Powered by Farsight Security. ThreatSTOP proactively blocks newly observed domains to fill a challenging gap for companies.

The Challenge

Dozens of new domains are created and published every minute as part of the Domain Name System (DNS) – but not all are created for legitimate purposes. Attackers use new domains for spam, malware distribution, phishing, botnets, and more, all within just minutes of creating them. Blocking these new and potentially malicious domains is difficult, and has left virtually every organization with a security gap that drives up risk.

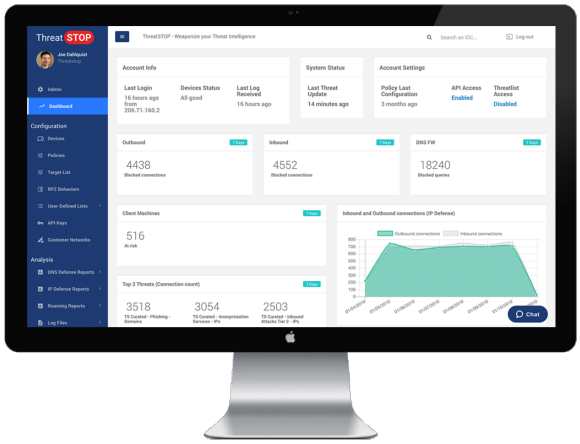
To block these threats, security practitioners need accurate, comprehensive and real-time information about new domains, and then they need to apply immediate rule changes to firewalls, routers, DNS servers and other network enforcement points to block access until the new domains are deemed safe. Completing this workflow efficiently and accurately is a challenge even for the largest dedicated security teams.

The Data Solution

ThreatSTOP's Newly Observed Domains (NOD) data provides organizations with real-time actionable insights based on the newness of a domain. This enables them to protect their users from newly configured and used domains until those domains are better understood by the security industry. ThreatSTOP NOD is powered by Farsight Security's real-time Passive DNS sensor array, and their industry-leading DNSDB™ Passive DNS database.comprehensive malvertising threat intelligence available.

The Automation Platform

ThreatSTOP is a cloud-based security automation platform that delivers dynamic policy updates to network traffic enforcement devices such as DNS servers, firewalls, routers and more. Customers can choose from curated, best-in-class threat intelligence from authoritative sources. ThreatSTOP has partnered with Farsight Security to offer an automated way to take action on Newly Observed Domains (NOD).



ThreatSTOP customers can now take automated security action against newly observed domains, choosing to block, redirect, or allow (but log) these potentially harmful DNS requests as a component of their network enforcement policy. By automating this protection security practitioners can avoid the arduous and time-consuming requirements

ThreatSTOP is a SaaS company with a platform that automates the collection and delivery of diverse threat intelligence as enforceable security policy to a broad range of network devices. To request a demo or speak with a salesperson, please contact sales@threatstop.com or call 760 542 1550. Visit www.

How it Works

1. Select from expert-crafted threat protection policies. Tailor a perfect fit by creating your own whitelists and block-lists.
2. Policy updates are sent automatically to your devices containing up-to-the-minute threat intelligence to protect against current threats.
3. Devices can now enforce those policies to protect your network from inbound attacks and outbound malicious connections.
4. Event logs are generated providing visibility into the traffic that was blocked prior to a serious network breach.
5. View powerful reports about the threats targeting your environment, and details of potentially infected devices to expedite remediation.

Proactive Security

ThreatSTOP's Newly Observed Domains (NOD) data empowers organizations to prevent breaches by blocking communication with the infrastructure attackers use to carry out attacks, which frequently include newly registered domains, or domains that have been dormant and are being observed in DNS requests for the first time. These often short-lived domains are frequently used as infection points, as websites designed to spoof a legitimate business in order to steal credentials, and as exfiltration points for stolen data. ThreatSTOP's proactive approach to mitigating these threats means security teams can take a preventative approach to blocking requests for these types of domains, vastly reducing their risk exposure and shrinking their exposed attack surface.

The Complete Solution

ThreatSTOP is the only complete end-to-end solution for automating the process of blocking harmful or unwanted network connections using actionable threat intelligence data, a workflow known as Operationalizing Threat Intelligence. The ThreatSTOP platform includes customizable policies, broad compatibility with leading network appliances, and robust reporting to detail the protection received while providing visibility into affected host machines to speed remediation. The platform also includes advanced security research tools, extensible API services, and SIEM integration capabilities, offered entirely as a SaaS service.