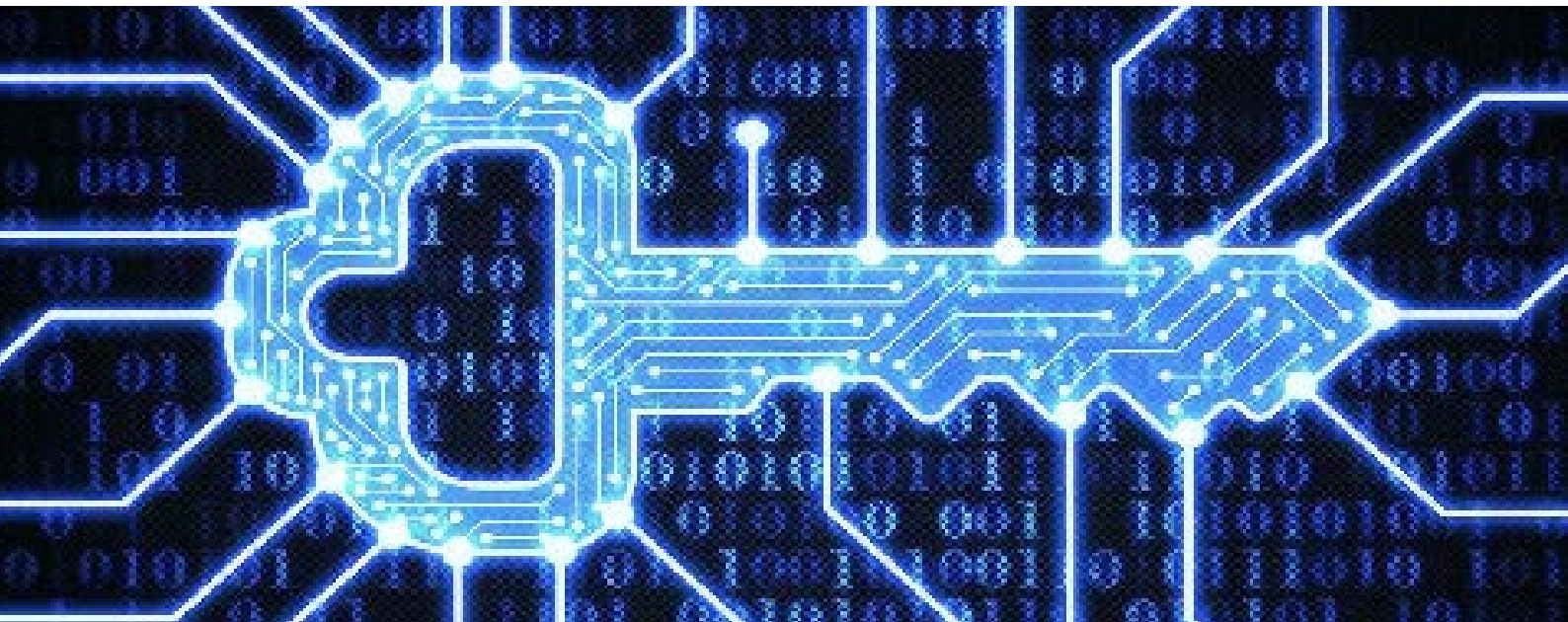
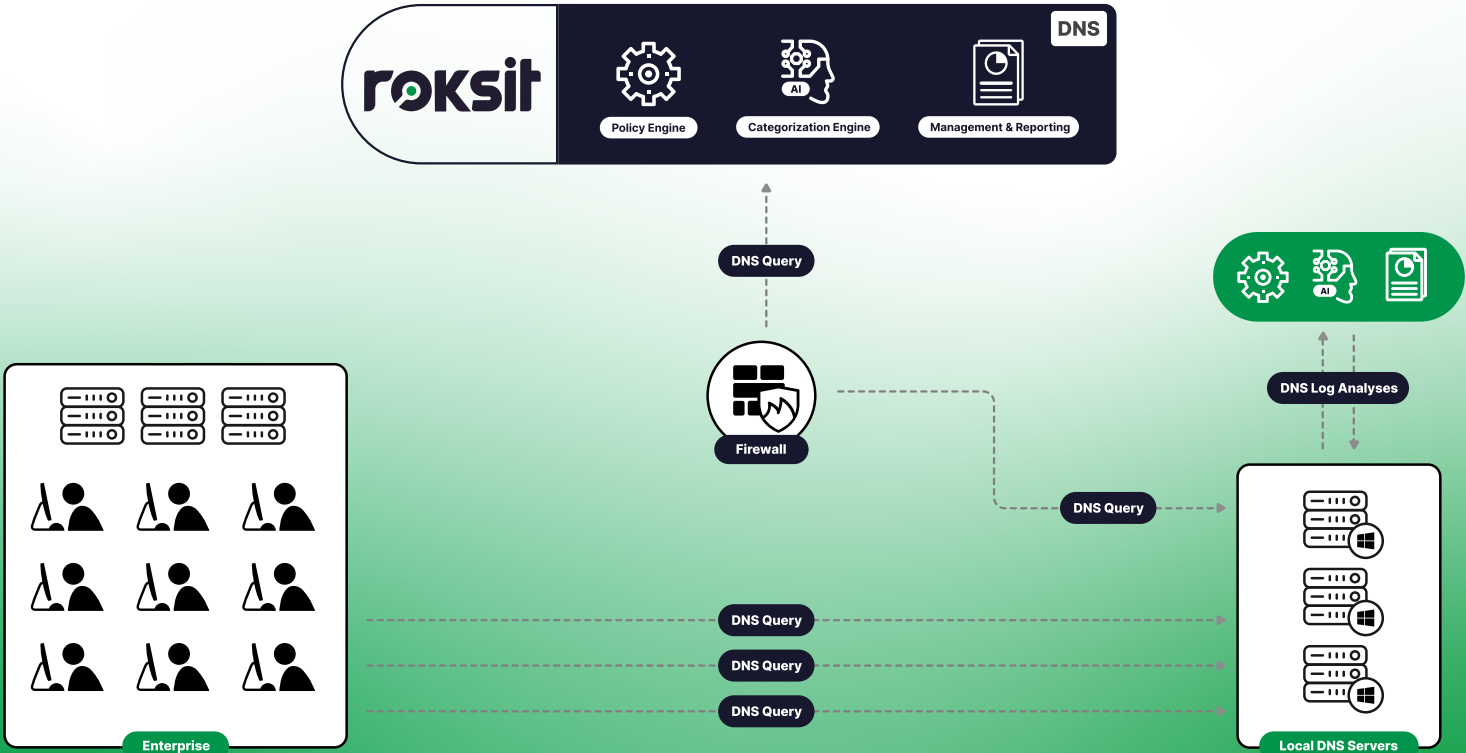


**DETECT
UNBLOCKABLE
MALWARE TRAFFIC
ON YOUR NETWORK**



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.





Roksit's Solutions

Roksit **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 Roksit 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- Tests with DNS query from the existing DNS server

2- Tests with Http/Https request via the proxy server

3- Tests to reach a malicious domain using a direct connection Http/Https through Gateway



How does the Security Gap work?

Roksit 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



roksit.com

About Roksit

Roksit started out as a domain classification project. After developing a dynamic domain classification infrastructure, in 2016 it went on to provide cloud-based secure DNS service for enterprise-level customers. Soon after, it has focused on DNS analysis and Advanced DNS Visibility products for the needs of enterprise networks. Today, with three integrated products, it enables institutions to connect to the internet securely, while providing all DNS analysis data that SOC teams need.

Roksit's name and its logo are trademarks of Roksit Software R&D Inc, in the all countries. The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on Roksit's current product plans and strategy, which are subject to change by Roksit without notice. Roksit shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or similar materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from Roksit or its channel partners or licensors, or altering the terms and conditions of the applicable agreement governing access to the Roksit or related products and services. 15December2022-Version:001