ThreatSTOP

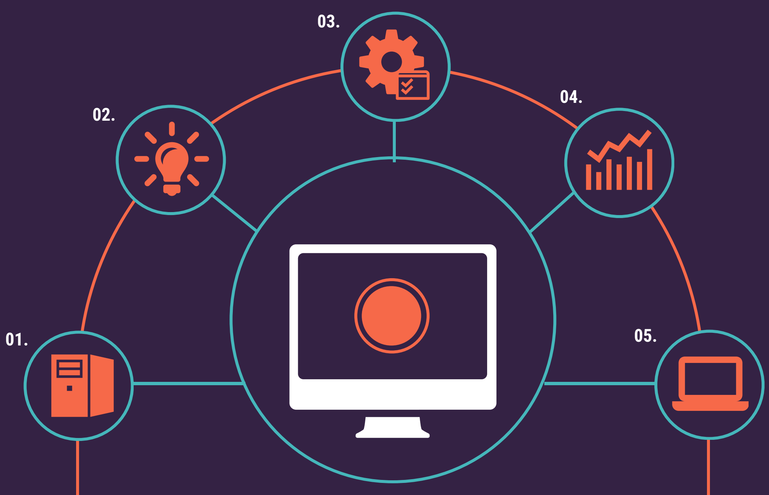
WHY YOU NEED THREATSTOP'S DNS DEFENSE

Securing DNS is more important than ever before, and now more affordable than ever. DNS is used in more than 95% of today's malware attacks, and it only takes about an hour to add ThreatSTOP's DNS Defense to protect your DNS. Start blocking these threats and gain the visibility into infected client machines needed to speed up remediation.

Malware Attacks

1 Hour to Set Up

DNS DEFENSE BENEFITS



01.
Turn your existing DDI/IPAM or DNS Servers into DNS Firewalls that proactively block unsafe or unwanted DNS requests.

02.
Leverage our real-time threat intelligence based cloud service to know about and block today's worst threats.

03.
Enjoy granular custom policy creation tools and security actions to be taken, including block, redirect and log-but-allow.

04.
Work with powerful but easy-to-use reports to see the blocked threats and impacted client machines on your network.

05.
Extend local DNS enforcement to roaming devices that leave the network without needing a VPN connection.

Protect every device on the network that uses DNS, from workstations to printers, with a central DNS Firewall for the entire network.

WITH DNS DEFENSE YOU'LL GET:

- A service that's compatible with your existing DDI/IPAM and DNS servers.
- Professional on-boarding service included, and it only takes about an hour to configure.
- Customizable policies, web and email reports and alerts, and security research tools.
- Roaming protection for mission-critical laptops that frequently leave the corporate network.

ThreatSTOP's cloud service converts the latest threat data into enforcement policies and automatically updates your firewalls, routers, DNS servers and endpoints to stop attacks before they become breaches. Get started with a free trial here.

www.threatstop.com