ThreatDown™
Powered by Malwarebytes

Data Sheet

ThreatDown DNS (Web Content) Filtering

Prevent web-based threats; protect productivity

Overview

90% of organizations experienced one or more DNS attacks.[1] Therefore, they need simple and effective protective against nefarious actors that exploit web-based attacks. ThreatDown DNS (Web Content) Filtering extends our cloud-based Nebula security platform to provide web protection that keeps your end users safe and productive. This builds on the protection against internet attacks already provided in the platform's prevention capabilities, such as brute force protection and anomaly detection.

You can easily block website and content to align internet access with your organization's cybersecurity or code of conduct policies.

ThreatDown DNS Filtering Advantages

Promote Productive Web Use

With ThreatDown DNS Filtering, you can manage access to whole categories of websites (e.g., gambling, adult content, etc.) while also maintaining controls to tailor access that meets your organization's specific requirements for security and compliance. These controls keep web-based threats and online content from wreaking havoc on your organization and reduce the risk and potential for productivity distractions.

Enforcing your policies on internet use provides your end users a safer, more productive internet experience and delivers the browser and protection for your essential web-based business apps.

By default, DNS queries are in plaintext, making them susceptible to interception and misdirection. DNS Filtering uses DNS over HTTPS (DoH) protocols to encrypt and protect your DNS queries, allowing you to hide DNS from attackers and third parties.

And for the web-based apps that run your operations, DNS Filtering helps protect against risks introduced by vendors, partners, or other third-party collaborators who need to interact with your CRM, ERP, or other enterprise systems. And if malicious content sneaks into your environment, ThreatDown's real-time protection capabilities have your back, helping you detect and respond to suspicious content.

Challenges

- **Greater risks** - 90% of organizations experienced one or more DNS attacks[1]
- **Loss of productivity** - 7.5 hours a week employees spend browsing social media at work[2]
- **Need for compliance** - 137 countries have legislation to secure the protection of data and privacy[3]

Benefits

Protect your organization, improve employee productivity and satisfy compliance requirements, all without adding complexity

- **Improve security** - Reduce threats posed by malicious domains and phishing site
- **Increase employee productivity** - Prevent employees from accessing time-wasting websites that have no business purpose
- **Satisfy regulatory mandates** - Reduce the risk of fines imposed for failing to meet government and industry regulations

[1] IDC 2023 Global DNS Threat Report. [2] Teamstage. [3] Unctad.

Deploy Quickly and Easily

ThreatDown customers can instantly add DNS Filtering to their existing instance of ThreatDown EDR, EP, IR, or server solutions. As with other ThreatDown solutions for Nebula, activation simply appears within the menu, so it's simple to employ safer web content policies directly from the same ThreatDown console you already trust for protection and remediation.

New ThreatDown users can deploy DNS Filtering at the same time as deploying the Ultimate bundle via the ThreatDown platform. The platform stands up within a day, enabling you to realize security improvements on day one.

Nebula Security Platform

When it comes to managing endpoint protection, organizations need a simple solution that relieves constrained IT and security resources by offering visibility into prioritized vulnerabilities and emerging threats. ThreatDown DNS Filtering is built to extend our cloud-based Nebula security platform, making it easy to manage all your ThreatDown solutions.

ThreatDown DNS Filtering: Your Safest Choice

- ✓ Gain a single, unified platform for endpoint protection and web content filtering
- ✓ Insulate browser and web app interactions against threats
- ✓ Allow exceptions, backed by real-time protection against malicious downloads
- ✓ Understand activity for website exceptions, blocked sites, and potential DDoS attacks
- ✓ Encrypt DNS traffic to protect against leaked domain information
- ✓ Safeguard against threat actors that create false web domains
- ✓ Deploy easily in under a day and add functionality immediately

Request a Trial

To learn more, please contact your account team or your authorized channel partner. You may also contact us to communicate with a local sales expert: www.threatdown.com/custom-quote/