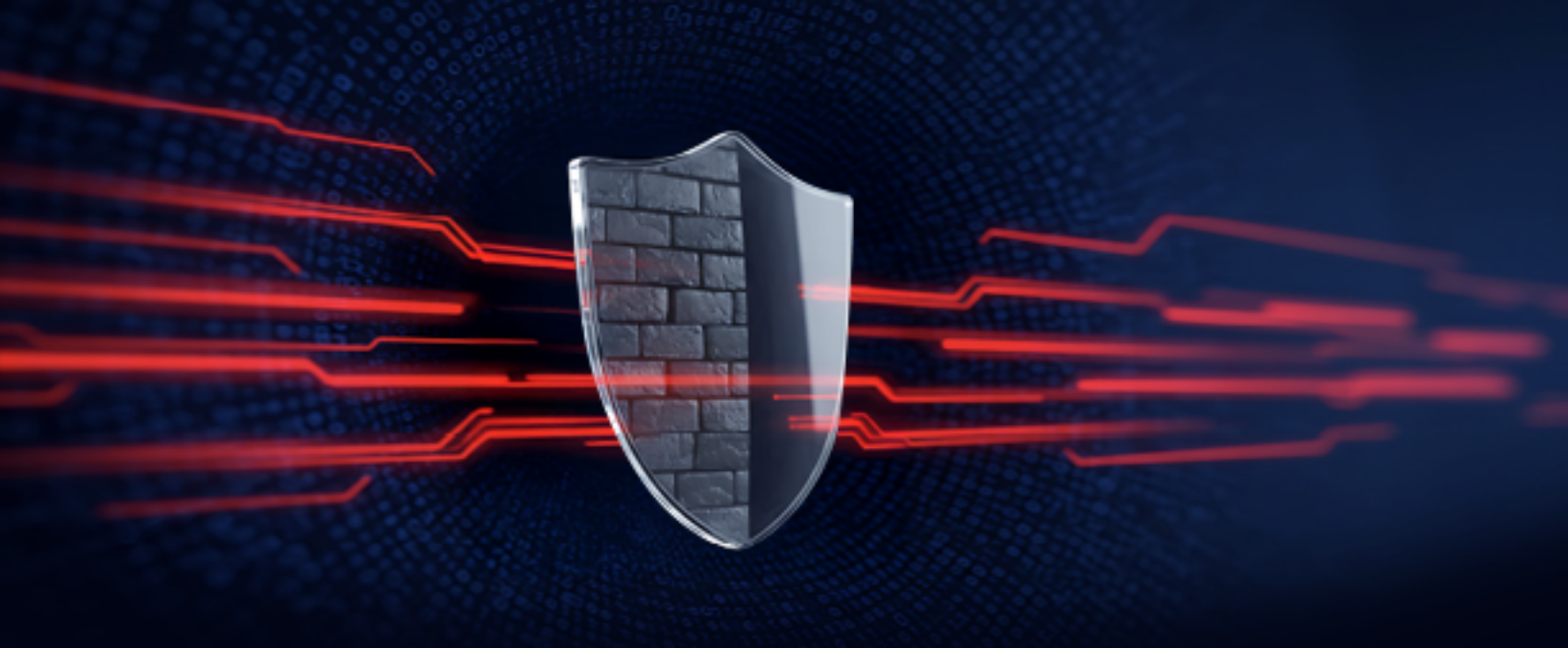

ManageEngine
DDI Central

Protective DNS for real time ever-evolving cyberthreats.

DDI Central Protective DNS shields every device, user, and application with enterprise-grade DNS security by:

- Filtering malicious content
- Preventing data loss
- Ensuring complete network visibility.

Zero-day ready • Enterprise-wide real-time threat protection • Multi-site security

Key features

Threat intelligence

- Combats Zero-day attacks.
- Real-time threat protection using curated and vetted, continuously updated feeds from trusted vendors.
- Bring your own intel with custom STIX/TAXII servers.
- Blends and diversifies threat feeds for optimal protection.
- Identifies the whole infrastructure behind rotating domains and disrupt C2 connections.
- Secure DNS query inspection.
- Granular asset context and response.

Anomaly detection

- **Detects Domain Generation Algorithm (DGA) domains** with random, long, digit-heavy, or suspicious TLD patterns.
- **DNS tunneling:** Flags high-volume, TXT-heavy, base64/encoded subdomains with fixed query timing.
- **Windows/DNS policy abuse:** Catches WPAD misuse, policy violations, and high REFUSED/NXDOMAIN rates.
- **DHCP anomalies:** Detects stale/duplicate leases, spoofed MAC/IPs, rapid lease requests, and starvation attacks (IPv4 & IPv6).

DNS Firewall (DNS FRW)

- Blocks known malicious domains at source.
- Response Policy Zone (RPZ) for custom redirection.
- Response Rate Limiting (RRL) policies for DNS volumetric attacks.
- DNS security analytics and logging.

DNS Detection and Response (DDR)

- Blocks re-entry for compromised devices.
- **DNS based quarantine:** Denies DNS queries.
- **DHCP based quarantine:** Flags MACs, blocks leases.

Why prefer DDI Central Protective DNS

Block evolving threats at source

Stop zero-day and known-bad domains with DNS firewall rules powered by live, curated threat feeds.

Shrink attackers' dwell time

Quarantine compromised clients by denying DNS queries and IP leases in real time.

Context that powers action

Trace how deep the breach runs—from the flagged domain to the last querying device.

Faster SOC and incident response

High-context IOCs built for precise DNS fire-walling and SOAR playbooks.

Plug-and-Play feeds

Curate your mix of threat intel—bring every feed updated in real time with confidence scores under one roof, no portal shuffle.

Bring your own intel

Easily onboard custom STIX/TAXII sources, enabling tailored and proactive DNS-layer threat prevention.

Vendor-curated categories, Admin-ready context

Leverage TAXII feed classifications—malware, phishing, or C2—without rework, to instantly identify the type of threat.

Policy enforcement at network scale

Automation turns threat intelligence into live DNS firewall rules and DHCP policies instantly.

DDI Central weaves security into your DNS layer, making protection seamless, scalable, and always on.

Start your 30-day free trial today and turn your
DNS into the first line of defense for your enterprise.

Shoot us an email at:

ddi-support@manageengine.com

For sales enquiries, contact us at:

sales@manageengine.com

Give us a call

USA: +1 312-635-6530

UK: +44 151-351-5601

India: +91 4469656020

ManageEngine
DDI Central

Take centralized control over your distributed network infrastructure .