

Webroot® DNS Protection

Kombinieren Sie Datenschutz und Sicherheit für Cyber-Resilienz

Übersicht

Der Domain Name Service (DNS) ist das Adressbuch für das Internet. Eine vollständig verwaltete DNS-Sicherheitslösung ist ein wesentlicher Bestandteil der Cyber-Resilienz-Strategie jeder Organisation und grundlegend für die Gewährleistung der Sicherheit und des Datenschutzes Ihrer Internet-Konnektivität. Böswillige Akteure haben es zunehmend auf DNS-Anfragen abgesehen, da der Inhalt jeder Anfrage sichtbar ist und die Integrität der Anfrage kompromittiert werden kann. DNS-Anfragen können nicht nur verraten, welche Anwendungen verwendet werden, sondern sie zeigen auch im Klartext, welche Websites besucht werden.

Webroot® DNS Protection unterstützt DNS über HTTPS (DoH) vollständig und bietet gleichzeitig Datenschutz und Sicherheit als Kontrolloptionen, die sicherstellen, dass die Filterung von DNS-Anfragen und die Integrität weiterhin funktionieren. Im Gegensatz dazu lassen sich die DNS-Sichtbarkeit und die Protokollierungsstufen anpassen. Webroot® DNS Protection wird sicher über die gehärtete DNS-Resolver-Infrastruktur von Webroot in der Google Cloud™ gehostet und nutzt die Zugänglichkeit, Zuverlässigkeit, Stabilität und Leistung der globalen Rechenzentren von Google.

Schützender DNS-Dienst bietet nativen DoH-Datenschutz und Sicherheit

Unterstützt von erstklassigen Threat Intelligence-Services in Echtzeit

Webroot® DNS Protection wurde als SaaS-Lösung entwickelt, um niedrige Latenzzeiten, Zuverlässigkeit und sicheres Hosting zu gewährleisten und die Widerstandsfähigkeit eines Unternehmens gegen Cyberangriffe zu verbessern. Als SaaS-Lösung ist die Bereitstellung über die cloudbasierte Webroot-Verwaltungskonsole schnell, einfach und unkompliziert, egal ob in einem Netzwerk oder auf Roaming-Geräten. Das bedeutet, dass DNS-Anfragen über DoH auf der Ebene des Netzwerks und des Roaming User Agents vollständig gefiltert werden. Administratoren können steuern, wie alle DNS-Anfragen protokolliert werden. So können sie den Datenschutz so konfigurieren, dass er mit der DSGVO übereinstimmt, während sie diese Anfragen dennoch vollständig filtern können.

Webroot® DNS Protection nutzt die 6. Generation des maschinellen Lernens von BrightCloud® Threat Intelligence, um Website-Domains zu untersuchen und Websites in genaue Kategorien einzuordnen. BrightCloud® Threat Intelligence Services korrelieren Daten zwischen Domänen, URLs, IPs, Dateien, mobilen Anwendungen und mehr, um einen umfassenden und ständig aktualisierten Überblick über die Bedrohungslandschaft im Internet zu erhalten – nicht nur über URLs und IPs.

Wichtigste Vorteile

- ~75 % weniger Malware-Downloads mit unserem DNS-basierten Netzwerk-Filterdienst
- Vollständige Transparenz der Internetnutzung mit vollständigem Einblick in alle Anfragen, die an das Internet gestellt werden
- Weniger Infektionen durch Verringerung der Anzahl von Antworten auf bösartige und verdächtige Internetseiten
- Granulare und durchsetzbare Zugriffsrichtlinien
- Maximale Privatsphäre ohne Beeinträchtigung der Sicherheit und betrieblichen Effizienz

SaaS-Lösung mit schneller und einfacher Bereitstellung im Netzwerk oder auf Roaming-Geräten

Wie es funktioniert

Indem alle DoH-Internetanfragen über unsere gehärteten DNS-Server geleitet werden, die im hochsicheren Google Cloud™-Dienst gehostet werden, ermöglicht Webroot® DNS Protection die maximalen Datenschutz- und Sicherheitsvorteile von DoH und bietet gleichzeitig die Protokollierung, Transparenz, Filterung und Sicherheitskontrollen, die Sie für den Schutz und die effektive Verwaltung von DNS-Anfragen benötigen. Da Anwendungen beginnen, DNS-Anfragen direkt zu verschlüsseln, verlieren Firewalls den Überblick und die Kontrolle darüber, worauf im Internet zugegriffen wird. Webroot® DNS Protection verfolgt und filtert DoH-Anbieter und stoppt diese Verbindungen bereits bei der ersten Anfrage, so dass Sie die Kontrolle behalten.

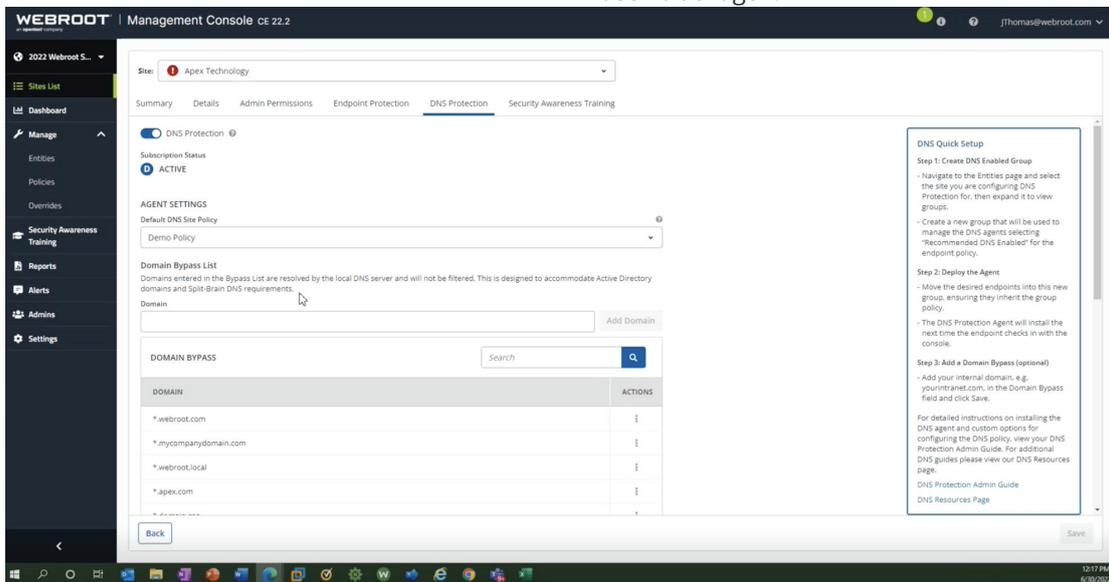
DNS-Anfragen über DoH werden auf Netzwerk- und Roaming-User-Agent-Ebene vollständig gefiltert. Mit Hilfe von Webroot® DNS Protection bleiben alle DNS-Anfragen für Ihr Unternehmen privat und für Ihren ISP oder andere neugierige Augen unsichtbar. Webroot® DNS Protection schützt alle Gerätetypen, einschließlich Windows-, Linux-, Apple®- und Android®-Geräte, die über Firmen-Wi-Fi, LAN und sogar Gast-Wi-Fi-Verbindungen auf das Internet zugreifen. Außerdem können Partner und Kunden das gesamte Netzwerk problemlos schützen, ohne eine statische IP-Adresse zu benötigen. Webroot® DNS Protection verbessert die DNS-Funktionalität bei Verbindungen über die beliebtesten VPN-Lösungen.

Speziell entwickelt, um die Widerstandsfähigkeit einer Organisation gegen Cyberangriffe zu verbessern

Richtlinienbasierte, granulare Zugriffskontrolle, die zu einer Verringerung der Anzahl von Kompromittierungen führt

OpenText Security Solutions vereint erstklassige Lösungen, die Ihrem Unternehmen helfen, cyber-resilient zu bleiben. Carbonite und Webroot können Sie dabei unterstützen, Bedrohungen von vornherein zu verhindern und zu schützen, die Auswirkungen durch schnelle Erkennung und Reaktion zu minimieren, die Daten nahtlos wiederherzustellen, um die Auswirkungen zu verringern, und Sie bei der Anpassung und Einhaltung der sich ändernden Vorschriften zu unterstützen.

Webroot® DNS Protection bietet Ihnen Transparenz und Vorteile bei der DNS-Filterung und Zugriffskontrolle, einschließlich vollständiger Unterstützung von DoH auf Netzwerk-, Gruppen-, Gerätebrowser-, Benutzer- und Roaming-Benutzerebene. Darüber hinaus bietet es einen vollständigen Einblick in die Internetnutzung mit allen Anfragen, die an das Internet gestellt werden, so dass Administratoren fundiertere Entscheidungen über Zugriffsrichtlinien treffen können. Weniger Infektionen durch eine geringere Anzahl von Antworten auf bösartige und verdächtige Internetadressen. Das bedeutet, dass DNS-Filterung die Anzahl der Kompromittierungen, Infektionen und die damit verbundenen Kosten für die Beseitigung von Problemen drastisch reduziert. Granulare und durchsetzbare Zugriffsrichtlinien ermöglichen es Administratoren, die Produktivität der Mitarbeiter, die Sorgfaltspflicht des Arbeitgebers sowie HR- und Compliance-Anforderungen durch erweiterte, anpassbare Richtlinienkontrollen nach Einzelpersonen, Gruppen oder IP-Adressen zu erfüllen. Insgesamt können Sie mit Webroot® DNS Protection Ihre Privatsphäre bewahren, ohne die Sicherheit und betriebliche Effizienz zu beeinträchtigen.



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.

© 2022 OpenText. Alle Rechte vorbehalten. OpenText, Carbonite und Webroot sind Marken von OpenText oder dessen Tochtergesellschaften. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. DS_071522

Erfahren Sie mehr unter
webroot.com.

CARBONITE® + WEBROOT®
OpenText Security Solutions