whalebone

Whalebone Immunity

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

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.

Secure overlooked vectors

Secure overlooked vectors which are not in the scope of the standard security stack, such as firewall, endpoint protection, and EDR.

Manage and monitor

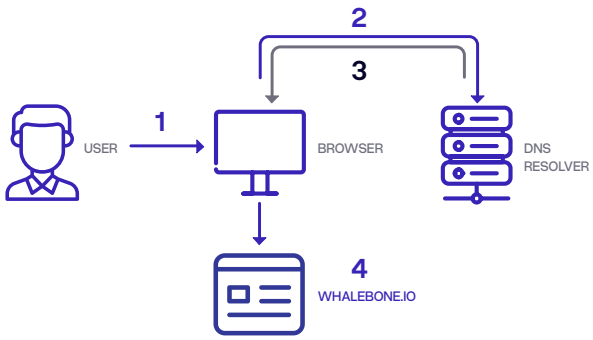
Manage and monitor DNS resolution from one place.

Protection from wide range of threats

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

ADASTRA O2 BAUHAUS Panasonic

Complex security for DNS communication – use cases

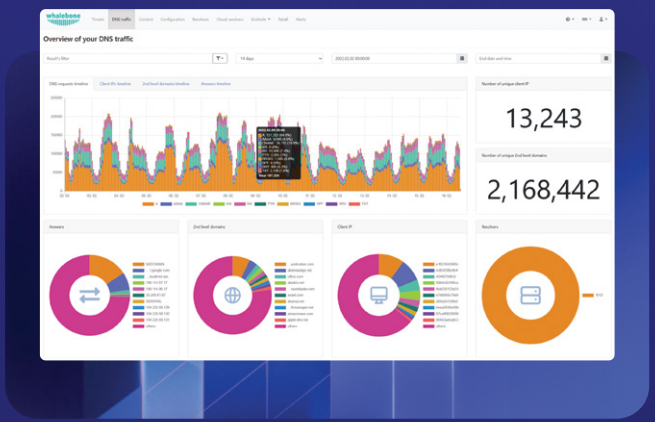


1. Wants to visit whalebone.io
2. What is the IP adress of whalebone.io?
3. The IP adress of whalebone.io is 88.86.121.135
4. Let's browse!

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.domain controllers and separate configurations have to be prepared for each resolver.



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.

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.

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.

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.

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.

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.

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.

Protection against DNS Tunneling

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

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.

DNSSEC validation

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.

Cloud vs. on–premises resolver

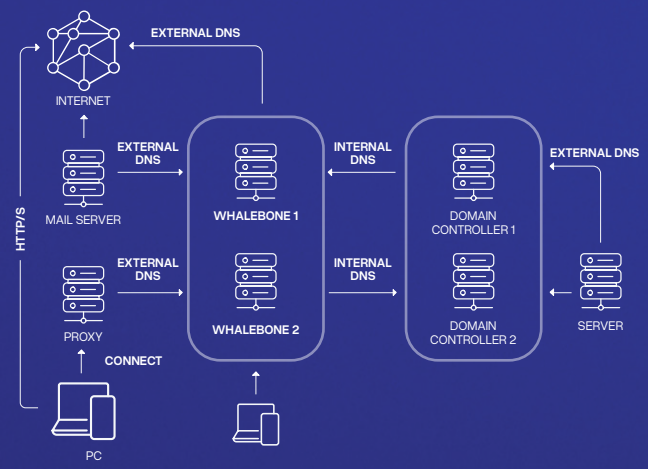
Whalebone technologies support both on–premises deployment and the use of cloud services.

1. The on–premises resolver should be implemented primarily to gain full visibility into DNS communication up to endpoint IP addresses and to heighten DNSSEC validation security.

2. The cloud resolver is ideal for smaller organizations that want to block threats and monitor DNS communication across their network but lack the infrastructure or resources to manage a security product.

Both deployment methods can be combined within a single multi–tenant account. For example, larger organizations may have certain branches or entities using DNS resolution through a provider, while their central office operates its own resolvers or prefers to run the service on their internal network.

	Cloud	On–premises
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)		✓



Integration options

Whalebone's solution typically integrates with various operational and security technologies, including Active Directory, monitoring, helpdesk, SIEM, log management, anomaly detection, honeypots, endpoint security, and HTTP proxies.

Availability

Whalebone resolvers are designed to ensure DNS resolution is fully independent of other functions. Even if some or all cloud services are down, DNS resolution remains unaffected and continues operating.

WHALEBONE'S KEY FEATURES

✓ **Not dependent on platforms**
Within the network itself, no agent installation is necessary for endpoints; functions the same for all operating systems.

✓ **Superior blocking rate**
Tests with AV–TEST data show 80% more threats detected compared to next–gen firewalls alone. Multiple security layers are essential for complete protection.

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

✓ **Immediate value**
Over 50% of customers discover unknown threats during the free trial, and more than 50% find leaked sensitive data linked to their domain.

✓ **Zero administration costs**
Whalebone operates autonomously on set policies, sending automated reports on intercepted incidents and threats when internal capacity is limited.

Easily redirect part of your network traffic to Whalebone resolvers and try out our trial.

immunity@whalebone.io

We will be more than happy to answer any questions. Mutual satisfaction is our main goal and we will do our best to fulfill your requests.

www.whalebone.io

Learn more about our products at: **whalebone.io/immunity**

Follow us on LinkedIn for more information on DNS security.