SECURE64®

# Secure64® DNS Authority for x86™
## Secure, High Performance Authoritative DNS

DATA SHEET

# DNS AUTHORITY

### KEY BENEFITS

- Remains fully responsive during DDoS attacks
- Eliminates BIND security vulnerability patching
- Enables 99.999% service availability
- Simplifies integration with external software systems
- Scales up without requiring hardware upgrades
- Reduces TCO because servers need no protective security appliances

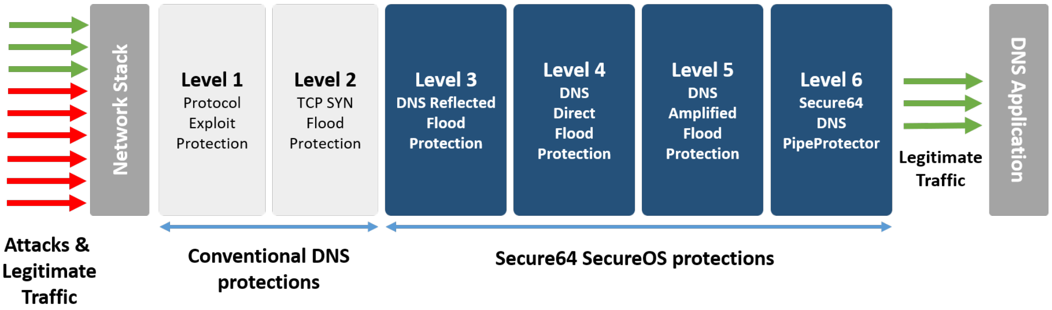
### KEY FEATURES

- Secure kernel eliminates entire classes of vulnerabilities
- Built-in advanced DDoS protection
- Non-BIND based DNS
- Dynamic configuration changes
- Dynamic zone additions and deletions
- Comprehensive RESTful API
- Physical or virtual appliances
- License-controlled capacity

Virtualization, Software Defined Networking and Network Functions Virtualization are top of mind issues as many organizations seek ways to increase flexibility and reduce capital and operating expenses. But increased attacks on the DNS make security a high priority even for organizations moving to a virtual environment.

DNS Authority for x86 is authoritative name server software that provides unmatched levels of security and attack resiliency while making it easy to integrate with orchestration software and other systems running in the network. Additionally, because it is not based on open-source BIND, it is immune to the many critical security vulnerabilities found in BIND each year.

## Built-In DDoS Defenses Ensures Service Continuity


Network Stack
Level 1
Protocol Exploit Protection
Level 2
TCP SYN Flood Protection
Level 3
DNS Reflected Flood Protection
Level 4
DNS Direct Flood Protection
Level 5
DNS Amplified Flood Protection
Level 6
Secure64 DNS PipeProtector
Legitimate Traffic
DNS Application
Attacks & Legitimate Traffic
Conventional DNS protections
Secure64 SecureOS protections

## Industry-leading Security

The Secure64 name reflects our heritage and focus: we offer truly secure platforms for mission-critical, carrier-grade DNS.

### Built-In DDoS protection

DNS Authority for x86 provides fine-grained DDoS detection and mitigation rules, allowing the server to continue to respond to legitimate queries while dropping queries from attackers—unlike conventional DNS solutions that crash or become unavailable at much lower levels of attack traffic. The system can be configured to monitor and throttle traffic to a user specified level or drop traffic that exceeds normal use patterns, such as excessive bandwidth consumption or excessive IP packet rates in general, IPv4 or IPv6 packets in particular.

### Non BIND-based DNS

BIND is the most widely deployed DNS software in the world, which makes it a primary target for attackers seeking to cause maximum worldwide damage. DNS Authority for x86 is a completely different implementation that shares no code with BIND, making it immune to all BIND-specific vulnerabilities

### Secure kernel

DNS Authority for x86 features a secure kernel which completely eliminates entire classes of vulnerabilities, including buffer overflow attacks and remote code execution. Those eliminated classes are typically associated with the most critical vulnerabilities so the need to “drop everything and patch” is greatly reduced. Additionally, overall patching is significantly reduced, saving on costs.

### Full DNSSEC support

DNS Authority for x86 supports all of the DNSSEC RFCs, ensuring that signed zones can be validated by appropriately configured resolvers.

### Response Rate Limiting

Authoritative DNS servers can be abused by attackers to reflect large amounts of DNS response traffic towards a victim server. Response Rate Limiting algorithms detect patterns in arriving queries and reduce the rate at which replies are sent if the patterns suggest abuse, thus protecting server load, network bandwidth and the end victim server itself.

## High Availability

### Dynamic zones

Adding or deleting zones in traditional DNS servers requires that the server be restarted before changes take effect. But restarts can take a long time, leading to reduced service availability during the restart. Conversely, restarting the server only during a scheduled maintenance window preserves service availability SLAs, but may not meet zone propagation SLAs, as new zones may not be visible for many hours.

DNS Authority for x86 allows zones to be added and deleted on the fly, with no restart required and no loss of query responsiveness during the update, allowing operators to meet even the most stringent requirements for both service availability and zone propagation time.

### Dynamic configuration changes

The DNS is a mission-critical networking service that must always be available to service client requests. Conventional DNS servers must be restarted to make changes to configurations or to turn on diagnostic tools. DNS Authority for x86 allows changes to a running server, including rules modification, to be made on the fly with no loss of service continuity, ensuring that the service can meet even the most stringent availability requirements.

### Anycasting with fast failover

BGP anycasting has long been deployed by root and top level domain operators as a best practice for high DNS availability and resiliency. DNS Authority for x86 not only supports BGP anycasting, but allows it to be augmented by Bidirectional Forwarding Detection (BFD) for sub- second failover in the event of a server failure, thus ensuring high levels of DNS service continuity.

## Scalable Performance

### Throughput

DNS Authority for x86 provides the highest performance of any nameserver software, minimizing hardware resources required and saving on both capital and operating expenses.

## Simple Management and Monitoring

### SNMP

DNS Authority for x86 allows customers to monitor the network, operating system and application in real time, while supporting a variety of leading network monitoring systems. Detailed information is available through SNMP v3, allowing the monitoring system to easily determine the server’s availability, security and operational health in real time.

### Centralized management

DNS Authority for x86 servers can be managed individually, or can be centrally managed and monitored through Secure64® DNS Manager™. DNS Manager simplifies the management of a large DNS network deployment by managing configurations and revisions, upgrading software versions, and monitoring key performance indicators across multiple Secure64 servers in the network.

### Query statistics

A wealth of aggregate statistics is available from the server including number of queries broken down by type, class and opcode, over udp versus tcp, over ipv4 versus ipv6 as well as responses broken down by response code. Statistics can also be gathered and reported on a per zone basis.

### NFV-Ready

Authority for x86 provides a rich RESTful API that enables external orchestration and management systems to configure, monitor and manage it throughout its lifecycle. This promotes network automation and elastic scaling – two key goals in the shift towards virtual network functions.

## Feature-Rich

### Split Horizon DNS

Views allow configuration of an authoritative server to provide different functionality and responses basedon characteristics of the requesting client.

### Synthesized PTR Records

Reverse DNS records for IPv6 addresses or other large address blocks can be generated on the fly, preserving compatibility with other systems that rely upon the existence of these reverse records

Learn more about Secure64 DNS solutions at www.secure64.com

Secure64 Software Corporation 303-242-5890 www.secure64.com