opentext™ | Cybersecurity

WHITE PAPER

Webroot DNS Protection

Protect your anywhere workforce and network from web-based threats

The internet is part of today's everyday work life. Employees need to use the web for countless work-related purposes, but without secure, private, and visible control over internet traffic, it can expose organizations to a wide range of security threats.

That's because the domain name system (DNS) is a coveted attack vector for malicious actors. DNS is an Internet system for the assigning of Internet Protocol (IP) addresses to domain names. Simply put, DNS interprets human-friendly host names to PC-friendly IP addresses.

Serving as the address book for the internet, DNS by default provides threat actors visibility into the content of each request, and the integrity of the request can be compromised. It's not a surprise, then, that cybercriminals are increasingly using DNS request to deliver their attacks:

- Over one third of all attacks are delivered via DNS[1]
- Phishing and malware are the top two DNS based attacks experienced by organizations[2]
- 43% of organizations do not secure their DNS Server[2]

80%

of malware uses DNS to deliver the attack.

If left unprotected, DNS creates a security concern for organizations because 80% of malware uses DNS to unleash an attack and steal data.[3] Also, with organizations commonly providing a remote and hybrid work model, the network firewall no longer serves as the single, failsafe solution for web security. Collectively, these market dynamics are driving the need for organizations to adopt DNS security.

DNS security provides a layer of protection between an employee and the internet by blocking access to inappropriate sites by leveraging threat intelligence. Of course, the right solution also needs to maximize privacy without compromising security and operational efficiency. By adopting DNS security, organizations can better control their networks while maintaining the security and privacy needed to protect their users (whether they're remote or in the office) from accessing malicious sites.

This paper explores the security issues that DNS brings and how Webroot DNS Protection helps organizations safeguard against the risks of web-based threats.

Internet access is essential for today's 'online' work life. But what security risks does it create for organizations?

Remote workforce needs additional security

With today's remote and hybrid workforce, users take their devices home, on the road, and into the local coffee shop. With internet usage no longer restricted by the corporate firewall to keep the bad actors out, it increases the attack surface of the organization's digital environment.

Security leaders agree that this expanded attack surface is a concern with 66% of CISOs indicating that remote working make their organization more vulnerable to cyberattack.[4]

Successful attacks leading to financial losses

DNS was built first and foremost to respond to internet queries correctly and efficiently, not question their intent. As a result, cyberattacks using DNS have become one of the most significant threats to modern work life.

In fact, nearly 79% of organizations have experienced DNS attacks, and they cost a lot of money, too. Each successful DNS attack cost companies an average of USD 924,000. [5]

Attacks creating operational downtime

Cybercriminals use a range of techniques to unleash their DNS attack and deliver their payload. Once inside, the bad actor can install malware, steal sensitive data, change code, and even install new access points.

We've all heard the horror stories: just one successful attack can disrupt operations and occupy IT teams for weeks to successfully restore the systems. Indeed, 82% of the companies experienced application downtime, whether in-house or in the cloud, significantly due to the DNS attacks.[5]

A modern approach to protecting internet access: Webroot DNS Protection

Webroot makes it easy for organizations to address DNS security risks with accurate, effective protection for all your users, whether they're working remotely or in the office.

Webroot DNS Protection secures your network and roaming users by filtering DNS and eliminating malware and other network-based attacks. Our DNS Protection is powered by our industry leading BrightCloud Threat Intelligence that uses sixth generation ML and AI to provide your organization with timely and accurate filtering of domains, URLs, and IP addresses. Plus, our solution fully supports DoH (DNS over HTTPS), to ensure all encrypted DNS requests are secure and accurate

Safeguarding your organization with Webroot DNS Protection

DNS simply resolves internet requests and translates them into their unique Internet Protocol (IP) addresses. Bad actors exploit this clear text service many different ways. With Webroot DNS Protection, your organization can safeguard against the security risks inherent in DNS.

Webroot DNS Protection empowers you to control your organization's network while maintaining the security and privacy needed to protect your users (remote and roaming) from accessing malicious sites.

Remote protection

Webroot provides an effective DNS security layer to safeguard your remote workforce. Through the DNS Protection Agent, all DNS requests (including remote users) can be filtered and logged, regardless of what internet connection is in use. Policies can be set at the group or individual level to restrict access to malicious and unauthorized domains and stop breaches before they impact the network.

Accurate filtering

Our DNS Protection is powered by our BrightCloud Threat Intelligence (BCTI), which uses sixth generation ML and AI to provide timely and accurate DNS filtering. It accurately filters DNS requests, blocking phishing and malware sites in real time, while enabling organizations to avoid the administrative burden of false positives.

DNS over HTTPS (DoH) Support

With the advent of DoH, encrypted DNS traffic has become difficult to control. Webroot addresses this for organizations with our solution that fully supports DoH. The Webroot DNS Protection remote agent also leverages DoH for all communication with the core, providing secure DNS resolution while ensuring all communication is encrypted and from a trusted source. This enables organizations to align with NSA recommendations.

Flexible deployment options

Webroot DNS Protection provides two deployment options: as a standalone solution or in combination with Webroot Endpoint Protection (EPP). The DNS Protection agent can be installed directly on a system or managed through Webroot EPP. The Webroot EPP option provides an integrated approach, allowing organizations to centrally manage endpoint and DNS security. This combination can help reduce threats entering your organization by about 33%. The standalone DNS option enables organizations to deploy Webroot DNS Protection as a security layer while separately leveraging existing investments in a third party EPP or EDR solution.

Ease of management

It's simple to manage DNS Protection from the Webroot Management Console, which provides a single-pane-of-glass for managing all Webroot products. Through the console, customers can quickly deploy and manage DNS Protection, enabling IT and security teams to reduce admin time and improve efficiency.

Reduce helpdesk costs

DNS Protection prevents threats from entering your organization at the DNS layer therefore reducing the number of compromises, infections, and associated remediation costs that your IT staff have to deal with. This helps reduce the number of calls to your helpdesk staff due to infections.

A success story: MSP reduces helpdesk calls by 40% with Webroot DNS Protection

Founded in 1986, Sedona Technologies is a large and established IT and engineering services firm with a successful managed services division. The company has offices in over 30 US cities and annual sales of over $110 million.

DNS security challenges

When looking to add network-level protection to the MSP's security services offerings, they hit snags during the rollout phase of a proxy-based solution. Sedona clients with users making DNS requests to malicious sites had been experiencing frequent infections.

"We originally didn't go with a DNS solution, but more of a proxy-based solution. But our partner became very difficult to work with. The number of steps it took to get the product up and running for a client required far more resources than it should have."

That led Sedona to investigate other options for protecting their clients while also conserving resources.

How Webroot DNS Protection delivered benefits

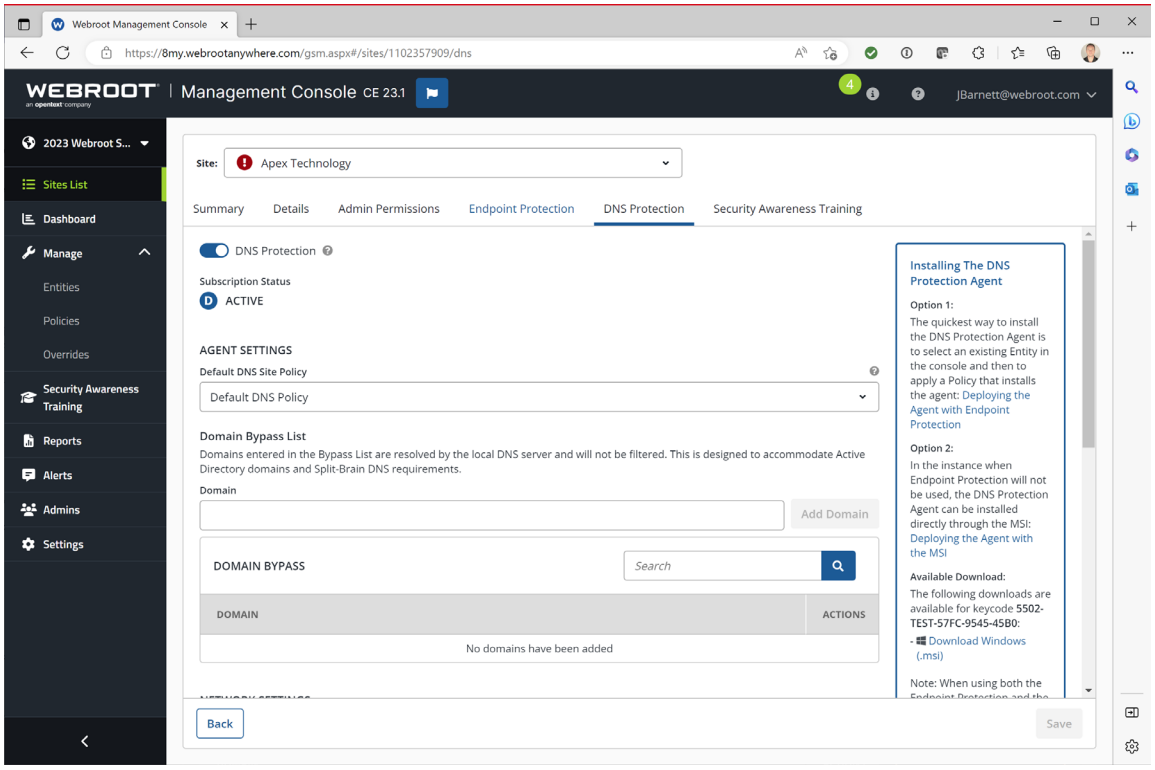
"We needed a simpler, more streamlined solution. We evaluated a lot of vendor products and ultimately the decision to go with Webroot was based on the experience of working directly with the staff. You guys listened. There was no delay. The level of service was just beyond everything else."

What happened after Sedona switched to Webroot DNS Protection?

- 270 internet threats blocked daily across its customer base
- 51 spear phishing attempts blocked monthly over a single quarter
- 40% fewer help desk calls

"For our clients with DNS Protection, help desk calls are reduced by almost 40%."

- Jason Ballard
IT Solutions Manager
Sedona Technologies



1. Global Cyber Alliance, 2021
2. EfficientIP 2022 Global DNS Threat Report, conducted by IDC
3. Cyber Theory. The Threats from Unsecured DNS and Domains.
4. Verizon. Mobile Security Index. 2022.
5. Webinar Care. DNS Security Statistics 2023. January 2023.

opentext™ | Cybersecurity

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. WP_021323