



System Capabilities

Advanced DNS Layer Security

Badware Filter

Content Filter

Safe Search/YouTube Safe Modes

Application Filter

Advanced DNS Threat Protection

Multi-Site Management

Network Relay

Scout360 Roaming Clients

Custom Allow/Block Lists

Trusted TLD Filtering

Real-Time Log Access

Detailed Insights

Sub-Organization Management

System Infrastructure

Information and Links

Advanced DNS Layer Security

ScoutDNS is a powerful cloud managed RPZ (response policy zone) option for adding DNS Layer security to the network. Although an effective content filter in the age of HTTPS sites, RPZs go much further in protecting your network through advanced DNS security controls. ScoutDNS can prevent DNS Rebinding attacks, block Covert Channel attempts, and limit the scope of available domains for Malware C&C.

ScoutDNS provides protection by five methods.

- Badware Filter
- Content Filter
- Safe Search and YouTube Safe Modes
- Application Filter
- DNS Based Threat Protection

In addition to protection and filtering, ScoutDNS provides best in class DNS layer visibility for system operators and administrators.

This document outlines ScoutDNS capabilities and functionality at a high level. Keep in mind, the ScoutDNS platform is regularly updated with new functions and features so be sure to ask your ScoutDNS solutions expert about anything not listed that you may be looking for.

Badware Filter

DNS Filtering is an important part of a good multi faceted network security plan.

ScoutDNS provides protection from major online threats by blocking the domain name requests used in malicious emails, applications, and web scripts. The increase in polymorphic malware means that client device antivirus and malware solutions become less effective on their own every year. With comprehensive data-sets updated real-time from sources every effort is made to provide a safer and more secure internet experience for network users.

ScoutDNS Badware and Security Category Details

← Guest Policy EDIT POLICY

DELETE POLICY

SETTINGS SECURITY CONTENT APPLICATIONS

Security

ADWARE	INFECTED HOSTS
MALICIOUS SCRIPTS	MALWARE
PHISHING	VIRUSES

Content Filter

Content filtering can reduce liability and ensure compliance.

ScoutDNS provides comprehensive multi category internet content filtering that is indifferent to HTTPS without the latency of forced endpoint, firewall, and proxy based solutions. DNS filtering is significantly more efficient in terms of cost and performance than any other method of content control.

With 99% of known domains covering 200 languages in our content database and more than 10 million categorized each day, ScoutDNS users can be confident in protecting their users from inappropriate and sometimes illegal web based content. ScoutDNS content filters exceed CIPA requirements.

[ScoutDNS Content Category Details](#)

DNS Policy ScoutDNS ? 👤

Policies + NEW

Search by name

- No Policy
- Low
- High
- Moderate
- Badware Block
- Guest Policy**
- Guest WiFi
- Remote
- SRCCO
- Staff Policy

Guest Policy EDIT POLICY

DELETE POLICY

SETTINGS **THREATS** **CONTENT** **APPLICATIONS**

Adult

ABORTIONS	ADULT MIXED
ALCOHOL	CRIMINAL SKILLS
EXTREME	GAMBLING
HATE SPEECH	INTIMATE APPAREL
MATCH MAKING	MATRIMONIAL
NUDITY	OCCULT
PAY TO SURF	PORNOGRAPHY
PROFANITY	SUBSTANCE ABUSE
TOBACCO	WEAPONS

Information

ALTERNATIVE LIFESTYLES	CLASSIFIEDS
EDUCATION	ENVIRONMENTAL
FINANCIAL SERVICES	GENERAL NEWS
HEALTH	JOURNALS AND BLOGS
LEGAL	MEDICATION
POLITICAL	PORTALS
REAL ESTATE	RELIGION
SEX EDUCATION	TECHNOLOGY

Safe Search/YouTube Safe Modes

Apply content restrictions within search engines and YouTube.

Limiting the access of websites alone is not enough to prevent pornographic and inappropriate material access to end users. Popular modern search engines such as Bing and Google provide direct access to images and video without leaving the search platforms themselves. By taking advantage their native builtin methods for safe search, ScoutDNS is able to force and lock all network wide access to these platforms in their respective safe and restricted access modes. In addition, when safe search is active ScoutDNS can auto-block all other non-safe search engines to end users.

Another popular content application, YouTube contains content often deemed inappropriate for young children and certain environments. ScoutDNS supports both Strict and Moderate YouTube safe modes to keep users safe.

[Safe Search Explained](#)

[YouTube Restrictions Explained](#)

🗑️ DELETE POLICY

SETTINGS THREATS CONTENT APPLICATIONS

Copy a policy

No Policy ▼

Base settings

Policy name

Staff Policy

Policy description

For staff network users

White/Black list (multi selection)

Global list ▼

Youtube safe mode

- Unrestricted
- Moderate
- Strict

Safe search

Forced ▼

Advanced settings ▼

Application Filter

Take control and manage time and bandwidth wasting applications

ScoutDNS is able to block 14 application categories that are key to effective policy controls. By managing allowed applications, administrators can help ensure that only authorized network activity is able to be used by end users. From time wasting applications such as games and social media, bandwidth hogs such as streaming video, or potential illegal activity at end clients, application filtering via DNS gives administrators a powerful additional resource in managing their network.

← Guest Policy

EDIT POLICY

DELETE POLICY

SETTINGS

SECURITY

CONTENT

APPLICATIONS

Applications

EDUCATIONAL GAMES

EMAIL

FILE SHARING

GAMES

INSTANT MESSAGING

PEER TO PEER

REMOTE ACCESS TOOLS

SOCIAL NETWORKING

STREAMING MEDIA

VOICE OVER IP

WEB CHAT

WEB EMAIL

WEB PROXY

WEB STORAGE

Advanced DNS Threat Protection

Prevent hard to block but common DNS based malicious attacks

Hackers and malicious developers are constantly finding new and more effective methods to execute their attacks. There has been a heavy increase in malicious code that takes advantage of the DNS protocol to execute well hidden attacks that bypasses both anti-malware applications as well as next generation firewalls. These signature based defensive methods suffer from several key limitations in addressing these types of attacks.

ScoutDNS provides the following DNS protocol protections:

Maximum Domain Length

By limiting and controlling maximum domain administrators are able to dodge several dangerous and suspicious domains that exceed certain desired lengths

DNS Rebinding

ScoutDNS blocks DNS Rebinding attacks that are often used to gain access to internal network resources from the outside.

Mailer Worms

Internal networks that do not host their own inside mail server are best served by blocking MX domain records to prevent SPAM attacks. These attacks can have negative consequences on domain and IP reputation as well as consume network resources.

Covert Channel

DNS covert channeling allows hidden malicious code to create encrypted tunnels for complete and total network and system access to outside attackers. This type of attack can easily bypass signature based protection points such as firewalls and

anti-malware software. ScoutDNS uses the DNS protocol itself to examine and reconstruct domain responses in a post domain resolution method that fundamentally blocks covert channel attacks.

White-List Mode

For maximum protection of critical networks with sensitive information, ScoutDNS offers a White-List only mode where network admins can set authorized only domains virtually eliminating the threat of zero day/zero hour attacks from bad domains.

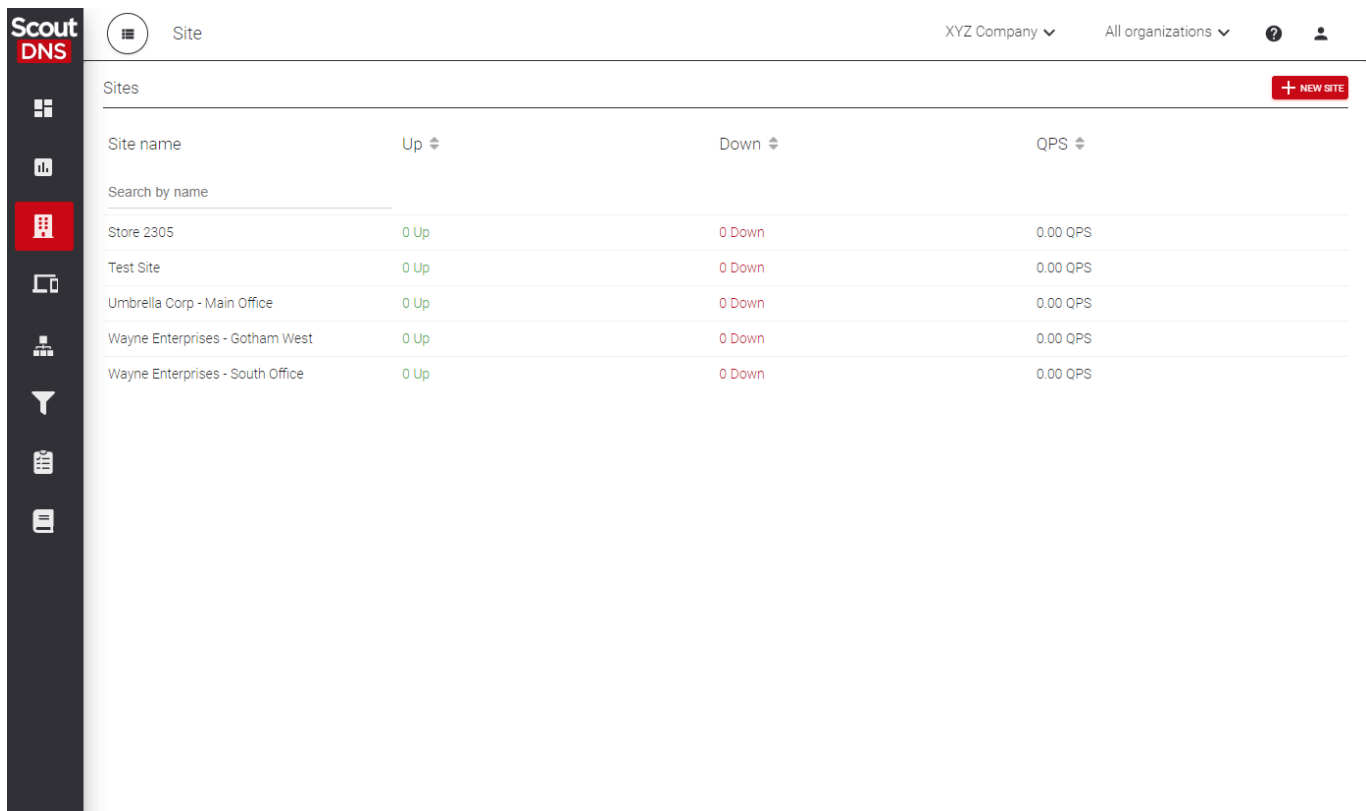
The screenshot shows the 'Staff Policy' configuration page in ScoutDNS. At the top, there is a back arrow, the title 'Staff Policy', and 'SAVE' and 'CANCEL' buttons. Below the title is a 'DELETE POLICY' button. A navigation bar contains 'SETTINGS', 'THREATS', 'CONTENT', and 'APPLICATIONS', with 'SETTINGS' selected. The 'Advanced settings' section is expanded, showing the following options:

- TLD filter: Main TLD (dropdown menu)
- White-list Only:
- Block Mailer Worm (MX Records):
- Allow 'A' Record Only:
- Logging only:
- Block Unclassified:
- Block Covert Channel:
- Block DNS Rebinding:
- Max Domain Length: 120

Multi-Site Management

Get Single Pane View on single and multi-site networks

ScoutDNS allows administrators to easily manage multiple locations as well as multiple WAN links per site. Our modern GUI provides quick access to critical network and DNS traffic health information for every network across all sites.



Site name	Up	Down	QPS
Search by name			
Store 2305	0 Up	0 Down	0.00 QPS
Test Site	0 Up	0 Down	0.00 QPS
Umbrella Corp - Main Office	0 Up	0 Down	0.00 QPS
Wayne Enterprises - Gotham West	0 Up	0 Down	0.00 QPS
Wayne Enterprises - South Office	0 Up	0 Down	0.00 QPS

Set and manage policies per WAN easily whether you are managing 1 or 1000 sites.

ScoutDNS Site

XYZ Company All organizations

Sites

[+ NEW SITE](#)

Search by name

- Store 2305
- Test Site
- Umbrella Corp - Main Office
- Wayne Enterprises - Gotham West
- Wayne Enterprises - South Office**

Wayne Enterprises - South Office

[DELETE SITE](#)

Dashboard ^ Last Hour

Status

1 WANS up 0 WANS down

Performance

0.77 Requests/Second 8 ms Avg Response

Allowed/Blocked

3597 Allowed
49 Blocked
3646 Total

WAN LAN LOCAL FORWARDING REDIRECTS RELAYS INFO

WAN

[+ NEW WAN](#)

Search by name

- Umbrella South Site Com...**

Umbrella South Site Comcast

[DELETE WAN](#) [EDIT WAN](#)

WAN name: Umbrella South Site Comcast

Net address (IPv4, IPv6 or DymDNS): 72.182.184.102

Block Page: Default

Policy: Wayne Enterprises - Staff Policy

State:


Network Relay

Deploy a Zero-Touch managed relay for greater control and visibility

ScoutDNS supports a Relay configuration which allows operators to install a lightweight service inside their network. The relay is a local forwarding resolver service that processes queries inside the operator network while relaying public queries to the ScoutDNS cloud resolver. Queries meant for internal services remain inside the network. The purpose of this is to enable the following ScoutDNS resolver functionality:

- Set Policy by subnet
- Log LAN IP for queries
- Encrypt DNS traffic
- Configure local network aliases
- Configure local DNS forwarding
- Automatic updating of the relay software

Configuring ScoutDNS Relay

WAN	LAN	RELAYS	REDIRECTS	LOCAL FORWARDING	INFO
Relays					
ID	Status	WAN	Version	Last Config	Actions
Search by ID		Search by WAN name		Search by version	
46c4oddd-7d19-4a7e-9f2f-1e...	Not adopted	Spectrum Primary	1.1.3	—	

Scout360 Roaming Clients

Protect devices in and out of the office with Full Zero-Touch roaming clients

Today's workforce extends beyond the office network and requires powerful protective tools to reduce exposure. ScoutDNS Scout360 roaming clients enable admins to easily deploy and manage DNS security for devices in and out of the office, on and off the VPN.

- Zero touch deployment for Windows and MacOS
- Full single click remote disable and uninstall for easy management
- Session tracking to ID users and remote networks
- Profile based configuration for easy group device management
- Encrypts 100% of DNS queries at all times
- Automatic updates

Configuring Scout360 Clients

The screenshot shows the ScoutDNS Scout360 client management interface. The interface is divided into several sections:

- Client List:** A list of clients with 'winclient2' selected.
- Client Details:**
 - Client Name:** winclient2
 - Client Name:** DESKTOP-T2RRMGR
- Threats:**
 - ADWARE: 0
 - MAL SCRIPTS: 0
 - PHISHING: 0
 - INF. HOSTS: 0
 - MALWARE: 0
 - VIRUSES: 0
- Performance:**
 - Requests/Second: 0.01
 - Avg Response: 48 ms
- Allowed/Blocked:**
 - Allowed: 67
 - Blocked: 0
 - Total: 67
- Device Info:**
 - Name: winclient2
 - Hostname: winclient2
 - Full Hostname: winclient2.scoutdns.lan
 - Profile: Sales Team
 - Policy: Default: Remote
 - Last Sync: 2022-10-03 09:42:01 CDT
- Network Info:**
 - Status: Online
 - WAN IP: 192.168.1.102
 - LAN IP: 192.168.4.84
 - Username: [redacted]
 - Site: South Office
 - Domain: scoutdns.lan

Custom Allow/Block Lists

Dynamic control of your network's access through custom lists

ScoutDNS allows administrators to create and manage allowed and blocked lists at both the policy and global access levels for their locations and users. Custom lists are managed as objects making it easy to update hundreds of network location by managing a single assigned list. Administrators can create multiple lists and assign them as local policy lists or make them global across all sites/networks.

Working with Allow/Block Lists

The screenshot displays the ScoutDNS web interface for managing custom lists. The main header shows 'ScoutDNS' and 'Custom lists'. Below this, there are tabs for 'ALLOW/BLOCK' and 'TLD FILTER'. The left sidebar contains a navigation menu with icons for various functions, including a red icon for lists. The main content area is titled 'South Campus Domains' and features a '+ NEW W/B LIST' button. Below the title, there are tabs for 'INFORMATION', 'ALLOW', and 'BLOCK'. The 'ALLOW' tab is active, showing a list of domains. The list includes:

- livetiles.health.apex.bing.com
- loc-sc-jpl.com
- loc-sc-jpl.com
- lockerdom.com
- log.adaptiv/advertising.com
- log.olark.com
- log.outbrainmg.com
- log.pinterest.com
- login.dotomi.com
- login.live.com
- login.microsoftonline.com
- login.windows.net
- login.yahoo.com
- logix.optimizely.com
- loli.delve.office.com
- lpores.delve.office.com
- lqo-thequestionsnetw.neton-ssl.com
- m.addthis.com
- m.addthisedge.com
- m.hotmail.com
- m.wsj.net
- magnetic.t.domdex.com
- mail.google.com
- mail.yahoo.com
- manychat.com
- maps.googleapis.com
- maps.gstatic.com
- markets.books.microsoft.com
- match.adnvr.org
- maxcdn.bootstapcdn.com
- maxcdn.bootstrapcdn.com
- mbay.co
- mcdp-nydc1.outbrain.com
- messenger.yahoo.com
- mesu.apple.com
- metrics.api.drift.com

Trusted TLD Filtering

Create a pre-policy filter based on trusted top level domains

With nearly 1600 top level domains and new ones added regularly, managing access based on top level domains used to require adding many TLDs to a block list. This old method is also aligned with the outdated security model of Allow-All-Block-Bad policy management. With the popularity of zero-trust practices ScoutDNS created a method aligned with Block-All-Allow-Necessary. This required a new approach beyond simple allow/block list policy mechanics.

Allow Listing policy actions is typically an end of policy function overriding all other policy rules. This is necessary in order to allow white-listing of business critical domains and to minimize disruption. It would not be advisable to whitelist all of a particular top level domain as this would over-ride all other threat controls. For this, ScoutDNS created Trusted TLD Filtering as a pre-stage policy filter that acts as a permit or deny check before all other policy functions. This way, if a domain is within a Trusted TLD, it is not automatically approved, but still must pass all other policy checks including threats and allow/block lists.

Using TLD filters, administrators can trust just the TLDs required for their business or system applications and not worry about high threat ratio top level domains or newly created top level domains.

New TLD filter

SAVE CANCEL

INFORMATION TLD LISTS

Move to permit list: All Top 25 Top 50 Top 100

Search All

Block list

Select all

Deselect

Name	Type	Manager
hk	ccTLD	Hong Kong Internet Registration Corporation Ltd.
rs	ccTLD	Serbian National Internet Domain Registry (RNIDS)
lt	ccTLD	Kaunas University of Technology
link	gTLD	Uniregistry, Corp.
ph	ccTLD	PH Domain Foundation
club	gTLD	.CLUB DOMAINS, LLC
si	ccTLD	Academic and Research Network of Slovenia (ARNES)
site	gTLD	DotSite Inc.
mobi	gTLD	Afilias Technologies Limited dba dotMobi
by	ccTLD	Reliable Software, Ltd.
cat	sTLD	Fundacio puntCAT

Previous

Page

3

of 53

Next

Permit list

Select all

Deselect

Name	Type	Manager
com	gTLD	VeriSign Global Registry Services
net	gTLD	VeriSign Global Registry Services
org	gTLD	Public Interest Registry (PIR)
uk	ccTLD	Nominet UK
it	ccTLD	IIT - CNR
gov	sTLD	General Services Administration Attn: QTDC, 2E08 (.gov Domain Registration)
edu	sTLD	EDUCAUSE

Previous

Page

1

of 1

Next

Real-Time Log Access

ScoutDNS gives administrators access to detailed daily log activity in real-time. ScoutDNS provides 30 days of queries with 24 hour log exports. Log options allow search by action taken, domain text, category type, and give administrators the ability to specify criteria to specific day and time ranges.

The screenshot displays the ScoutDNS 'Log' interface. At the top, there is a navigation bar with the ScoutDNS logo, a 'Log' button, and a user profile for 'XYZ Company'. Below this is a 'Create logs' section with a date filter set to '09/13/2022' and a site filter set to 'All'. There are 'EXPORT', 'RESET', and 'SUBMIT' buttons. The main area is titled 'Logs' and contains a 'Logging table' with a 'Hide filters' option. The table lists various DNS queries with the following columns: Date/Time, Site name, Domain, Resolver, Decision, Record type, Reason, Policy, Categories, Latency, and WAN IP.

Date/Time	Site name	Domain	Resolver	Decision	Record type	Reason	Policy	Categories	Latency	WAN IP
2022-09-13 19:41:15 C...	South Office	p42-contacts.icloud.com.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	File Sharing	5	72.182...
2022-09-13 19:41:14 C...	South Office	c3.shared.global.fastly.net.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Technology	4	72.182...
2022-09-13 19:41:14 C...	South Office	remote-data.urbanairship.com.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Business	5	72.182...
2022-09-13 19:41:14 C...	South Office	s3.amazonaws.com.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Technology File Sharing Business Application	2	72.182...
2022-09-13 19:41:14 C...	South Office	d1ktuw48jntz3n.cloudfront.net.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Content Server	4	72.182...
2022-09-13 19:41:14 C...	South Office	firebaseanalytics-pa.googleapis.com.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Content Server	2	72.182...
2022-09-13 19:41:14 C...	South Office	app.ringcentral.com.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Phone Cards	1	72.182...
2022-09-13 19:41:14 C...	South Office	s3.amazonaws.com.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Technology File Sharing Business Application	2	72.182...
2022-09-13 19:41:14 C...	South Office	app.launchdarkly.com.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	General	4	72.182...
2022-09-13 19:41:14 C...	South Office	app.launchdarkly.com.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	General	21	72.182...
2022-09-13 19:41:14 C...	South Office	app.ringcentral.com.	dal1.scoutdns.com	ALLOWED	HTTPS	Neither of th...	Staff Policy	Phone Cards	2	72.182...
2022-09-13 19:41:14 C...	South Office	bam-cell.nr-data.net.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Content Server	32	72.182...
2022-09-13 19:41:14 C...	South Office	bam-cell.nr-data.net.	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Content Server	2	72.182...
2022-09-13 19:41:12 C...	South Office	aqm3wd1qlc3dy.iot.us-east-1.amazona...	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Technology	2	72.182...
2022-09-13 19:41:10 C...	South Office	aqm3wd1qlc3dy.iot.us-east-1.amazona...	dal1.scoutdns.com	ALLOWED	A	Neither of th...	Staff Policy	Technology	2	72.182...

Detailed Insights

In addition to Realtime query logs, ScoutDNS Insights allows administrators to get detailed visibility into their DNS use with multiple aggregate style views. ScoutDNS admins can take deeper looks into the following aggregate views and filter their views by a number of parameters including site, policy, WAN or LAN IP, allowed or blocked, category or categories type and more. You can even perform searches based on whole or part domain names across all locations for the last 30 days.

- **Domains:** View up to the top 1,000 domains for selected time period up to 30 days
- **Category:** View all DNS activity based on category. Drill down into log or aggregate domain view within selected category
- **TLD:** View all DNS activity based on Top Level Domains. Drill down into log or aggregate domain view with selected TLD.
- **Record Type:** View all DNS activity by record type. Drill down into log or aggregate view based on selected record type.

Filter by <

- Site
- Policy
- Category Type
- Category
- Record Type
- WAN IP
- LAN IP

APPLY **CLEAR**

Result **ALL** ALLOWED BLOCKED Rows **50** 100 500 1000

Last Hour REFRESH

Search: Domain Name X

Domains

Domain	Category	Category Type	Count
aqm3wd1q1c3dy.iot.us-eas...	Technology	Content	2417
api.scoutdns.com.		White/black list	695
resolver1.scoutdns.com.		White/black list	342
connectivity-check.ubuntu....	Technology	Content	125
registry-1.docker.io.	Technology	Content	98
connectivitycheck.gstatic.c...	Content Server		89
images.vizio.com.	Entertainment, Sales	Content	81
kinesis.us-west-2.amazona...	Technology	Content	72
a79f7b502bae9945a.awsgl...	Content Server		72
www.google.com.	Search Engine	White/black list	65
auth.docker.io.	Technology	Content	50
clients4.google.com.	Technology	Content	33
ib.adnxs.com.	Ad Blocking		32
US.lgtvsdp.com.	Content Server		28
device-metrics-us-2.amazo...	Sales	Content	26
czfe84-front01-iad01.trans...	General		26
api.amazon.com.	Sales	Content	20

Sub-Organization Management

ScoutDNS gives managed service providers and large enterprise customers the ability to create and manage suborganization units and objects. With sub-organization management, admins are able to create, manage, and designate access as needed.

- **Org Policies:** Create and assign policies for specific organizations
- **Org Allow/Block Lists:** Create custom list for specific organizations
- **Org Stats:** View all DNS activity on a per organization basis
- **Org Users:** Create manage or view only access to users and the specific organizations desired.
- **Org UI Selector:** View/filter any ScoutDNS tab from the organization's perspective



- Organizations + NEW ORGANIZATION
- Organization Search
- A New Organization
- Dunder Mifflin Paper Company
- Nakatomi Trading Corp
- Umbrella Corp
- Wayne Enterprises

Wayne Enterprises

DELETE ORGANIZATION

Dashboard

All Sites

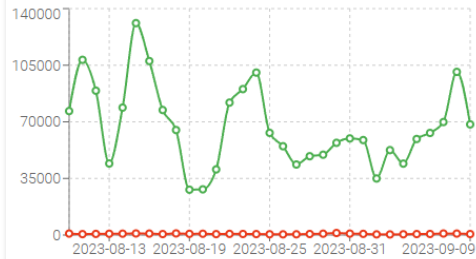
All Profiles

Last 30 Days

Threats

ADWARE 0 INF. HOSTS 0
 MAL. SCRIPTS 0 MALWARE 2
 PHISHING 0 VIRUSES 0

Allowed/Blocked



Performance

0.79 **14 ms**
 Requests/Second Avg Response

- SITES
- PROFILES
- INFO

Sites

LINK

Site	WANs Up	WANs Down	QPS	Allowed	Blocked	Total	Unlink
Wayne Enterprises - Sout...	1	0	0.78	2064030	22296	2086326	X

System Infrastructure

ScoutDNS is designed as a high availability distributed architecture with our global anycast network within data centers all around the world. Our highly efficient design allows for scalability at a lower cost driving better value to customers.

Our platform was created from the ground up in order to allow high availability clusters for maximum redundancy and scale. All systems are designed with replicated relationships for key data built into every cluster allowing full DNS filtering operations without access to the network core. This has allowed us to deliver 100% network uptime on the anycast network for 3 years running while processing over 3 billion queries per month.



Information and Links

Schedule a Demo

Helpful Topic	Link
14 Day Trial	https://www.scoutdns.com/try_now/
Support Portal	https://help.scoutdns.com
Terms of Use	https://www.scoutdns.com/terms/
Privacy Policy	https://www.scoutdns.com/privacy/