OpenText Core DNS Protection

Prevent attacks by taking full control of DNS

Features

- Block alternate or unauthorized sources of DNS
- Prevent access to malicious domains or Command-and-Control (C&C) servers
- Encrypt all DNS requests to prevent DNS hijacks
- Log all DNS requests to identify threats, vulnerabilities, and suspicious behaviors
- Stop data exfiltration through DNS

Benefits

- Reduce malware by an additional 27.1% vs AV alone (OpenText Cybersecurity Threat Report 2023)
- Prevent data exfiltration and malware proliferation through DNS
- Protect remote and hybrid workers on any network
- Deploy easily with immediate results; completely transparent for users

It's always DNS!

DNS is integral to everything accessed on networks and the internet, so control of DNS is essential to a stable and secure network. Unfortunately, effective control of DNS has become more challenging since the advent of DNS encryption, the "work from anywhere" reality of hybrid work, and now process-level DNS requests that can be used by malware to bypass system-level controls.

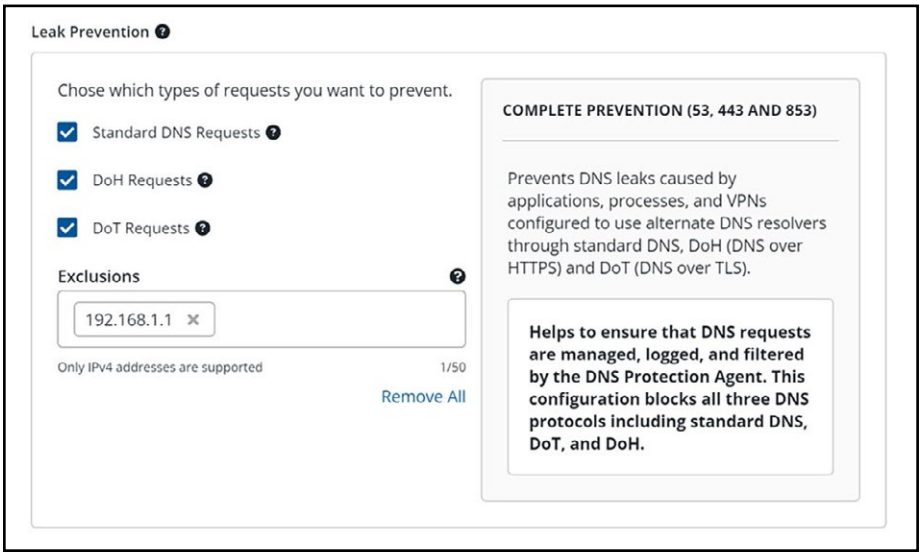
Beyond the browser

DNS filtering is often associated with browsing websites on the internet and then filtering the corresponding DNS requests. Unfortunately, just filtering browser requests is inadequate because malware and other attacks can leverage DNS at a process level, bypassing browser controls to advance attacks. By filtering DNS for all processes, OpenText™ Core DNS Protection can also block communication with C&C servers, prevent data exfiltration, and increase visibility with comprehensive logs to combat infections.

DNS Leak Prevention and DoH

OpenText Core DNS Protection Leak Prevention continues to lead the industry in innovation, creating new methods to control and secure DNS with three patents filed and more on the way.

For example, our patented DNS Leak Prevention feature acts as a device-level DNS firewall to stop any process from deriving DNS resolution outside of the agent.



OpenText Core DNS Protection was the first protective DNS solution to tackle the challenge of encrypted DNS or DNS over HTTPS (DoH), which can bypass system configurations by allowing encrypted DNS resolution from alternate sources. By tracking and controlling access to DoH providers, OpenText Core DNS Protection stops unauthorized connections as DNS requests are attempted.

Though DoH needs control, it is also a very powerful mechanism for DNS resolution. The OpenText Core DNS Protection agent leverages DoH for reliable and encrypted DNS resolution, which ensures all DNS requests remain private to your organization and invisible to your ISP or other prying eyes.

Easy to implement and transparent to users

OpenText Core DNS Protection is a born-in-the-cloud SaaS solution proven to be secure, reliable, scalable, and performant. Whether protecting the entire network or roaming devices, the web-based console provides intuitive DNS policy controls and reporting. The DNS Protection agent can simply be pushed to devices as an MSI or—optionally—as an extension of OpenText™ Core Endpoint Protection. Admins can control how all DNS requests are logged, allowing configuration of what information is captured to help comply with GDPR.

Network or roaming devices

OpenText Core DNS Protection can be configured to secure the entire network, including corporate Wi-Fi, LAN and even guest Wi-Fi connections, reducing threats on BYOD and other devices on which an agent is not possible or desirable.

For roaming devices, the OpenText Core DNS Protection agent ensures control of DNS. The agent routes all DNS requests through our hardened DNS servers, enforcing the filtering, logging, and security controls you need to empower hybrid and remote work no matter what network the device is using.

Avoid false positives

False positives are often caused by poor threat intelligence, impacting users by interrupting workflows and creating headaches for administrators. OpenText Core DNS Protection minimizes false positives by leveraging our proprietary OpenText™ Threat Intelligence platform. OpenText's mature, sixth-generation machine learning provides unmatched threat intelligence with reliability, accuracy, depth, and timeliness.

Enhance your Organization's Resilience against Cyberattacks

OpenText Cybersecurity brings together best-in-class solutions to help your business remain cyber resilient. OpenText can help you prevent and protect from threats happening in the first place, minimize the impact by quickly detecting and responding, recover the data seamlessly to reduce the impact, and help you adapt and comply with changing regulations.

To learn more or request a trial, visit OpenText Core DNS Protection.

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_030623

opentext™