SECURE DOMAINS

FIRST HYBRID DNS FIREWALL IN THE GCC

CLOUD DNS FIREWALL

# DNS ARMOR™ PROTECT

## Enhanced threat protection and network visibility at the DNS layer

DNS is the gateway to nearly every connected service — and the vector behind **91% of DNS-based exploits**, from malware and APTs to command-and-control. DNS Armor™ Protect is the frontline defense: a cloud-native DNS firewall delivering proactive detection and mitigation with centralized control of web content and security policy.

Advanced query filtering, real-time threat intelligence and customizable local policies let security teams neutralize threats before they escalate — blocking malware, C2, phishing and data exfiltration where it starts.

IDEAL FOR

- Enterprises
- MSPs
- Government & sovereign
- Roaming workforce
- Multi-tenant estates

**52**
Global data centers with in-region log storage

**20M+**
Threat indicators in the intelligence graph

**700+**
Applications & services under control

**91%**
Of DNS exploits addressed at resolution

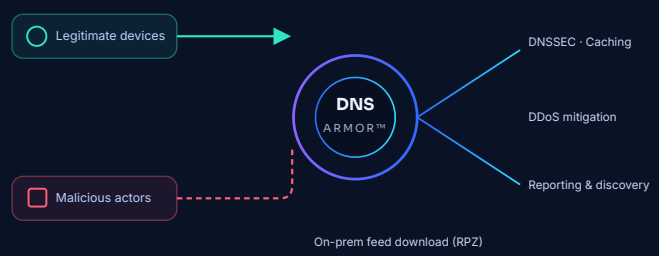
## At a Glance

Everything DNS Armor™ Protect delivers, in one view

- First hybrid DNS firewall provider in the GCC
- Web filtering and content categorization
- AI-powered DNS tunneling & exfiltration defense
- Discovery analytics — visibility before enforcement
- Dual deployment: on-prem (local AI + firewall) or cloud
- Modular design for confidential, in-region log storage
- Control of 700+ applications and services
- Time-based and geo-based policy control
- Full multi-tenancy for B2C, B2B and MSPs
- SIEM log connector: HTTP/S, TCP, UDP

## How It Works

Queries flow through a single enforcement point




Recursive DNS channels inspect every query in real time — allowing, blocking or redirecting based on threat intelligence, web category, application and policy before a connection is ever made.

### WHY DNS-LAYER SECURITY

DNS sees **every** connection attempt before it happens. Enforcing at resolution stops threats earlier, lighter and cheaper than packet inspection — with no traffic to backhaul and nothing to install on every host.

### SOVEREIGN BY DESIGN

A true modular design keeps confidential logs **in the customer's assigned geolocation** — critical for data-residency compliance where competitors centralize storage.

## Technical Capabilities

A complete DNS security stack, delivered as a service

- DNSSEC support for enhanced integrity
- Ultra-fast resolution for minimal latency
- Automated threat-intelligence feeds
- Web filtering feeds for content control
- DoH & DoT encrypted DNS queries
- Robust DDoS mitigation and protection
- Dual operating modes (cloud & on-prem)
- Lightweight endpoint agent
- Direct forwarding for efficient data flow
- Automated feeds sharing with 3rd party
- Integrates with third-party security tools

### Managed Service Providers

Full multi-tenancy across control and data planes — deliver value-added security and scale with clients.

### Multi-Tenancy Support

Complete per-tenant data isolation for customers or business units on shared infrastructure.

### Detailed Logging & Reporting

90-day in-region retention with rich statistical reporting for compliance and auditing.

### Endpoint Agent

Secure DNS encryption and forwarding for roaming clients — same protection off-network.

## Policy & Control

Adaptive enforcement across time, place and intent

### Time-Based Scheduling

Automate policy by operational hours or dates — no manual changes.

### Geo-Based Policy

Enforce security and content policy by geographic location across sites and users.

### Application Control

Allow or block 700+ applications by business need — curb shadow IT and data leaks.

### Discovery Analytics

Monitor-only mode discovers apps, categories, threats and geos — visibility before enforcement.

### Automated Security Feeds

Real-time threat intel and web categorization, exportable in RPZ to on-prem DNS.

### AI-Powered Detection

Detects and blocks DNS tunneling, exfiltration and C2 in real time from query behavior.

## Technical Specifications

At-a-glance reference

| | | | |
|---|---|---|---|
| **Delivery** | SaaS (cloud-native) | **Operating modes** | On-prem or cloud |
| **Protocols** | DNS, DoH, DoT, DoQ | **Endpoint** | Lightweight roaming agent |
| **Threat indicators** | 20M+ (real-time) | **App control** | 700+ applications |
| **Policy** | Time-based & geo-based | **Log retention** | 90 days, in-region |
| **Feed export** | RPZ (MS DNS, BIND, PowerDNS) | **Tenancy** | Full multi-tenancy |
| **Availability** | 52 global data centers | **Detection** | AI tunneling & exfiltration |
| **SIEM export** | Log connector: HTTP/S, TCP, UDP | | |

## Deployment Modes

On-prem or cloud

Run DNS Armor™ one of two ways. **On-premises** — the DNS firewall and AI threat detection run locally on your site, so filtering, tunneling detection and enforcement all happen on-prem for maximum performance, offline resilience and full data locality. **Cloud** — endpoints forward queries to the DNS Armor™ cloud, which performs the filtering and detection as a fully hosted service. Choose per site; policy and reporting stay centrally cloud-managed either way.

### INTEGRATIONS & LOG CONNECTOR

Stream cloud logs straight into your SIEM with the built-in **Log Connector** — delivery over HTTP, HTTPS, TCP and UDP. Plus RPZ feed export to Microsoft DNS, BIND and PowerDNS, and API-driven policy and reporting.

## Service Availability

52 data centers across four regions, each with in-region log storage

| | | | |
|---|---|---|---|
| **Americas**<br>Virginia, California, Toronto, São Paulo … | 13 | **Europe**<br>London, Frankfurt, Amsterdam, Madrid … | 11 |
| **Middle East & Africa**<br>Dubai, Doha, Riyadh, Istanbul, Cairo … | 6 | **Asia Pacific**<br>Singapore, Tokyo, Mumbai, Sydney, Seoul … | 22 |

Full list of all 52 locations available on request · localized log storage in every region.

## Deploy DNS Armor™ Protect

Cloud-native DNS firewalling with sovereign, in-region log storage — live across 52 global data centers.

**Secure Domains**
First hybrid DNS firewall in the GCC
secure-domains.org/products/protect