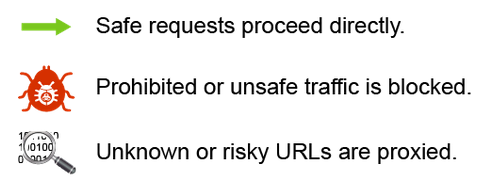
**Cisco umbrella**

* Cisco Umbrella is a security mechanism based on Domain Name System (DNS) and can provide common security for both on-premise and off-premise endpoint
* Cisco Umbrella becomes your DNS resolver, and it resolves malicious destinations to a block page to prevent the connection.



**Cisco Umbrella currently comes in three different offerings:**

* **Cisco Umbrella DNS Security Essentials:** the basic offering which enables you to:
  1. Protect users on the corporate network via integration with network devices.
  2. Protect off-network users via integration with roaming clients.
  3. Block domains associated with malware, phishing, botnets, and other threats.
  4. Perform web filtering by domain and domain category.
  5. Create policies and view reports.
  6. Integrate with existing tools and workflows with application programming interfaces (APIs) for enforcement, reporting, management, and deployment.
* **Cisco Umbrella DNS Security Advantage:** allows to do everything in DNS Security Essentials plus:
  1. Block direct IP connections that bypass DNS, if clients use roaming client.
  2. Use Intelligent Proxy, to proxy traffic for risky domain for URL filtering and Cisco AMP and decrypt and inspect Secure Sockets Layer (SSL) traffic associated with risky domains.
  3. Use Umbrella Investigate for deeper context during investigations.
* **Cisco Umbrella Secure Internet Gateway (SIG) Essentials:** allows to do everything in DNS Security Advantage plus:
  1. Use secure web gateway, which proxies all web traffic for URL and Cisco AMP inspection, decrypts and inspects all SSL traffic, performs web filtering by domain, URL, and category, use Cisco Threat Grid cloud sandbox to analyze suspicious files, and see retrospective AMP events.
  2. Use cloud-delivered firewall, which allows you to create Layer 3 and 4 policies to block specific IP addresses, ports, and protocols, in a combination with having a permanent IPsec tunnel in place between your company and Umbrella cloud.
  3. Use cloud access security broker, which allows you to discover and block shadow systems based on URLs, and create policies with granular control for selected cloud-based applications.

**Deploying CISC umbrella**

Most endpoints on your network will receive their DNS settings from DHCP. So, to **implement Cisco Umbrella, you can simply update the DNS settings in your DHCP scope** without having to visit all endpoints in the organization

**Cisco Umbrella Roaming Client**

Two lightweight options are available to identify off-network clients:

* **Cisco Umbrella Roaming Client:** Is a lightweight agent deployed on a Windows or Mac endpoint. The Roaming Client is downloaded from the Cisco Umbrella dashboard. Each organization downloads Cisco Umbrella from their specific Umbrella dashboard. When the Roaming Client is downloaded, an organizationally unique identifier is embedded with the install package. When the endpoint queries Cisco Umbrella for DNS, the Roaming Client presents the organizationally unique identifier along with the DNS request, and Cisco Umbrella evaluates the DNS query against the appropriate policy.
* **Cisco Umbrella Roaming Security module for Cisco AnyConnect Secure Mobili**t**y Client:** Is a lightweight module that is installed on top of existing Cisco AnyConnect installation. You have to install the module using Cisco AnyConnect installation methods. Then you download an OrgInfo file from your Cisco Umbrella dashboard. The file instructs the Roaming Security module which organization instance subscription to report to and which policies to enforce.

**Cisco Umbrella is managed through a public cloud-based dashboard**. Network and User Identities, Security and Reporting Policies, Block Page settings, Active Directory integration, and other configuration tasks are performed directly in the cloud-based dashboard.