OpenText Core DNS Protection Leak Prevention Feature

Benefits

Control Regained

Administrators regain control of DNS, preventing leaks and ensuring that DNS requests are in line with configured settings.

Enhanced Security

When DNS requests are filtered, logged and reportable, administrators enhance protection by not providing access to resources that could compromise a device or system, while maintaining visibility into activity and potential threats.

Encrypted DNS

DNS Protection fully supports DoH and leverages it for communication to the DNS Protection resolvers. This ensures that DNS requests are resolved by the expected server, and that they are encrypted, safeguarding DNS from redirection and unauthorized resolutions.

DNS leaks pose a significant threat to network security, potentially exposing sensitive information, compromising privacy, and bypassing security measures. OpenText™ Core DNS Protection offers a robust solution to counteract these risks through its innovative DNS Leak Prevention feature.

What is a DNS leak and why does it matter?

A DNS leak occurs when DNS resolution is unexpectedly performed by an unknown or unauthorized source, putting the integrity of DNS, network stability, and privacy at risk. Without a solution that addresses DNS leaks, organizations allow the potential for malware to proliferate through mechanisms like:

- Circumvention of DNS Filtering
- Uncontrolled DNS Resolution
- Missed Logging and Visibility
- Data Exfiltration

Malware Exploiting DNS Leaks

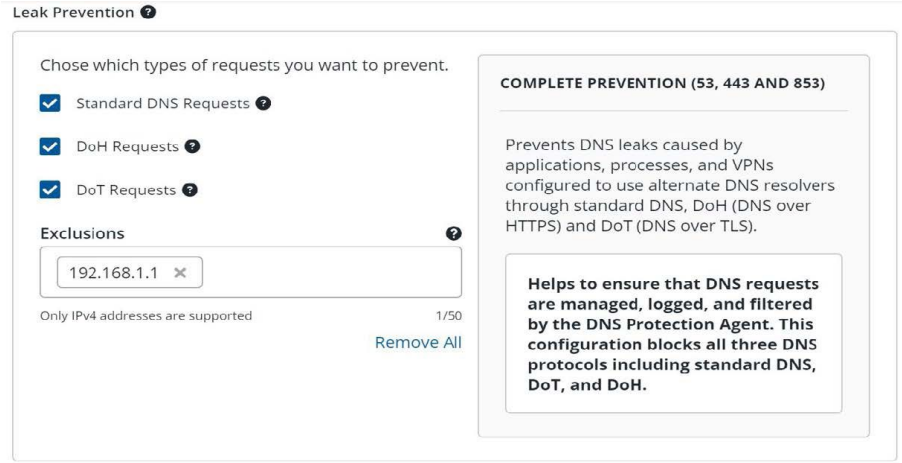
Here are just a few of the many examples of malware that spreads from DNS leaks:

DNSMessenger is a malware that uses DNS queries to communicate with its command and control (C2) server. It does not rely on the system's DNS settings, but instead uses its own resolver to send DNS requests over TCP port 853, which is usually used for DNS over TLS (DoT). This way, it can evade network monitoring and firewall rules that only inspect UDP port 53, which is the standard port for DNS.

PowerDNS is a malware that also uses DNS queries to communicate with its C2 server, but it uses a different technique to bypass DNS controls. It uses the Windows API function DnsQuery to resolve domain names at a process level, instead of using the system's DNS resolver. This allows it to avoid DNS cache poisoning and DNS hijacking attacks that modify the system's DNS settings.

DNSpionage is a malware that targets government and private entities in the Middle East. It uses two methods to bypass DNS controls: one is to use DoT to encrypt its DNS traffic and avoid detection, and the other is to use a rogue DNS resolver that is controlled by the attackers. The rogue resolver can return malicious IP addresses for legitimate domains, redirecting the victims to phishing or malware sites.

OpenText Core DNS Protection Leak Prevention Feature



As seen in the figure above, DNS control is easily established through DNS Policy settings in the online Management Console, providing control of DNS. DNS Leak Prevention acts as a DNS firewall, selectively stopping unauthorized sources of DNS resolution, thereby significantly improving stability and security.

Standard DNS:

Port 53 is blocked to stop alternate DNS resolution, ensuring DNS is only provided by approved DNS resolvers and the DNS Protection agent.

DNS over TLS (DoT):

Encrypted DNS over port 853 is blocked to stop processes from deriving DNS resolution directly, even when encrypted.

DNS over HTTPS (DoH):

DNS requests encrypted over HTTPS are the most challenging to prevent. To achieve this, encrypted DNS requests are blocked on port 443 to DoH providers.

OpenText Core DNS Protection, with its powerful DNS Leak Prevention feature, not only addresses the vulnerabilities associated with DNS, but also empowers administrators with enhanced control, visibility, and security. By preventing unauthorized DNS resolution, this feature establishes a robust layer of defense against potential threats while ensuring the integrity and privacy DNS.

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