threatER

EnforceDNS

threatER ENFORCE DNS

EnforceDNS is a cutting-edge protective DNS solution that leverages extensive authoritative domain intelligence and unparalleled insight into attacker infrastructure. EnforceDNS blocks known-bad domains and detects and blocks 'unknown' malicious domains faster and more effectively than any other solution in the industry. EnforceDNS is designed to meet the cybersecurity needs of organizations of all sizes. From those with minimal IT staff to the most complex enterprises, EnforceDNS offers an intuitive, easy-to-deploy, and scalable solution. It seamlessly integrates with existing infrastructure, providing deep, insightful, and comprehensive protection for both small and large organizations.

HIGHLIGHTS & BENEFITS

- Real-time protection with the EnforceDNS Decision Engine
- Unrivaled intelligence from the threatER Adversary Infrastructure Platform
- Enforce appropriate use policies with flexible content filtering
- Flexible deployment options adapt to your environment
- Get visibility on blocked and suspicious traffic
- Robust API for custom automation

ENFORCEDNS KEY FEATURES

threatERs real-time decision engine evaluates each outbound DNS request on your network or endpoint to determine whether it should be permitted. Utilizing over 50 meticulously refined rules and processes, our engine instantly responds to user requests, enabling access to safe sites while blocking malicious or inappropriate ones.

The threatER Decision Engine is powered by infrastructure intelligence sourced from the threatEr Adversary Infrastructure Platform. This platform processes billions of data points daily, utilizing unique and proprietary, restricted, commercial, and open-source intelligence sources. It profiles the latest malware infrastructure, suspicious domain registrations, and various other risk indicators to ensure robust protection.

Set appropriate use policies by configuring specific internet categories that employees are prohibited from accessing. You can also establish allow and blocklists and create custom rules for additional protection. Integrate your Microsoft Entra ID (Azure AD) groups with custom policies for streamlined, enterprise-wide enforcement.

Dashboards, custom filters, and alerts provide visibility into blocked, malicious, and suspicious traffic, helping you stay proactive and enhance your organization's resilience.

EnforceDNS APIs give you the power to build automation that supports your operational goals, whatever they are.

threatER

PROTECTIVE DNS USE CASES

- **Malware, Ransomware & Phishing Protection** EnforceDNS blocks access to malicious domains with the highest level of efficacy in the industry, preventing malware infections, ransomware and phishing attacks. By filtering out harmful websites, EnforceDNS safeguards users from inadvertently downloading malware or falling victim to phishing scams.
- **Data Exfiltration Prevention** With its advanced monitoring capabilities, EnforceDNS detects and blocks suspicious DNS queries that indicate data exfiltration attempts. This is crucial for identifying and stopping command-and-control (C2) communications used by attackers to transfer stolen data out of the network.
- **Customizable Filtering Policies** EnforceDNS adapts to your security needs by allowing customizable filtering policies that block both malicious content and websites that violate company standards. It continuously integrates with real-time threat intelligence feeds to ensure up-to-date protection against emerging threats while also enforcing compliance with regulatory requirements and internal policies. This ensures that company devices and networks remain secure, productive, and compliant.
- **Unmatched Visibility for Effective Risk Management** EnforceDNS provides comprehensive visibility into the risks facing your organization by analyzing patterns of employee behavior and identifying potential security threats. This insight enables you to understand how users interact with online resources, highlighting risky behaviors and areas of vulnerability. By leveraging this information, you can take informed actions to enhance your security posture and build organizational resilience against cyber threats.
- **Enhanced Investigation Capabilities** EnforceDNS enables thorough investigations by allowing analysts to delve into blocked or suspicious traffic, providing detailed insights into the nature of potential threats, including their origins and methods. By empowering analysts to conduct these investigations, organizations can proactively address security concerns and strengthen their overall cybersecurity posture.

DEPLOYMENT AND SCALABILITY

EnforceDNS can be deployed in just minutes by reconfiguring your organization's DNS service, eliminating the need for agents or sensors. threatER also supports various deployment options to accommodate diverse endpoint and network configurations and integrates seamlessly with existing network security solutions. Moreover, you can combine deployment options to suit the needs of almost any organization.

threatER focuses on deployment methodologies that make EnforceDNS scalable for any size organization. In well under an hour, EnforceDNS can be deployed and begin safeguarding anywhere from 1 to over 25,000+ endpoints.

DEPLOYMENT OPTIONS

DNS Resolver

threatER has DNS resolvers placed all over the world, ensuring there's always one close to you. Our resolvers are fast and secure ensuring you have the best and safest experience at all times. Configure in minutes across your entire infrastructure using the self-service feature in the EnforceDNS UI.

EDR/Endpoint Protection Integration

EnforceDNS integrates seamlessly with Endpoint Detection and Response (EDR) and endpoint protection solutions to enhance security posture. By leveraging EnforceDNS's advanced threat intelligence and real-time monitoring capabilities, organizations can bolster their existing EDR and endpoint protection strategies, ensuring a comprehensive defense against sophisticated cyber threats.

threatER Agent

The EnforceDNS Agent is crafted to deliver EnforceDNS's exceptionally high level of security to all your mobile devices. It is tailored for macOS, iOS, Windows, and Android, protecting about 99% of mobile and 87% of desktop/laptop devices. With EnforceDNS's centralized agent management, administrators can easily monitor status, enable or disable agents, conduct in-place updates, restart devices, and run diagnostics.

threatER Relay

The EnforceDNS Relay bridges the gap between agent-based and resolver-based deployments. It installs in front of your DNS infrastructure, either physically or logically, to receive metadata associated with your DNS queries, including IP address and device name. It then forwards local traffic to your local DNS resolvers and external requests to EnforceDNS.

1.855.765.4925 | sales@threater.com