NAYAtel

Secure DNS

Cisco Umbrella

Secure DNS

Nayatel Secure DNS services, powered by CISCO Umbrella, offers cloud-based security to detect compromised systems and protect users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

▶ How it works:

- 🔒 **Encrypted**
- ✓ **Authentication**
- 🛡 **Security Filtering**
- 🚫 **Content Filtering**

Umbrella Servers

Umbrella

Roaming Client

Root DNS Server
(.com, .net)

Public Queries
(google.com)

Local Queries
(pcl.mycarp.local)

Local DNS Server

(mycarp.local)

Authoritative
DNS Server
(domain1.com,
domain2.net)
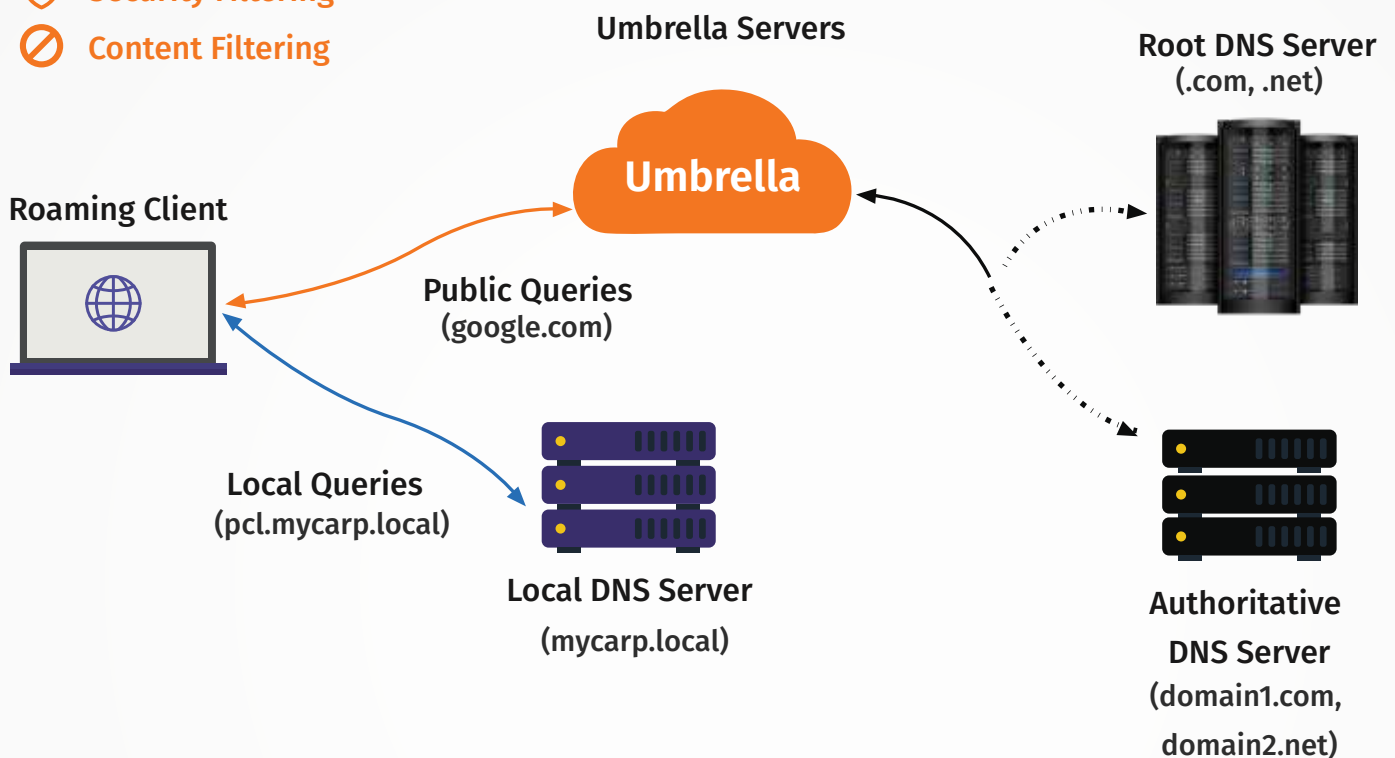
▶ Secure DNS Features:

- 🚫 Block domains associated with phishing, malware, botnets, and other high risk categories (crypto mining, newly seen domains, etc.)

- 📞 Prevent web and non-web callbacks from compromised systems

- 🔽 Enable web filtering using 85+ domain categories

- ☰ Create custom allow and block lists

- Pinpoint compromised systems using real-time security activity reports

- Discover and block shadow IT (based on domains) with the App Discovery report

- Protect mobile and roaming users who are off-network

- Create policies and view reports by user (Active Directory), network (egress IP), network device, internal subnet, or roaming device

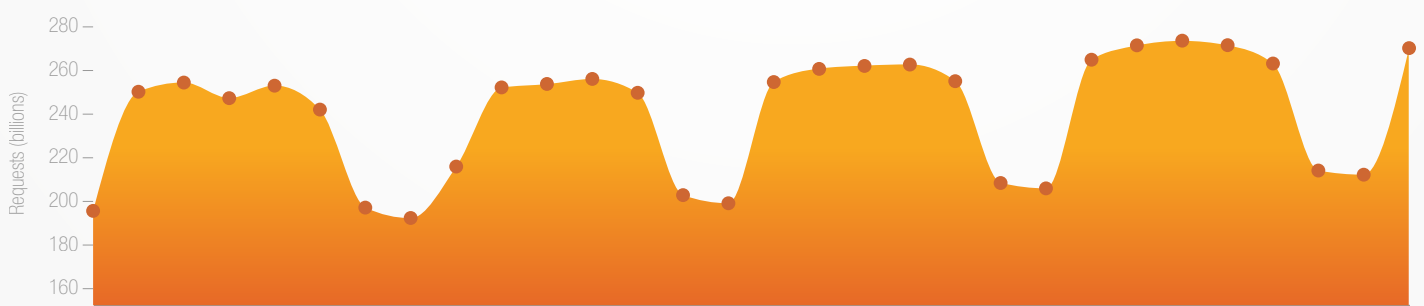- Use customizable block pages and bypass options

- Access to Umbrella's APIs and ability to retain logs with Amazon S3 bucket DNS & IP layer enforcement

Why Nayatel Secure DNS is powered by Cisco Umbrella?

Every day, the Cisco Umbrella global network processes over **250 billion** recursive DNS requests.

Average Daily DNS Requests

More than 30 data centers worldwide with automated failover. The Cisco Umbrella global network of data centers delivers 100% business uptime

92% of surveyed organizations reduced malware infections by 10 – 24% or more after using Cisco Umbrella.

92%

CISCO | TechValidate by SurveyMonkey

Leveraging the internal visibility into 200 billion web requests a day, Umbrella runs over 30 different machine learning algorithms to detect emerging attacks. Umbrella gives the most complete view of the relationships and evolution of internet domains, IPs, and malware

60K
New malicious destinations (domain, IPs, and URLs) identified daily

70M
Malicious domains and IPs enforced, while at the same time Delivering fast internet access