nur Windows XP, in anderen Windows-Versionen bereits enthalten)
.NET Framework 3.5



Malwarebytes ENDPOINT SECURITY

Malwarebytes Management Console (nur verwalteter Modus)

Version: 1.6

Verfügbare Sprachen:

Englisch

Hardware

CPU: 2 GHz (Dual Core 2,6 GHz oder mehr empfohlen)

RAM: 2 GB (4 GB empfohlen)

Verfügbarer Speicherplatz: 10 GB (20 GB empfohlen)

Bildschirmauflösung

Min. 1024 x 768

Aktive Internetverbindung für Datenbank- und

Produktaktualisierungen

Software

Browser Microsoft Internet Explorer (ab Version 6), Firefox,

Chrome oder Opera

.NET Framework 3.5

.NET Framework 4.0

Unterstützte Betriebssysteme

(ohne Serverkerninstallationsoption)

Windows Server 2012 R2 (64 Bit)

Windows Server 2012 (64 Bit)

Windows Server 2008 (32/64 Bit)

Windows Server 2008 R2 (32/64 Bit)

Unterstützte Microsoft SQL Server

SQL Server 2014

SQL Server 2012

SQL Server 2008 (für größere Installationen)

SQL Express 2008 (im Lieferumfang enthalten, wird überprüft, Datenbankgröße auf max. 10 GB begrenzt)