



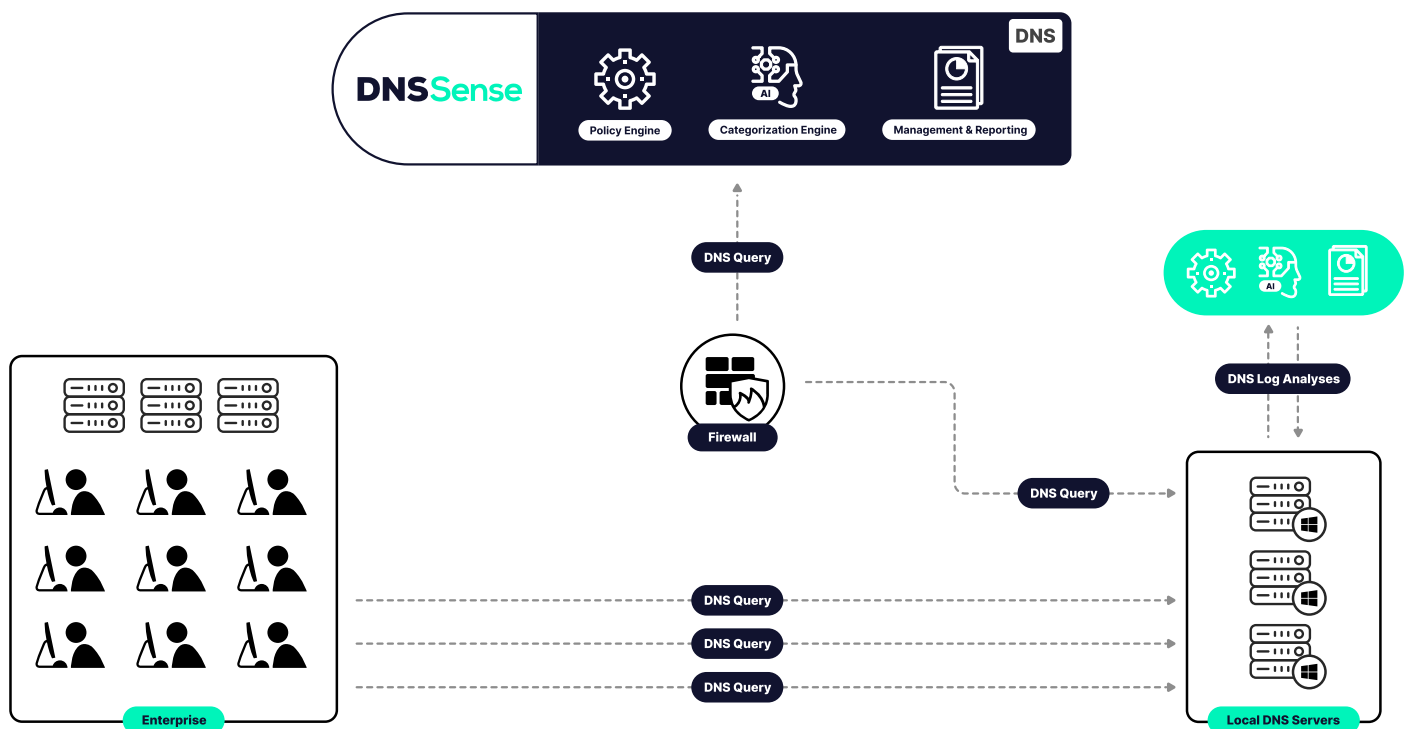
DNSSense

# **DETECT UNBLOCKABLE MALWARE TRAFFIC ON YOUR NETWORK**

**USE CASE**

**It is arguably true that you would find loads of malicious activities on a network with thousands of machines and users.**

In fact, what you would find may not be all of this malware activity but rather just what your current security devices are reporting. And therefore, what about the malicious traffic that your current security measures are unable to detect? How could you measure the efficiency of your current security investments? These are the significant challenges that we face in the enterprise networks.




# DNSSense's Solutions

DNSSense **Cyber X-Ray** classifies the domains on the Internet according to their "historical and relational data" with artificial intelligence algorithms. It detects current malicious domains. The Security Gap feature of DNSSense reports malicious traffic that the Organisations' existing security devices cannot detect. Thus, it is ensured that successful attacks are given priority. For example, in a detected phishing attack, users who make the connection to the malicious link as a result of the failure of the existing security devices to be detected are aimed to be determined instantly and to take quick action.

## Security Gap simulates connecting to the malicious domain in 3 different ways

- 1 Test with DNS query from existing DNS server.
- 2 Test with HTTP/HTTPS request via the proxy server.
- 3 Tests to reach a malicious domain with direct connection HTTP/HTTPS through Gateway.

[dnssense.com](https://dnssense.com)

 338a Regents Park Road, Office 3 And 4, N3 2LN London, United Kingdom  
 +44 (0) 203 376 03 30  [info@dnssense.com](mailto:info@dnssense.com)



# How Does the Security Gap work?

DNSSense DNSEye product is a VM appliance that works in your network, and it has this security gap feature. It can read all DNS logs and simulate the malicious traffic.

It sends the malicious connection request to our cloud-based malicious simulation service with specific metadata. If the simulation service did not get the metadata, which means the malicious connection was blocked, It also shows which device (Proxy or UTM) blocked the malicious traffic.

When the malicious simulation service gets the metadata, your existing security devices could not block the malicious connection.

Domain	Category	User	Hostname	UTM HTTP Request	Proxy HTTP Request	DNS Request	Attack Result
qjcycc.com	DGA Domain	CEO	CTO-Macbook	Passed	Passed	Passed	Attack Successful
Faccebook.com	Phishing	Darek Baker	Sales-PC1	Passed	Blocked	Passed	Attack Blocked By Proxy
zzgg123.com	Malware/Virus	Daniel	Daniel-Mac	Passed	Passed	Passed	Attack Successful
51news.xyz	Pornography	Natalie Burkard	Natalie's Iphone	Passed	Passed	Passed	Attack Successful
realsvr.com	Malware/Virus	TatianaK	TaniaPC	Passed	Blocked	Passed	Attack Blocked By Proxy
instaggrm.com	Phishing	Johan	230X130	Passed	Passed	Passed	Attack Successful

