OpenText Core DNS Protection

Angriffe durch volle Kontrolle über DNS verhindern

Merkmale und Funktionen

- Alternative oder nicht autorisierte DNS-Quellen blockieren
- Zugriff auf schädliche Domänen oder Command-and-Control (C&C)-Server verhindern
- Alle DNS-Anfragen verschlüsseln, um DNS-Hijacks zu verhindern
- Alle DNS-Anfragen protokollieren, um Bedrohungen, Schwachstellen und verdächtiges Verhalten zu identifizieren
- Datenexfiltration über DNS stoppen

Vorteile

- Reduzierung von Malware um weitere 27,1 % verglichen mit nur AV (OpenText Cybersecurity Threat Report 2023)
- Datenexfiltration und Malware-Verbreitung durch DNS verhindern
- Remote- und Hybrid-Mitarbeiter in jedem Netzwerk schützen
- Einfache Bereitstellung mit sofortigen Ergebnissen; vollständig transparent für Benutzer

Es ist immer DNS

Das DNS ist ein wesentlicher Bestandteil aller Inhalte, auf die über Netzwerke und das Internet zugegriffen wird. Daher ist die Kontrolle des DNS für ein stabiles und sicheres Netzwerk unerlässlich. Leider ist die effektive Kontrolle über DNS seit der Einführung der DNS-Verschlüsselung immer schwieriger geworden. Dazu tragen auch die „Arbeit von überall aus“-Realität des hybriden Arbeitens und DNS-Anfragen auf Prozessebene, die von Malware verwendet werden können, um Kontrollen auf Systemebene zu umgehen, bei.

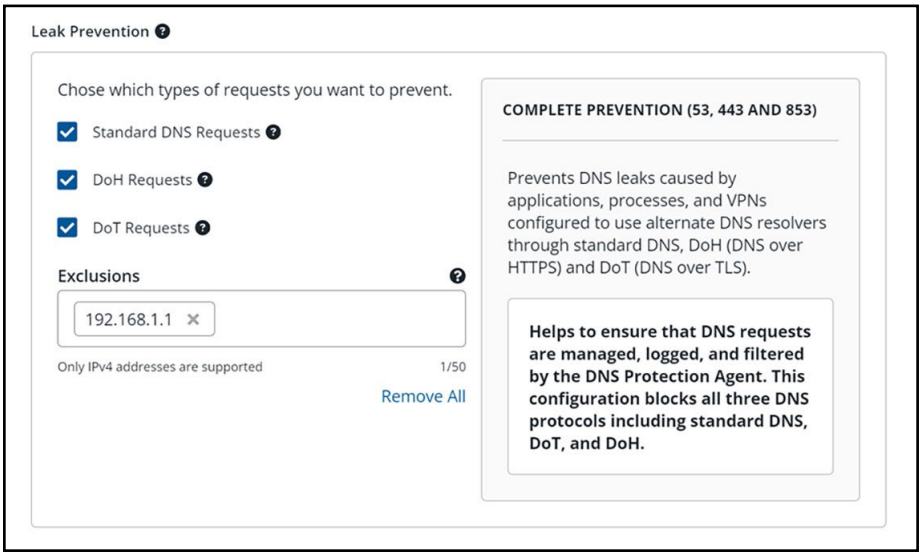
Über den Browser hinaus

Die DNS-Filterung ist oft mit dem Surfen von Websites im Internet und dem anschließenden Filtern von entsprechenden DNS-Anfragen verbunden. Leider reicht es nicht aus, Browser-Anfragen zu filtern, da Malware und andere Angriffe DNS auf Prozessebene nutzen können und die Browsersteuerung umgehen, um Angriffe voranzutreiben. Durch das Filtern von DNS für alle Prozesse kann OpenText Core DNS Protection auch die Kommunikation mit C&C-Servern blockieren, die Datenexfiltration verhindern und die Visibilität erhöhen, indem umfassende Protokolle zur Bekämpfung von Infektionen bereitgestellt werden.

DNS Leak Prevention und DoH

OpenText Core DNS Protection Leak Prevention ist in der Branche weiterhin führend in puncto Innovation und entwickelt weiterhin neue Methoden für DNS-Kontrolle und -Schutz. Drei Patente sind angemeldet und weitere in Arbeit.

Unsere patentierte DNS Leak Prevention dient beispielsweise als DNS-Firewall auf Geräteebene, damit Prozesse die DNS-Auflösung außerhalb des Agenten nicht ableiten können.



OpenText Core DNS Protection war die erste DNS-Schutz-Lösung, die die Herausforderung von verschlüsseltem DNS oder DNS über HTTPS (DoH) gemeistert hat. Diese Lösung kann Systemkonfigurationen umgehen, indem sie eine verschlüsselte DNS-Auflösung aus alternativen Quellen ermöglicht. Durch die Nachverfolgung und Kontrolle des Zugriffs auf DoH-Anbieter verhindert OpenText Core DNS Protection unbefugte Verbindungen, wenn DNS-Anfragen versucht werden.

Obwohl DoH Kontrolle benötigt, ist es auch ein sehr leistungsstarker Mechanismus für die DNS-Auflösung. Der OpenText Core DNS Protection Agent nutzt DoH für eine zuverlässige und verschlüsselte DNS-Auflösung, wodurch sichergestellt wird, dass alle DNS-Anfragen für Ihr Unternehmen privat bleiben und vor Ihrem ISP und anderen neugierigen Augen verborgen bleiben.

Einfach zu implementieren und für Benutzer transparent

OpenText Core DNS Protection ist eine cloudbasierte SaaS-Lösung, die sich als sicher, zuverlässig, skalierbar und leistungsstark erwiesen hat. Ob Sie das gesamte Netzwerk oder Roaming-Geräte schützen, die webbasierte Konsole bietet intuitive DNS-Richtlinienkontrollen und -Berichte. Der DNS Protection Agent kann einfach als MSI oder optional als Erweiterung von OpenText Core Endpoint Protection auf Geräte übertragen werden. Administratoren können steuern, wie alle DNS-Anfragen protokolliert werden, und so konfigurieren, welche Informationen erfasst werden, um die DSGVO zu erfüllen.

Netzwerk- oder Roaming-Geräte

OpenText Core DNS Protection kann so konfiguriert werden, dass das gesamte Netzwerk, einschließlich Unternehmens-WLAN, LAN und sogar Gast-WLAN-Verbindungen, geschützt wird, um Bedrohungen durch BYOD (Bring-Your-Own-Device) und andere Geräte, auf denen ein Agent nicht möglich oder erwünscht ist, zu verringern.

Bei Roaming-Geräten gewährleistet der OpenText Core DNS Protection Agent die DNS-Kontrolle. Der Agent leitet alle DNS-Anfragen über unsere gesicherten DNS-Server und setzt Filter-, Protokollierungs- und Sicherheitskontrollen ein, die Sie benötigen, um hybrides und mobiles Arbeiten zu ermöglichen, unabhängig davon, in welchem Netzwerk das Gerät verwendet wird

Fehlalarme vermeiden

Fehlalarme werden häufig durch schlechte Bedrohungsinformationen verursacht, die sich auf Benutzer auswirken, indem sie Workflows unterbrechen und Administratoren Probleme bereiten. OpenText Core DNS Protection minimiert Fehlalarme durch Nutzung unserer proprietären OpenText Threat Intelligence Platform. Das ausgereifte Machine Learning der sechsten Generation von OpenText bietet unübertroffene Bedrohungsinformationen mit Zuverlässigkeit, Genauigkeit, Tiefe und Pünktlichkeit.

Die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberangriffen verbessern

OpenText Cybersecurity vereint branchenführende Lösungen, die Ihr Unternehmen dabei unterstützen, cyberresilient zu bleiben. OpenText kann Ihnen dabei helfen, das Aufkommen von Bedrohungen bereits im Ansatz zu verhindern und die Folgen einer erfolgreichen Attacke durch eine schnelle Erkennung und eine nahtlose Wiederherstellung betroffener Daten möglichst gering zu halten, damit Sie die sich immer ändernden behördlichen Vorschriften weiterhin einhalten können.

Weitere Informationen oder eine Testversion erhalten Sie unter OpenText Core DNS Protection.

OpenText Cybersecurity bietet umfassende Sicherheitslösungen für Unternehmen und Partner jeder Größe. Von Prävention, Erkennung und Reaktion bis hin zu Wiederherstellung, Untersuchung und Compliance: Unsere einheitliche End-to-End-Plattform unterstützt Kunden dabei, mit einem ganzheitlichen Sicherheitsportfolio ihre Cyber-Resilienz zu verbessern. Basierend auf praxisbezogenen Erkenntnissen aus unseren kontextrelevanten Echtzeitinformationen zu Cyberrisiken profitieren Kunden von OpenText Cybersecurity von hochwirksamen Produkten, Einhaltung aller Compliance-Vorschriften und einer einfachen Sicherheitslösung, die sie bei der Verwaltung von Unternehmensrisiken unterstützt. DS_030623

ELOVADE

Kontaktdaten für Deutschland & Österreich:
ELOVADE Deutschland GmbH
security@elovade.com
DE: +49 6441 67118 842
elovade.com/opentext-cybersecurity
AT: +43 820 0010 36

Kontaktdaten für die Schweiz:
ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/opentext-cybersecurity