DNSSense
Easiest way to be secure

DNSSense

DETECT DNS TUNNELING ATTACKS

USE CASE

DNSSense

Theft or unauthorised movement of any data from a company is one of the biggest cybercrime in today's world and is called Data exfiltration.

It typically involves a cybercriminal stealing data from personal or corporate devices, such as computers and mobile phones, through various cyberattack methods.

Last two years, the average annual cost of insider threats has skyrocketed, rising 31% to $11.45 million *(ObserveIT, 2020)*.

dnssense.com

338a Regents Park Road, Office 3 And 4, N3 2LN London, United Kingdom

+44 (0) 203 376 03 30 info@dnssense.com

Gartner peerinsights

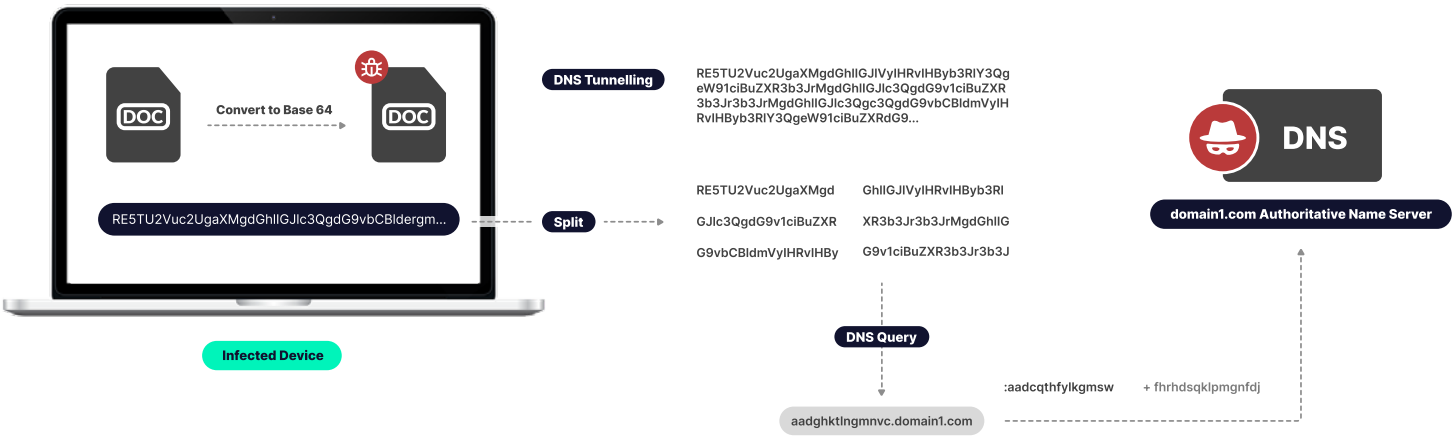
DNSSense

DNS Tunneling

Cybercriminals know that DNS is a well-established and trusted protocol and have figured out that many organisations do not examine their DNS traffic for malicious activity. DNS tunnelling enables these cybercriminals to insert malware or pass stolen information into DNS queries, creating a covert communication channel that bypasses most firewalls. That's why DNS Tunnelling is one of the most common attacks to make a data theft.

DNS Tunnelling is not always detectable with a Firewall or Proxy because they are designed to work in the application layer (layer 7). DLP technologies (Data Loss Prevention) are designed to monitor the protocols to which files can be attached, such as HTTP, FTP, IM, Telnet, TCP/IP, SMTP, POP3, and IMAP; however, it does not analyse the DNS logs.

Blocking DNS-based threats is a major challenge, and cybercriminals use it's pervasive but easily overlooked attack surface to their advantage. Targeted data, for example, can be converted to Base 64 and then exported using the DNS protocol, which can be easily overlooked. As a result, companies are losing their money and reputation.



dnssense.com

338a Regents Park Road, Office 3 And 4, N3 2LN London, United Kingdom

+44 (0) 203 376 03 30 info@dnssense.com

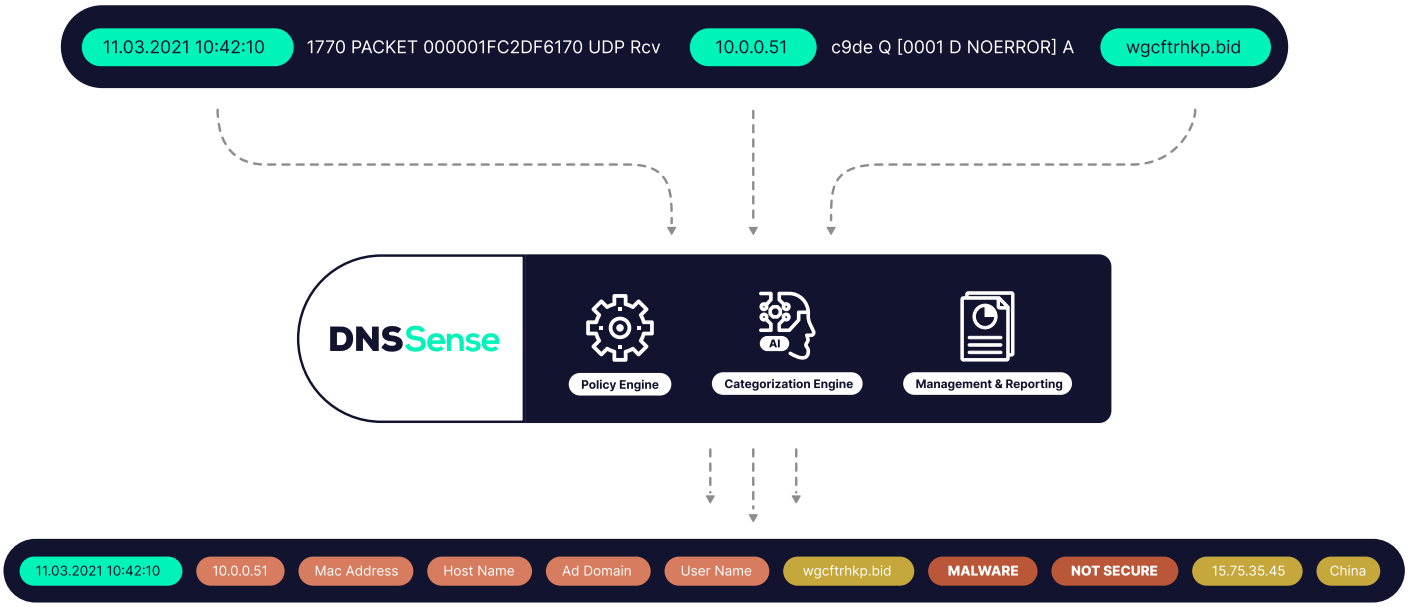
Gartner peerinsights

DNSSense

DNSSense's Solutions

One of the many futures of our 'DNSDome' cloud base product is detecting and preventing DNS Tunnelling. With DNSSense's 'DNSDome' cloud solution, 'DNS Tunnelling' attacks can be detected, blocked, and reported to a SIEM solution instantly before any malicious activity is completed.

DNSSense uses heuristics and behavioural ways like impulsive increasing DNS query volumes or query numbers from per source IP to detect DNS Tunnelling. More importantly, It has the most advanced AI-based dynamic threat intelligence database, **Cyber X-Ray**, which has entire internet domain data chronically where the magic happens to detect the most advanced DNS tunnelling attacks with **nearly zero false positive**. It is the most effective solution to save your data, money and reputation from DNS Tunnelling attacks.



dnssense.com

338a Regents Park Road, Office 3 And 4, N3 2LN London, United Kingdom

+44 (0) 203 376 03 30 info@dnssense.com

Gartner peerinsights