



# Protecting enterprises from malware, viruses, ransomware, and phishing



## INTELLIGENT CYBER SECURITY & CONTENT FILTERING

Thunder DNS software re-engineers DNS to protect organizations against cyber threats, offer in-depth content controls, and provide analytics for optimization.

### DNS Cyber Security

Secure all network devices including IoT devices with DNS Firewall. All devices use DNS to navigate the Internet. Our firewall contains millions of known security threats, updates in real time, and protects all network devices.

### Anomaly Detection

Detect and intercept malicious communications. Malware takes control of infected devices and attempts to contact its mothership. We crawl all queries for malware communications and quarantine infected devices.

### Organization Efficiency

Avoid distractions with granular content controls. DNS content filtering provides 60+ content categories that can be adjusted based on business needs.

### L2TP Tunneling

Connect offices with private/NAT connections to Thunder DNS. Thunder DNS L2TP tunneling also allows for granular security & filtering controls based on IP address or Wi-Fi SSIDs.

# Anomaly Detection + DNS Firewall

Thunder DNS protects organizations using Intelligent Analytics and our DNS Firewall. Intelligent Analytics use machine learning to identify and contain **unknown threats** and the DNS firewall protects against **known threats** using powerful filters.

## INTELLIGENT ANALYTICS

**Historic Benchmarking:** On-going analysis of every IP address within the network over time. Anomalies are identified and reported for further investigation.

**Query Profiling:** Identification of unknown threats through DNS query pattern analysis. New threats are quarantined and security definitions are pushed to all network partners.

**300+  
Million**

queries processed **daily** from

**180 Countries**

## DNS FIREWALL

### Block List



Integrates real time updates from 15+ security feeds.

### White List



Leverages database access to the largest certificate authority in the world.

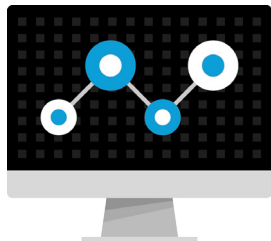
### Local Customization



Allows up to 10,000 entries. Local entries override the system DNS Firewall.

# Solution Overview

## Subscriber



Subscribers are automatically secured by Thunder DNS. Once enabled, all domain requests are sent to Thunder DNS instead of traditional DNS servers.

## THUNDER DNS



Thunder DNS receives the DNS request and determines the domain threat level. Risky domain requests are sent to cloud servers for analysis. If harmful, the domains are blocked.

## Public Internet



Low risk and non-harmful domain requests are resolved and the subscriber securely navigates the Internet.

# Technical Specifications

Features	
Security Domain Updates	Real time (cloud + local architecture)
Smart Caching	Pre-fetch supported
DNS Failover	Up to 3 failover servers
DNS Lookup Latency	< 1 ms for 98.5% of traffic
A.I. Anomaly Detection	Supported
EDNS0	Supported
Supported Image Formats	VMDK, QCOW2,
Local or Cloud Hosting	Both supported

Minimum Server Requirements	
HVA supported	Yes
Processor	Dual Core 1.5+ GHz
Cache	2+ MB
RAM	1+ GB
Network Interface	2 Interfaces (10/100/1000)
IP Allocation	1 public IP per server
Bandwidth	20+ Mbps
Disk Space	5+ GB