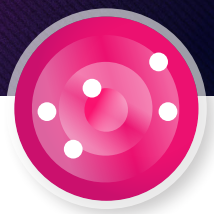
DATASHEET

# NS1 Domain Security Suite.

DNS is a mission-critical service and is one of the most commonly attacked applications on the internet. Attackers are going after DNS like never before. In response, the US Department of Homeland Security and the Internet Corporation for Assigned Names and Numbers (ICANN) have issued clear warnings and required measures enterprises should take to secure their DNS.

By applying well-established defenses and best practices, every enterprise can avoid joining the growing list of companies that have fallen victim to DNS attacks.

The Domain Security Suite from NS1 is a turnkey package of DNS services and capabilities designed to keep your business and your customers safe from DNS exploitation.



## Turnkey Redundant DNS

If your DNS is down, your business is down. The Domain Security Suite includes a turnkey dual DNS solution that solves the complexities and limitations of traditional approaches to DNS redundancy.

## DNSSEC Without Compromise

DNSSEC is a must have for preventing misuse of your domain, but implementing it has traditionally meant trading off traffic management functionality for security. Not any more. With NS1 Domain Security Suite, your dual DNS includes full traffic management support for your DNSSEC secured zones.

## Overage Price Protection

No charge for query overages due to DDoS or other malicious traffic.

## The Threats are Real

Because DNS is so fundamental to IT operations, attackers use it and misuse it to:

- Make entire enterprises "disappear" from the internet by taking down their DNS.
- Misdirect users to bogus websites masquerading as legitimate sites.
- Hijack domain names.

The consequences to your business and your customers can be devastating.

## NS1 Domain Security Suite Includes:

### Dual DNS Network Redundancy with Dedicated DNS

For the ultimate in DNS availability assurance, the NS1 Domain Security Suite includes Dedicated DNS:

- A fully managed, single tenant, globally anycasted DNS network dedicated to your zones
- Hosted with a 3rd party vendor on hardware, IPs, and ASNs that are physically and logically separate from the NS1 Managed DNS network.
- Single pane of glass management
- Support for full traffic management and DNSSEC

### Prevent DNS Hijacking with No Compromise DNSSEC

DNS hijacking is becoming more common as attackers find new and creative ways to subvert the DNS system into misdirecting users and applications to malicious sites. DNSSEC is THE defense recommended by the IETF, ICANN and regional internet registries around the world. NS1 has removed the barriers and trade-offs to DNSSEC:

- Easy point and click or API implementation
- Compatible with turnkey redundant DNS
- Full traffic management for your signed zones
- No other DNSSEC solution supports these capabilities.

### Intelligence, Visibility and Control

NS1 gives your teams visibility into DNS usage that can provide insight into potential misuse by external actors.

- Record-level reporting
- Integrations with monitoring and reporting systems
- Visibility into anomalous traffic, and unused records reports.
- Netfencing for the control to prevent your sites from receiving traffic from countries or regions you wish to exclude.

### Secure Management Access

Securing your DNS starts with strong access controls to DNS administration. The NS1 platform supports a comprehensive suite of controls that meet and exceed the recommendations recently issued by the CISA division of the Department of Homeland Security.

### Security That is Good for Your Business

The NS1 Domain Security Suite puts it all together. You get the tools and services you need to manage your DNS securely, efficiently and consistently deliver the performance your business needs to safely thrive on the internet.

## FEATURES AND BENEFITS

| | |
|---|---|
| **Managed and Dedicated DNS** | Dual DNS networks for redundancy |
| **DNSSEC** | DNSSEC on both primary and backup DNS networks, with traffic routing |
| **Single Sign-On** | Support for IdPs including Okta and Azure AD |
| **Easy to use Team Management** | Strong team management with role-based access controls |
| **Granular Permissions System** | Zone-level permissions for read or write access per user, team, or API key |
| **IP Whitelisting** | Whitelist office VPNs, individual users, and API keys |
| **Blacklist Netfencing** | Filter bad actors' IPs and ASNs at the edge, or only return answers to known approved IPs |
| **Unused Record Reports** | Discover and remove unused records, reduce complexity and minimize your attack surface. |
| **TSIG Support** | Adds strong authentication to DNS updates made via AXFR/IXFR |
| **Customizable Session Management** | Customize concurrent session limits and timeouts |
| **Hardened Platform** | SOC 2 Type 2 + regular pentests performed by industry leading 3rd party |
| **Activity Logging for Audits** | Audit all account activity on a per user and API-key basis |
| **Record-level Query Statistics** | Query stats for every single DNS record, zone, and network |
| **Integration with Your Dashboards** | API calls and integrations that allow you to pull stats and metrics into reporting tools such as Tableau, Qlik, PowerBI |
| **Growth Reports** | Get insight into what's driving traffic spikes |
| **Customizable Dashboard** | Instantly get usage reports and graphs for your most important records/monitors |
| **Activity Logging** | Every change is logged - data can be exported to SIEM and monitored |
| **Two Factor Authentication** | Enforce 2FA account-wide, required enrollment on user creation |
| **Strong Password Enforcement** | Known weak pw blacklist, password reuse policy, complexity requirements |
| **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 |