Malwarebytes

DATENBLATT

Malwarebytes **Endpoint Protection & Response**

Wir warnen nicht nur bei Bedrohungen, wir beseitigen sie auch

Tatsache ist, dass in der heutigen Bedrohungslandschaft kein Anbieter hundertprozentigen Schutz bietet: www.malwarebytes.com/remediationmap.

Verletzungen sind unvermeidlich. Beseitigung von Schadsoftware ist unerlässlich.

Die heutigen Unternehmen suchen nach Mitteln und Wegen, gegen Zwischenfälle vorgehen zu können, die von ihren vorhandenen Verteidigungsmechanismen nicht erfolgreich abgewehrt wurden. Wenn Angreifer Verteidigungen umgehen, bleibt dies oft wochen- oder monatelang unbemerkt. In einer weltweiten Studie des Ponemon Institutes im Jahr 2017 betrug die durchschnittliche Erkennungszeit einer Verletzung 191 Tage.

„Endpoint Detection and Response (EDR)"-Fähigkeiten haben zum Ziel, die Bedrohungserkennung zu beschleunigen und die Verweildauer zu verkürzen. Je schneller eine Verletzung der Datensicherheit identifiziert und eingedämmt werden kann, desto geringer sind die anfallenden Kosten. Moderne EDR-Lösungen identifizieren eine Bedrohung, die einen herkömmlichen Schutz umgangen hat, und begegnen ihr gewöhnlich in Form von Protokollen, Warnungen und E-Mails. Anschließend nutzt ein Bedrohungsanalytiker Tools zur Auswertung des Codes und auf den infizierten Geräten wird ein Reimaging durchgeführt.

Malwarebytes Endpoint Protection and Response verfolgt einen anderen Ansatz. Mit dem Einsatz unserer firmeneigenen Linking Engine zur Beseitigung und Ransomware Rollback geht Malwarebytes weit über Warnmeldungen und Reimaging zur Schadensbehebung hinaus. Mit Endpoint Protection and Response müssen Sie keine Kompromisse zwischen Kosten und Komplexität schließen.

TECHNISCHE MERKMALE

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

Anwendungshärtung
Verringert die Angriffsfläche für Exploits, Fingerprinting-Versuche durch raffinierte Angriffe werden proaktiv erkannt

Exploit-Abwehr
Erkennt und blockiert proaktiv Versuche, Schwachstellen auszunutzen und Codes dezentral auf dem Endpunkt auszuführen

Schutz des Anwendungsverhaltens
Verhindert, dass Anwendungen zum Infizieren des Endpunkts genutzt werden

Erkennen von Anomalien durch Machine Learning
Erkennt Viren und Schadsoftware proaktiv durch Machine-Learning-Technologien

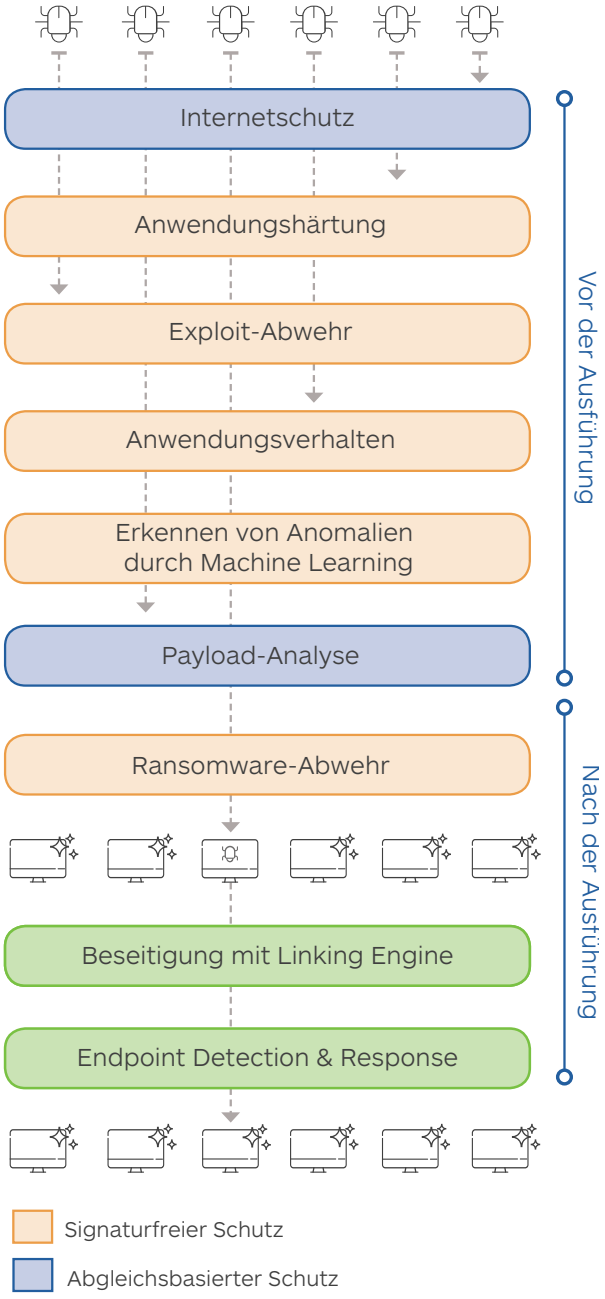
Payload-Analyse
Erkennt vollständige Familien von bekannter und relevanter Schadsoftware anhand heuristischer und verhaltensbasierter Regeln

Ransomware-Abwehr
Erkennt und blockiert Ransomware mit einer Technologie zur Verhaltensüberwachung

Linking Engine und Beseitigung
Erlaubt die vollständige und gründliche Beseitigung von Schadsoftware, sodass der Endpunkt wieder in einen vollkommen unversehrten Zustand zurückversetzt wird, während gleichzeitig die Auswirkungen für den Endbenutzer minimiert werden

Endpoint Detection and Response (EDR)
Transparenz an den Endpunkten für eine kontinuierliche Verhaltensanalyse und Forensik. Reduziert die Verweildauer von Zero-Day-Bedrohungen. Bietet Sicherheitsoptionen, die über Warnmeldungen hinausgehen

ENDPOINT PROTECTION & RESPONSE



Wichtigste Vorzüge

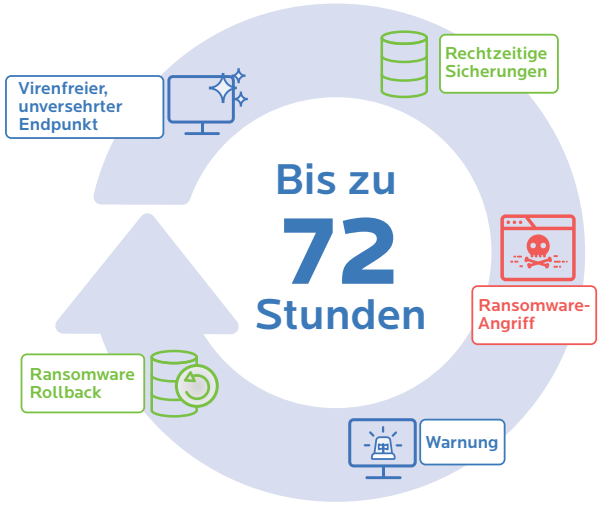
Mehrschichtiger Schutz
Malwarebytes Multi-Vector-Schutz (MVP) nutzt einen siebenschichtigen Ansatz mit sowohl statischen als auch dynamischen Erkennungstechniken, um bei allen Angriffsphasen zu schützen. Dieser Ansatz bietet Schutz vor allen Bedrohungsarten: von traditionellen Viren bis hin zu noch raffinierteren Bedrohungen von morgen.

Transparenz an den Endpunkten für eine kontinuierliche Kontrolle
Flight Recorder ermöglicht eine ständige Überwachung und Transparenz von Windows-Desktops, um wertvolle Einblicke zu erhalten. Sie können problemlos Dateisystem-, Netzwerk-, Prozess- und Registrierungsaktivitäten verfolgen. Flight-Recorder-Ereignisse werden sowohl lokal als auch in der Cloud gespeichert.

Drei Arten der Endpunkt-Isolierung
Wenn ein Endpunkt gefährdet ist, stoppt Malwarebytes die Bedrohung, indem der Endpunkt isoliert wird. Eine schnelle Beseitigung verhindert eine Lateralbewegung. Die Schadsoftware kann Ihre Daten nicht weiterleiten und Angreifer werden ferngehalten. Endpoint Protection and Response ist das erste Produkt, das drei Methoden zur Endpunktisolierung anbietet. Die Netzwerkisolierung schränkt ein, welche Prozesse kommunizieren können. Die Prozessisolierung bestimmt, welche Prozesse laufen dürfen. Die Desktopisolierung warnt den Endbenutzer und stoppt weitere Interaktionen. Sie hält das System sicher online für eine detaillierte Analyse.

Vollständige und gründliche Entfernung von Bedrohungen
Malwarebytes bietet die populärste Beseitungssoftware der Branche. Dies belegen weltweit 500.000 Downloads und die Beseitigung von drei Millionen Infektionen pro Tag. Malwarebytes Endpoint Protection and Response nutzt die firmeneigene Linking-Engine-Technologie, um nicht nur den primären Bedrohungs-Payload, sondern sämtliche Spuren von Infektionen und verbundenen Artefakten zu entfernen. Dieser Ansatz spart Zeit, die sonst durch das Bereinigen und Reimaging von Endpunkten verloren geht.

Ransomware Rollback
Die Ransomware-Rollback-Technologie ermöglicht es Ihnen, die Uhr zurückzudrehen und den Schaden durch Ransomware dank rechtzeitiger Sicherungen zu verhindern. Malwarebytes protokolliert und verbindet Änderungen mit bestimmten Prozessen. Jede durch einen Prozess erfolgte Änderung wird aufgezeichnet. Wenn ein Prozess „etwas Schlechtes tut“, können Sie diese Änderungen schnell rückgängig machen und Dateien wiederherstellen, die verschlüsselt, gelöscht oder verändert wurden. Datenspeicherung wird durch die Nutzung einer firmeneigenen dynamischen Ausschlusstechnologie minimiert. Diese Technologie lernt, wie sich „gute Anwendungen“ verhalten.



Zentrale cloudbasierte Verwaltung
Durch die geringere Komplexität vereinfacht diese Verwaltungsart die Installation und Verwaltung, unabhängig von der Anzahl der Endpunkte. Außerdem ist es nicht mehr notwendig, vor Ort Hardware zu erwerben und zu warten.

malwarebytes.com/business
desales@malwarebytes.com
+49 800 723 4800

Malwarebytes ist ein Unternehmen für Cybersicherheit, dem Millionen Menschen weltweit vertrauen. Malwarebytes schützt Endanwender und Unternehmen proaktiv vor bösartigen Bedrohungen, einschließlich Ransomware, die herkömmlichen Antivirusprogrammen entgehen. Das führende Produkt des Unternehmens verwendet signaturfreie Technologien, um einen Cyberangriff zu erkennen und zu stoppen, bevor er Schaden anrichtet. Erfahren Sie mehr dazu unter www.malwarebytes.com.