Cisco Secure Access - DNS Defense (Formerly Cisco Umbrella DNS)

Affordable, simple to deploy and manage, and effective

May 2025

Contents

Why strong DNS-layer security is essential to thwarting ransomware and phishing attacks

The U.S. Cyber and Infrastructure Agency (CISA) states that over 90% of successful attacks begin with a link or webpage. The DNS protocol associates domain names with IP addresses. As DNS requests precede IP connections, regardless of protocol or port, DNS-layer security rapidly evaluates requests before they are established. With strong DNS-layer security, access to malicious domains and threats like ransomware are blocked before they reach your network and endpoints.

Today, many organizations leave DNS resolution to their ISP. But the growth of direct enterprise Internet connections and remote work make DNS optimization for threat defense, privacy, compliance, and performance ever more important. **Along with core "security hygiene," like a patching program, strong DNS-layer security is the leading cost-effective way to improve security posture**. It blocks threats before they even reach your firewall, dramatically reducing the alert pressure your security team manages.

The world's #1 ranked DNS-layer security just got even better

Material improvement to network security posture is typically expensive, slow, and costly. SOCs and DFIR teams are often overwhelmed with alert pressure, and smaller organizations need security that does not require day-to-day management.

Secure Access - DNS Defense is different. **Security should be simple, and effective**, and Cisco meets the need. Over 40,000 customers entrust over 800 billion daily connections to us. In 2024, GigaOM published that Cisco Secure Access - DNS Defense is #1 in the industry in DNS-layer security.

Further, our DNS leadership has contributed to our #1 SSE threat efficacy and DNS latency rankings in Miercom's Benchmark Report.

Now, we extend the lead: Cisco raises the bar with AI-based DNS tunneling enhancements and Domain Generation Algorithm (DGA) detection.

The result? More thwarted threat actors, with superior threat protection at the DNS layer before traffic hits your firewall. Cisco protects better and drastically reduces the alert pressure your security team faces.

Even more, Secure Access - DNS Defense goes further than Cisco's previous DNS-centric packages, including an enhanced policy framework compared to Cisco Umbrella DNS, plus SaaS API DLP and cloud malware scanning. These enhancements are delivered without higher cost.

Foundational security, with room to grow as needed

It is up to you: stay DNS-centric, or over time upgrade to full Secure Access SSE, Cisco Universal Zero Trust Network Access (UZTNA), or integrated Cisco Secure Access Service Edge (SASE) with Cisco's market leading Software Defined WAN (SD-WAN).

The Secure Internet Access (SIA) package of Secure Access includes all DNS Defense capabilities noted in this datasheet, plus Experience Insights digital monitoring powered by Cisco ThousandEyes, full DLP, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Remote Browser Isolation (RBI), Firewall as a Service (FWaaS), and more. Secure Access - DNS Defense includes a no-cost trial of up to 100 seats of the Secure Private Access (SPA) package of Secure Access, featuring the industry's first integrated ZTNA + VPN as a Service (VPNaaS) capability. For a comparison of Cisco's cloud-delivered security packages, please visit this link.

Features and benefits

Feature	Benefit
DNS-layer security	Unlike competing SSE vendors offering DNS-layer security, Cisco operates a recursive DNS Service. The result is proven lower latency, and a better user experience. Filtering at the DNS layer blocks requests to malicious and unwanted destinations, over any port or protocol, before a connection is established to the network or endpoints. • Protect internet access across all network devices, office locations, and roaming users and mobile devices. • Block access to domains with malware, phishing, botnet, and other high-risk items. • Application discovery, monitoring, blocking, and risk scoring. • Provides detailed reporting for DNS activity by type of security threat or web content and the action taken. • Advanced artificial intelligence mitigates DNS Tunneling techniques, thwarting lateral movement by threat actors and providing real-time detection and protection against data exfiltration. • Enables rapid rollout to thousands of locations and users for immediate protection. • Provides visibility in reports and applied policies – down to the user level.
Global Infrastructure	• Secure Access - DNS Defense includes a global network of 50+ recursive DNS resolvers for high performance security that stops threats before they reach your users and network.

Feature	Benefit
Secure Web Gateway (partial)	• Enable content filtering by category or specific URLs to block destinations that violate policies or compliance requirements. • Selectively proxy and inspect web traffic.
SaaS API DLP	Uses third-party SaaS APIs (Cloud-to-Cloud) to scan and control sensitive data without requiring visibility into internet-bound traffic. It discovers sensitive data residing in cloud services, and continuously monitors those services for additions of sensitive data.
Cloud malware detection	Detects and removes malware from cloud-based file storage apps. Enhances protection by detecting malicious files before they reach an endpoint. • Increases effectiveness and efficiency of security administrators. • Once activated, all files in cloud-based services are hashed and scanned for malware automatically. Malicious files are flagged for remediation, quarantine, and/or deletion. • Supports Box, Dropbox, Webex®, Microsoft 365, and Google Drive, AWS S3, Azure.
Talos Threat Intelligence	Cisco Talos, one of the world's largest commercial threat intelligence teams, continuously runs AI, statistical, and machine learning models against its massive database of threat data to provide deeper insight and context into cyber threats. Talos research is continuously used to enrich the efficacy of Secure Access - DNS Defense.
Single management and reporting console	Unified security policy creation and management, using intent-based rules. If you require additional capability beyond DNS-layer security over time, the Secure Access unified console provides a single point for consolidate policies across internet access protection, public SaaS app, and private app access. Provides extensive logging and the ability to export logs to enterprise Security Operations Center (SOC). • Single place to define policy for any user to any app. Simplifies the process of building security policies and drives consistency in policy definition for entire organization. • Unified source (users, devices) and unified resources (apps, destinations) allow the security policy to follow the users no matter the point of attach and or which app they access. • Reduces ongoing policy management activities. • Improves visibility and time-to-detection with aggregated reporting. • Simplifies the overall SOC/security analyst investigation process.
Device support Included with Secure Access - DNS Defense at no added cost.	• Secure Client on Windows and MacOS, iOS, and Android. • Cisco Security for Chromebook Client.

Cisco Secure Access: Software Support Service

Cisco Secure Access requires a separate Stock Keeping Unit (SKU) for Software Support–Enhanced, with the option to upgrade to Software Support Premium.

Cisco Software Support Enhanced

- Technical Support (24x7 access to Cisco Cloud Security Support – phone/online).
- Technical onboarding and adoption assistance.
- Software updates.
- Primary point of contact with software expertise.

Cisco Software Support Premium (recommended upgrade)

Includes Enhanced level features plus:

- Prioritized case handling over Enhanced support.
- Support case analytics.
- Assigned expert who provides incident management.

To learn more about Cisco Support Services for and proactive consultation and recommendations to Security Software, click here.

For more information

For more information, please visit: Cisco Secure Access.

C78-5130097-00 05/25