DNSCyte

DNSCyte Firewall

www.CyberCyte.io

DNSCyte Firewall

Key Benefits

◆ DNSCyte Firewall provides reliable protection against DNS Query based attacks.

◆ Protects your network against threats such as Ransomware, Malware, Phishing, and Botnets.

◆ Prevents attacks using a specific port or application at the DNS level.

◆ Stops malware before it reaches the end users or their network.

◆ DNSCyte Firewall is managed centrally by a web console.

◆ Reports all DNS and Internet traffic at a given moment. Provides customized historical reports.

◆ Company based comprehensive policies can be created by using 120+ domain categories.

DNSCyte Firewall

Protecting your network against today's threats are getting more difficult and complex each day. Pieces of malware are designed more to the target, using zero-day-vulnerabilities more frequently, can by-pass signature-based solutions easily, can adapt themselves against behavioral based defense systems and execute silent and covert attacks. Although in practice, every user, computer and server must use DNS protocol to access the Internet, its security is mostly overlooked.
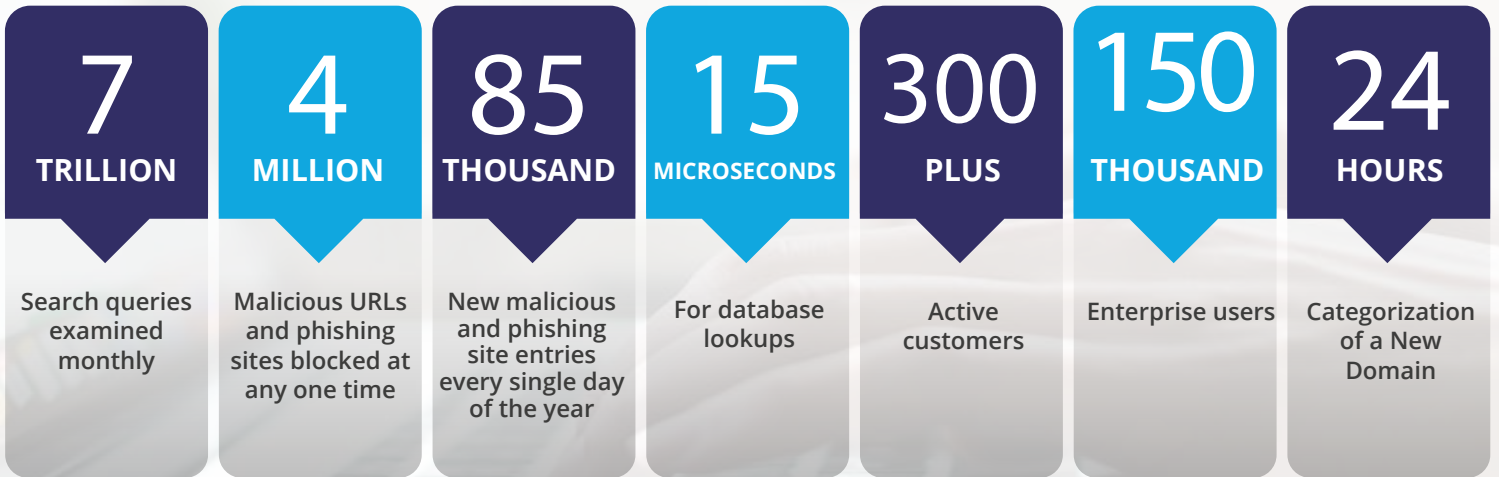
DNSCyte Firewall offers you the most basic security with Artificial Intelligence and Deep Learning capabilities in the most straightforward methods and approaches.

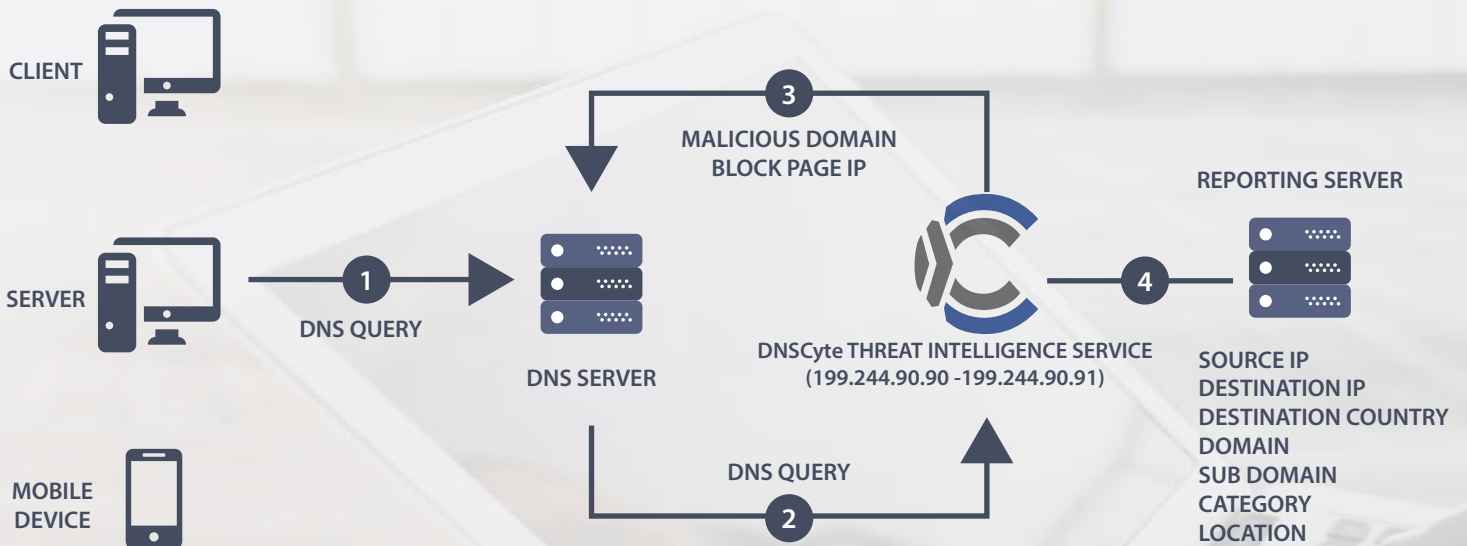## INDEPENDENT AND EFFECTIVE SECURITY ON THE APPLICATION LEVEL

Approximately 90% of the malicious software is using DNS protocol to communicate with Command and Control servers, to steal your data or redirect your Internet connection to malicious websites. Current security solutions such as Next Generation Firewalls, Intrusion Prevention Systems, Secure Web Gateways, Sandboxes are not designed to prevent malicious software-based threats.

DNSCyte Firewall is designed and developed to protect against DNS based threats, blocking malicious code that require DNS protocol to operate. Infected users are quarantied and access to Command and Control Centers is blocked and reported.

DNSCyte

7 TRILLION	4 MILLION	85 THOUSAND	15 MICROSECONDS	300 PLUS	150 THOUSAND	24 HOURS
Search queries examined monthly	Malicious URLs and phishing sites blocked at any one time	New malicious and phishing site entries every single day of the year	For database lookups	Active customers	Enterprise users	Categorization of a New Domain

SecureDNS

CLIENT

SERVER

MOBILE DEVICE

1 DNS QUERY

DNS SERVER

3 MALICIOUS DOMAIN BLOCK PAGE IP

2 DNS QUERY

DNSCyte THREAT INTELLIGENCE SERVICE
(199.244.90.90 -199.244.90.91)

REPORTING SERVER

4

SOURCE IP
DESTINATION IP
DESTINATION COUNTRY
DOMAIN
SUB DOMAIN
CATEGORY
LOCATION

1- Every device and user trying to access Internet sends a DNS query to the DNSCyte Firewall.

2- DNSCyte Firewall forwards the request to the DNSCyte Threat Intelligence Service.

3- If the Resolved Domain Name has malicious content, access to the page is blocked, and a block page is sent to the user as a response. If the page is compliant with the corporate policies or does not have malicious content, access is granted.

4- Information about the requested page is reported.

DNSCyte

DNSCyte Firewall is a Cloud-based Security Service powered by Deep Learning and Artificial Intelligence which provides Web Security, Application Security, and Advanced Reporting by analyzing users' DNS traffic.

Davidson House, Kings Road, Reading, UK
+44 118 900 1422 ✉ info@CyberCyte.com