

## PowerDNS **DNSdist Defender**

Advanced DNS Security. **Simplified.**

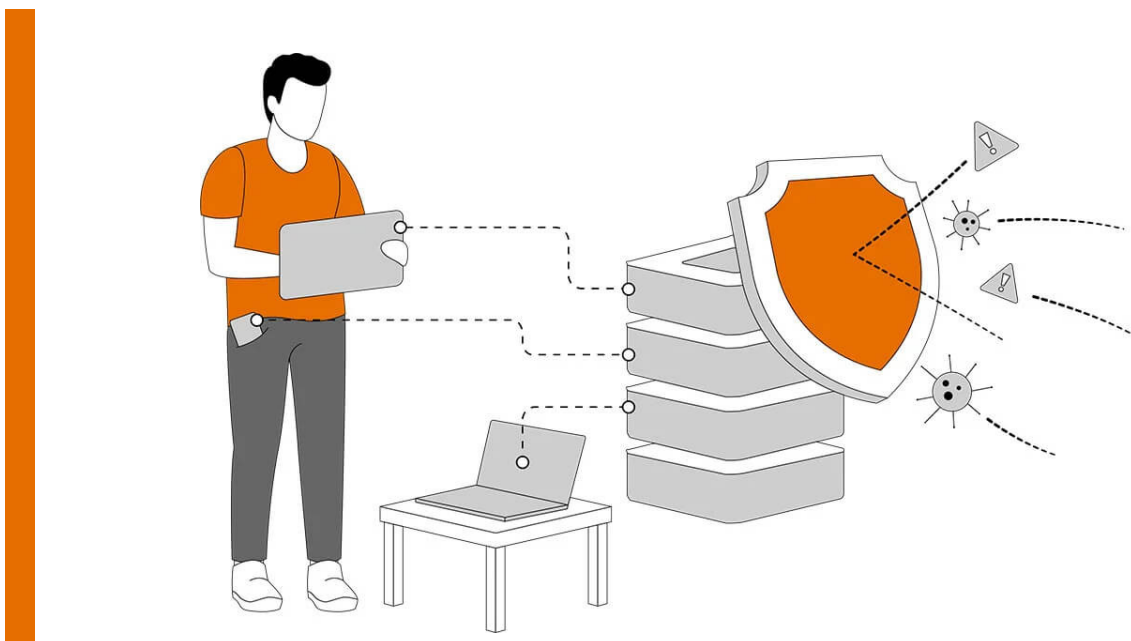
### The Challenge

DNS serves as the essential entry point into the connected, online world for nearly all internet-based activities. While it opens up a wealth of opportunities, it also introduces unique challenges. DNS has become one of the most attractive attack vectors in modern networks. Beyond traditional DDoS attacks, organizations increasingly face DNS tunneling, data exfiltration, pseudo-random subdomain (PRSD) attacks, and command-and-control (C2) communication.

While DNSdist already provides powerful traffic management and filtering capabilities,

implementing advanced DNS security often requires extensive Lua scripting and deep knowledge of DNS internals. Maintaining custom security rules across distributed environments can quickly become complex and operationally demanding.

**Organizations need a solution that delivers enterprise-grade DNS protection without the complexity of developing and maintaining custom filtering logic.**



## The Solution

**PowerDNS DNSdist Defender** extends DNSdist with advanced DNS security, automated threat mitigation, and simplified policy management. Built on top of DNSdist, Defender transforms your DNS infrastructure into an intelligent DNS firewall that continuously monitors DNS traffic, detects malicious behavior, and automatically applies mitigation policies in real time.

Using intuitive YAML configuration, curated security rules, and a simplified API, DNSdist Defender makes enterprise-grade DNS protection easy to deploy, operate, and scale across distributed environments.

| Threat                                                                                                       | Protection |
|--------------------------------------------------------------------------------------------------------------|------------|
|  DNS Tunneling              | ✓          |
|  Data Exfiltration          | ✓          |
|  PRSD Attacks               | ✓          |
|  Reflection & Amplification | ✓          |
|  C2 Communication           | ✓          |

## Key Capabilities

### Advanced DNS Threat Protection

DNSdist Defender automatically detects and mitigates a wide range of DNS-based attacks before they impact your infrastructure.

Delivers protection against:

- ✓ **DNS tunneling**
- ✓ **Data exfiltration**
- ✓ **Pseudo-Random Subdomain (PRSD) attacks**
- ✓ **DNS reflection and amplification attacks**
- ✓ **Command-and-Control (C2) communication**

### Automated Threat Detection & Mitigation

Defender continuously analyzes DNS traffic patterns and generates mitigation rules based on observed behavior. Dynamic rules are synchronized across multiple DNSdist instances, ensuring consistent protection throughout distributed deployments.

Malicious traffic can automatically be:

- ✓ **blocked**
- ✓ **rate limited**
- ✓ **redirected**
- ✓ **logged**

## Simplified Security Configuration

Instead of writing and maintaining complex Lua scripts, Defender uses a modern YAML configuration model combined with curated rule sets maintained by PowerDNS. Benefits include:

- ✓ **Simplified deployment**
- ✓ **Easier policy management**
- ✓ **Faster implementation**
- ✓ **Reduced operational complexity**
- ✓ **Regular rule updates**

## Enterprise-Ready Distributed Security

DNSdist Defender is designed for large-scale deployments. Its capabilities improve scalability while ensuring all DNS nodes respond consistently to evolving threats.

Enterprise capabilities include:

- ✓ **Synchronization of dynamic rules**
- ✓ **Session Ticket Encryption Key (STEK) sharing**
- ✓ **Distributed communication using NATS**
- ✓ **Consistent protection across multiple DNSdist instances**



## Extensible Policy Framework

Organizations with specialized requirements can extend Defender using its intuitive API, built on top of DNSdist's high-performance Lua FFI interface.

This provides the flexibility to implement custom filtering logic without exposing administrators to the complexity of the native FFI interface.

- ✓ **Simplified development of custom security policies**
- ✓ **Rapid implementation of organization-specific detection logic**
- ✓ **Access to and interaction with DNS traffic statistics**
- ✓ **High-performance extensibility without FFI complexity**

## Key Benefits at a Glance



Enterprise-grade DNS **firewall**



Dynamic rule **synchronization**



Advanced DNS **threat detection**



**Distributed security** for clustered deployments



Automated **attack mitigation**



**Reduced** operational complexity



Simplified **YAML configuration**



**Flexible APIs** for custom policies

### Need Simplified DNS Security?

Discover how DNSdist Defender transforms DNSdist into an intelligent DNS firewall with automated threat detection, simplified policy management, and enterprise-grade protection for modern DNS infrastructures.

[Contact us](#)

[doc.powerdns.com](https://doc.powerdns.com)

