AKAMAI PRODUCT BRIEF

Edge DNS — Comprehensive DNS Security

The Domain Name System (DNS), which translates human-readable domain names into numerical IP addresses, is a fundamental component in delivering quality web experiences for your website visitors and application users.

If your DNS goes down, your online presence goes down. Akamai Edge DNS provides you with comprehensive protection from a wide range of DNS attacks on your DNS infrastructure, whether it be in cloud, on-prem, or hybrid. The solution also offers a high level of DNS performance, resiliency, and availability.

Today's DNS distributed denial-of-service (DDoS) attacks come with record-breaking scale and sophistication, making protection against them incredibly challenging for global businesses that depend on the 24/7/365 availability of their DNS infrastructure.

Akamai Edge DNS is an external authoritative DNS solution that offers:

- **Comprehensive security.** Protect your DNS infrastructure from increasingly large, frequent, and sophisticated attacks — in cloud, on-prem, or hybrid
- **Unmatched performance.** Let the world's most distributed network alleviate origin load, provide 24/7 availability, and reduce page load time
- **Intuitive management.** Self-configure and manage your DNS zones and enforce your own dynamic policies in real time

Built on a globally distributed anycast network, Edge DNS can be implemented as a primary or secondary DNS service, replacing or augmenting existing DNS infrastructure as needed.

Key capabilities

Nonstop DNS availability

Your mission-critical DNS availability is underscored by Akamai Connected Cloud with several thousands of DNS servers worldwide. Additionally, your DNS availability can be fortified by using internet-facing secondary zones.

Edge DNS comes with a 100% uptime service level agreement (SLA), providing you with the confidence that your customers and employees can reliably connect to your web and application servers.

Benefits for your business

Defend your DNS against DDoS attacks. Protect your critical DNS infrastructure against DNS forgery, and monitor zones for brand spoofs and phishing.

Experience nonstop DNS availability. Akamai's several thousands of globally distributed DNS servers, internet-facing secondary zones, and 100% uptime SLA keep your DNS available at all times.

Simplify workflows with a unified DNS solution. Provision and configure zone and traffic management policies and workflows.

Improve user experience with rapid responses. Achieve faster, more reliable resolution of DNS queries.

Empower your security team. Easily customize DNS zones, automate workflows, and minimize changes to your network.

©2025 Akamai Technologies | Support | | Published 04/25

Comprehensive defense against DNS DDoS attacks

Edge DNS provides a highly scalable DNS platform with an intelligent architecture that absorbs even the largest DNS DDoS attacks while responding to legitimate user requests.

You can use the optional DNSSEC feature to prevent attacks caused by DNS forgery and to monitor zones for brand spoofs and phishing domain names.

Your users continue to access uncompromised online experiences even if you are under attack.

Fast and optimized responses to DNS queries

Edge DNS improves and optimizes the responsiveness of your DNS infrastructure by intelligently responding to user queries from the closest high-performing DNS server based on network conditions.

The globally distributed anycast network accelerates DNS resolutions for users connecting to your websites and applications from anywhere in the world. Zone apex mapping reduces DNS lookup times even further for sites on Akamai Connected Cloud for additional performance boost.

Flexible configuration and integration

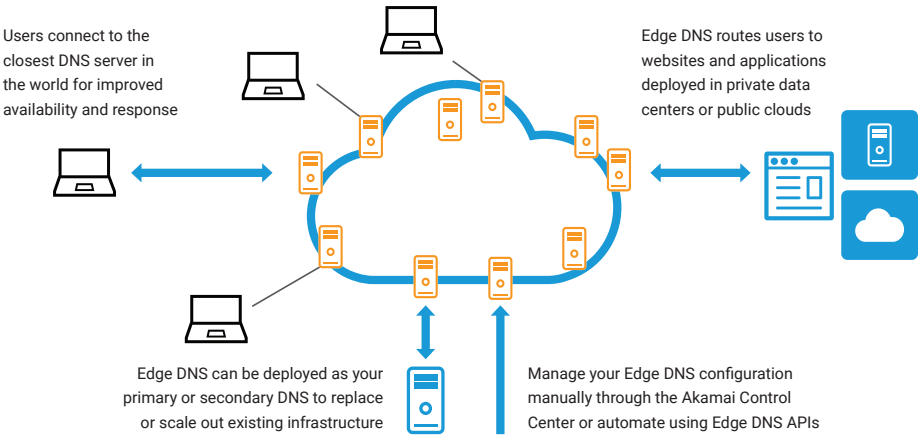
Edge DNS enables you to customize your primary and secondary DNS zones via the Akamai Control Center, APIs, or tools such as Terraform.

Additionally, your network infrastructure team can easily simplify and automate DNS workflows by integrating Edge DNS with standard DevOps toolkits and resources through APIs.

Dynamic response policy

Akamai understands that having a single solution for provisioning and configuring both zone and traffic management can be important for you. Edge DNS includes the capabilities of Akamai Global Traffic Management to offer:

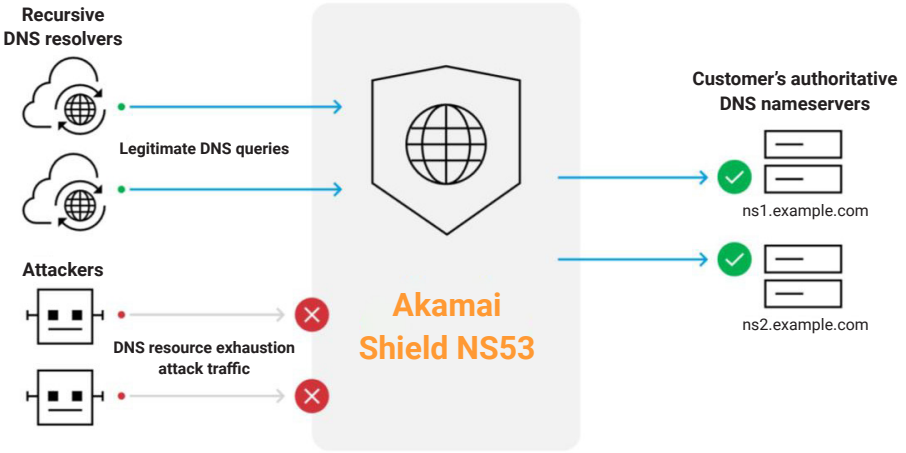
- Simplified workflows to configure policies, such as region-specific responses
- Access to extensibility and flexibility for DNS workflow
- A low-cost way to handle unique addressing requirements, such as compliance



Protect your on-prem and hybrid DNS infrastructure

Akamai Shield NS53 is a bidirectional DNS reverse proxy solution that protects on-prem and hybrid DNS infrastructure — including Global Server Load Balancers (GSLBs), firewalls, and nameservers — from resource exhaustion (e.g., NXDOMAIN) attacks. You can self-configure, administer, manage, and enforce your own dynamic security policies in real time. Illegitimate DNS queries and DNS attack floods are dropped at the edge of your network, thereby protecting the critical DNS infrastructure that supports your online presence.

Shield NS53 also helps alleviate the load on your on-prem infrastructure by responding to legitimate queries from the cache and forwarding queries to the origin name servers only when necessary. Additionally, the solution reduces latency and improves user experience by accessing Akamai's global anycast network of servers to respond to user queries from the closest point of presence.



Power your DNS security and performance

Akamai Edge DNS and Shield NS53 are purpose-built to stop even the largest DNS DDoS attacks at the edge of your network while reliably and quickly responding to legitimate user queries.

To sign up for a free trial, visit the Akamai Edge DNS page or contact your Akamai sales team today!

©2025 Akamai Technologies | Support | | Published 04/25