Webroot® DNS-Schutz

Der erste DNS-Schutzdienst, der Datenschutz und Sicherheit wirklich kombiniert, für mehr Cyberresilienz

Übersicht

Eine vollständig verwaltete DNS-Sicherheitslösung ist ein wesentlicher Bestandteil der Cyberresilienz-Strategie jeder Organisation und grundlegend für die Gewährleistung der Sicherheit und des Datenschutzes Ihrer Internet-Konnektivität. Da immer mehr Datenverkehr über HTTPS verschlüsselt wird, können Firewalls diese Kommunikation nicht mehr kontrollieren, wodurch die Notwendigkeit entsteht, diese Verbindungen bereits bei ihrem Aufbau zu verwalten. Darüber hinaus verwalten Anwendungen DNS-Abfragen zunehmend direkt und nicht mehr über die auf dem System konfigurierten DNS-Server.

DNS-Abfragen werden immer mehr von böswilligen Akteuren ins Visier genommen, da der Inhalt jeder Abfrage sichtbar ist und die Integrität der Abfrage gefährdet sein kann. DNS-Abfragen können nicht nur anzeigen, welche Anwendungen verwendet werden, sondern auch, welche Websites besucht werden, und zwar im Klartext.

Infolgedessen haben Organisationen erkannt, wie wichtig es für ihre Sicherheit und Privatsphäre ist, den Schutz der DNS-Schicht zum Schutz ihrer Netzwerke und einzelner Benutzer zu nutzen. Wenn staatliche Akteure DNS-Abfrageprotokolle zur Strafverfolgung von Bürgern verwenden oder die Internetnutzung für Analysen oder gezielte Werbung profiliert wird, ist es klar, warum DNS sich weiterentwickelt, um die Verschlüsselung mit DNS über HTTPS (DoH) zu verwenden.

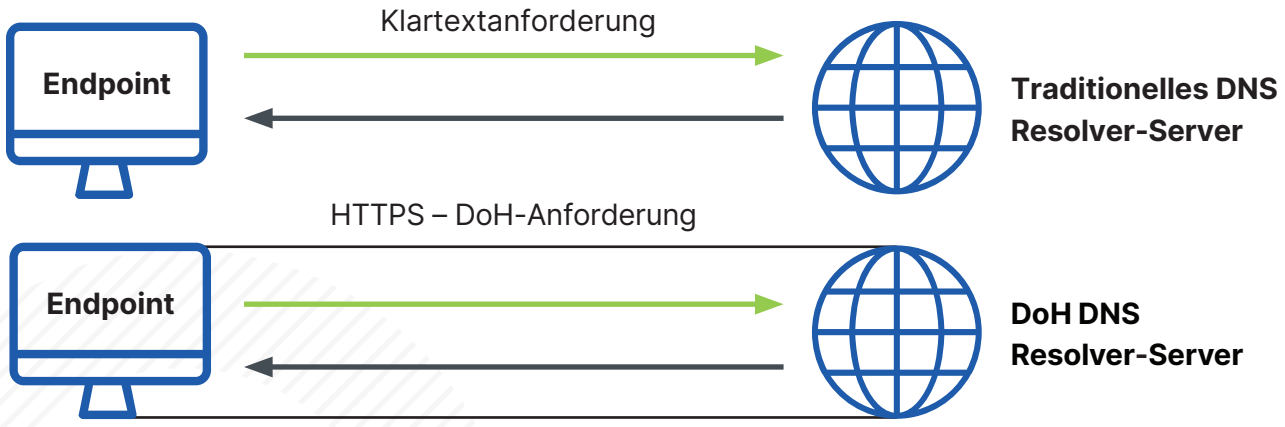
Wenn der Datenschutz verbessert wird, ist die Sicherheit leider oft gefährdet. Lösungen zum Filtern und Verwalten von DNS-Abfragen können die Sichtbarkeit und Kontrolle verlieren, die sie einst hatten. Die Verwendung von DNS über HTTPS nimmt zu. Internetbrowser und sogar Betriebssysteme beginnen, die Vorteile von DoH zu nutzen, da es den Datenschutz verbessert und gleichzeitig sicherstellt, dass Quelle und Inhalt der DNS-Abfrage echt sind.

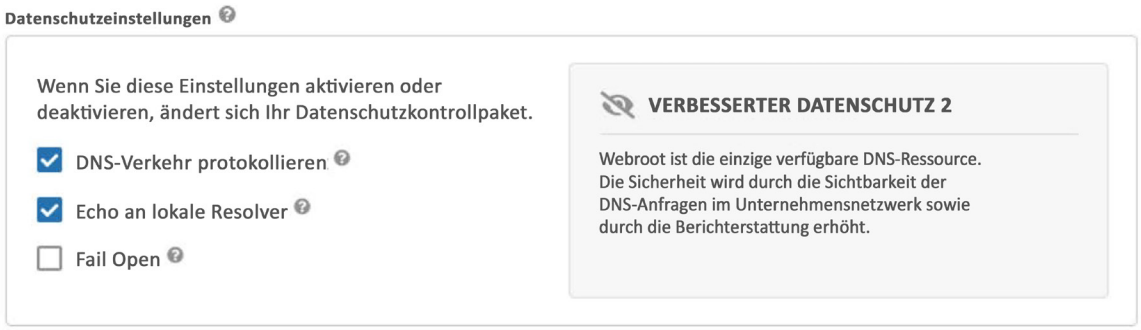
Um dem entgegenzuwirken, bieten die meisten kommerziellen und privaten DNS-Filterlösungen ebenfalls folgende Funktionen:

1. Blockieren der Verwendung von DoH, um die DNS-Filterung und Sichtbarkeit der Abfragen beizubehalten.
2. Erlauben von DoH-Abfragen, aber Verzicht darauf, DNS-Abfragen aus Sicherheitsgründen zu filtern und zu verwenden.

Erster DNS-Schutzdienst, der Privatsphäre und Sicherheit kombiniert

DoH ist eine logische Weiterentwicklung von DNS und sollte zur Verbesserung der Privatsphäre, der Sicherheit und





der allgemeinen Widerstandsfähigkeit gegen Cyber-Bedrohungen genutzt werden. Der neue Webroot® DNS-Schutz unterstützt DoH vollständig und bietet gleichzeitig Privatsphäre und Sicherheit als Kontrolloptionen, die sicherstellen, dass die Filterung und Integrität von DNS-Abfragen weiterhin funktioniert, während die Sichtbarkeit und Protokollierungsebenen von DNS anpassbar werden.

Das bedeutet:

- DNS-Abfragen über DoH sind vollkommen sicher und der Zugriffsinhalt wird auf Netzwerk- und Roaming-Benutzeragentenebene gefiltert.
- Alle Abfragen bleiben für Ihre Organisation völlig privat und für Ihren ISP oder andere neugierige Augen unsichtbar.
- Alle DNS-Abfragen werden mit hoher Genauigkeit mit marktführender Webroot BrightCloud® Threat Intelligence basierenden Richtlinien gefiltert, die auf IP-, Gruppen- oder Benutzerebene zugewiesen werden.
- Administratoren können steuern, ob DNS-Abfragen protokolliert werden, sodass sie den Datenschutz für jeden Benutzer entsprechend konfigurieren können.
- Der Webroot® DNS-Schutz wird sicher über die gehärtete DNS-Resolver-Infrastruktur von Webroot innerhalb von Google Cloud™ gehostet und nutzt die Zugänglichkeit, Zuverlässigkeit, Stabilität und Leistung der globalen Rechenzentren von Google.
- Durch die sichere Filterung aller DNS-Abfragen für risikoreiche Domänen können Unternehmen ihre Gefährdung durch Bedrohungen drastisch reduzieren.
- Administratoren können die Sichtbarkeit der lokalen Resolver konfigurieren, indem sie das Echo von DNS-Abfragen aktivieren und anderen Tools (z. B. SIEMs usw.) die Sichtbarkeit von DNS-Abfragen ermöglichen.

DNS-Abfragen sollten verschlüsselt werden, um ihre Privatsphäre und Integrität zu gewährleisten. Zusätzlich sollten DNS-Abfragen gefiltert werden, um die Gefährdung durch potenziell schädliche Internet-Domains zu verringern.

Maximaler Datenschutz

Indem wir alle Internet-Abfragen von DoH über unsere gehärteten DNS-Server leiten, die im Internet im hochsicheren Dienst Google Cloud™ gehostet werden, ermöglicht der Webroot® DNS-Schutz die maximalen Datenschutz- und Sicherheitsvorteile von DoH und bietet gleichzeitig die Protokollierung, Sichtbarkeit, Filterung und Sicherheitskontrollen, die Sie benötigen, um DNS-Abfragen effektiv zu schützen und zu verwalten.

Maximale Sicherheit

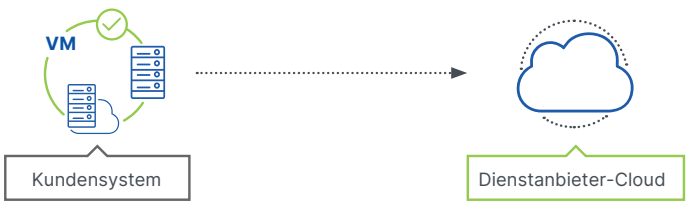
Grundsätzlich geht es bei der Sicherheit auf DNS-Ebene darum, dass Sie Ihren ausgehenden Netzwerk-/Benutzerverkehr genau filtern können. Um dies effektiv tun zu können, benötigen Sie umfassende, aktuelle Informationen über Web-Bedrohungen. Webroot BrightCloud® Threat Intelligence Services, die hinter dem Webroot® DNS-Schutz stehen, korrelieren Daten zwischen Domains, URLs, IPs, Dateien, mobilen Anwendungen und mehr, um einen umfassenden und ständig aktualisierten Überblick über die Internet-Bedrohungslandschaft – nicht nur URLs und IPs – zu erhalten.

Wenn Anwendungen beginnen, DNS-Abfragen direkt zu verschlüsseln, verlieren Firewalls an Transparenz und Kontrolle darüber, worauf im Internet zugegriffen wird. Der Webroot® DNS-Schutz verfolgt und filtert DoH-Anbieter, stoppt diese Verbindungen bei der ersten Abfrage und überlässt Ihnen die Kontrolle. Ergebnisse aus der Praxis zeigen, dass das Filtern ausgehender DNS-Abfragen über den Webroot-Dienst Malware und unerwünschten eingehenden Netzwerkverkehr stoppt, bevor er überhaupt Endpunkte oder Netzwerke erreicht.

Über die Webroot®-Plattform, nutzt der Webroot® DNS-Schutz Machine Learning der 6. Generation, um Website-Domänen zu untersuchen und Websites in genaue Kategorien einzuordnen. Webroot geht bei der Genauigkeit noch einen Schritt weiter, indem es diesen Kategorisierungen ein Vertrauensniveau zuweist, um einen zusätzlichen Datenpunkt zur Berücksichtigung bereitzustellen. Unsere Prozesse kategorisieren und bewerten Bereiche mit einer Fehlerquote von 1,5 % oder weniger, verglichen mit einer durchschnittlichen menschlichen Fehlerquote von 8 %.[1] (Anmerkung: die menschliche Fehlerquote der Experten ist die durchschnittliche Fehlerquote der Feststellungen eines Sicherheitsexperten).

Maximale Effizienz und Leistung

Webroot® DNS-Schutz wurde als SaaS-Lösung konzipiert und verwendet Google Cloud™, um niedrige



[1] Basierend auf internen Tests von Webroot.

Latenzzeiten, Zuverlässigkeit und sicheres Hosting zu gewährleisten. Der Dienst wurde speziell entwickelt, um die Widerstandsfähigkeit einer Organisation gegen Cyberattacken zu verbessern. Als SaaS-Lösung ist die Bereitstellung über die cloudbasierte Webroot-Verwaltungskonsole schnell, einfach und unkompliziert, egal ob auf Geräten innerhalb oder außerhalb des Netzwerks.

RMM- und PSA-Integrationen tragen ebenfalls dazu bei, Abläufe zu automatisieren und Kosten zu minimieren. Die zusätzliche Flexibilität des Webroot® Unity API und das Universal Reporter-Tool ermöglichen die vollständige Anpassung von Berichten und Datenprotokollauszügen für weitere Analysen.

DNS-Schutz im Überblick

- **Sicheres Google Cloud™ Hosting –** Das globale Netzwerk von Webroot mit gehärteten DNS-Resolver-Servern gewährleistet Datenschutz, Sicherheit und ständige Verfügbarkeit.
- **Keine vor Ort zu installierende Hardware –** Webroot® DNS-Schutz ist eine cloudbasierte Netzwerk- (Domänen-) Sicherheitsschicht, deren Einrichtung nur wenige Minuten dauert.
- **80+ URL-Zugriffskategorien –** Umfangreiche, granulare und hochgenaue Domänenfilter-Kategorisierungen ermöglichen die Durchsetzung des Benutzerzugriffs sowohl innerhalb als auch außerhalb des Netzwerks.
- **Schutz von WLANs und Gastnetzwerken –** Der Webroot® DNS-Schutz sichert alle Gerätetypen (einschließlich Windows-, Linux-, Apple®- und Android®-Geräten), die über Firmen-WLAN, LAN und sogar WLAN-Gastverbindungen auf das Internet zugreifen.
- **Roaming-Benutzerschutz –** Ein Windows-Agent steht für konsistente netzunabhängige Filterung für Roaming-Benutzer zur Verfügung.
- **Richtlinie nach Benutzer, Gruppe oder IP-Adresse –** Wir bieten flexible Einsatzoptionen und Richtlinienkontrollen für die meisten Verbindungssituationen.
- **Detaillierte Berichte auf Abruf –** Der Webroot® DNS-Schutz bietet vollständige Einsicht in alle DNS-Abfragen.
- **Unterstützung für eine breite Palette von Firewall-VPNs –** Wir haben den DNS-Agenten so konzipiert, dass er mit den Tools funktioniert, die Unternehmen und Managed Service Provider (MSPs) bereits verwenden, und dass er viele gängige VPNs unterstützt, darunter SonicWALL und andere.
- **Bildungswesen und Einhaltung von Vorschriften –** Der Webroot® DNS-Schutz hilft Organisationen bei der Einhaltung der Datenschutzgesetze in den USA und der EU, des HIPAA, PCI, des Family Educational Rights and Privacy Act (FERPA) und des Child Internet Protection Act (CIPA). Webroot ist auch Mitglied der Internet Watch Foundation.

Zu erwartende Ergebnisse

Webroot® DNS-Schutz bietet Ihnen Sichtbarkeit und Vorteile der Zugriffskontrolle durch DNS-Filterung, darunter:

- Volle Unterstützung von DoH auf Netzwerk-, Gruppen-, Geräte-Browser-, Benutzer- und Roaming-Benutzerebene.
- Vollständige Transparenz der Internetnutzung mit vollständigem Einblick in alle an das Internet gerichteten Abfragen, sodass die Administratoren besser informierte Entscheidungen über die Zugangsrichtlinien treffen können.
- Weniger Infektionen durch Verringerung der Anzahl der Reaktionen auf bösartige und verdächtige Internet-Sites, d. h. durch DNS-Filterung wird die Anzahl der Kompromittierungen, Infektionen und die damit verbundenen Kosten für die Behebung von Problemen drastisch reduziert.
- Mit granularen und durchsetzbaren Zugriffsrichtlinien können Administratoren die Produktivität der Mitarbeiter, die Sorgfaltspflicht des Arbeitgebers, HR- und Compliance-Abfragen durch fortschrittliche, anpassbare Richtlinienkontrollen nach Einzelpersonen, Gruppen oder IP-Adressen bedienen.

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.

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.

Kontaktieren Sie uns, um mehr zu erfahren – Webroot US

E-Mail: wr-enterprise@opentext.com

Telefon: +1 800 772 9383

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.