ThreatSTOP

www.threatstop.com

ThreatSTOP DNS Firewall for Windows Server 2016

Key benefits:

- Continuous automatic delivery of user-defined policies containing real-time threat intelligence to your Windows 2016 DNS Server.
- Granular controls empower you to create tailored network security policies that block DNS queries to a broad range of malware types or geographic locations.
- Prevents data theft and corruption by stopping malware from "phoning home" to threat actors. Prevents activation of ransomware.
- Easy to deploy and manage highly scalable cloud-based service.

Block Today's Advanced Threats Using DNS

To help ensure the security of your network ThreatSTOP turns Windows Server 2016 into a powerful DNS Firewall delivering highly scalable, easy-to-use protection that blocks known and emerging threats immediately, and best of all, it can be deployed quickly and easily without adding new software or hardware to your environment.

ThreatSTOP DNS Firewall is a powerful service that automatically blocks unwanted and dangerous outbound DNS communication with command and control infrastructure used by threat actors across a broad range of attack vectors.

ThreatSTOP DNS Firewall delivers up-to-the-minute protection against advanced threats, and enhances your existing network security posture by adding a layer of security at the DNS infrastructure level. DNS Firewall delivers immediate protection against unwanted and dangerous outbound network connections used for ransomware, phishing, botnet infections, and other advanced malware by blocking the call home to command & control infrastructure required for an attack to succeed.

Custom Security Policies, Powered by Threat Intelligence

ThreatSTOP empowers users to customize and manage network security policies composed of threat types, severity levels, and user-defined block lists. Once enabled, these policies function as a set of dynamic DNS Firewall rules to protect your networks. Then, ThreatSTOP's real-time reporting provides visibility into blocked threats and affected client machines to aid in quick remediation.

The service protects networks using Windows Server 2016 by automatically delivering real-time threat intelligence policy updates to the DNS server for enforcement. As a cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure, new software or hardware. Once deployed, ThreatSTOP DNS Firewall immediately begins preventing the exfiltration or corruption of data, defending against ransomware attacks, and blocking unwanted outbound connections that consume bandwidth and pose risks to network security.

Operationalizing Best-in-Class Threat Intelligence

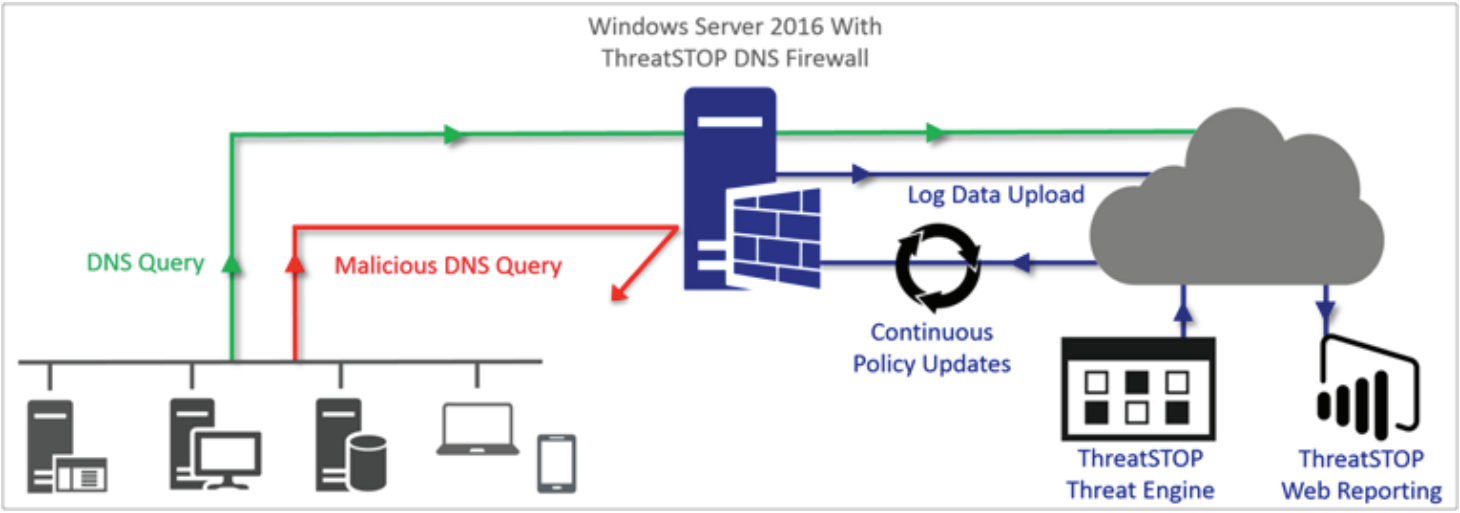
ThreatSTOP DNS Firewall leverages a comprehensive and authoritative database of live threat intelligence that tracks the infrastructure used for cyberattacks. ThreatSTOP's world-class security team curates the latest threat information and cross-correlates threat data against multiple public and private sources to ensure a high degree of accuracy and prevent false positives. These policies, enforced at the DNS Firewall, are continuously and automatically updated to protect against new and emerging threats.

Additionally, ThreatSTOP also offers powerful research tools such as Check IOC, which enables users to input domain names and receive valuable information such as if the target is currently present or has been detected on any of your assets in the past. Plus Whois, DNS Lookup, and Passive DNS data.

How it Works: DNS Firewall for Windows Server 2016

ThreatSTOP's DNS Firewall service turns Windows Server 2016 into an effective new security layer that protects your mission-critical DNS. ThreatSTOP provides flexible outbound protection against threats using malicious domains, including wildcards, and provides actionable visibility into blocked threats and client machines needing remediation through web-based reporting.

1. Define a policy that fits your network security posture, including custom block lists
2. Policies are automatically and continuously updated with real-time threat data
3. Blocks malicious and unwanted DNS queries, preventing malware from completing attacks
4. Deploys in an hour or less and easily scales to secure your entire network surface area
5. Powerful reporting delivers visibility to blocked threats and aids in remediation



How it Works: DNS Firewall for Windows Server 2016

Add a new layer of security to your cloud or on-premise network environment. ThreatSTOP delivers automated continuous protection against today's active threats.

Operationalize Threat Intelligence

Unlike traditional threat intelligence used to investigate incidents after they occur, ThreatSTOP's dynamic threat updates deliver real-time proactive protection directly to your Windows DNS server.

Secure Your Environment Quickly

Deployment of ThreatSTOP DNS Firewall for Windows Server 2016 takes less than an hour, and requires no new software or hardware to be installed or maintained.

ThreatSTOP provides essential security to manage risk, offering broad protection for your environment that protects all devices from attack and prevents data theft. To request a demo or speak with a salesperson, please contact sales@threatstop.com or call 760 542 1550. Visit www.threatstop.com for more information.