CARBONITE® + WEBROOT®
OpenText Security Solutions

DATENBLATT

# Webroot® Business Endpoint Protection

## Führende Multi-Vektor-Sicherheitslösung der nächsten Generation

## Übersicht

Heutzutage sehen sich Unternehmen jeder Größe konstant Angriffen ausgesetzt. Angesichts der Vielfalt, des Umfangs und der Geschwindigkeit von Angriffen war es noch nie so wichtig wie heute, Malware, Ransomware, Phishing, Cryptomining und andere schädliche Angriffe auf Ihre Benutzer und Systeme zu stoppen.

Webroot® Business Endpoint Protection löst diese Probleme und mehr, indem es eine preisgekrönte, intuitive Verwaltungskonsole bereitstellt. Mit über 40 Integrationen von Drittanbietern, einer RESTful API sowie vollautomatischer Endpunkt-Erkennung, -Prävention und -Beseitigung bietet Webroot einen umfassenden Endpunktschutz, der die Cyber-Resilienz-Strategie eines Unternehmens ergänzt. Webroot nutzt in einzigartiger Weise die Leistungsfähigkeit von Cloud Computing und maschinellem Lernen in Echtzeit, um die Endpunktverteidigung jedes Systems kontinuierlich zu überwachen und an die individuellen Bedrohungen anzupassen, denen ein Endbenutzer oder System ausgesetzt ist.

## Proaktiver, vorausschauender und mehrschichtiger Ansatz für die Sicherheit

### Unterstützt von erstklassigen Threat Intelligence-Services in Echtzeit

Der Multi-Schutzschild von Webroot umfasst Echtzeit-Verhaltens-, Kernsystem-, Web-Bedrohungs-, Identitäts-, Phishing-, Ausweich- und Offline-Schutzschilde zur Erkennung, Vorbeugung und zum Schutz vor komplexen Angriffen. Die patentierte Webroot® Evasion Shield Technology erkennt, blockiert und beseitigt (Quarantäne) Angriffe mit ausweichenden Skripten, unabhängig davon, ob diese dateibasiert, dateilos, verschleiert oder verschlüsselt sind. Außerdem verhindert es mit seinem Script Shield, dass bösartige Verhaltensweisen in PowerShell, JavaScript und VBScript ausgeführt werden. Die neue Komponente Foreign Code Shield stoppt Exploits und Advanced Persistent Threats (APTs).

Webroot® Business Endpoint Protection basiert auf der BrightCloud® Threat Intelligence-Plattform, die das Beste aus künstlicher Intelligenz und maschinellem Lernen kombiniert, um Unternehmen bei der Bekämpfung der sich schnell verändernden Bedrohungslandschaft zu unterstützen. BrightCloud genießt das Vertrauen von mehr als 140 Netzwerk-, Sicherheits- und Technologieanbietern

## Wichtigste Vorteile

- Endpunktverwaltung und -steuerung erfolgt vollständig remote
- Hochautomatisierter, kostengünstiger Betrieb
- Reibungslose Implementierung
- Überlegene Wirksamkeit gegen Zero-Day-Bedrohungen
- Maßgeschneiderte Lösungen für Managed Service Provider und kleine bis mittlere Unternehmen

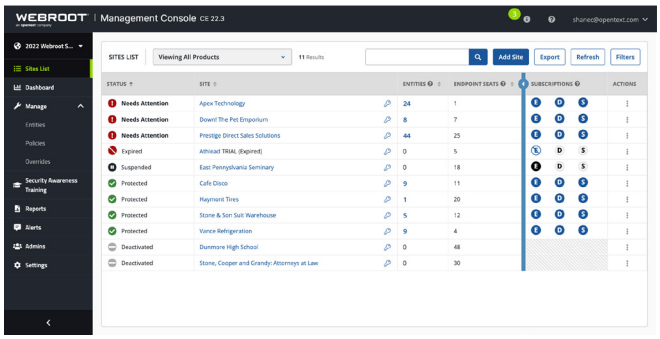
# Propriety-Technologie zur Überwachung, Protokollierung und Eindämmung von Infektionen, selbst wenn ein Endpunkt offline ist

## Endpunktverwaltung und -steuerung erfolgt vollständig remote

### Wie es funktioniert

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 dann eine zuvor unbekannte Datei (z. B. eine potenzielle Infektion) ausgeführt wird, überwacht und protokolliert der Webroot-Schutz die Aktivität der Datei, bis er sie entsprechend klassifizieren kann. Wenn die Datei als Bedrohung eingestuft wird, werden alle an den lokalen Laufwerken vorgenommenen Änderungen 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.

Es müssen keine Signaturen oder Definitionen aktualisiert werden, da die Bedrohungsabwehr in Echtzeit über die Cloud erfolgt. Die Aktualisierungen des Webroot-Agenten erfolgen automatisch und dauern in der Regel 3 Sekunden, während sie für den Benutzer völlig transparent sind. Infektionswarnungen und Abhilfemaßnahmen sind automatisiert, während die regelmäßige Berichterstattung in Bezug auf Inhalt, Zeitpunkt und Verbreitung geplant ist. 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. Ein wesentlicher Vorteil unseres cloudgesteuerten Ansatzes besteht darin, dass die rechenintensive Verarbeitung der Erkennung und Analyse von Malware in der Cloud durchgeführt wird.




*Webroot cloudbasierte Verwaltungskonsole*

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

## Sichere und widerstandsfähige verteilte Cloud-Architektur mit mehrschichtigem Schutz für Benutzer und Geräte

OpenText Security Solutions vereint erstklassige Lösungen, die Ihrem Unternehmen helfen, cyber-resilient zu bleiben. Carbonite und Webroot können Ihnen dabei helfen, Bedrohungen und Angriffe von vornherein zu verhindern und zu schützen, indem sie die Auswirkungen durch schnelle Erkennung, Reaktion und Wiederherstellung von Daten nahtlos minimieren und Ihr Unternehmen bei der Anpassung und Einhaltung sich ändernder Vorschriften unterstützen. Webroot® Business Endpoint Protection hilft Unternehmen, Cyber-Resilienz 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. Das bedeutet weniger Infektionen und sicherheitsrelevante Vorfälle – ganz zu schweigen von weniger Sanierungsfällen und Produktivitätsverlusten.

**Über Carbonite und Webroot**

Carbonite und Webroot, Unternehmen von OpenText, nutzen die Cloud und künstliche Intelligenz, um umfassende Cyber-Resilienz-Lösungen für Unternehmen, Privatpersonen und Managed Service Provider anzubieten. Cyber-Resilienz bedeutet, dass Sie in der Lage sind, selbst bei Cyberangriffen und Datenverlusten den Betrieb aufrechtzuerhalten. Deshalb haben wir unsere Kräfte gebündelt, um Lösungen für den Schutz von Endpunkten, den Schutz von Netzwerken, die Schulung des Sicherheitsbewusstseins, die Datensicherung und die Notfallwiederherstellung sowie Bedrohungsanalysen anzubieten, die von marktführenden Technologieanbietern weltweit genutzt werden. Wir nutzen die Möglichkeiten des maschinellen Lernens, um Millionen von Unternehmen und Privatpersonen zu schützen und die vernetzte Welt zu sichern. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie mehr über Cyber-Resilienz unter carbonite.com und webroot.com.



**Erfahren Sie mehr unter webroot.com.**

CARBONITE® + WEBROOT®
OpenText Security Solutions