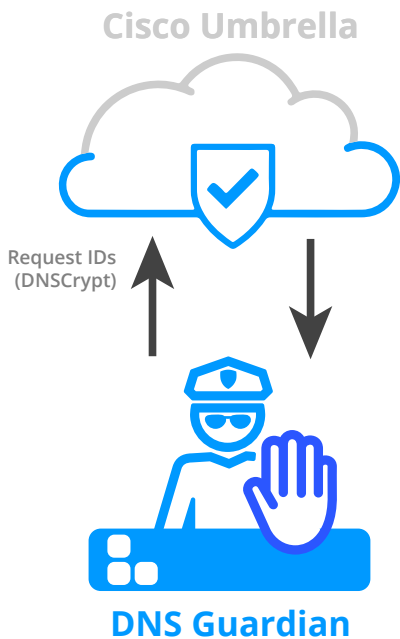# Cisco Umbrella & EfficientIP Technology Alliance
Extend Enterprise Security Perimeters & Strengthen Network Defenses

In a security context where the threat landscape is constantly evolving and attacks becoming more and more sophisticated, DNS has become a primary target and assault vector for hackers, damaging brand reputation, revenue and operational efficiency of companies in all sectors.

The combination of Cisco Umbrella and EfficientIP technologies extends the enterprise security perimeter and strengthens network defenses. The technology alliance combines threat intelligence services to protect against malicious domains, with behavioral detection of attacks and adaptive security. It offers a best-of-breed market solution to defend against the widest range of DNS menaces, protecting on and off-network users, safeguarding data confidentiality and ensuring both internal and external service continuity.

Best-of-Breed Security to Protect Against the Widest Range of DNS Threats, On & Off-Network

The joint solution offers an unprecedented level of in-depth visibility and security of DNS services for the most comprehensive threat protection. On-premise, SOLIDserver™ DNS Guardian is a purpose-built security appliance enabling DNS Transaction Inspection (DTI) technology for real-time advanced analytics and context-aware behavioral attack detection over client traffic, at ultra-high speed (up to 10M Queries per Second). Patented adaptive countermeasures (block, quarantine, or rescue mode) ensure service continuity and data confidentiality while mitigating risk of false positives. When internet recursive DNS queries are identified as trustworthy, DNS Guardian tags, encrypts (DNSCrypt) and forwards them to the Cisco Umbrella platform to take advantage of the secure Cloud-based gateway. Cisco Umbrella checks filtering policies and resolves or denies the queries, offering a complementary layer of defense based on destination domain reputation thanks to Internet-wide big data analytics and machine learning.

This combination of complementary security technologies extends the enterprise security perimeter by protecting both on/off-network users and internal DNS services availability - resolver and authoritative. Thanks to "on-the-fly" traffic tagging with Cisco IDs, DNS Guardian enables detailed visibility of the client behind each query, via the Cisco Umbrella portal. Additionally, DNS-DHCP-IPAM data offers key information on associated devices such as location or name, improving network control, reporting capacity and remediation efficiency.

Cisco Umbrella

Request IDs (DNSCrypt)

DNS Guardian

Simple, Fast, Secure Deployment

Cisco Umbrella Platform
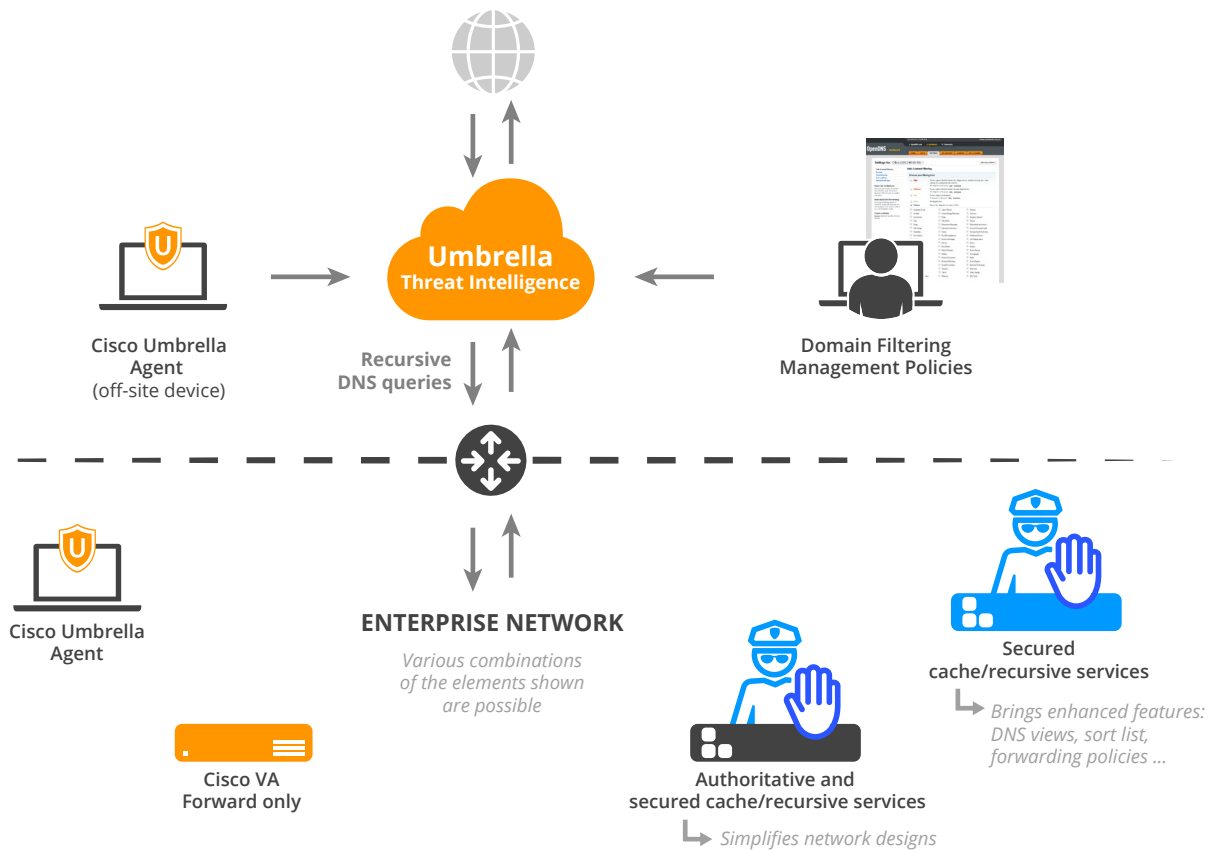
Detailed Traffic Visibility

Solution Features

Ease of Use and Deployment

- Plug & play solution thanks to native integration
- Encrypted flow with DNScrypt
- Detailed visibility over enterprise-wide internet traffic via Cisco Umbrella portal: IP source, DNS server, destination domain, category, action
- Faster remediation with DDI data (port connection, name)
- Strengthened network security ecosystem with SIEM integration

Full Coverage of the DNS Threat Landscape for On & Off-Network Users

- Prevent initial infection and phishing, and stop communication with CnC server, with threat intelligence on reputation domains for on/off-network users
- Detect data exfiltration beyond domain reputation, by combining requested domains with context-aware client behavior analysis
- Enhance predictive security with contextual traffic analysis
- Strengthen resiliency and mitigate zero-day attacks with hybrid deployment
- Ensure continuity of internal DNS services by applying adaptive countermeasures

Umbrella
Threat Intelligence

Cisco Umbrella Agent
(off-site device)

Recursive DNS queries

Domain Filtering Management Policies

Cisco Umbrella Agent

ENTERPRISE NETWORK

Various combinations of the elements shown are possible

Cisco VA Forward only

Authoritative and secured cache/recursive services

Simplifies network designs

Secured cache/recursive services

Brings enhanced features: DNS views, sort list, forwarding policies ...

Flexible Deployment Models