WEBROOT
Smarter Cybersecurity

Webroot SecureAnywhere® Business Endpoint Protection

Multivektorschutz für Endpunkte und Benutzer in allen Phasen eines Cyberangriffs

Übersicht

Moderne Bedrohungen nutzen mehrere Angriffsvektoren, von schädlichen E-Mail-Anlagen über infizierte Internetwerbung bis hin zur Phishing-Sites. Kriminelle kombinieren mehrere Bedrohungstechnologien, die in unterschiedlichen Phasen eingesetzt werden, um Computer und Netzwerke zu infizieren. Diese kombinierte Vorgehensweise erhöht die Erfolgswahrscheinlichkeit, die Infektionsgeschwindigkeit und die Schwere des Schadens.

Multivektorangriffe nutzen die Schwachpunkte signaturbasierter Sicherheitslösungen aus, sodass Malware unerkannt in Systeme eindringen kann. Allerdings verwenden moderne Endpunktlösungen - zumindest in Teilen - immer noch signaturbasierte Erkennungsmodelle. Dadurch werden Endbenutzer erst dann geschützt, wenn die Bedrohung bekannt ist und nachdem vom Hersteller eine Signatur erstellt und auf dem Endpunkt bereitgestellt wurde. Dann ist es aber oftmals bereits zu spät.

Sogar neuere, so genannte Endpunktlösungen der „nächsten Generation“, die normalerweise wirksamer sind als herkömmliche Konkurrenzprodukte, sind schlecht für die Abwehr moderner Angriffe gerüstet, da viele Endpunkte nur in der Infektionsphase und nur gegen einen einzelnen Vektor schützen.

Die einzige Möglichkeit, Zero-Day-Angriffe abzuwehren, ist ein Multivektor-Endpunktschutz, der Benutzer und deren Geräte in jeder Phase eines Angriffs vor allen möglichen Angriffsvektoren schützen kann.

Der SecureAnywhere®-Unterschied

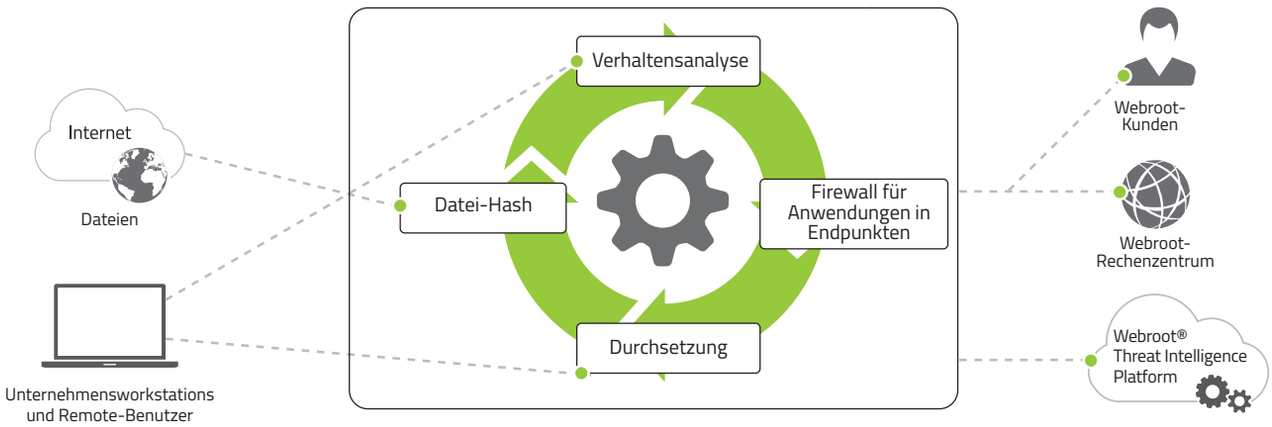
Webroot SecureAnywhere® Business Endpoint Protection zeichnet sich durch einen einzigartigen Sicherheitsansatz aus, der vor Bedrohungen mit mehreren Vektoren schützt, z. B. E-Mails, Webbrowsing, Dateianhänge, Hyperlinks, Werbeanzeigen, Social Media-Apps und angeschlossene Geräte wie USB-Laufwerke sowie andere kombinierte Bedrohungen, die in der Lage sind, schädliche Daten zu übertragen.

Unterstützt durch die branchenführende, cloudbasierte Webroot Threat Intelligence Platform vereinen Webroot-Lösungen die neuesten Echtzeitinformationen von Webroot BrightCloud®-Diensten mit modernen maschinellen Lernfunktionen und verhaltensbasierten Heuristiken. Durch Verwendung unserer stets aktuellen, cloudbasierten Technologie kann Webroot Bedrohungen der jeweiligen Endpunkte in Echtzeit analysieren, klassifizieren, bewerten und äußerst präzise prognostizieren.

Durch Kombination von SecureAnywhere-Erkennungstechnologien für Dateimuster und Verhaltensprognosen mit hochmodernen maschinellen Lernfunktionen und der hohen Verarbeitungsleistung durch Cloud-Computing kann Webroot Infektionen mit Malware verhindern und Zero-Day-Angriffe effektiv abwehren, wenn sie stattfinden. Die Vorgehensweise von Webroot ist effektiver und nachvollziehbarer als von Einzelvektor-Konkurrenzprodukten. Sie müssen sich nicht mehr auf ein veraltetes Erkennungsmodell verlassen, das durch die heutige Malware leicht überfordert wird - ein Modell, bei dem die Einwirkzeit unbekannt ist, Benutzer erst dann geschützt werden können, nachdem die Malware bereits in das System eingedrungen ist, und Angriffe erst lange Zeit nach dem Eindringen erkannt werden.

Da SecureAnywhere Business Endpoint Protection vollständig cloudbasiert ist, müssen keine Definitionen oder Signaturen bereitgestellt und verwaltet werden. Die Malwareerkennung erfolgt fortlaufend in Echtzeit, sodass Leistungsprobleme verschwinden. Geplante Systemscans dauern normalerweise ca. 18 Sekunden und beeinträchtigen nie die Geräteleistung - auch nicht in virtuellen Desktop- und Serverumgebungen und eingebetteten Betriebssystemen. Der Softwareagent kann problemlos zusammen mit anderen Virenschutzlösungen verwendet werden, sodass vorhandene Lösungen weiterhin verwendet werden können nicht ersetzt werden müssen.

Der weltweit kleinste, schnellste Client für Endpunktsicherheit bietet einzigartigen Schutz vor Multivektorbedrohungen.



Aufdecken von Zero-Day-Malware

Sichtbare Wirksamkeit

SecureAnywhere Business Endpoint Protection ist die erste Technologie zum Schutz vor Malware, die die eigene Wirksamkeit bei der Erkennung von Infektionen und Abwehr von Malware meldet. Die Meldung der Einwirkzeit ermöglicht einen transparenten Einblick in Infektionen auf Endpunkten in Ihrem Netzwerk, der zeigt, wann die Infektion erstmals aufgetreten ist und wie lange Webroot gebraucht hat, um sie zu beseitigen.

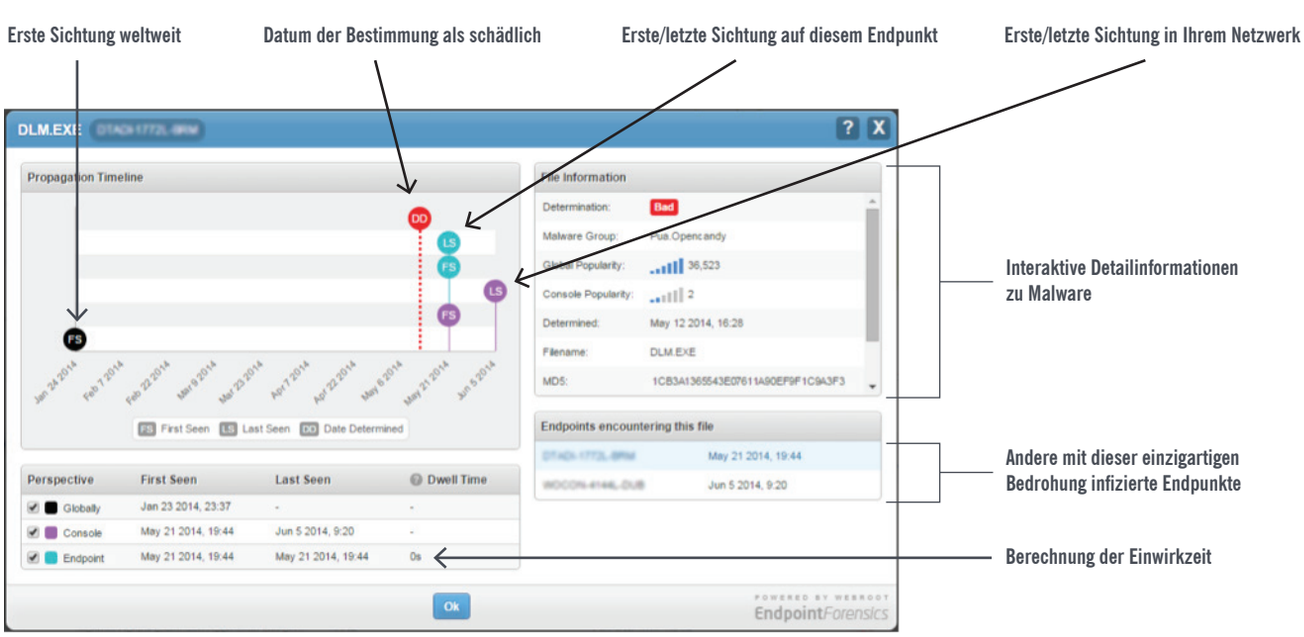
Wesentliche Faktoren, die die Wirksamkeit von SecureAnywhere Business Endpoint Protection beeinflussen, sind die kontinuierliche Infektionsüberwachung, Protokollierung und automatische Problembehebung. Wenn neue oder geänderte Dateien und Prozesse nicht sofort als „bekanntermaßen" gut oder schlecht klassifiziert werden können, beginnt der Agent sofort mit der Überwachung und Protokollierung aller Ereignisse. Wird ein beobachteter Prozess als schädlich klassifiziert, werden alle Änderungen am System rückgängig gemacht und der Endpunkt automatisch in den letzten als funktionierend bekannten Zustand versetzt. Durch diese zusätzliche Ebene wird sichergestellt, dass es zu möglichst wenigen Fehlalarmen kommt. In den seltenen Fällen, in denen ein Fehlalarm auftritt, können Administratoren Dateien in der Verwaltungskonsole ggf. in eine Whitelist eintragen.

Flexible cloudbasierte Verwaltung

Webroot SecureAnywhere-Lösungen verwenden eine cloudbasierte Verwaltung, d. h. es ist keine Hardware oder Software vor Ort erforderlich und die Konsole ist immer auf dem neuesten Stand. Die Webroot Global Site Manager-Konsole ist für die Verwaltung von bis zu 100000 Endpunkten vorgesehen. Durch die hierarchische Verwaltungsarchitektur können Sie problemlos mehrere Websites und Standorte den jeweiligen Unternehmensanforderungen entsprechend verwalten. Global Site Manager unterstützt außerdem Richtlinien auf globaler Ebene und für einzelne Websites sowie lokale Zugriffsrechte und Berechtigungen für Websiteadministratoren, die ohne großen Aufwand neben der zentralen Verwaltung aller Websites verwaltet werden können.

Daher ist Global Site Manager ideal für Unternehmen jeder Größe, u. a. globale Unternehmen oder Unternehmen mit mehreren Standorten, sowie Anbieter von verwalteten Services (MSPs) geeignet, die eine Vielzahl von Kundenwebsites verwalten. Die cloudbasierte Verwaltung mit einer umfassenden Endpunktverwaltung macht außerdem die Bereitstellung einer globalen Verwaltung im Vergleich zu konventionellen Virenschutzlösungen extrem kostengünstig.

Einwirkzeit der Infektion: Sichtbarkeit von Eindämmung und Problembehebung



Vorausschauende Abwehrfunktionen

Alle Webroot SecureAnywhere-Lösungen und BrightCloud-Bedrohungsinformationsdienste basieren auf der Webroot® Threat Intelligence Platform. Durch Nutzung umfangreicher Analysedaten, maschinelle Lernfunktionen und Bedrohungsinformationen von Kunden und Technologiepartnern auf der ganzen Welt erkennt Webroot Threat Intelligence Platform Infektionen sofort. Diese Big-Data-Architektur verarbeitet, analysiert, korreliert und kontextualisiert laufend umfangreiche grundverschiedene Informationen. Geichzeitig wird ein patentiertes System der fünften Generation mit maschinellen Lernfunktionen für die Erkennung von schädlichem Code verwendet, um sofort und mit beeindruckender Genauigkeit eine Verhaltensprognose für Malware abzugeben.

Die Verarbeitung umfangreicher Daten ermöglicht es SecureAnywhere Business Endpoint Protection, Malware aufzudecken, sobald versucht wird, den Endpunkt eines Benutzers zu infizieren. Gleichzeitig werden alle anderen SecureAnywhere-Endpunkte vor gleichartigen Angriffen geschützt. Durch diese kollektive Strategie für Bedrohungsinformationen entsteht ein großes Netz für die Erkennung von Malware in Echtzeit, das über eingehendes Wissen über mehr als 300 Millionen ausführbare Dateien verfügt, z. B. Verhaltensmerkmale und Interaktionen zur Ausführungszeit. Zusammen mit vielen hundert Terabyte Bedrohungsdaten wird so sichergestellt, dass Webroot-Kunden stets vor bestehenden und neuen Bedrohungen geschützt sind.

Wichtige Sicherheitsfunktionen

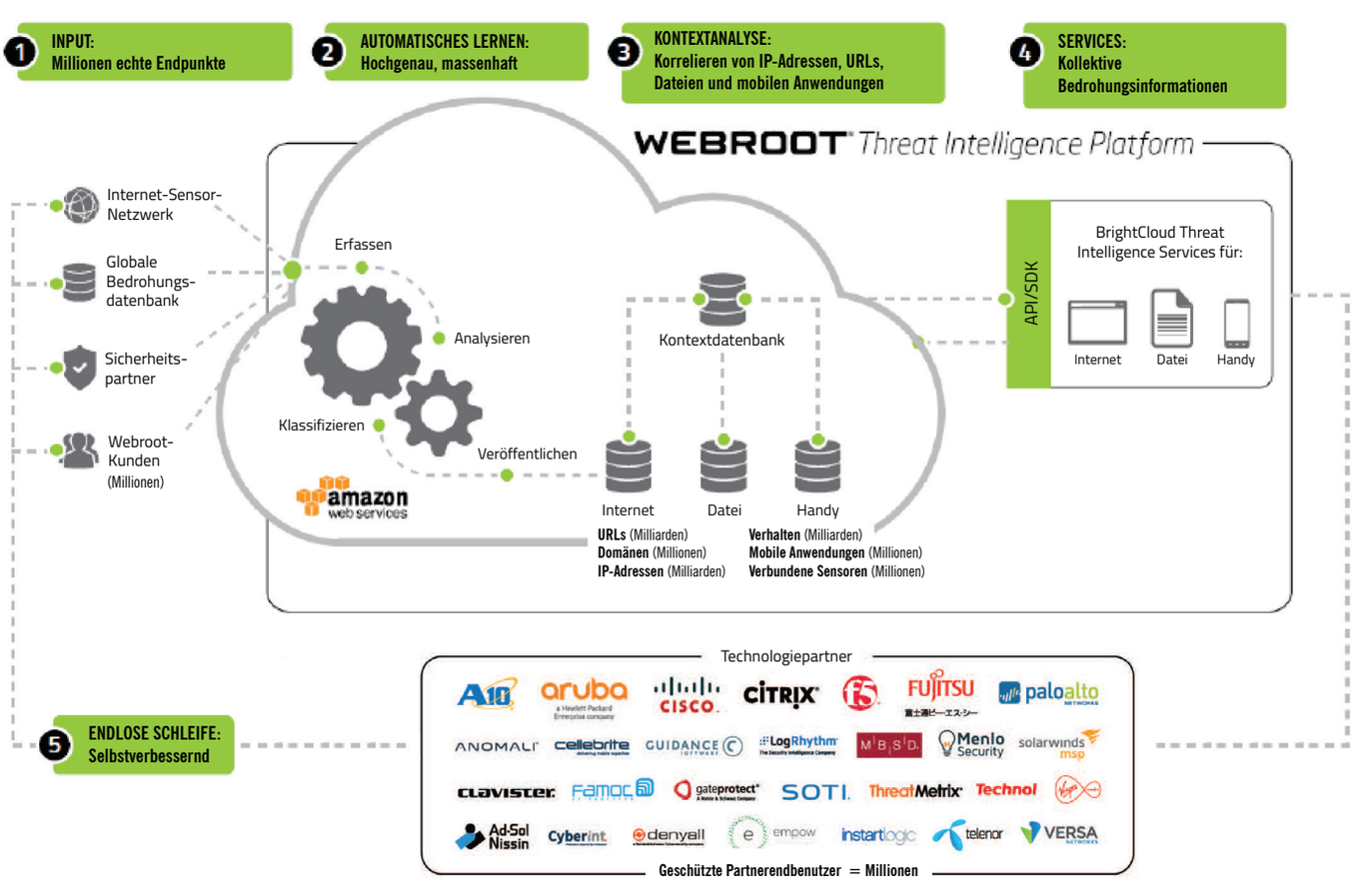
Webroot SecureAnywhere Business Endpoint Protection ermöglicht eine präzise und effektive Abwehr von Malware auf Endpunkten sowie weitere Sicherheitsfunktionen für den Schutz von Benutzern und Geräten.

Identitätsschutz

Diese Schutzfunktion sorgt für den Schutz von Benutzern, indem davon ausgegangen wird, dass der Endpunkt bereits mit einer noch nicht bekannten Malware infiziert ist. Sie schützt Benutzer- und Transaktionsdaten, die bei Onlinetransaktionen offen gelegt werden können, z. B. durch Phishing, DNS-Poisoning, Protokollierung von Tastaturanschlägen, Bildschirmerfassung, Cookieaussonderung, Kaperung der Zwischenablage sowie Browser- und Session-Hijacking durch Schadsoftware, die Man-in-the-Middle-Angriffe durchführt. Die Schutzfunktion sperrt Betriebssystem und Browser, um alle Benutzerdaten und Anmeldeinformationen zu schützen, sogar freigegebene Kennwörter. Abgesehen vom Schutz von Browseraktivitäten kann der Identitätsschutz nach Maßgabe der Benutzer auf andere zu schützende Endpunktanwendungen erweitert werden.

Infrared

Infrared ist ein mehrstufiges Abwehrsystem, das mehrere Aspekte von Webroot-Bedrohungsinformationen nutzt, um Bedrohungen frühzeitig zu erkennen und zu vereiteln – oftmals bevor ein Bedrohungsforscher überhaupt ein einzelnes Exemplar zu sehen bekommt. Diese Funktion untersucht die Reputation der besuchten Websites und verwendet Webroot-Bedrohungsinformationen, um die jeweilige Gefährdung zu



Webroot® Threat Intelligence Platform – die weltweit leistungsfähigste, echtzeitfähige Bedrohungsanalyseengine

Webroot-Multivektorschutz

ermitteln. Wenn der Benutzer häufig Websites mit geringer Reputation aufsucht, wechselt der Agent in einen Zustand erhöhter Achtsamkeit, in dem alle neuen Dateien oder Prozesse, die in das System gelangen, eingehend untersucht werden. Infrared interpretiert außerdem das Benutzerverhalten und das Gesamtsicherheitsniveau. Wenn ein Benutzer als „hochriskant" klassifiziert wird, passt Webroot den Malwareschutz für den betreffenden Benutzer dynamisch an, während Fehlalarme für weniger risikofreudige Benutzer verhindert werden.

Webbedrohungsschutz

Der Webbedrohungsschutz nutzt die Anti-Phishing-Technologie von Webroot, um einen einzigartigen Echtzeitschutz vor polymorphen Phishing-URLs sowie schädlichen und hochriskanten Websites und Domänen zu ermöglichen.

Intelligente Ausgangsfirewall

Neben den integrierten Schutzfunktionen umfasst SecureAnywhere Business Endpoint Protection eine intelligente anwendungskonsistente Ausgangsfirewall mit Systemüberwachungsfunktion, die die Microsoft Windows®-Firewall erweitert, um Benutzer innerhalb und außerhalb des Unternehmensnetzwerks zu schützen. Durch die Überwachung des gesamten ausgehenden Datenverkehrs schützt die Firewall vor Eindringlingen, die versuchen, eine Verbindung nach außen herzustellen, und stellt somit sicher, dass nur zugelassene Anwendungen über das Netzwerk kommunizieren können. Außerdem werden bekannte schädliche und nicht schädliche Programme automatisch erkannt, damit Benutzer nicht laufend durch Pop-up-Fenster belästigt oder zu leichtfertigen Entscheidungen gezwungen werden.

Effektive Heuristik

Die Heuristikeinstellungen können abhängig vom tolerierbaren Risiko einer Dateiausführung angepasst werden. Die Heuristikeinstellungen umfassen:

» **Erweitert**
Analysiert neue Programme auf verdächtige Aktionen, die für Malware typisch sind.

» **Alter**
Analysiert neue Programme anhand der Dauer, für die eine Datei bereits in den Webroot-Bedrohungsinformationen vorhanden ist.

» **Beliebtheit**
Analysiert neue Programme anhand der Häufigkeit, mit der das Programm in den Webroot-Bedrohungsinformationen verwendet oder geändert wurde.

Offline-Schutz

Während des Offline-Betriebs eines Endgeräts werden Angriffe dank separater Richtlinien für ausführbare Dateien gestoppt, die auf lokale Festplatten, USB-Sticks und CD-/DVD-Laufwerke angewendet werden.

Unterstützung von Virtualisierung, Terminal Server und Citrix

Neben der Unterstützung von Windows PC-Umgebungen unterstützt SecureAnywhere Business Endpoint Protection auch Windows Server-, Virtualisierungs-, Terminal Server- und Citrix-Umgebungen.

Unterstützung von mobilen Smartphones und Tablets

Webroot SecureAnywhere® Business Mobile Protection ist für Smartphones und Tablets mit Android® und iOS® verfügbar.

Widerstandsfähige verteilte Cloud-Architektur

Mehrere sichere Rechenzentren auf der ganzen Welt versorgen Niederlassungen in unterschiedlichen Ländern und mobile Benutzer über das nächstgelegene Rechenzentrum und bieten ausfallsichere Flexibilität und Redundanz.

Info zu Webroot

Webroot ist Anbieter für Netzwerk- und Endgerätesicherheit der nächsten Generation und stellt Bedrohungsinformationsdienste bereit, die dem Schutz von Unternehmen und Privatpersonen rund um den Globus dienen. Gestützt werden unsere smarten Dienste von den Bedrohungsdaten Millionen echter Geräte, die in der Cloud gespeichert und gesammelt werden. Das Resultat sind ein Echtzeitschutz gegen Bedrohungen und Sicherheit für die vernetzte Welt. Unsere preisgekrönten SecureAnywhere® Lösungen für Endgeräte und BrightCloud® Threat Intelligence Services schützen Millionen Geräte in Unternehmen, bei Privatanwendern und im Internet der Dinge. Marktführende Unternehmen wie Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks und A10 Networks vertrauen auf Webroot. Unser Unternehmen operiert in Nordamerika, Europa und Asien, unsere Firmenzentrale befindet sich in Colorado. Entdecken Sie Smarter Cybersecurity™ -Lösungen unter webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021, USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

©2017 Webroot Inc. Alle Rechte vorbehalten. Webroot, Webroot BrightCloud und BrightCloud sind Marken oder eingetragene Marken von Webroot Inc. in den Vereinigten Staaten von Amerika und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.
DS _ 062817 _ A4