www.threatstop.com

ThreatSTOP Shield DNS Firewall for Microsoft Azure

Key benefits:

- Automatically delivers continuous, real-time threat intelligence to your Azure DNS servers based on user-defined policies.
- Granular controls empower you to block, allow, or redirect DNS queries to a walled garden by IP and domain, including wildcards.
- Prevents data theft and corruption by stopping malware from “phoning home” to threat actors. Prevents activation of ransomware.
- Cloud-based scalable service is easy to deploy and manage

Operationalized Threat Inteliigence for Microsoft Azure

Securing your Azure environment is paramount. The ThreatSTOP Shield Platform delivers scalable, easy-to-use protection for cloud workloads that blocks known and emerging threats immediately. ThreatSTOP DNS Firewall can be deployed quickly on new and existing Azure networks.

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 security posture by adding a layer of security at the DNS infrastructure level. DNS Firewall delivers granular control over the actions taken against unwanted and dangerous outbound network connections including the ability to block, log, or redirect queries to walled gardens based on DNS query data and resolution path.

Protect your Azure DNS Infrastructure

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

The service protects Azure environments by automatically delivering real-time threat intelligence policy updates to the Azure DNS server for enforcement. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, ThreatSTOP DNS Firewall provides immediate relief by 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 the company’s Shield Platform, a comprehensive and authoritative database of IP addresses, domains and 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. Policies created using the Shield Platform are continuously and automatically updated to protect against new and emerging threats.

How it Works

ThreatSTOP's DNS Firewall protects the DNS infrastructure of your Azure cloud or hybrid deployment. The ThreatSTOP Shield platform provides flexible outbound protection against threats using malicious IP addresses and domains, including wildcards, and provides granular control over actions taken.

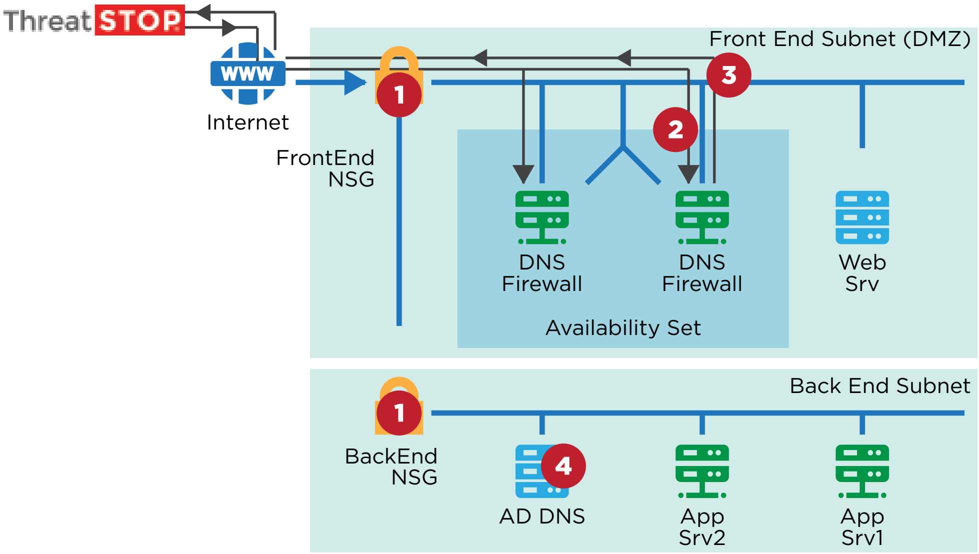
Step 1 Define a policy that fits your security posture, including custom whitelists and block lists

Step 2 Policies are automatically and continuously updated with real-time threat data

Step 3 Granular control over outbound threat actions including block, log, and redirection to a walled garden based on DNS query data and resolution path

Step 4 Deploys in an hour and easily scales to secure your entire cloud surface area

Step 5 Powerful reporting delivers visibility to blocked threats and aids in remediation



1 Network Security Group (NSG) enforces use of ThreatSTOP DNS shield as a DNS Server

2 Security policies from ThreatSTOP are transmitted with TSIG authentication

3 RPZ logs sent to ThreatSTOP for analysis and reporting, and are received via SSL

4 AD queries are sent to internal DNS for lookup

Shield Your Azure Workloads

Protect your workloads, VDI, and data hosted on Azure with an effective new security layer. ThreatSTOP Shield delivers automated continuous protection against today's active threats

Operationalize Threat Intelligence

Unlike traditional threat intelligence used to investigate incidents after they occur, ThreatSTOP Shield's dynamic threat updates deliver real-time proactive protection directly to Azure

Secure Your Cloud Quickly

Deployment of ThreatSTOP Shield in your new or existing Azure environment is straightforward and quick with easy to use, scalable solution templates that automate implementation