

Webroot SecureAnywhere® DNS Protection

Malware abwehren, bevor sie Ihr
Netzwerk erreicht



Einführung

Heutzutage stellt die Nutzung des Internets ein hohes Risiko für jedes Unternehmen dar, unabhängig von der jeweiligen Größe. Von Benutzern, die unbeabsichtigt zu Websites mit Malvertising navigieren, zu ungewollten Downloads, die sofort Ransomware oder andere Malware von einem Befehls- oder Kontrollserver herunterladen, ist die unkontrollierte Internetnutzung im Unternehmensnetzwerk voller Risiken.

Direkter Schutz über unsere DNS-Cloud

Das Domain Name System (DNS) ist eine hierarchische Namenskonvention für Dienste, Computer und andere Ressourcen, die mit dem Internet oder einem privaten Netzwerk verbunden sind. DNS-Server übersetzen textbasierte Browsereingaben in eindeutige IP-Adressen, die Geräte und Dienste an die gewünschte Website leiten. Durch Umleitung der Webbrowser von Benutzern über die Webroot DNS-Cloud erlangen Administratoren sofortige Kontrolle. Die meisten gefährlichen Websites werden blockiert, sodass sie keine Malware in Ihrem Unternehmen verbreiten können.

Webroot überprüft mindestens dreimal täglich den gesamten IPv4-Adressraum und die verwendeten IPv6-Adressen, um mehr als 95 % des Internets zu klassifizieren. Alle Webroot-Sicherheitsprodukte und -dienste basieren auf Webroot BrightCloud® Threat Intelligence, das laufend mehr als 4 Milliarden IP-Adressen, 600 Millionen Domänen und 27 Milliarden URLs analysiert und klassifiziert. Webroot deckt so täglich mindestens 25.000 schädliche URLs, 6.000 neue Phishing-Sites und mehr als 100.000 neue schädliche IP-Adressen auf.

Mit Webroot SecureAnywhere® DNS Protection gibt es eine direkte und hochwirksame Möglichkeit, um zu verhindern, dass die alltägliche Internetnutzung ein größeres Sicherheitsrisiko wird. Die intuitive webbasierte SecureAnywhere DNS Protection-Konsole bietet Administratoren die Möglichkeit, Webzugriffsrichtlinien für IP-Adressen

oder IP-Adressbereiche zu optimieren und den Zugriff auf andere Websites zu beschränken, die ein Risiko für das Netzwerk darstellen könnten. Webroot bietet über 82 URL-Kategorien, von Medikamentenmissbrauch über Gewalt und Waffen, mit denen Administratoren die richtigen Nutzungsrichtlinien für ihr Unternehmen festlegen können.

Durch Nutzung umfangreicher Informationen und leistungsfähiger Dienste von Webroot zum automatischen Blockieren von schädlichen Websites und Filtern unerwünschter Websitetypen können Sie die Anzahl der Malwarebedrohungen, die Ihr Netzwerk und Ihre Endpunkte infizieren, um bis zu 90 % oder mehr verringern.

Vorteile von Webroot SecureAnywhere DNS Protection

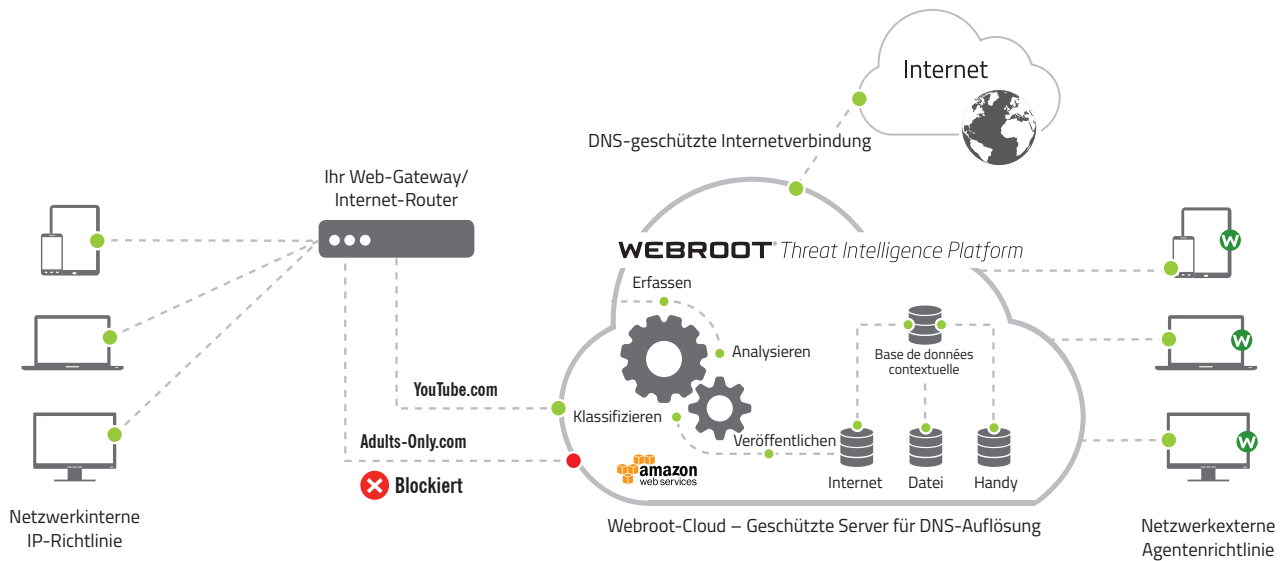
Keine Installation von Hardware oder Software erforderlich

Sie können diese Schutzebene für Internetbedrohungen in wenigen Minuten einrichten, um alle verbundenen Geräte von Benutzern und Gästen zu schützen, z. B. Windows®- und Linux-Betriebssysteme sowie Apple®- und Android®-Geräte.

Blockierung von Malware und anderen Bedrohungen auf der Domänenebene

Die grundlegenden Schutzfunktionen und Richtliniensteuerung filtern automatisch Phishing-, Botnet-, Malware-, Porno-Websites und andere fragwürdige Website-kategorien wie Betrügereien, Waffen und Glücksspiel. Granulare Filteroptionen über die Webroot BrightCloud URL-Klassifizierung mit 82 Kategorien bieten die Möglichkeit, Websites zuzulassen bzw. zu sperren.

Webroot überprüft mindestens dreimal täglich den gesamten IPv4-Adressraum und die verwendeten IPv6-Adressen, um mehr als 95 % des Internets zu klassifizieren.



Einfache DNS-Schutzeinrichtung

Richtlinien für IP-Adressen und/oder dynamische IP-Adressen

Vorkonfigurierte und benutzerdefinierte Richtlinien bieten die Möglichkeit, Ihr Unternehmen schnell, bequem und effektiv zu schützen. Darüber hinaus bietet ein innovativer Agent die Möglichkeit, Geräte und Benutzer auch dann zu schützen und zu verwalten, wenn sie unterwegs oder abwesend sind.

Bedarfsgesteuerte Berichte für Detailabfragen/-analysen

Diese Berichte enthalten Informationen zu allen Bedrohungen, für die Benutzer und/oder andere Sicherheitsebenen ohne Webroot SecureAnywhere DNS Protection anfällig gewesen wären.

Unterstützt durch Webroot BrightCloud® Web Classification

Webroot BrightCloud-Bedrohungsinformationen sind zuverlässig und werden von über 40 führenden Technologieanbietern verwendet, um verschiedene Aspekte ihrer Lösungen und Dienste zu verbessern. Sie schützen Millionen Webroot-Benutzer auf der ganzen Welt in Echtzeit.

Info zu Webroot

Webroot ist Anbieter für Netzwerk- und Endgerätesicherheit 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®-Endpunktlösungen, BrightCloud® Threat Intelligence Services und FlowScape®-Netzwerkverhaltensanalysen schützen Millionen Geräte in Unternehmen, bei Privatanwendern und im Internet der Dinge. Marktführende Unternehmen wie Cisco, F5 Networks, Citrix, 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