DNS Defence

DNS.Secure
Real-time DNS Analysis against Threats
by advanced machine learning &
leading threat intelligence

A Safer Corporate Network

Threat remediation through DNS filtering can be achieved through two main methods:
Threat intelligence driven filtering and real time scanning & analysis through machine learning.
DNS Defence combines these methods to provide a safer network for your organization.

Centera DNS Defence classifies domains according to content and security in real-time.
This operation is performed behind the scenes when users visit a new website.

Real-time Interstitial Filter

If users on our platform access a domain which has never been seen, the scanner performs a real- time analysis & classification. The domain is fetched, categorized, and then matched against the policy set by the organization to determine if the user is allowed access.

Feed Augmentation

The engine incorporates Intelligence sources from multiple security feeds, ensuring Botnet, Crypto mining, and Malware threats are mitigated. Partnerships with organizations such as New Scotland Yard and the Internet Watch Foundation ensure that we cast a wide net against Terrorism & Abuse websites.

Image Analysis

The scanner defeats phishing websites by examining the logo content of a site and comparing it to authorized domains for that brand. It is able to detect login screens for Microsoft, Google, Facebook etc. being used on illegitimate websites. The domain is then flagged as a security risk and our detection databases are instantly updated.

Continuous Crawl

The scanner performs an open crawl of Internet domains, including newly registered domains.
Domains are continuously scanned and classified.

New Domain Greylisting

Suspicious Domains registered in the last 30 days can be blocked in order to gain proving time. Research shows that many Phishing attacks are launched through newly established domains which are often weaponized after emails has been scanned.

DNS Defence

GDPR Compliant DNS
through a High Performance Anycast
Network

A More Resilient DNS Service

DNS Defence offers comprehensive content filtering and threat protection for all your network and endpoints. Our cloud topology is spread across multiple providers, ensuring a solid platform to control what your users are allowed to access online. Advanced machine learning classifies content in real-time as well as detect threats encountered on the internet, such as phishing and malware domains

Over the lifetime of DNS Defence, it has achieved 100% uptime. Engineered to be able to recover from multiple sources of degradation, you can always depend on us to DNS filter your networks.

Global Network

Our servers are spread across 35 cities around the globe. No matter where your offices are, your employees will always reach the nearest server to their location. This is true even if they are roaming internationally. When your employees step off the plane, they'll get the same performance as back home.

Fully Redundant

Our entire network topology is fully redundant between DNS1 and DNS2. In the event of degraded service at one of our datacenters, your network will experience no loss in service as our network adjusts within seconds.

GDPR Compliant Top Tier Datacenters

Multiple high-quality datacenters are home to our servers. We use separate providers so that if any single provider experiences issues, our customers remain unaffected. We closely monitor server activity and performance, consistently scaling datacenter presence as our traffic grows.

Total Security Coverage

DNS Defence takes only a few minutes to configure on your network. After initial configuration, all adjustments are made through our online dashboard. As a DNS based solution, all endpoints in your network are instantly protected. For users outside your corporate network,
we offer roaming clients on all major platforms: **Windows, MacOS, ChromeOS, Android & iOS**.
You can also easily assign policies which are unique to devices or device groups.

CENTERA
DNS DEFENCE

Feature List

1st of May 2020

	Business	Advantage	Enterprise
Threat Protection			
Protection with Machine Learning	yes	yes	yes
Real-time URL analysis	yes	yes	yes
Malware Protection	yes	yes	yes
Phishing Protection	yes	yes	yes
Botnet Protection	yes	yes	yes
Crypto mining Protection	yes	yes	yes
Block Newly created Domains	yes	yes	yes
Content Filtering			
Block 36 Categories	yes	yes	yes
Network Level Policies	yes	yes	yes
Per User Policies		yes	yes
Scheduled Policies	yes	yes	yes
Custom Block Pages	yes	yes	yes
Enforce Google SafeSearch	yes	yes	yes
YouTube Restricted Mode	yes	yes	yes
Custom Whitelist / Blacklist	yes	yes	yes
Bypass by Password Option	yes	yes	yes
Internet Watch Foundation Intel	yes	yes	yes
Block Parked Sites	yes	yes	yes
Ad Blocking	yes	yes	yes
Deployment			
DNS Server Network Level	yes	yes	yes
Roaming Clients (Desktop)	yes	yes	yes
Roaming Clients (Mobile)			yes
NAT IP Support	yes	yes	yes
DNS Relay		yes	yes
DNS over TLS		yes	yes
DNSSEC Support		yes	yes
Reporting			
Network Level Reports	yes	yes	yes
Per Group Reports		yes	yes
Active Directory Reporting		yes	yes
Report Retention	30 Days	60 Days	90 Days
Alerting & Security			
Weekly Threat Reports	yes	yes	yes
Two-factor Authentication	yes	yes	yes
Real-Time Threat Alerts		yes	yes
Data			
Audit Log		yes	yes
Query Log Export		yes	yes
SIEM Integration			yes
API Access		yes	yes
Data Centres			
EU Datacentres	yes	yes	yes
GDPR Compliant	yes	yes	yes
Anycast Global Datacentres	yes	yes	yes
Support			
E-Mail	yes	yes	yes
Phone		yes	yes

Business | Advantage | Enterprise