

Leistungsstarke Verteidigung gegen Schadsoftware

Kein ausreichender Netzwerkschutz durch Ihre aktuelle Antivirenlösung allein

Mit der zunehmenden Häufigkeit und Raffinesse von Cyberangriffen erkennen IT-Manager allmählich, dass eine einzige Antivirentechnologie für ihr Unternehmen nicht ausreicht. Ihr Netzwerk ist dadurch für Angriffe anfällig. Jeder Endpunkt benötigt mehrere Ebenen der Erkennung und Beseitigung von Schadsoftware, um einen vollständigen Schutz sicherzustellen.

Malwarebytes Anti-Malware for Business erfüllt dieses Erfordernis. Malwarebytes Anti-Malware for Business bietet einen schnellen und schlanken Schutz vor Schadsoftware zur Ergänzung Ihrer aktuellen Endpunktsicherheitslösung. Unsere robuste heuristische Scan-Engine erkennt und entfernt Zero-Hour-Schadsoftware, die von anderen Sicherheitslösungen unerkannt bleibt. Dies verbessert Ihre Sicherheitslage und schließt Lücken bei der Erkennung bösartiger Inhalte.

Die zentrale Verwaltungskonsole von Malwarebytes vereinfacht und rationalisiert die Verwaltung der Endpunktsicherheit. Auf einem einzigen Bildschirm können Sie bis zu Tausende von verteilten Malwarebytes-Clients aktualisieren, überwachen und verwalten.

Malwarebytes Anti-Malware for Business ist nicht einfach eine andere Lösung – es ist der nächste Schritt bei der Endpunktsicherheit für Unternehmen.

Merkmale und Vorteile

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 bösartiger Websites

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

Blockierung der Dateiausführung

Hindert bösartige 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.

Leistungsstarke Verteidigung gegen Schadsoftware

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 Management Console

- 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.

Leistungsstarke Verteidigung gegen Schadsoftware

Technische Spezifikationen

Version: 1.80

Verfügbare Sprachen:

Englisch, Arabisch, 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.

Endpunktsystemanforderungen

Hardware

CPU: 800 MHz
RAM: 2048 MB (64-Bit-/Server-Betriebssystem), 1024 MB (32-Bit-Betriebssystem, außer 256 MB für Windows XP)
Speicherplatz: 25 MB
Bildschirmauflösung: Min. 800 x 600
Aktive Internetverbindung für Datenbank- und Produktaktualisierungen

Zusätzliche Anforderungen für den verwalteten Modus

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

Softwareanforderungen

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)

Systemanforderungen für die Verwaltungskonsole

Version: 1.6

Verfügbare Sprachen: Englisch

Hardware:

CPU: 2 GHz (Dual Core 2,6 GHz empfohlen)
RAM: 2048 MB (4096 MB empfohlen)
Speicherplatz: 10 GB (20 GB empfohlen)
Bildschirmauflösung: Min. 1024 x 768
Aktive Internetverbindung für Datenbank- und Produktaktualisierungen

Software:

.NET Framework 3.5
Windows Installer 4.5
Browser Microsoft® Internet Explorer (ab Version 6), Firefox, Chrome oder Opera

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)