CARBONITE an opentext company | WEBROOT an opentext company

Webroot®
Business Endpoint Protection

Intuitive, automatisierte Cybersicherheit, die Unternehmen dabei hilft, resilient (widerstandsfähig) gegenüber Angriffen zu sein

Übersicht

Heutzutage sehen sich Unternehmen jeder Größe konstant Angriffen ausgesetzt. Während manche Angriffe zufällig, automatisiert und wahllos sind, sind viele andere hochgradig zielgerichtet, invasiv und präzise. Angesichts der Vielfalt, Menge und Geschwindigkeit der Angriffe war es noch nie so wichtig wie heute, eine effektive Endpunktsicherheit mit breitem Spektrum zu installieren, die in Verbindung mit anderen Abwehrmechanismen Ihre Benutzer und Systeme vor Malware, Ransomware, Phishing, Kryptomining und anderen schädlichen Angriffen schützt.

Die Sicherheitsherausforderungen sind für Unternehmen jeder Größe gleich: Reduzieren von Komplexität, Integrieren von Lösungen in vorhandene Tools, Umgehen mit der Tatsache, dass nicht alle Administratoren die gleichen Erfahrungen mit Sicherheitsbedrohungen haben, und letztendlich Steigern der Resilienz/Widerstandsfähigkeit gegenüber Cyberangriffen.

Webroot® Business Endpoint Protection löst diese und weitere Probleme mit einer preisgekrönten[1] intuitiven Verwaltungskonsole, über 40 Integrationen von Drittanbietern, einer RESTful API sowie Erkennung, Abwehr, Schutz und Problembehebung bei Endpunkten (und zwar vollautomatisch), sodass eine umfassende Cyberresilienz-Strategie entsteht. Dabei wird die Leistungsfähigkeit von Cloud-Computing und maschinellem Echtzeit-Lernen ideal ausgenutzt, um die Endpunktabwehr jedes einzelnen Systems kontinuierlich zu überwachen und an die jeweiligen Bedrohungen anzupassen, denen System und Benutzer ausgesetzt sind.

Durch einen patentierten proaktiven, vorausschauenden und mehrschichtigen Sicherheitsansatz bietet Webroot Business Endpoint Protection hochwirksame Abwehrmaßnahmen gegen die heutigen Cyberbedrohungen.

Der einzigartige Ansatz von Webroot

Webroot® Business Endpoint Protection unterscheidet sich diametral von anderen Endpunkt-Sicherheitslösungen. Als Software-as-a-Service (SaaS)- und cloudgesteuerte Endpunkt-Sicherheitslösung bietet sie eine Reihe von Vorteilen, darunter:

Reibungslose Implementierung
Die Installation des Agenten (<5 MB) dauert durchschnittlich 3 Sekunden[2], und er ist so konzipiert, dass keine Konflikte mit anderer Sicherheitssoftware auftreten. Durch diese Kompatibilität geht die Implementierung von Webroot-Software und das Ersetzen älterer Sicherheitssoftware schneller und einfacher als bei anderen Lösungen, da Administratoren sich keine Sorgen um die Beeinträchtigung der Benutzerproduktivität während der Einführung der effektiven Endpunktsicherheit machen müssen.

Endpunktverwaltung und -steuerung erfolgt vollständig remote
Unsere cloudbasierte Verwaltungskonsole bietet Einblicke und Kontrollmöglichkeiten für jedes Gerät, auf dem der Webroot-Agent installiert ist. Sie können mehrere Standorte verwalten und leistungsstarke Befehle über Remote-Agenten ausführen. Es gibt keine lokale Serververwaltung, und mit der Konsole können Sie auch andere Webroot-Lösungen wie Webroot® DNS-Schutz und Webroot®-Schulung zur Steigerung des Sicherheitsbewusstseins problemlos testen, bereitstellen und verwalten, falls Sie dies wünschen.

Hochautomatisierter, kostengünstiger Betrieb
Webroot® Business Endpoint Protection wurde von Grund auf so entwickelt, dass es einfach bereitzustellen, zu verwalten und zu warten ist. Sie können detaillierte, vorkonfigurierte Richtlinienvorlagen nutzen oder sie einfach ändern, um Ihre eigenen zu erstellen. Es müssen keine Signaturen oder Definitionen aktualisiert werden, da die Bedrohungsabwehr in Echtzeit über die Cloud erfolgt. Webroot-Agentenaktualisierungen sind automatisiert, dauern normalerweise 3 Sekunden[2] und sind für den Benutzer völlig transparent. Infektionswarnungen und -behebungen sind automatisiert, während regelmäßig Berichte zu Inhalten, Zeitpunkten und der Verbreitung erstellt werden. All dies führt zu sehr niedrigen Betriebskosten.

1 G2.com. „Usability Index for Endpoint Protection Suites" (Herbst 2019)
2 PassMark Software. „Webroot SecureAnywhere® Business Endpoint Protection vs. Eight Competitors" (März 2019)

Schutz online und offline
Webroot verwendet eigens entwickelte Technologie, um Infektionen zu überwachen, zu protokollieren und einzudämmen, selbst wenn ein Endpunkt offline ist. Ebenso werden System- und Benutzerdaten auch offline geschützt. Anstatt die Windows®-Volumeschattenkopie zu verwenden, die auch durch Malware beeinträchtigt sein könnte, verwendet Webroot einen patentierten Ansatz, um Gerätedaten abzusichern und das lokale Host-Laufwerk vor einer Gefährdung oder einer Schädigung zu schützen, die eine völlige Neuinstallation (Re-Imaging) nötig machen würde.

Niedrige Systembelastung (durch unabhängiges Benchmarking bestätigt)
Ein wesentlicher Vorteil unseres cloudgesteuerten Ansatzes besteht darin, dass die rechenintensive Verarbeitung der Erkennung und Analyse von Malware in der Cloud durchgeführt wird. Unabhängige Tests durch PassMark Software zeigen, dass der Webroot-Schutz im Vergleich zu führenden Produkten von Wettbewerbern die geringste Gesamtsystemressourcennutzung aufweist.[2] Die umfassenden, geplanten Scans sind für Benutzer transparent, und die CPU- und RAM-Auslastung des Systems ist gering und belastet die Ressourcen nicht übermäßig.

Innovative Erkennungstechnologie
Im Gegensatz zu herkömmlichen Ansätzen, bei denen nur eine Möglichkeit besteht, eine Bedrohung zu erkennen und zu stoppen, funktioniert der Webroot-Schutz der nächsten Generation in mehreren Schritten. Zuerst soll vorausschauend verhindert werden, dass Malware in das System eindringt. Anschließend soll verhindert werden, dass Malware und unbekannte Dateien ausgeführt werden, wenn sie böswilliges Verhalten aufweisen. Wenn eine bisher unbekannte (und damit potenziell infizierte) Datei ausgeführt wird, wird ihre Aktivität von Webroot überwacht und protokolliert, bis sie entsprechend klassifiziert werden kann. Wird die Datei als Bedrohung eingestuft, werden alle Änderungen an lokalen Laufwerken, die durch sie vorgenommen wurden, rückgängig gemacht und die Laufwerke automatisch auf den Zustand vor der Infizierung zurückgesetzt. Diese mehrstufige Strategie ist nicht nur wirksamer gegen moderne Bedrohungen, sondern verringert auch die Wahrscheinlichkeit von Fehlalarmen.

Unterstützt von erstklassigen Threat Intelligence-Services in Echtzeit
Alle Webroot-Lösungen beruhen auf der Webroot® Plattform, in die Webroot BrightCloud® Threat Intelligence integriert ist. Auf diesen Dienst vertrauen mehr als 100 Netzwerk-, Sicherheits- und Technologieanbieter, um die Sicherheit für ihre Produkte und Dienstleistungen zu erhöhen. Unsere Architektur für maschinelles Lernen der 6. Generation verarbeitet täglich mehr als eine halbe Billion Bedrohungsobjekte aus verschiedenen geprüften Quellen sowie zig Millionen realer Kundenendpunkte. So können wir täglich rund 1.000 neue oder überarbeitete Modelle für maschinelles Lernen generieren, um Kunden und Partnern auf der ganzen Welt dabei zu helfen, Cyberresilienz zu erreichen.

Webroot® Business Endpoint Protection auf einen Blick

- **Sichere und resiliente verteilte Cloud-Architektur:** Verwendet weltweit mehrere sichere Rechenzentren, um Kunden und Roaming-Benutzer durch Full-Service-Resilienz und Redundanz zu unterstützen.
- **Mehrschichtige Benutzer- und Geräteverteidigung:** Stoppt auch Angriffe, bei denen ein mangelndes Sicherheitsbewusstsein von Benutzern ausgenutzt wird, und nicht nur solche, die auf Sicherheitslücken im Gerät abzielen.
- **Erkennung und Abwehr von Malware:** Blockiert Viren, Malware, Trojaner, Phishing, Ransomware, Spyware, browserbasierte Angriffe, Kryptojacking, Malware zum Stehlen von Anmeldeinformationen, skriptbasierte und dateilose Angriffe sowie eine Vielzahl anderer Bedrohungen.
- **Schutz durch vielfältige Schilde:** Die Schutzschilde von Webroot umfassen Echtzeit-, Verhaltens-, Kernsystem-, Webbedrohungs-, Identitäts-, Phishing-, Tarnungs- und Offline-Schutz zur Erkennung und Abwehr von komplexen Angriffen.
- **Schutz vor bösartigen Skripten:** Die patentierte Webroot® Evasion Shield-Technologie erkennt, blockiert und isoliert (durch Quarantäne) getarnte Skriptangriffe, unabhängig davon, ob sie dateibasiert, dateilos, verschleiert oder verschlüsselt sind, und verhindert, dass böswilliges Verhalten in PowerShell, JavaScript und VBScript ausgeführt wird.
- **Benutzeridentität und Datenschutz:** Der Identitätsschutzschild (Browser- und Anwendungsisolation) wird von weltweit führenden Banken als vertrauenswürdig eingestuft, um Angriffe wie DNS-Poisoning, Keylogging, Screen-Grabbing, Cookie-Scraping, Clipboard-Grabbing sowie Browser- und Sitzungs-Hijacking durch bösartige Software zu stoppen.
- **Weiße und schwarze Listen:** Bieten direkte Kontrolle über die Ausführung von Anwendungen.
- **Intelligente Firewall:** Die systemüberwachende und anwendungsorientierte ausgehende Firewall ergänzt die integrierte Windows®-Firewall zum Schutz von Benutzern innerhalb und außerhalb von Unternehmensnetzwerken.
- **Dynamische Infrarot-Risikoprävention:** Analysiert das Verhalten einzelner Benutzer, um die Heuristiken zur Malware-Prävention dynamisch anzupassen.
- **Leistungsstarke Heuristik:** Ermöglicht Administratoren die Anpassung der heuristischen Erkennung basierend auf der Risikotoleranz für die Dateiausführung.
- **Umfassender Offline-Schutz:** Stoppt Angriffe auch im Offline-Modus und ermöglicht Administratoren das Erstellen separater Richtlinien für die Dateiausführung auf lokalen Festplatten, USB-, CD- und DVD-Laufwerken.
- **Unterstützung für mehrere Betriebssysteme, Virtualisierung, Terminalserver und Citrix:** Unterstützt MacOS®-Geräte, Windows®-Computer und -Server, Virtualisierung, Terminalserver und Citrix-Umgebungen.

- **Mehrsprachige Unterstützung:** Der installierte Agent unterstützt 13 Sprachen.
- **Kostenloser, preisgekrönter telefonischer Support:** Unser internes Support-Team steht bereit, um Probleme mit einer Kundenzufriedenheitsrate von 95 % zu lösen.
- **Transparente Nutzung und Abrechnung:** Die Webroot My Usage- und My Billing-Portale in der Verwaltungskonsole machen Nachverfolgung und Zahlungsvorgänge transparent.

Welche Ergebnisse dürfen Sie erwarten?

Webroot® Business Endpoint Protection hilft Unternehmen, Cyberresilienz zu erreichen, indem es einen erweiterten Schutz gegen die ständig wachsenden und sich weiterentwickelnden Bedrohungen durch moderne Angriffe bietet. Dank der hochautomatisierten und effektiven Endpunktsicherheit benötigen Sie keine dedizierten IT-Sicherheitsressourcen oder Experten mehr, um die „digitale Fitness" Ihres Unternehmens sicherzustellen. Und bei weniger Infektionen und sicherheitsrelevanten Vorfällen – und dadurch natürlich auch weniger Problembeseitigungen und Produktivitätsverlusten – können sich Administratoren auf das konzentrieren, was am wichtigsten ist: ihrem Unternehmen zum Erfolg zu verhelfen.

Testversion und nächste Schritte

Weitere Informationen erhalten Sie bei Ihrem Webroot Account Manager oder unserer Verkaufsabteilung. Besuchen Sie webroot.com, um eine KOSTENLOSE 30-Tage-Testversion zu starten. Bestehende Webroot-Kunden können Testversionen auch direkt über die Webroot-Verwaltungskonsole starten.

Contact us to learn more – Webroot EMEA

Email: DACH-smbc@opentext.com

Phone: +49 (0)2162 91980 20

Über Carbonite und Webroot

Carbonite und Webroot, OpenText-Unternehmen, nutzen die Cloud und künstliche Intelligenz, um Unternehmen, Einzelpersonen und Managed Services-Anbietern umfassende Lösungen für mehr Cyberresilienz anzubieten. Cyberresilienz bedeutet, dass Systeme trotz Cyberangriffen und Datenverlusten jederzeit aktiv und betriebsbereit sind. Mit diesem Ziel haben wir unsere Kräfte gebündelt, um Endpunktschutz, Netzwerkschutz, Schulungen zur Steigerung des Sicherheitsbewusstseins, Datensicherungs- und Notfallwiederherstellungslösungen sowie Threat Intelligence-Services bereitzustellen, die von marktführenden Technologieanbietern weltweit verwendet werden. Webroot nutzt die Leistungsstärke des maschinellen Lernens zum Schutz von Millionen von Unternehmen und Einzelpersonen und sichert die vernetzte Welt. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie unter carbonite.com und webroot.com mehr über Cyberresilienz.