whalebone

Take Full Control of Your DNS Traffic and Secure Your Network's Blind Spots

Panasonic · O2 · RPC · Moravskoslezský kraj · Česká Zbrojovka · DNS4EU

Equa bank · Union Pojišťovna · ADASTRA · ALD Automotive · HBM Pharma

Whalebone Immunity provides enterprise networks with full control and protection of DNS communication and resolution regardless of their size or complexity.

90% of malware uses DNS resolution over the course of its life cycle, yet the majority of organizations still don't have direct control over their DNS resolution, and also do not monitor DNS traffic or secure this communication.

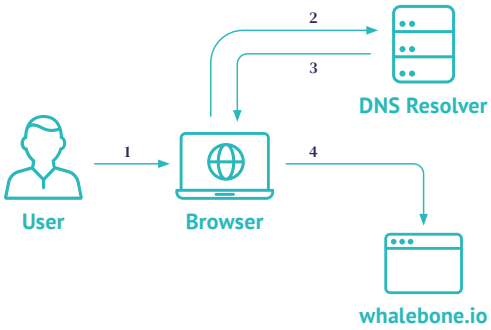
Key benefits

Manage and monitor DNS resolution from one place regardless of the application.

Secure communications against DNS-based threats.

Protection from: compromised email communication, targeted phishing campaigns, and harmful code on the network level.

Complex security for DNS communication – use cases



1. Wants to visit **whalebone.io**
2. What is the IP adress of whalebone.io?
3. The IP adress of whalebone.io is 88.86.121.135
4. Let's browse!

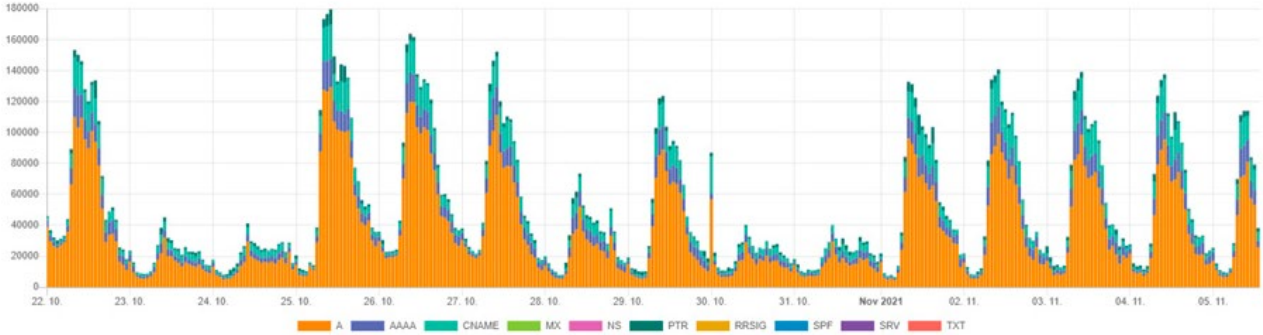
1 — Full control of DNS resolution and access control

Thanks to the Whalebone resolver, Immunity provides full control of DNS resolution for organizations that traditionally rely on their internet provider for the resolution of external domains. With Whalebone Immunity, you gain the ability to manage and control domain resolution for individual domains, and set whitelists and blacklists for the whole network, or any segment or individual device you choose. You also have the opportunity to define specific content filtering policies, like blocking P2P torrents, adult content, social media, improving team productivity, and reducing demand on network resources.

2 — Whalebone Home Office Security

Immunity allows administrators to protect employees even when they are off the organization's network. Using the Home Office Security (HOS) app, users are able to work from any location - either at home, airport, café, or otherwise, and have the same level of security as though they were in the office. HOS includes the full set of Immunity security features. Furthermore, the app is an integrated part of Immunity, so providing it to employees (remote or otherwise) does not increase costs to your organization.

Overview of your DNS traffic

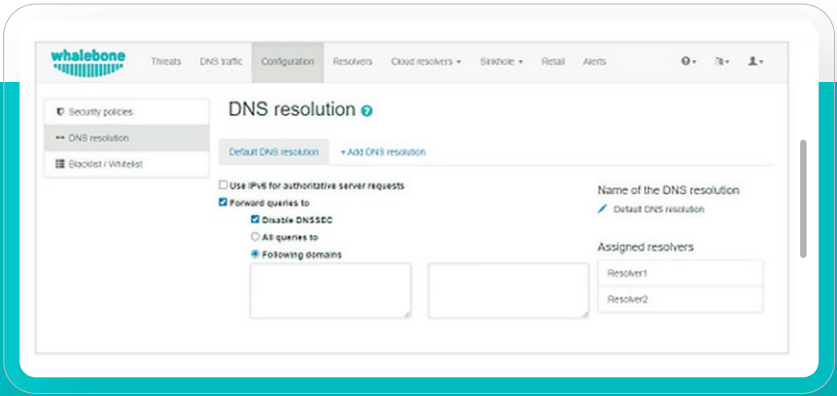


3 — Full visibility of DNS communication, analysis, and anomaly detection

Administrators have full visibility all the way up to the level of the IP of individual devices and makes it possible to stay one step ahead of attackers by identifying threats more quickly before they become serious. Alerting makes administrators' work easier by setting notifications when anomalies occur in DNS traffic. The option to create custom alerts is also included.

4 — Protection against phishing

The Whalebone Threat Intelligence database blocks access to sites that use phishing in real-time, effectively preventing the user from ever accessing a phishing site. Domain spoofing attacks can be intercepted automatically on the DNS level. If phishing does take place, the detailed DNS traffic overview makes it possible to easily identify the device that tried to access the fraudulent domain and quickly start the process of changing access credentials for users whose access data may have been compromised.



5 — DNS Firewall (for Office 365, Skype for Business, and selected internal applications)

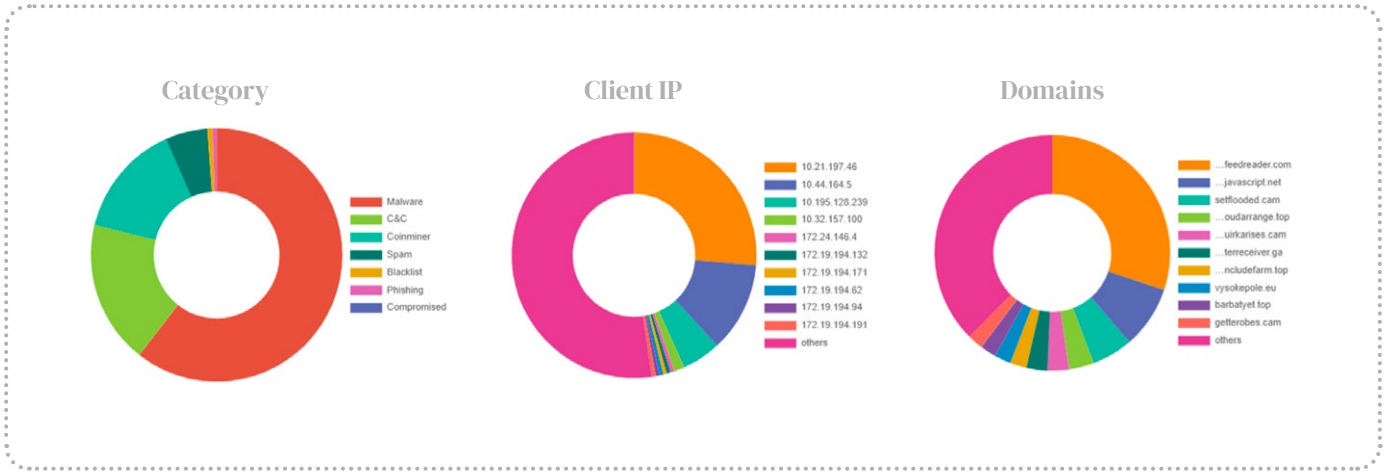
For Office 365, Microsoft requires endpoints to be able to resolve external domains and a filtered proxy exception. This requirement often disrupts the security architecture and security policy. Whalebone deals with these problems like a DNS Firewall; filtering communication and domains belonging to services such as Office 365, Skype for Business, or internal applications. These domains bypass Whalebone, while the other external domains can be allowed only through a web proxy. This preserves the original purpose of the security policy and security architecture remains undisturbed.

6 — DNSSEC validation

Immunity's DNSSEC validation feature allows administrators to mitigate abuse of SMTP protocol vulnerabilities against a change in the MX record of the reply when sending or receiving an email and prevents confidential communications being sent to the attacker.

7 — Protection against harmful code and harmful communication on the network level

Immunity blocks attempts to resolve a problematic domain. This happens regardless of the harmful code's life cycle phase in which the given incident occurs. This includes the resolution of domains known for spreading malware, attempts at downloading a portion of harmful code via a downloader or infector, and communication by infected devices with Command & Control servers.



8 — Prevention against DNS Tunneling

DNS Tunneling Protection is a significant element of DNS security. Various malware families use the tunneling attack to exfiltrate sensitive data to Command & Control servers. Whalebone prevents and mitigates malicious DNS tunneling.

9 — Alerting & simplifying administrators' work

In the event that the administrator doesn't have the capacity to deal with a particular alert, Immunity may be left to carry out work on its own and automatically enforce security policies in DNS traffic, allowing you to deal only with a short assessment of automatic reports sent by email.

10 — Domain name visibility

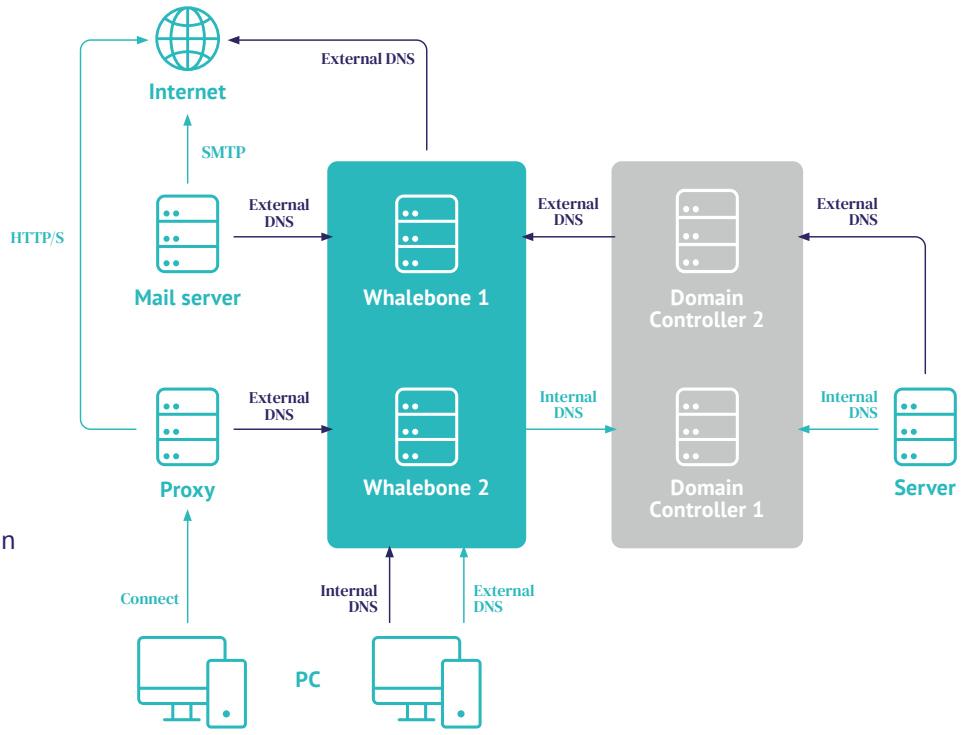
Immunity identifies the domain name of the device from which a blocked security incident occurred, allowing you to mitigate the threat vector quickly and effectively.

11 — Identity protection

Hackers often sell breached data on the dark web, including passwords, key-card codes, and other sensitive information connected to company domains. Immunity notifies you of any new and historic identified leaks, allowing you to take steps to prevent potential attacks.

Integration options

Whalebone's solution is usually integrated with various operation and security technologies including Active Directory, operation monitoring, helpdesk, SIEM, log management, anomaly detection systems, honeypot, endpoint security, and http-proxies.



Availability

Whalebone resolvers are designed so that the DNS resolution itself is completely independent from the operation of other functions. Even in cases when some or all cloud services are unavailable, DNS resolution will not be affected and this critical service will continue to function.

Cloud vs. on-premise resolver

Whalebone technologies support both on-premise deployment and the use of cloud services.

- **The on-premise resolver** should be implemented primarily to gain full visibility into DNS communication up to endpoint IP addresses and to heighten DNSSEC validation security.
- **The cloud resolver** is more suitable for smaller organizations that want to fully block threats in the whole network and have an overview of DNS communication in their organization but do not have their own infrastructure on which to run a security product or the human resources to manage it.

	Cloud	On-premise
Protection of DNS traffic	✓	✓
Web management	✓	✓
Fulltext search in DNS traffic	✓	✓
Content filtration	✓	✓
Visibility of local IP		✓
Local DNSSEC validation		✓
DNS firewall (including Office 365)		✓

Both methods of deployment can be combined within one multi-tenant account (e.g. when larger organizations have selected branches or entities that carry out DNS resolution at the provider but their central office has its own resolvers or wants to run the given service on their internal network)

Whalebone's key features

Immediate deployment

DNS resolvers are the **only things** that need to be configured.

Absolute availability

Availability is included in the product's design, which supports **High Availability deployment without affecting the cost** of the solution.

Zero administration costs

Whalebone **can work independently** based on configured policies and **sends automated reports** about intercepted incidents and threats in cases of insufficient internal capacity.

Not dependent on platforms

Within the network itself, **no agent installation is necessary for endpoints**; functions the same for all operating systems.

www.whalebone.io

Full network protection ····· Home Office Security ····· Full network visibility