

Malwarebytes Endpoint Protection

Schutz vor modernen Bedrohungen

TECHNISCHE MERKMALE

Internetschutz

Verhindert den Zugang zu bösartigen Websites, Werbenetzwerken, Scammer-Netzwerken und gefährlichen Umgebungen.

Anwendungshärtung

Verringert die Angriffsfläche und macht den Computer robuster. Fingerprinting-Versuche durch fortschrittliche Angriffe werden proaktiv erkannt.

Exploit-Abwehr

Erkennt und blockiert Versuche, Schwachstellen auszunutzen und Code dezentral auf Endpunkten auszuführen, auf proaktive Weise.

Schutz des Anwendungsverhaltens

Verhindert, dass Anwendungen zum Infizieren des Endpunkts genutzt werden.

Anomalieerkennung

Erkennt Viren und Schadsoftware proaktiv durch Techniken des maschinellen Lernens.

Payload-Analyse

Erkennt komplette Familien von bekannter und relevanter Schadsoftware mit heuristischen und verhaltensbasierten Regeln.

Ransomware-Abwehr

Erkennt und blockiert Ransomware über eine Technologie zur Verhaltensüberwachung.

Die effektivste Schutzstrategie beginnt mit einer proaktiven Prävention, aber es gibt kein Patentrezept zur optimalen Verhinderung von Infizierungen. Aus diesem Grund raten Sicherheitsexperten davon ab, Unternehmensendpunkte nur mit einer einzigen Technologie oder Technik zu schützen. Für eine effektive Prävention ist ein mehrstufiger Ansatz erforderlich, der sowohl die Bedrohungen von heute als auch die von morgen berücksichtigt.

Malwarebytes Endpoint Protection ist eine fortschrittliche Lösung zur Bedrohungsprävention für Endpunkte, bei der ein mehrstufiger Ansatz mit verschiedenen Erkennungstechniken zum Einsatz kommt. Unternehmen erhalten dadurch einen umfassenden Schutz vor Angriffen durch bekannte und unbekannte Schadsoftware, Ransomware und Zero-Hour-Bedrohungen. In einem einzigen Agenten konzentriert reduziert Malwarebytes Endpoint Protection die Komplexität und die Kosten, die häufig mit der Bereitstellung von mehreren Einzellösungen verbunden sind.

Die branchenweit beste informationsgestützte Telemetrie sorgt für eine äußerst hohe Effizienz der Erkennungstechniken von Malwarebytes Endpoint Protection. Malwarebytes ist der Goldstandard für eine vollständige und gründliche Entfernung von Bedrohungen, wenn vorhandene Sicherheitslösungen versagen. Jeden Tag laden 500.000 Privatanwender und Unternehmen die Technologie von Malwarebytes herunter – diese Zahl spricht eine deutliche Sprache. Malwarebytes findet und entfernt täglich 3 Millionen Infizierungen. Diese einzigartige Telemetrie vermittelt umfangreiche Erkenntnisse über Bedrohungen und Techniken, die in Benutzerumgebungen erforderlich sind. Wir erhalten dadurch ein besseres Verständnis davon, warum diese Angriffe effektiv sind und wie sie am besten in den Griff zu bekommen sind.

Threat	Category	Status	Type	Location	Endpoint	Detection Time
PUP.Optional.Dadfish	PUP	Quarantined	File			06/05/2017 - 10:51:17 AM
Trojan.Killbox	Malware	Quarantined	File			06/05/2017 - 10:51:13 AM
PUP.Optional.Amazon1But...	PUP	Quarantined	File			06/05/2017 - 10:18:16 AM
Spyware.Zeus	Malware	Quarantined	File			06/05/2017 - 07:41:40 AM
PUP.Optional.Amazon1But...	PUP	Quarantined	File			06/05/2017 - 07:41:34 AM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-		06/02/2017 - 03:10:57 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-		06/02/2017 - 03:08:08 PM
Trojan.Killbox	Malware	Quarantined	File			06/02/2017 - 02:32:46 PM
PUP.Optional.Advancedsty...	PUP	Quarantined	File			06/02/2017 - 02:32:43 PM
Ransom.Carber	Ransomware	Quarantined	File			06/02/2017 - 02:31:26 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-		06/02/2017 - 02:30:57 PM
Malware.Exploit.Agent.Gen...	Exploit	Blocked	Exploit	-		06/02/2017 - 02:29:42 PM
Ransom.Filecoder	Ransomware	Quarantined	File			06/02/2017 - 02:28:11 PM
Ransom.WannaCrypt	Ransomware	Quarantined	File			06/02/2017 - 02:17:23 PM
web	Website	Blocked	OutboundConnection			06/02/2017 - 02:16:29 PM
web	Website	Blocked	OutboundConnection			06/02/2017 - 02:16:29 PM
web	Website	Blocked	OutboundConnection			06/02/2017 - 02:16:29 PM

Echtzeitschutz über die Cloud-Konsole von Malwarebytes

Wichtigste Vorteile

Techniken für eine mehrstufige Erkennung

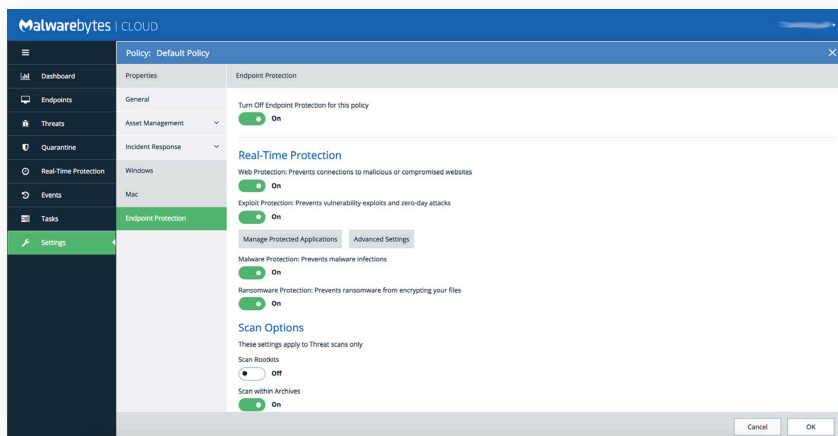
Bei Malwarebytes Endpoint Protection kommen verschiedene Techniken zum Einsatz, um Angriffe in allen Phasen der Angriffskette zu identifizieren und abzuwehren. Die dabei verwendeten signaturfreien und Abgleichstechnologien sind äußerst effektiv und wirken sowohl vor als auch nach der Ausführung von Schadsoftware. Durch die Nutzung der besten informationsgestützten Telemetrie werden die Techniken für eine Erkennung vor der Ausführung von Schadsoftware fortlaufend aktualisiert, um Bedrohungen so früh wie möglich in der Infizierungskette zu erkennen.

Vollständige und gründliche Entfernung von Bedrohungen

Malwarebytes Endpoint Protection nutzt unsere Linking-Engine-Technologie, um nicht nur den primären Bedrohungs-Payload, sondern sämtliche Spuren von Infizierungen und verbundenen Artefakten zu entfernen. Dieser signaturfreie Ansatz beschleunigt die Suche nach Bedrohungen und spart Zeit ein, die normalerweise für das Bereinigen und Reimaging von Endpunkten aufgewendet werden muss.

Cloudfähiges Management

Malwarebytes Endpoint Protection wird über die cloudbasierte Endpunktmanagementplattform von Malwarebytes bereitgestellt. Diese Cloud-Plattform reduziert die Komplexität, sodass Malwarebytes Endpoint Protection und andere Lösungen von Malwarebytes unabhängig von der Anzahl von Endpunkten auf einfache Weise bereitgestellt und verwaltet werden können. Dank dieser zentralen Cloud-Konsole ist es nicht mehr notwendig, vor Ort installierte Hardware zu erwerben und zu warten.



Sicherheitsrichtlinieneinstellungen für Malwarebytes Endpoint Protection

SYSTEMANFORDERUNGEN

Zugehörige Komponenten

- Malwarebytes-Cloudplattform
- Malwarebytes Endpoint Protection (persistenter Windows-Agent)
- E-Mail- und Telefonsupport

Hardwareanforderungen

Windows

CPU: 1 GHz

RAM: 1 GB (Clients); 2 GB (Server)

Speicherplatz: 100 MB (Programm + Protokolle)

Aktive Internetverbindung

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® mit SP3 (nur 32 Bit)

* Windows Server 2016® (32 Bit, 64 Bit)

* Windows Server 2012/2012R2® (32 Bit, 64 Bit)

* Windows Small Business Server 2011

* Windows Server 2008/2008R2® (32 Bit, 64 Bit)

* Windows Server 2003® (nur 32 Bit)

Bitte beachten Sie, dass Windows Server, bei denen das Serverkerninstallationsverfahren verwendet wird, ausdrücklich ausgeschlossen sind.

** Die Integration von Windows Action Center wird für Windows-Server-Betriebssysteme nicht unterstützt.*



malwarebytes.com



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes ist das Internetsicherheitsunternehmen der nächsten Generation, dem Millionen Anwender weltweit vertrauen. Malwarebytes schützt Menschen und Unternehmen proaktiv vor gefährlichen Bedrohungen wie Schadsoftware, Ransomware und Exploits, die von herkömmlichen Antivirenprogrammen nicht erkannt werden. Das führende Produkt des Unternehmens kombiniert eine fortschrittliche Heuristik zur Bedrohungserkennung mit signaturfreien Technologien, um Cyberangriffe zu erkennen und zu stoppen, bevor Schäden entstehen. Mehr als 10.000 Unternehmen auf der ganzen Welt nutzen, vertrauen und empfehlen Malwarebytes. Das im Jahr 2008 gegründete Unternehmen mit Hauptgeschäftssitz in Kalifornien verfügt über Standorte in Europa und Asien und beschäftigt ein global agierendes Team von Bedrohungs- und Sicherheitsexperten.

Copyright © 2017, Malwarebytes. Alle Rechte vorbehalten. Malwarebytes und das Malwarebytes-Logo sind Warenzeichen von Malwarebytes. Sonstige Marken- und Warenzeichen können Eigentum Dritter sein. Alle hier aufgeführten Beschreibungen und technischen Daten können ohne vorherige Ankündigung geändert werden und werden ohne jedwede Gewährleistung zur Verfügung gestellt.