DNSSense

DNSSense

DETECT UNBLOCKABLE MALWARE TRAFFIC

ON YOUR NETWORK

USE CASE

DNSSense

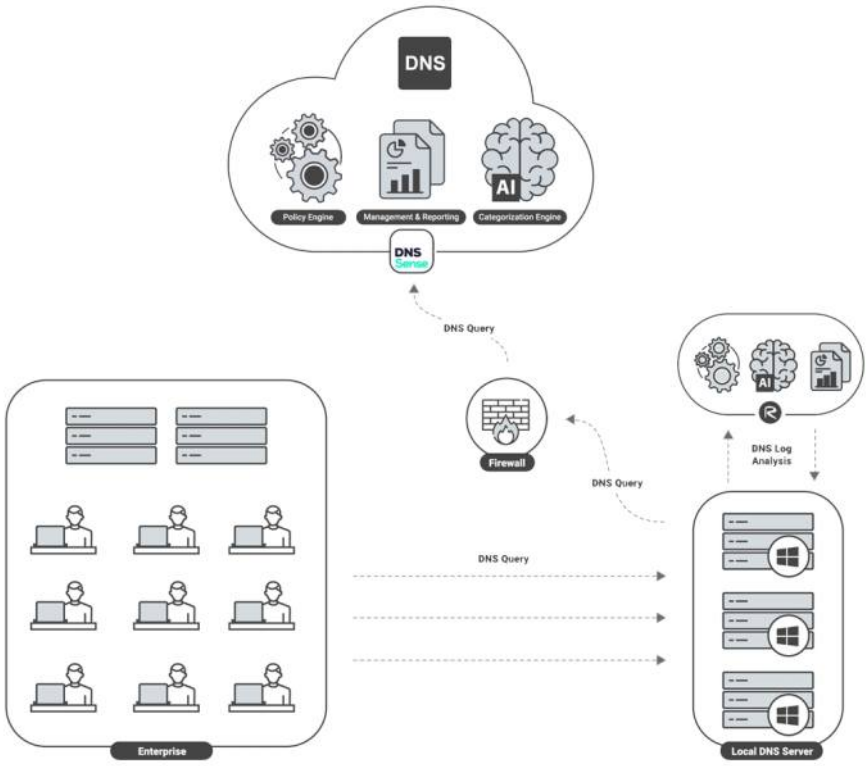
Detect Unblockable Malware Traffic on Your Network

Malware Traffic on Your Network

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.com 7 Bell Yard London, WC2A 2JR +44 7307 062505 info@dnssense.com

Gartner peerinsights™

DNSSense

Security Gap

Our Solution to these challenges

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.

Security Gap = False if malicious traffic is blocked,
Security Gap = True if not blocked.

dnssense.com 7 Bell Yard London, WC2A 2JR +44 7307 062505 info@dnssense.com

Gartner peerinsights™

DNSSense

How Does the Security Gap Block the Attacks?

Security GAP

How Does the Security Gap Block the Attacks?

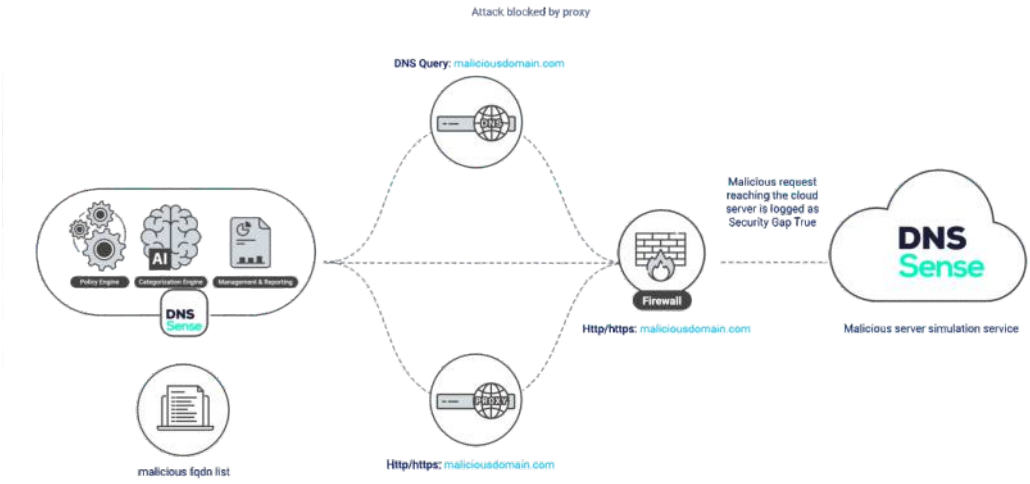
DNSSense DNS visibility product is a VM appliance that works in your network, and it has this security gap feature. It can read all DNS logs and simulate the malicious traffic. It sends the malicious connection request to our cloud-based malicious simulation service with specific metadata. If the simulation 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.

Domain	Categorory	User	Hostname	UTM HTTP Request	Proxy HTTP Request	DNS Request	Attack Result
qjcycc.com	DGA Domain	Jack Talk	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 W.	Daniel-Mac	Passed	Passed	Passed	Attack Successful
51news.xyz	Potentially Dangerous	Natalie B.	Natalie's Iphone	Passed	Passed	Passed	Attack Successful
realsrv.com	Malware/Virus	Tatiana K.	TanyaPC	Passed	Blocked	Passed	Attack Blocked By Proxy
instaggrm.com	Phishing	Johan	230X130	Passed	Passed	Passed	Attack Successful

DNSSense

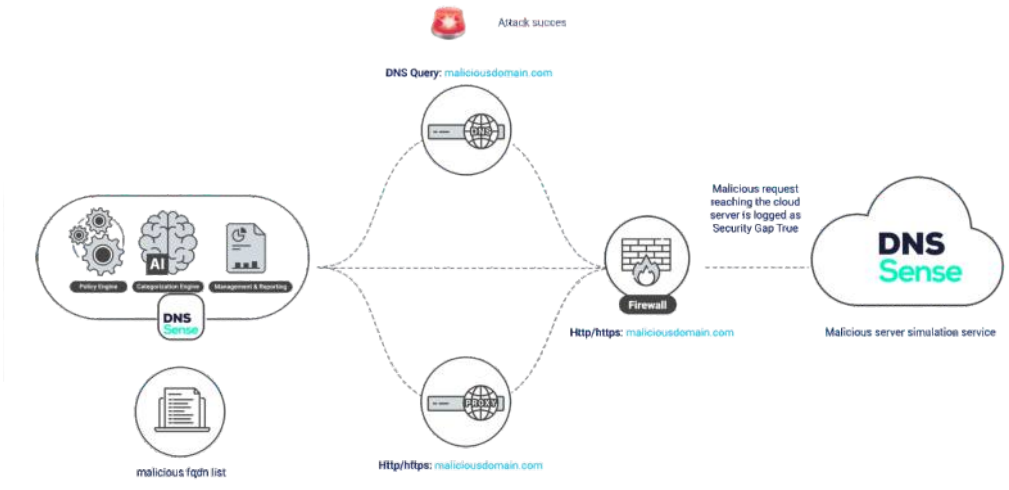
How Does the Security Gap Block the Attacks?

Simulation 1: Security Gap False



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

Simulation 2: Security Gap True



In the following picture, It can be seen that By courtesy of the Security Gap Feature, DNSSense reports the existing malicious activities which have managed to pass through each current security asset (UTM Firewall, Proxy, DNS Firewall, etc.) in your network without even being detected.