ThreatDown™
Powered by Malwarebytes

DATA SHEET

THREATDOWN DNS FILTERING

Prevent web-based threats; protect productivity

OVERVIEW

Over the past two years, the traditional enterprise has been turned inside out. With remote work established and hybrid work taking shape, organizations will need an always-connected defensive posture to remain secure against the business risks remote users may introduce. In addition, recent geopolitical unrest is causing new security and risk trends, highlighting ongoing strategic shifts in the cybersecurity ecosystem. These crises are expected to have a broad industry impact and significant potential for threat actors.

Most organizations recognize vendor consolidation as an avenue for more efficient security, with many navigating this path. And consolidation, while challenging, is achievable today. More streamlined operations and reduced risk are viable, and ThreatDown, powered by Malwarebytes, delivers with better-integrated solutions that predicate operational efficiency.

Organizations need simple and effective protection from nefarious actors. ThreatDown DNS Filtering module 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.

CHALLENGES

26% of all breaches originate from web application attacks.[1]

88% of malware-infected websites aren't blacklisted by search engines.[2]

With remote work, organizations need more than network perimeter controls to **stop web-based threats**.

Employing website and content filtering capabilities as part of an endpoint protection solution helps keep your digital ecosystem safe and further protect your business, providing many benefits:

- Blocks connections to malicious web servers attempting to deliver malware payloads to your system
- Protects users from falling for a phishing attempt by blocking their access to the malicious website
- Restricts employees from website categories, such as social media, gambling, or shopping that may decrease productivity

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

PREVENT THREATS FROM ONLINE ACTIVITY

Keep web-based threats and online content from wreaking havoc on your organization. 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.

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

ThreatDown DNS Filtering module gives your IT and security teams the control and flexibility to manage and secure internet use to mitigate your organization's exposure to internet-originated threats. 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.

[1] Verizon. Data Breach Investigation Report. 2021.
[2] Expert Insights. 50 Web Security Stats You Should Know In 2022. January 2022.

PROMOTE PRODUCTIVE WEB USE

The internet is a great resource but can also be a time-sink that shreds productivity. ThreatDown DNS Filtering allows you to reduce your organization's risk from threats, as well as the potential for productivity distractions.

And for the web-based apps that run your operations, our DNS Filtering module 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. 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.

DEPLOY QUICKLY AND EASILY

ThreatDown, powered by Malwarebytes, customers can instantly add the DNS Filtering module to the existing instance of ThreatDown EDR, EP, IR, or server solutions. As with other ThreatDown modules for Nebula—like our Vulnerability and Patch Management modules, 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 the DNS Filtering module at the same time as deploying 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 module is built to extend our cloud-based Nebula security platform, making it easy to manage all your ThreatDown solutions from a single platform: ThreatDown Incident Response (IR), Endpoint Protection (EP), and Endpoint Detection and Response (EDR).

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 modules 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: malwarebytes.com/business/contact-us

ThreatDown™ Powered by Malwarebytes | www.malwarebytes.com/business | corporate-sales@malwarebytes.com | 1.800.520.2796