

NS1 Domain Security Suite

Enterprises depend on modern DNS services to assure availability and optimize user experience of online business services, which makes DNS a critical attack vector. As a result, DNS redundancy is now a must have for many enterprises. Additionally, ICANN recommends that organizations adopt DNSSEC (Domain Name System Security Extensions) to prevent domain hijacking.

Implementing DNSSEC and other security controls across a redundant DNS infrastructure delivered by two different DNS providers often involves trade-offs in cost, manageability and functionality.

NS1 Domain Security Suite™ is a turnkey solution including Managed DNS, Dedicated DNS, and Overage Protection. With NS1, enterprises no longer have to sacrifice performance for security and resilience.



Assure Availability and Resiliency

Managed DNS is a global, over-built, DDoS resilient Anycast network with a strong reliability history backed by a 100% uptime SLA.

Mitigate Risk with Redundant DNS

Dedicated DNS is a fully managed, physically separate network that delivers DNS redundancy without the complexity and management limitations of dual providers.

Improve Operational Efficiency

Full traffic management, DNSSEC, and security features across both Managed DNS and Dedicated DNS networks are managed from the same portal and API, which means organizations get security and redundancy without needing to introduce additional management complexity.

Eliminate Overage Charges

There is no charge for query overages due to DDoS or other malicious traffic.





NS1 Domain Security Suite: Secure, Resilient & Smart Traffic Management

The Challenge of DNS Security & Dual Provider Redundancy

DNS security and redundancy is complicated for enterprises that rely on advanced routing and traffic management features.

- ▶ **No two providers offer the same set of advanced traffic management features.** No two providers implement features in the same way.
- ▶ **Synchronizing features and records between two providers is problematic.** The manual effort needed for initial set up and for updates can be costly and a reliability risk.
- ▶ **DNSSEC signing across providers that offer proprietary features** that tailor DNS responses is not feasible, since few vendors have implemented a standardized mechanism for sharing DNSSEC records and keys across multiple providers.

This can mean foregoing intelligent control over user experience, if enterprises revert to a common denominator feature set.

Domain Security Suite includes:

Managed DNS

A global, anycast network with a fully redundant architecture at 26 locations to meet a 100% uptime SLA.

Dedicated DNS

A single tenant network, managed by NS1, and that is isolated from network failures or congestion on Managed DNS.

Overage Protection

DDoS aimed at your domains can result in expensive overage charges. The Domain Security Suite includes no charge for overages due to DDoS.

Enterprises benefit from two physically separate DNS networks which are:

- ▶ **Synchronized with the same advanced feature set**
- ▶ **Protected with DNSSEC**
- ▶ **Managed from the same portal and API**

Features



Intelligent Traffic Management

Routing ensures that users get to servers, datacenters, CDNs, or cloud instances that deliver optimal performance.

Filter Chain

Code-free creation of sophisticated traffic management policies such as load balancing, load shedding, failover, latency-routing, and geographic routing.

DDoS Defense

Combination of global locations, massively provisioned infrastructure, autoscaling, sophisticated detection, filtering capabilities, and operational readiness drills to protect against attack.

DNSSEC

The integrity of DNS responses is protected by DNSSEC signing without compromising redundancy. Zones are signed on both the Dedicated and Managed nodes, something not easily accomplished with multiple vendors.

Secure Access

Single Sign On or Two Factor Authentication validates users, and Role Based Access Controls manage access.

Audit Logs

Actions are recorded with audit logs on a per user and API-key basis.

Single Pane of Glass Management

Maintain your DNS zones, records and advanced traffic management in a single portal and API.

Rapid, Transparent Synchronization

Custom traffic management policies to be transparently synchronized. Changes are made once and automatically propagated to all Managed and Dedicated DNS nodes in seconds.

Simplified Billing

Customers receive one bill from NS1 for both Managed and Dedicated networks, simplifying vendor management.

Simplified Support

Single point of contact for all support issues across both the Dedicated and Managed DNS deployments.