Cisco Umbrella Service Description

Cisco Umbrella is a cloud security platform that is designed to unify multiple security services in a single cloud-delivered platform to help secure internet access and help control cloud app usage from your network, branch offices, and roaming users. Depending on the package and deployment, Cisco Umbrella integrates secure web gateway, cloud-delivered firewall ("CDFW"), DNS layer security, cloud malware protection, in-line data loss prevention and other cloud access security broker (CASB) functionality, and remote browser isolation for effective protection. Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the internet and delivers deep inspection and control to support compliance and block threats. Cisco Umbrella is backed by the Cisco Talos threat intelligence team, and it provides interactive access to threat intelligence through Cisco Umbrella Investigate to aid in incident response and threat research.

Cisco Umbrella Investigate provides access to certain Cisco threat intelligence about malicious domains, IPs, networks, and file hashes. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the Internet, Cisco applies statistical models and human intelligence to identify attackers' infrastructures. Cisco Umbrella Investigate data can be accessed via a web-based console or an API.

Packaging options

Cisco Umbrella is available in different packages designed to provide the right fit for a variety of different sized organizations.

- The **Umbrella DNS Security Essentials** package includes core DNSlayer security capabilities, to work to block requests to malicious domains before they reach the network or endpoints. This base package includes off-network protection and mobile support, as well as access to Umbrella's APIs (policy, reporting and enforcement), log exporting, the multi-org console, integration with Cisco Threat Response, and identity-based policies (virtual appliance + Active Directory connector). Additionally, this package provides discovery and blocking of shadow IT (by domain) with the App Discovery report.

- The **Umbrella DNS Security Advantage** package includes all the capabilities of DNS Security Essentials plus it enables organizations to proxy risky domains for URL blocking and file inspection using AV engines and Cisco AMP.

- The **Umbrella SIG Essentials** package includes all of the capabilities of the DNS Security Advantage package plus access to a secure web gateway (full proxy), cloud-delivered firewall, sandbox file analysis with Cisco Threat Grid, and cloud access security broker (CASB) functionality.