Secure Access - DNS Defense

#1 Ranked DNS security

Affordable, effective, and simple to deploy

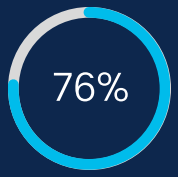


Why strong DNS-layer security is essential

The U.S. Cyber and Infrastructure Agency (CISA) states that over 90% of successful attacks begin with a link or webpage. The Domain Name System (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.

© 2025 Cisco and/or its affiliates. All rights reserved.



When surveyed, 76% of Cisco DNS-layer security customers saw value within one week of deployment.*



Over half of Cisco DNS security customers saw malware drop by over 50%.*

*TechValidate surveys of Cisco DNS customers.

© 2025 Cisco and/or its affiliates. All rights reserved.

Strong return on investment

With low up-front cost, security efficacy proven in independent third-party testing, no hardware to install, no software to manually update, and protection for workers both on and off the corporate network, Cisco® Secure Access - DNS Defense efficiently enhances threat defense. Over 40,000 organizations globally—from small startups to global enterprises—chose Cisco cloud-delivered security for quality and value.

Your choice: Stay DNS-centric, or evolve to full SSE

With Secure Access - DNS Defense, it's your choice: stay with our DNS-centric offering, or evolve over time to a fully integrated Security Service Edge (SSE) experience, with additional Secure Access packages: Secure Internet Access (SIA) and/or Secure Private Access (SPA). Regardless, you benefit from a single console, single client, and single policy framework for DNS, Zero Trust Network Access (ZTNA), Data Loss Prevention (DLP), AI Access, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Firewall as a Service (FWaaS), and more. In addition, DNS Defense subscriptions enable you to extensively trial our secure application access capabilities before making a commitment.

DNS Defense differentiators

We see more and protect better.

Across 190+ countries, Cisco processes 800+ billion internet requests daily, more than many of the world's largest ISPs. This global visibility contributes to our unmatched DNS threat intelligence. According to third-party Miercom laboratory testing, in its 2024 SSE Benchmark Report, Cisco outperformed other leading SSE vendors in threat efficacy and low-latency DNS performance. Additionally, GigaOM evaluated eleven DNS security vendors and named Cisco DNS Defense the leader.

More important than third-party recognition, however, is what customers have to say:

Lower latency architecture: the only SSE with recursive DNS. With most security solutions, there is a tradeoff between security and usability. Not so with Secure Access - DNS Defense, which accelerates connectivity. Cisco's 50+ global DNS data centers, and peering relationships with over 1000 top global ISPs, Content Delivery Networks (CDNs), and SaaS platforms, deliver superior speed and user experience. Using Anycast routing, our global DNS service uses a single IP address, and requests are transparently sent to the nearest, fastest data center, with automatic failover.

Deployment

On-network: With just three clicks for basic deployment, DNS Defense protects users and systems across your organization in minutes. Any network device (e.g. router, DHCP server) can connect to DNS Defense. Simply redirect your DNS to the DNS Defense (formerly Cisco Umbrella®) IP address. You can leverage your existing Cisco footprint—Cisco Integrated Services Routers (ISR) and Catalyst®, Meraki™, Cisco Secure Firewall, and more.

Roaming: We protect Windows, MacOS, iOS, Chrome OS, and Android devices outside the network security perimeter—without sacrificing performance. A part of the single Cisco Secure Client, the Secure Access roaming module includes DNS-layer security for roaming users, plus optional SWG, ZTNA, and VPN as a Service (VPNaaS) capability.

Open. Aggregate data from appliances and threat intelligence platforms with your DNS Defense workflow to extend visibility. DNS Defense includes a full API for programmatic protection of networks and users, log exporting, and identity-based policies, enabling seamless integration with other security solutions. Secure Access - DNS Defense also integrates with Cisco Splunk and Cisco Extended Detection and Response (XDR), plus the Cisco Security Cloud Control platform.

More than DNS-layer security. The Secure Access - DNS Defense package includes all of Cisco's DNS security capabilities, plus:

- **Cloud malware** scanning with popular cloud storage repositories.
- **SaaS DLP** to mitigate leakage of sensitive customer data and your intellectual property into the cloud.
- **An extended ZTNA+VPNaaS trial**, upto 100 seats.

DNS Defense customers get these capabilities without paying more.

Additional Features

New AI-enhanced DNS tunneling mitigation. Improves our already class-leading tunneling detection rate by a further 11.1%, while lowering false positives.

New AI-based Domain Generation Algorithm (DGA) detection. Further extends Cisco leadership in thwarting adversary callbacks and command and control (C2) communications from compromised devices.

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

Core web filtering using 100+ category-based content categories. Create custom block and allow lists. Pinpoint compromised systems using real-time security activity reports.

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

Identify malware in cloud storage repositories (Azure, Microsoft 365, S3, Box, and more).

SaaS Data Loss Prevention (DLP) mitigates leakage of sensitive data uploaded to the web.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-5121853-00 05/25