Peacemaker Service Specification Document

Version: August 4, 2025

Contents

Contents **2**
Glossary
4
1. Whalebone Peacemaker **7**
1.1 General product description 7
1.2 Product variants 8
1.2.1 Peacemaker Standard 8
1.2.2 Peacemaker Content Filtering 8
1.2.3 Peacemaker Profit 9
1.3 Comparison of Peacemaker variants 9

2. Core technology **15**
2.1 Whalebone DNS Resolver® 15
2.1.1 DNS traffic management 15
2.1.2 Leading DNS protocol security 16
2.1.3 End-user oriented DNS resolution 16
2.1.4 Resolver Management 16
2.2 Log management 17
2.3 Sizing and Hardware Requirements 17
2.3.1 Operating system requirements 17
2.3.2 CPU 17
2.3.3 Memory 18
2.3.4 Disk space 18
2.3.5 Performance benchmarking 18
2.4 Threat Intelligence Processor 18
2.4.1 Inputs 18
2.4.2 Processing 19
2.4.3 Output: Unique Reputation Value 21
2.4.4 Regional Threat Intelligence 21
2.4.5 Content Filtering Processing 22
2.4.6 False positive facilitation process 23
2.4.7 Database updates and new domains categorization 23
2.5 Log Analysis 24

3. Deployment options **27**
3.1. Primary and secondary resolvers 27
3.2. Resolvers behind a load balancer 27
3.3 Anycast IP Address managed on router level 28
3.4 Anycast IP Address managed on resolver level 28

4. Features **30**
4.1. Administration Portal 30
4.1.1. Threats Overview 30
4.1.2 Automated Threat Intelligence scoring 31
4.1.3 Segmented Network Policies 31
4.1.4 Custom allow lists and deny lists 32
4.1.5 Blocking Page and Bypass 32
4.1.6 Content Filtering overview 32
4.1.7 One-click Regulatory Blocking activation 33
4.1.8 DNS Traffic Overview 33
4.1.9 Reporting and Alerting 34
4.1.10 Service Line (Retail) Operator's View 36
4.1.11 Audit Trail 37
4.1.12 Acquisition and retention features 37
4.1.13 Data retention 37
4.2. End Customer Portal 38
4.2.1 Security Filtering 39
4.2.2 Content Filtering / Parental Control 40
4.2.3 Time-based Blocking 41
4.2.4 Custom Allow / Deny lists 43
4.3 Blocking or pop-up page with single click purchase 44
4.4 API 46
4.5 Multitenancy 46
4.5.1 Use Case for ISPs 47
4.6 Off-Net protection 47
4.6.1. Deployment 49
4.6.2 How the Off-Net works 49
4.6.3 VPN Connection Setup 50
4.6.4 Device pairing with the subscription 51
4.6.5 Service Provisioning 52
4.6.6 End-user Options 53

5. Support **55**
5.1 Areas covered by support 55
5.2 Areas not covered by support 55
Customer's on-premise infrastructure 55
Customers' network 55
5.3 Support communication channels 55
5.4 Ticket workflow 56

Glossary

Term	Definition
Whalebone Service	Whalebone provides a variety of services to ISPs. Either serving as ISP value added service for its End-users (i.e., Security, Parental/Content Control, Off-Net Protection, and related DNS resolution) Based on the commercial agreement Whalebone can serve as entire network infrastructure component (i.e., DNS resolvers with security filtering or DNS resolvers without security filtering).
Security Filtering	Whalebone's Security Filtering protects the end-users by blocking access to malicious domains. These domains are identified as hosting or distributing malware (ransomware, spyware, exploit kits etc.), being part of phishing campaigns, executing coin miners or facilitating botnet activity (command and control communication). The list is not exhaustive and is continuously enriched with emerging threat types.
Content Filtering / Parental Control	The Content Filtering / Parental Control feature of Whalebone Service provides a domain categorization and filtering mechanism. Based on their content, domains can be labeled as adult (pornographic content), crime (violence, drugs, terrorism etc.), entertainment (social networks, games, video-streaming) or advertisement (including those that track End-user activity). This list is not exhaustive and more fine-grained labelling can be provided. Especially for the entertainment domains, there is provisioned functionality to schedule the blocking timeframe.
End Customer Portal	The End Customer Portal is a graphical End-user interface that is presented to the End-user. Through this interface, the End-user configures the Content Filtering options, Off-Net protection options and accesses information about filtered and blocked events. .
Administration Portal	The Administration Portal is a graphical End-user interface to which the ISP's employees (administrators, operators, security analysts, etc.) have access to. In this interface, the employees manage the configuration of the Whalebone Service
Whalebone API	The API that Whalebone provides to the ISP. It can be used for End-user management or incident investigation.
Retail API	The API provided for configuration of End-user subscriptions, policies and provisioning of the devices.
Blocking Page	The webpage that the End-users are redirected to when they attempt to access a blocked domain.

Whalebone Cloud / Whalebone Backend	A general term encompassing all services that are operated, maintained and managed by Whalebone. All the services that are provided by Whalebone through the cloud. Relevant examples are the Retail and Administration Portals, Threat Intelligence data, Log Processing Pipeline and the Whalebone API.
Whalebone Resolver(s)	The DNS resolver that is provided by Whalebone. The term may refer to either the physical or virtual appliance running at the ISP's premises or to the software that is installed on the appliance.
Whalebone Cloud Resolver(s)	The term refers to a global cluster of DNS recursors that is managed, maintained and operated by Whalebone.
CPE	CPE stands for a customer-premises equipment. It is any terminal and associated equipment located at a subscriber's premises and connected with an ISP's network at the demarcation point.
CSAM	A shortcut for Child sexual abuse material. Illegal sites that spread pornographic or violent content featuring minors.
POC	Proof of Concept. A trial period during which the Whalebone Service is available to the ISP, free of charge. During the POC, the ISP has an option to try out the features, test the capabilities and verify vendor claims.
VAS	Value-Added Service.

Role	Description
End-User	The End-user for whom the service is provisioned.
End-User/Administrator	An administrator for End-users. In the case of SMBs this can be a System Administrator in the IT Department, while in the case of a family, this can be the parents.
ISP Operator	An operator is the person that can activate and deactivate End-users' licenses, make changes to policies and resolve End-users' issues. Typically this person is an employee or a contractor of the ISP.
ISP Administrator	An administrator at the ISP. They are responsible for managing Whalebone's resolvers and ensuring the desired traffic properties by defining and applying global policies.

1. Whalebone Peacemaker

1.1 General product description

Whalebone Peacemaker is a zero-disruption, multi-layer DNS security solution that helps Internet Service Providers (ISPs) address key operational challenges such as malware-related slowdowns, IP blacklisting, and abuse alerts. It provides network-level protection without requiring any software installation on end devices, operating transparently across all connected users.

By blocking malicious DNS requests, Peacemaker stops botnet communication, prevents bandwidth overload from infected devices, and reduces the effort needed to manage security incidents. It also automates compliance with national content regulations by integrating regulatory blocklists directly into DNS filtering. Designed for simple deployment and minimal resource usage, Peacemaker strengthens network security while allowing technical teams to focus on infrastructure, not incident response.

Whalebone Peacemaker is a product combining a local Whalebone DNS Resolver® within the ISP infrastructure and a global Whalebone Backend.

- Whalebone DNS Resolver® that is deployed on-premise, within the ISP infrastructure.
- Whalebone Backend spanning across the globe that updates Threat Intelligence and settings in real-time.

Whalebone DNS Resolver® filters DNS traffic directly in the network, offering protection for every end point (routers or devices connected to the router) without the need for apps, installs, or performance impact, regardless of connection method. When on-premises deployment is used resolution is done directly on the machine. Databases of threats are distributed on the individual machines based on the filtering settings. A key advantage of this setup is enhanced visibility into the local network, including localIP addresses, as well as reduced latency thanks to limited number of network hops between the client and the resolver.

Whalebone DNS Resolver® Cloud Hosted. If the ISP lacks resources for a virtual machine, the resolver can run entirely in the cloud. In this case, the operator simply configures their router to direct all network devices to Whalebone Cloud Resolver. This typically involves a straightforward change to the router's DHCP settings. Once configured, the router automatically forwards DNS requests from all connected devices to the Whalebone Cloud resolver, where security filtering is applied.

The Whalebone Backend handles:

- Constant updating and enrichment of the Whalebone Threat Intelligence
- Hosting the Administration Portal and related APIs
- Hosting the End Customer Portal and related APIs
- Service configuration for each individual subscriber is possible
- Real-time Threat Intelligence and configuration updates to the Whalebone DNS Resolvers®
- Data analysis, APIs and per-subscriber reporting
- Alerting to ISP's administrators

Perfect Fit for B2C and B2B
Whalebone's flexible deployment model is an excellent fit for small and medium-sized ISPs looking to protect both residential and business customers with minimal complexity.

For B2C, ISPs can easily secure all customer devices without requiring any installations or End-user actions. This allows for broad protection across the subscriber base with minimal operational overhead. This approach enhances customer loyalty, and reduces support costs and improves the overall quality of the service.

For B2B, Whalebone enables ISPs to offer security services to SMBs, protecting every device connected to the company network including servers, laptops, mobile devices, IoT, and even guest End-users. It adds value where traditional endpoint solutions fall short. This creates a compelling business case for ISPs to offer DNS security as part of their service portfolio, strengthening customer relationships and generating new revenue streams.

1.2 Product variants

Whalebone Peacemaker offers **three levels of integration (variants Peacemaker Standard, Content filtering and Profit)**, each with distinct features and use cases. The integration level you choose affects the End-user experience, deployment effort, and flexibility. The ISP can start simple with the Standard variant and scale up as needed.

1.2.1 Peacemaker Standard

Peacemaker Standard becomes your first layer of security. Provides comprehensive network protection and management using both on-premises and Cloud Resolvers. It also offers rich visibility, analytics, and policy management through the Administration portal.

It includes two core APIs:

- Whalebone API: for retrieving usage statistics
- Config API: for managing policies, assigning them to IP ranges, and setting allow/deny lists

In this tier, administrators can define and apply policies by subnet. However, policy control remains entirely with the ISP, and End-users do not have access. Importantly, Peacemaker DNS security and management also includes enforcement of country-specific regulatory restrictions, ensuring compliance with local internet governance.

Time required for implementation is usually less than 2 hours containing basic training of the administrators.

1.2.2 Peacemaker Content Filtering

This variant builds on the variant Standard by adding category-based traffic filtering. Administrators can block or allow access to specific content categories such as adult sites, social media, or streaming platforms.

Whalebone's Content Filtering offers a rich and customizable set of 4 major content filtering categories and 17 distinct subcontent categories, which administrators can enable or disable per policy and even schedule by time of day. In this variant, administrators can define and apply policies by subnet. (e.g., parental control, child-safe browsing ecc…) However, policy control remains entirely with the ISP. End End-users do not have access to modify the Content Filtering options themselves.

Time required for implementation is usually less than 2 hours containing basic training of the administrators.

1.2.3 Peacemaker Profit

Designed for ISPs aiming to deeply integrate security services into their own customer-facing platforms, Peacemaker Profit allows full customization of policies and reporting interfaces. Integration includes single sign-on with the ISP's customer portals and mobile apps, giving End-users clear visibility and management of the security features, something not achievable with the Standard or Content Filtering versions.

Whalebone's Retail API powers data access and configuration management and the frontend can be rebranded to the ISP brand (logo, colours, etc). Although Peacemaker Profit requires a larger initial integration effort, ongoing maintenance is straightforward and flexible.

Commercially speaking, particularly when rebranding or launching new customer-facing initiatives, the benefits of this variant are::

- Easy to sell and bundle VAS
- Instant activation, no End-user effort
- Works for mobile and fixed networks
- Multiple digital touchpoints to prove value

Time required for implementation and testing is usually 2 - 3 months.

1.3 Comparison of Peacemaker variants

Feature	Standard	Content Filtering	Profit	Description
Segmented Network Policies				
DNS Security Filtering	✓	✓	✓	Malware, botnet, phishing, spam, coinminers and C&C domains are all blocked. Optionally blocking of compromised domains is possible.
Segmented Network Policies	✓	✓	✓	Different policies to selected network segments in a very granular.

Custom Allow and Deny lists			 *	Unlimited number of lists, possible to assign to a particular IP or IP range. *For the Profit it is up to 1000 domains in both allow and deny list combined.
AI based filtration				Whalebone AI uses massive data generated by millions of end-users to constantly improve the accuracy of blocking.
Real-time Protection				Threat Intelligence information is communicated immediately on the DNS resolvers.
Custom Blocking pages				Logo, company name and contact is customizable. Full html configuration of the blocking page is available for Content filtering only.
Optional Blocking Bypass				The option to allow the end-user to continue to the original destination even after the redirect to the blocking page.
Single-click activation on the Blocking page				End-user can activate the service during the trial period from the Blocking page through a single click.
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Content filtering				
Regulatory restrictions blocking				Blocking of domains required by law.
Content Filtering Overview	only for domains from regulatory restrictions blocking			An interactive dashboard for investigation of content-related blocking (Adult / Entertainment / P2P networks / Ads / etc.).
Scheduled Policies				Individual categories can be turned on/off for specific time periods.

Enforce SafeSearch				Read more at: https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid
YouTube Restricted Mode				Read more at: https://support.google.com/youtube/answer/174084?hl=en&co=GENIE.Platform%3DAndroid
Parental / Content control on device level (iOS/Android)				Only with adoption and activation of the Off-Net feature.
Off-Net Protection				iOS / Android client that the End-user has to install and pair with the subscription via a QR / numeric code he will get on the End Customer Portal. Off-net will use the Whalebone Cloud Resolver.
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
DNS over HTTPS or TLS				
Client local IP visibility and management				Depending on the deployment scenario, the resolver is able to log private client IP addresses.
DNSSEC enforcement				Whalebone enforces DNSSEC by default, preventing man-in-the-middle attacks.
Support of encrypted DNS protocols - DoT and DoH				Whalebone provides support for usage of encrypted DNS protocols to ensure confidentiality of traffic.
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Deployment				
Full-fledged on-premises DNS resolver				Minimum requirements - a linux VM with 2 CPU, 4GB RAM 80GB HDD is required (70GB in /var partition).
Cloud DNS resolver				The ability to divert DNS resolution towards Whalebone's cloud resolvers.

Recursive resolver				Recursive resolver functionality.
Zero down-time upgrades and configuration changes				Thanks to a blue-green deployment, Whalebone Peacemaker is able to perform any updates and configuration changes with no interruption to the service.
Unlimited number of on-premise DNS resolvers				The number of DNS resolves deployed under one tenant is unlimited.
Live configuration changes propagation*				The changes to configuration and policies are applied immediately *for on-premises resolvers.
API for configuration				An API for WRITE operations is available on request. Suitable for integrations.
Integration directly to ISP's Web Portal				The configuration features can be integrated directly into the ISP's Customer Care portal for seamless experience.
Integration directly to ISP's Mobile Application				The configuration and reporting features are integrated directly into the ISP's Customer Care mobile application for seamless experience.
Fully branded End Customer Portal for B2C and SMB with the SSO access				Provisioned End-users are allowed to visit the fully branded End Customer Portal, usually, in the form of a single sign-on link from the ISP's customer care portal.
Customer de/provisioning through the API				Individual End-users and their details are de/provisioned through the API and for the End customer portal management.
Family and small-and-middle segment management				Permission and access levels suitable for family policies / protection and SMB use cases.

Individual policies including allow / deny list	✗	✗	✓	Users are allowed to define their own security policies including whitelists and blacklists.
Multi-tenancy	✗	✗	on request	Administration of multiple tenants, each with different policies, resolvers and settings.
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Resolver health alerting				
PDF reporting	✓	✓	✓	Optionally moreEnd-users can receive the reports.
Resolver Health Alerting	✓	✓	✓	Set up on Admin portal (e-mail, syslog, webhook).
Security incidents	✓	✓	✓	Set up on Admin portal (e-mail, syslog, webhook).
DNS traffic anomaly alerting	✓	✓	✓	Set up on Admin portal (e-mail, syslog, webhook).
*all alerts can be sent either as an email, a slack notification a syslog message or pushed as a webhook				
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Data retention				
Realtime Threat logs in GUI	✓	✓	✓	90 days
Realtime DNS data in GUI	✓	✓	✓	90 days
Storing of all data	✓	✓	✓	For a period of 6 months after logging a request/incident the data is archived with Whalebone
Showing specific data period in last 6 months	On request	On request	On request	All data not archived by the customers is erased permanently after 6 months

CSV Export of DNS and security logs				All logs are exportable in csv format for table processors
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Basic Support				
E-mail / Ticketing				Response time is 4 business hours. Resolution time is 6 business hours. Available languages: English Business hours are in CET timezone (GMT+2)
24/7 support + Phone hotline				24/7 support with always-available phone number. Available languages: English
Feature	**Standard**	**Content Filtering**	**Profit**	**Description**
Premium Support				
E-mail / Ticketing				Response time is 15 minutes Resolution time is 4 business hours. Available languages: English Business hours are in CET timezone (GMT+2)
24/7 support + Phone hotline				24/7 support with always-available phone number. Available languages: English

2. Core technology

2.1 Whalebone DNS Resolver®

Whalebone is a hybrid solution that consists of a *cloud-based* security and content filtering component that is delivered by an *on-premises* Whalebone DNS Resolver®. The Whalebone DNS Resolver® can be deployed either in a physical or a virtual environment, according to agreed deployment details between the ISP and Whalebone. The solution works on top of regular DNS traffic using the recursive resolver to get access to the DNS traffic and also has the ability to intercept the response in order to protect the client against threats that are present on the remote server. Whalebone puts a great deal of focus on the availability of the DNS service itself which runs non-hindered, without measurable added latency (Whalebone DNS Resolver® does not add any latency through cloud lookups or similar approach). Additionally, Whalebone provides both their security and content-filtering services in the form of a device client. This Off-Net asset is used to protect the end-users in the case that they are not directly connected to the ISP's network.

The service is available in different levels of integration, offering diverse sets of features. The ISP's product management decision about the particular service level will strongly influence what could be provided to theEnd-users, as well as, the deployment effort and duration. The decision is not final and the service could be upgraded to a more advanced variant in the future, should the ISP decide to start simple and advance over time.

As Whalebone works on the DNS level, the scaling is independent of growing bandwidth needs and thus removing the performance obstacles of deep packet inspection (DPI) or proxy solutions who handle the full packet stream. The DNS level filtering, also, allows Whalebone to support any operating system or browser.

Whalebone's resolvers can be deployed for the subscribed End-users only providing different behavior to individual devices (CPE), or they can be used as DNS resolvers for the entire network.

The caching recursive DNS resolver is based on the secure, high performing Knot resolver's technology. The whole scope of Knot Resolver's offering can be used when configuring Whalebone Service and its respective security policies.

2.1.1 DNS traffic management

The Resolver enables the ISP and its administrators to have complete control over the DNS resolution process and flow. Different views, according to the client's network, are easy to implement. For example, end-user devices such diverse customer-premises equipment (CPE) are easily defined and supported. Additionally, complete control of caching, DNSSEC validation and all other significant procedures are subject to configuration by the administrator.

Whalebone supports native use of the IPv4 and IPv6 addressing. Clients are able to communicate

with the resolver through both protocols, as well as, the resolver could use both protocols to do the recursive resolution process towards the authoritative servers.

2.1.2 Leading DNS protocol security

The security of the DNS protocol has been extended over the time with many different RFC documents and the coverage of available implementations differs a lot. Whalebone offers up-to-date protocols and algorithms to ensure maximum security for theEnd-users and the ISP's network. DNSSEC with NSEC3 negative caching is implemented and validated in real world traffic, stopping various misuse of DNS resolution such as outgoing DDoS attacks and malicious tunneling. Besides DNSSEC, case toggling is also implemented, to protect the resolver's cache against poisoning.

2.1.3 End-user oriented DNS resolution

The main objective of the DNS resolver is to provide a fast connection experience to the End-users. The DNS resolution strongly influences the End-user experience and it is highly important to provide fast responses at all times. Whalebone's resolver keeps the cache warm round-the-clock, through intelligent prefetching – should any record be due to expiration from the cache, the resolver will proactively refresh it.

Also, should any authoritative server around the Internet experience downtime, Whalebone's resolver keeps the cached records for that domain beyond their assigned TTL in order to be able to provide answers to the clients until the authoritative servers get back online.

Whalebone does not interfere with the DNS resolution process in any case, except when a malicious domain is being resolved. In that case the proper network and end-customer policies are applied. To sum up the key features are:

- The resolver is managed from Whalebone Cloud through the respective management service
- The resolver is based on Knot Resolver's technology and thus, it is fully configurable, RFC compliant and supports DNSSEC validation
- Eventual downtime of the Whalebone Cloud does not affect the resolver performance (threat updates and log analysis are postponed to the moment of the cloud connection revival)
- The resolver uses locally cached data that are obtained from Whalebone Cloud to identify threats
- The resolver also hosts the Blocking Page where the End-users are redirected to in case of detection of a malicious domain

2.1.4 Resolver Management

This service is also called the resolver agent. It maintains persistent and mutually authenticated TLS connection to Whalebone Cloud and acts as the main management service. Its functionality includes:

- Receiving software, policies and threat cache updates from Whalebone Cloud through an encrypted channel
- Reporting the state of the resolver to Whalebone Cloud

- Maintaining the End-user identity information obtained from an authentication server (e.g., RADIUS or DHCP server)
- Hosting the Blocking Page and being responsible for the bypass process

In addition, the resolvers' management frontend, as well as, Whalebone's API provide various metrics that can be used to evaluate quality of the service and predict potential issues. These metrics are:

- Health checks – achieved by simulating DNS resolution and detecting potential issues
- Hardware metrics – CPU, memory and swap usage, disk space availability
- DNS resolution metrics – latency, significant answers, DNS validation failures

2.2 Log management

The Log Management service that runs along Whalebone Resolver is responsible for gathering all the logs that are stored by other services and for ensuring their delivery to the cloud. Furthermore, the service monitors the size of individual log files and rotates (compresses, moves and removes) the old log files to ensure that disk space stays available for the ones to come. To summarize its functionality:

- Gathers and stores the logs to the disk
- Rotates the logs according to a predetermined policy
- Streams particular logs to Whalebone Cloud through an encrypted channel

All the generated logs (both regarding traffic and resolver's statistics) are also available to the ISP for gathering, evaluation and integration. The logs are stored in JSON format and can be also accessed through Whalebone's API. Additional guidance for their processing is provided by Whalebone. For more information on how to access the available data please refer to Table 2: Available Logs and respective Access

2.3 Sizing and Hardware Requirements

Local resolver is supported on a solely dedicated (physical or virtual) machine running a supported operating system and Docker engine. Running resolver on unsupported versions of OS and/or docker or with other services might lead to incorrect behavior or issues with service/resolution.

2.3.1 Operating system requirements

Whalebone supports operating systems that are supported by the standard support periods of OS publishers - namely 64bit server editions.

- Red Hat Enterprise Linux (Full support)
- CentOS Stream (Active support)
- Debian (Supported by LTS team)
- Ubuntu (Standard support)

OS Management and maintenance of the hardware deployed at the ISP on-premise environment is **not included** in Whalebone Service.

2.3.2 CPU

The main factor to consider when estimating the sizing of the resolvers is the CPU cores. The number of CPU cores depends on the number of expected DNS queries per second (qps). Under normal circumstances, each CPU core (recent Intel Xeon server processor) has been measured to be able to handle 10,000 qps with DNSSEC validation enabled. This number grows in a linear manner with the number of CPU cores available. As a minimum we recommend at least two CPU cores per resolver.

2.3.3 Memory

Recommended sizing is 4 GB per resolver. This sizing will handle all security features and a large DNS cache to ensure lowest possible latency for all the customers.

2.3.4 Disk space

Recommended disk space for an ISP deployment is at least 80 GB in the /var partition on SSD drive. More information can be provided by Whalebone based on the use case and the expected load.

2.3.5 Performance benchmarking

If DNS performance is of your concern, contact our business development managers to get more information about proper sizing for your use-case. Whalebone Peacemaker reliably handles traffic in a wide variety of networks. From small regional ISPs to the biggest tier-2 connectivity providers.

Whalebone technical consultants will go over the specifics of your network and are able to assist you with DNS performance benchmarking. We have performed dozens of tests in the past and Whalebone Peacemaker routinely beat the best performing public cloud resolvers on the popular comparison site https://www.dnsperf.com/.

2.4 Threat Intelligence Processor

The Threat Intelligence Processor resides in a central part of Whalebone Service. It consists of multiple custom microservices for ingesting, generating, evaluating and enriching threat intelligence that are combined in order to calculate *a* unique reputation output for each domain. In the following paragraphs Whalebone's Solution will be described in terms of a pipeline, as well as, how this enables Whalebone to always fight the latest threats.

2.4.1 Inputs

Whalebone's Threat Intelligence Processor takes as an input a wide range of domains that are processed and assessed based on best practices of the Threat Intelligence and threat assessment. As far as the Processor is concerned, each domain is considered as an Indicator of Compromise (IoC) and that allows for interoperability with other systems, such as SIEMS and thus, aids in the provision of threat intelligence data from Whalebone to the ISP's environment.

To further elaborate, Whalebone's Threat Intelligence Processor collects and processes worldwide data from a range of high quality and industry-standard Threat Intelligence sources. This vast number of feeds combines expertise from different fields of Threat Intelligence in order to cover as much of

the threat scenarios as possible. By utilizing these, Whalebone's solution is able to:

- prevent primary infection by utilizing information from companies that specialize in endpoint solutions
- stop Command and Control (C&C) communication by incorporating data from sandboxing companies
- detect early malware outbreaks by using data from network security companies (providers of Intrusion Detection and Prevention Systems (IDS, IPS))

All these sources are processed in a unique way and are enriched with data from Whalebone's research. When it comes to numbers, the daily volume of newly processed and consolidated, unique, IoCs, by the Threat Intelligence Processor is in millions. At the same time, *millions* IoCs are maintained internally at the Processor's engine.

2.4.2 Processing

The extensive quality evaluation that is taking place when a new IoC is ingested to the Processor generates a unique reputation numerical value. This reputation value is assigned in an initial phase to each and every of the IoCs and is updated in regular intervals in a continuous re-evaluation procedure. More details on how the Threat Intelligence Processor scores in this multi-phase manner the malicious domains can be found in the following paragraphs.

During the first phase of the reputation calculation, the Threat Intelligence Processor takes as input data from the available industry-standard Threat Intelligence, as well as, research-driven Whalebone's Threat Intelligence feeds. The processing that is occurring is based on state-of-the-art algorithms that utilize both existing traffic's behavioral attributes and available domain metadata.

The statistical models that are applied, are integrating the captured traffic from Whalebone's network of resolvers and as a result they are providing an extensive and characteristic view of the regional threat landscape. The output of the processing is a unique reputation metric value that is assigned to the IoC and is propagated to the database of each Whalebone's Resolver. This output becomes part of the resolver's cache and as a result can be accessed with vast speed and thus, block the danger in the making.

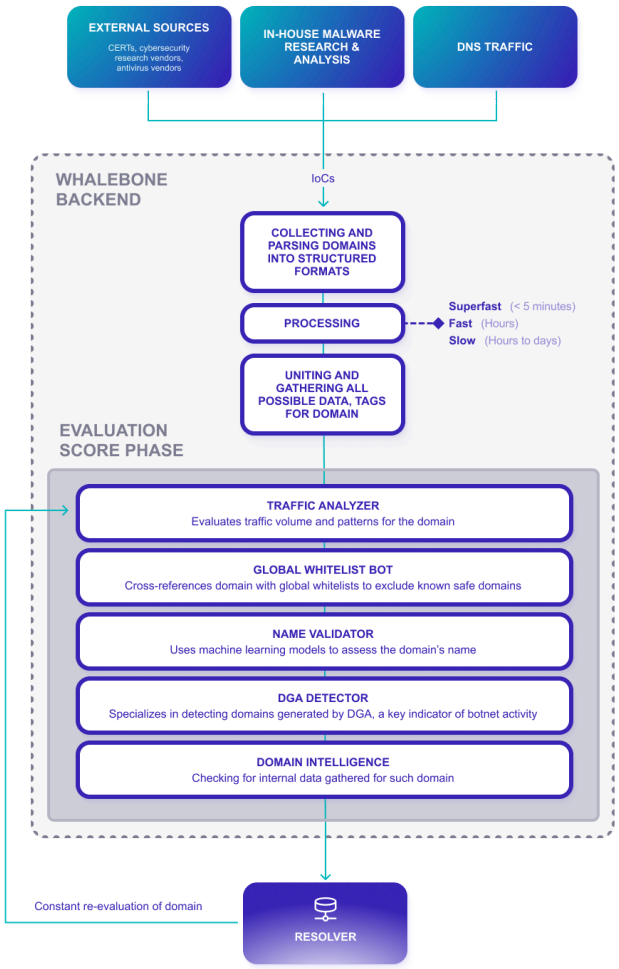


Figure 1: Initial Evaluation of Threat Intelligence

In addition, after the initial reputation calculation is accomplished, and the malicious IoCs are propagated to the resolvers, there is a second phase of IoC evaluation in order for Whalebone to guarantee their freshness and applicability on the specific deployment's environment. In order to achieve the expected quality of service, several cutting-edge microservices, including some that are a direct outcome of Whalebone's R&D are facilitated.

To further elaborate, at periodic fixed intervals, Whalebone's Cloud initiates a mutli-step process that includes, but is not limited to:

- a neural network that detects domains that are a product of Domain Generation Algorithms (DGA)
- a neural network that simulates the work a human analyst would do when they would perform a reputation check
- up-to-date reputation originating from industry-standard Threat Intelligence engines
- evaluation of the metadata that a domain offers (e.g., DNSSEC signatures, WHOIS data etc.)
- evaluation of the patterns that arise in the traffic for indicators of spam and Command and Control (C&C) behavior.

The output of all these services is taken into consideration and the reputation for each and every IoC is adjusted accordingly. This change is then propagated to the resolvers and thus they are ensured to have the most prevalent data.

2.4.3 Output: Unique Reputation Value

By using the aforementioned process, Whalebone's Resolvers have at every point in time a unique numerical reputation value assigned to each and every IoC. The value operates as the threshold that ISP administrators can tamper with, and shape their custom policies. By introducing this broad range, ISPs are able to create fine-grained policies and have control even on the slightest reputation change.

Based on this reputation value, two types of actions can be configured for each domain: audit and block.
On auditing, the emergence of a domain is recorded in the threat list but it is allowed to be resolved and the answer to be returned to the End-user. On the other hand, on blocking, the IP address of the Blocking Page is returned and the End-users are encountering the ISP's custom blocking message.

Whalebone provides default policies that are a product of the experience with already monitored traffic. The default policy of Auditing emerges when a reputation value of at least 40 is detected while Blocking in the case that reputation is at least 60.

At the same time, Whalebone offers the option of monitoring for a predefined period of time the ISP's network and then provide guidance to the Resolver's administrators on how to shape their own policies.
It is important to note that the reputation thresholds are fully configurable and enable not only the shaping of different policies but can be applied with different configurations to particular resolvers *or even to distinct End-users or devices*.

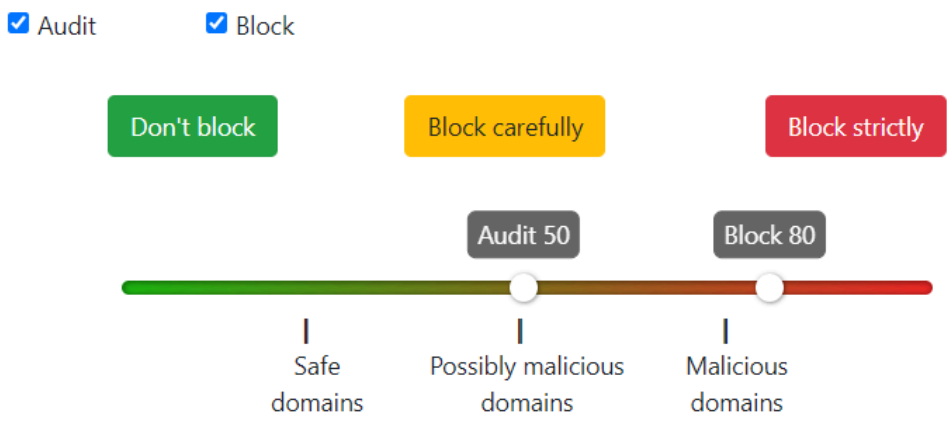


Figure 2: Default Audit and Block Thresholds

2.4.4 Regional Threat Intelligence

The process of the Regional Threat Intelligence is Whalebone's approach to the issue of localized regional threats, which differ from the Global Threat Intelligence by utilizing regional research of the regional at-risk economic sectors, cultural influences and lingual differences; all of which influence the regional threat landscape.

The process itself consists of three main phases forming an Intelligence Life-cycle:

- Research phase
- Detection phase
- Analysis/Blocking phase

The breakdown of Regional Threat Intelligence phases:

- Research phase: This phase consist of utilization of OSINT (Open-source intelligence) data gathering, social media threat-scouting and linguistic analysis, all of which outputs machine-readable data utilized in the next phase
- Detection phase: Results of the Research phase are applied to Whalebone's detection solution to detect potential new and emerging threats. Domains flagged by our detection solution are processed in the Analysis phase.
- Analysis phase: Domains flagged are analysed by Whalebone's AI powered analysis solution, where domain's behavior, context and metadata are evaluated for its potential maliciousness. If this solution flags the domain as malicious, it is blocked on Whalebone's backend for all Whalebone's customers. The results of this process are subject to constant scrutiny and updates; to make sure our AI-powered analysis solution is delivering the best possible results at all times.

As the process of the Regional Threat Intelligence is part of an Intelligence life-cycle, results of each step inform the next and the results of the analysis are evaluated and later inform the research phase during the scheduled revisit periods.

2.4.5 Content Filtering Processing

The content database is updated gradually over the time on the Whalebone Cloud level and multiple engines contribute to the state of the database. Whalebone combines different verified third-party databases and is constantly looking for new and unknown websites that are not properly categorized. The full database is then updated on the Whalebone Resolver level to ensure all the decisions can be made on-premise in the ISP environment – adding zero latency to the traffic and ensuring the service is fully available even in case there is any issue between the ISP premises and Whalebone Cloud.

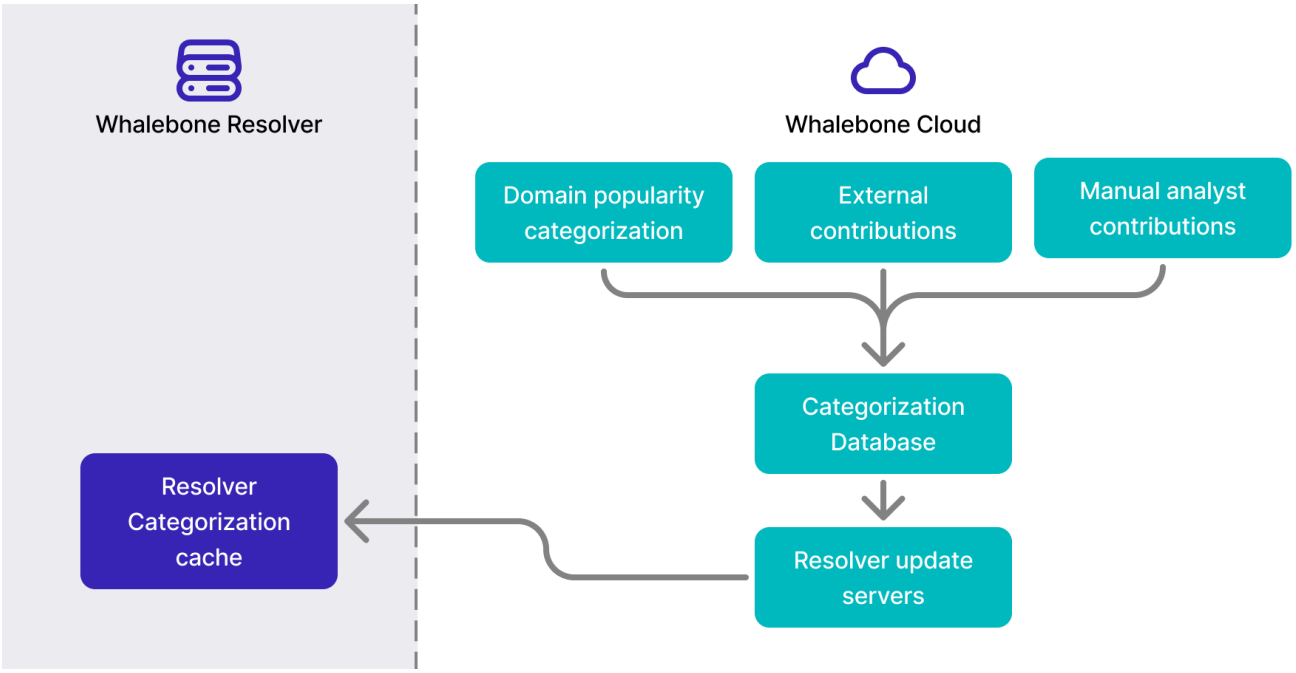


Figure 3: Categorization process from the Whalebone Cloud to the Resolver

In case of wrong categorization our customers are able to report such an event and the support team responds with an adjusted categorization set and pushes the updates to the Content Filtering database and the DNS resolvers providing this type of service.

Our database provides more granular categories than what is presented to the End-user. The reason is that more granularity gives Whalebone better flexibility in properly categorizing the content and this approach is more extensible for new particular content types in the future. These detailed categories are linked to the customer-oriented frontend where more general categories are provided as it is usually easier for the customer to set up the more general groups and higher granularity would lead to confusion. A single domain can be assigned to multiple categories.

2.4.6 False positive facilitation process

A team of threat intelligence specialists is dedicated to the task of investigating a false positive domain following customers' reports. In these situations, the administrator can simply report the domain straight from the Threats overview. The same can be done for a miscategorized domain.

2.4.7 Database updates and new domains categorization

As soon as such websites emerge on the internet and our telemetry recognizes that such website gains attention of visitors, we immediately categorize such a website and provide updates to the database in a matter of minutes.

New website categorization and verification is based on machine learning models working directly with the website content as a human analyst would do and they are able to categorize the website

with certain measurable accuracy. The results are used only if the algorithm is certain enough.

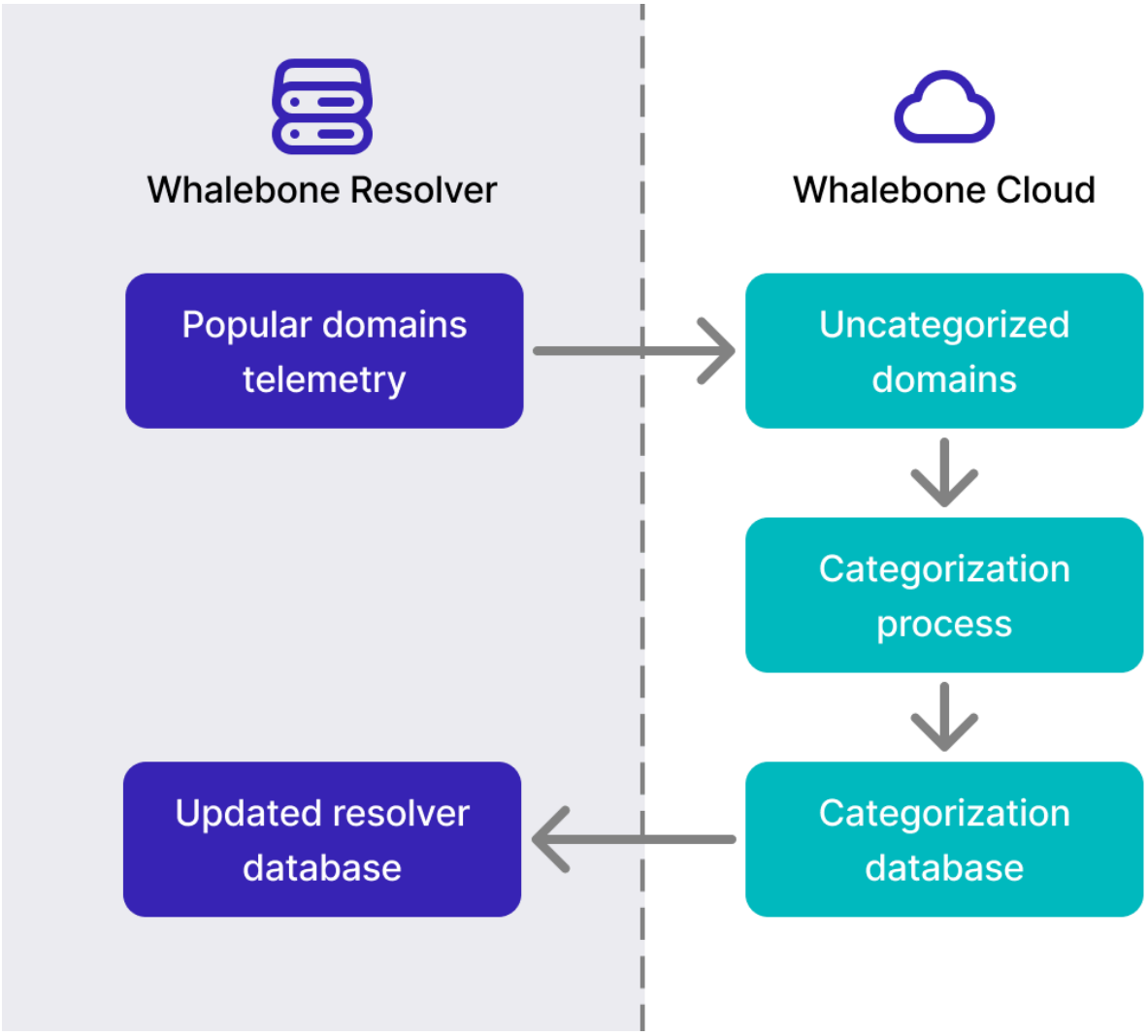


Figure 4: Categorization process based on domain popularity

2.5 Log Analysis

The log analysis component of Whalebone Cloud is responsible for processing and storing all the logs that are forwarded to the cloud and also those that are created directly in its premises. It offers services to many other components, including the Administration Portal and the End Customer Portal. Also, anything related to reporting and alerting makes a great use of the log analysis services. To sum up its role, the log analysis service's key features are:

- Data indexing in a cluster environment that facilitates the event storage, analysis and backup processes.
- Provision of inputs to all frontend and backend applications including alerting, reporting, APIs and portals
- Processing with Neural networks and anomaly detection engines in order to reveal advanced and long-term threats

- Supervision and storage of the audit trail of the Administrator Portal

All the data that are available on the log analysis service can be provided for further processing to the ISP either in JSON format or through the API. For more details see the following table.

Property	Source	Medium	Availability
Resolver Status Logs	Resolver	Whalebone API	Administrator Portal
		JSON Logs	Resolver
		Whalebone API	Compatible Endpoints
		Syslog	Compatible Endpoints
Passive DNS Data	Resolver	Whalebone API	End Customer Portal (Per End-user/Device)
		Whalebone API	Administrator Portal (Aggregated or Individual)
		JSON Logs	Resolver
		Whalebone API	Compatible Endpoints
		Syslog	Compatible Endpoints
Detected Threats	Resolver	Whalebone API	End Customer Portal (Per End-user/Device)
		Whalebone API	Administrator Portal (Aggregated or Individual)
		JSON Logs	Resolver
		Whalebone API	Compatible Endpoints
		Syslog	Compatible Endpoints
DNSSEC Validation Data	Resolver	Whalebone API	End Customer Portal (Per End-user/Device)
		Whalebone API	Administrator Portal

			(Aggregated or Individual)
		JSON Logs	Resolver
		Whalebone API	Compatible Endpoints
		Syslog	Compatible Endpoints
Audit Trail	Administrator Portal	Whalebone API	Administrator Por tal
		Whalebone API	Compatible Endpoints
Subscription Data	Whalebone Cloud	Whalebone API	Compatible Endpoints

Table 2: Available Logs and respective Access

3. Deployment options

There are multiple options on how to deploy Whalebone's resolvers on a network's premises. Most ISPs are opting for an architectural schema that includes at least two resolvers for reasons of stability and resilience. Furthermore, the client identification is a major factor and is taken into consideration upon all of Whalebone's approaches. In the next sections there are going to be four of the available deployment options but more alternatives are available upon discussion.

3.1. Primary and secondary resolvers

The most simple used deployment options is to deploy two resolvers in two different locations and use the secondary in cases where the primary's performance is degraded. For simple deployments this ensures high availability and stability of the DNS translation

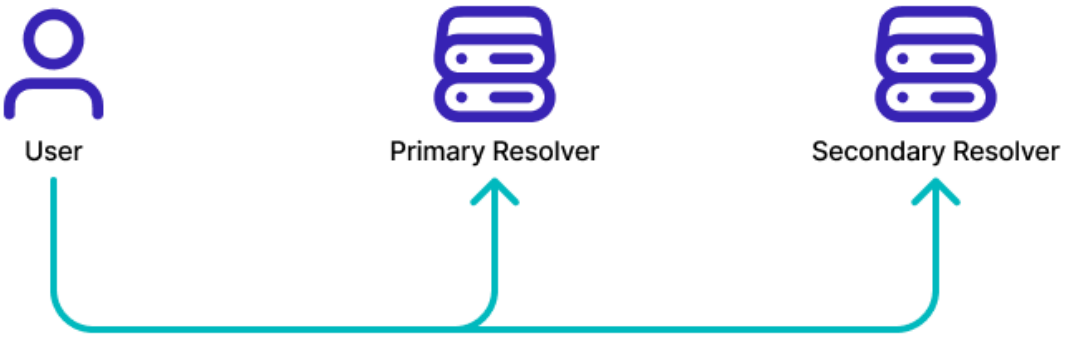


Figure 5: Primary and secondary resolver deployment

3.2. Resolvers behind a load balancer

For this approach to work, the two or more resolvers are placed behind a load balancer. The chosen balancer is expected to be transparent, keep the source IP address of the original client in the request and forward it to the resolver. Some additional processing by the balancer is also possible, as long as the supported EDNS header Client-Subnet is in place.

Figure 6: Loadbalancer deployment

3.3 Anycast IP Address managed on router level

Moreover, there is the scenario where there is a router in place that is advertising the anycast IP address for the resolvers. The availability monitoring is taking place on the router and, thus, it is the sole responsible for further traffic delegation.

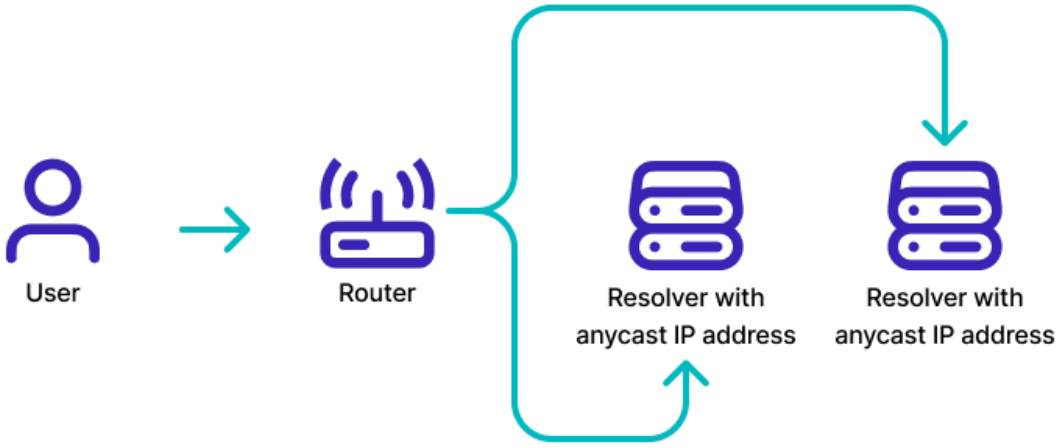


Figure 7: Anycast managed on router level deployment

3.4 Anycast IP Address managed on resolver level

Additionally, to the above paradigm, the resolvers that are broadcasting their own anycast IP address. In this scenario, the BGP routers are responsible for the availability updating and for the forwarding of the traffic to the best alternative resolver. No control on the traffic balancing is possible so multiple

resolvers should be deployed in order to handle the traffic effectively.

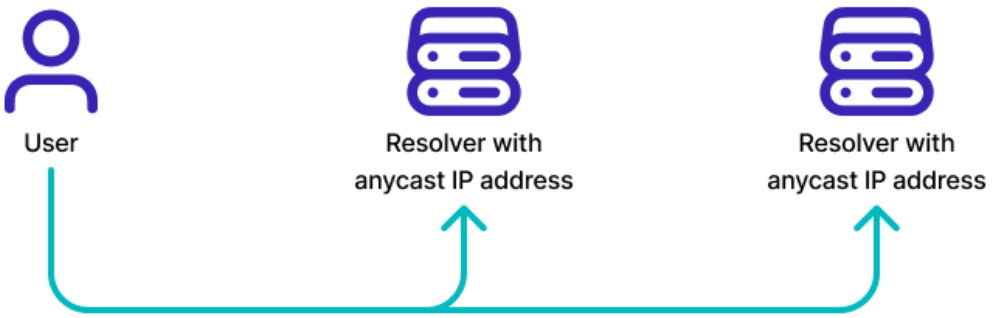


Figure 8: Anycast managed on resolver level

4. Features

The features of Whalebone Peacemaker are divided into the following categories: Security, Content filtering, Deployment, Reporting, Alerting, Data and integration and Support. The features differ between the three product variants: Whalebone Peacemaker DNS Security & Management and Whalebone Peacemaker for Content Filtering and Peacemaker Profit.

4.1. Administration Portal

The Administration Portal is used by the ISP administrators to ensure that proper configuration is applied to the DNS resolvers, that all services are running properly and that the traffic has the expected properties. The portal can be used for traffic troubleshooting, support access and account management.

Key features include:

- **Flexible Permissions:** Various permission sets for end-users, including restricted data access, partial configuration management (e.g., global blacklist), and read-only access. Single Sign-On (currently SAML) is also supported.
- **Comprehensive Data Access:** Access to all data from resolvers and their configuration details.
- **Advanced Threat Analysis:** Full-text filtering of security threats and traffic logs, with export capabilities for filtered views.
- **Customizable Policies:** Ability to customize policies and ISP-wide whitelists/blacklists.
- **Legal Compliance:** Option to block domains based on legal requirements (e.g., illegal gambling websites).

Further details on these capabilities are provided in the following sections.

4.1.1. Threats Overview

The Threat Overview page presents the incidents that are detected by Whalebone's solution. In the same manner as with the Traffic Overview, extensive filtering can be applied.

Furthermore, the reason why a query was blocked or audited is presented along with an identifier of a specific threat name, if available. A categorization based on the threat type can also give an overview of what is happening inside the network and which hosts are infected.

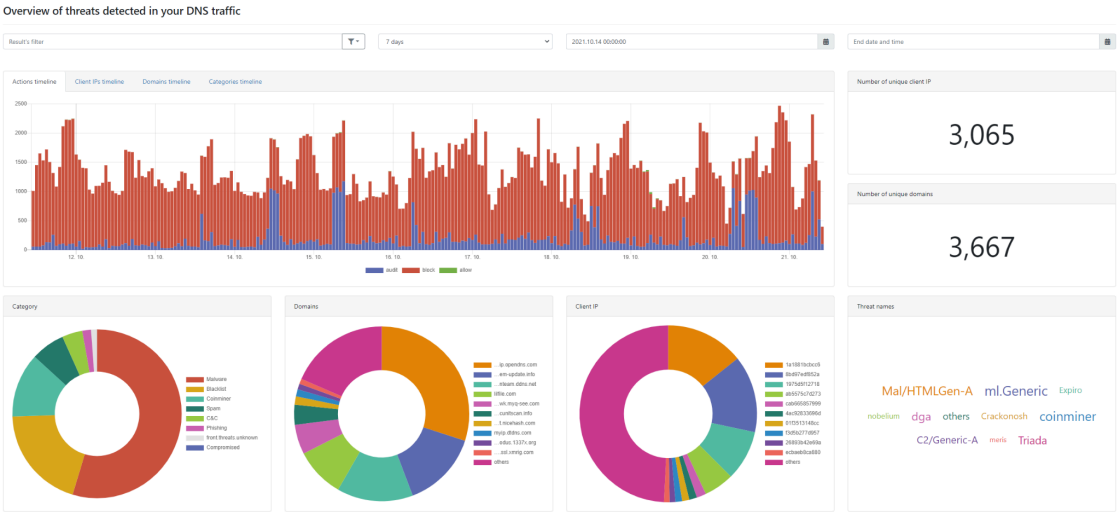


Figure 9: Threats dashboard

4.1.2 Automated Threat Intelligence scoring

Whalebone threat database is being constantly updated and the updates are pushed to the resolver in real-time. That way the resolver always operates with the most up-to-date information. No manual update from the Administrator is needed. New malicious domains are blocked automatically while the domains which have become harmless are removed.

4.1.3 Segmented Network Policies

The Administrator is able to apply different policies to selected network segments in a very granular manner. This enables it to have a default catch-all policy for all unspecified IP ranges, while offering security features to enterprise customers or content filtering to schools. The administrator is even able to configure a “deny-all” policy for customers who are late on their payments and only allow traffic to banking websites.

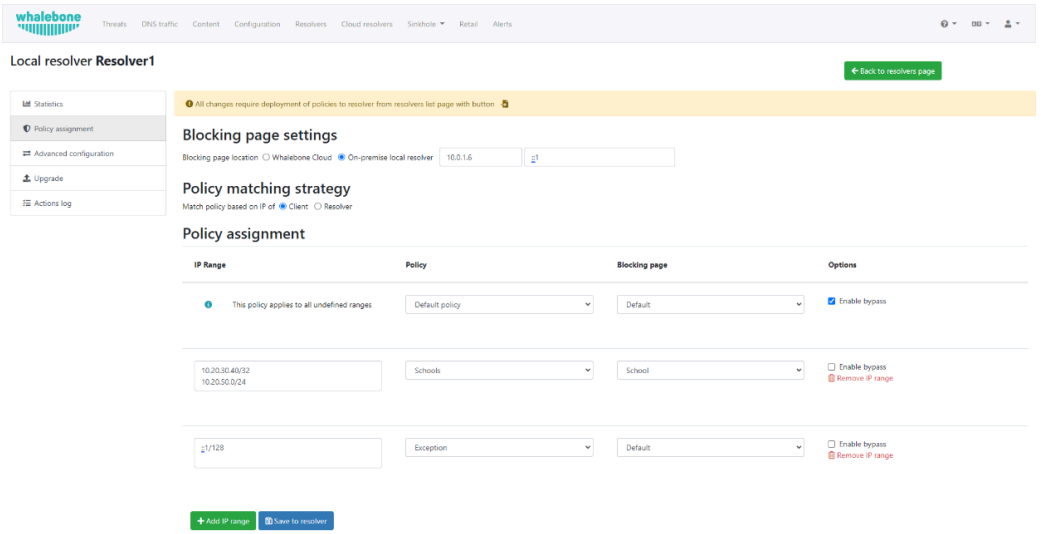


Figure 10: Policy assignment

4.1.4 Custom allow lists and deny lists

The administrator is able to configure an unlimited number of allow/deny lists and assign them to various policies. One list can hold 10 000 domains for the variants Peacemaker Standard and Peacemaker Content Filtering. For Peacemaker Proffit this number is limited to the 1000 domains.

4.1.5 Blocking Page and Bypass

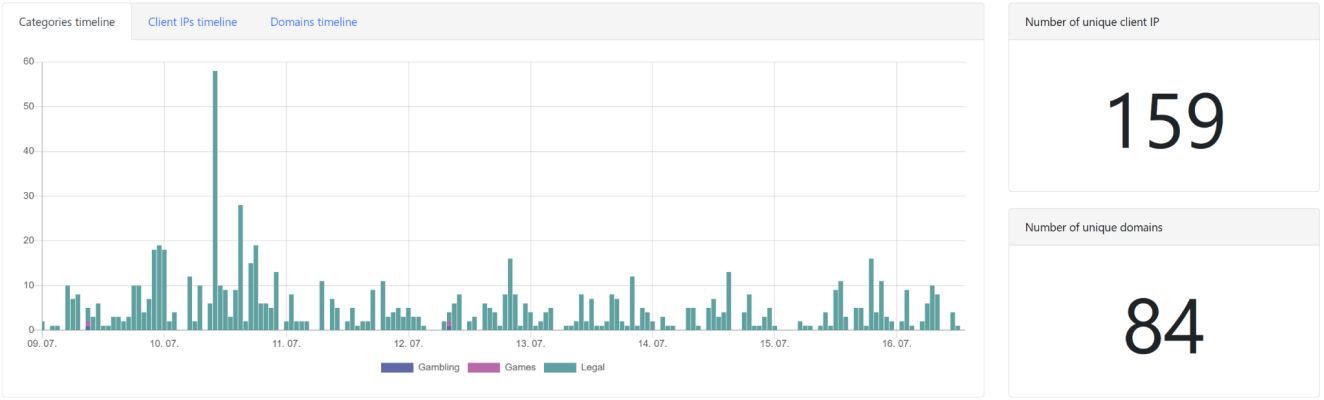
In the case of a malicious connection, blocking the DNS request means answering to the client with a specific IP address that leads to the Blocking page hosted on the resolver. Should the client initiate the HTTP/S connection towards the blocked domain, they are presented with the custom Blocking page with different content based on the original reason for blocking (e.g., malicious domain, legal reasons, explicitly denied content / ISP's blacklist or content filter.).

In particular cases (malicious domains) and if enabled the End-user is allowed to bypass the blocking and continue to the destination website if they want to. This bypass feature works directly on the DNS level. The resolver is informed that the End-user wishes to continue to the website and the browser is forced to retry the domain access. This is very important because Whalebone does not proxy the subsequent connection, thus, cannot access any sensitive information or cause any compatibility issue to the application.

The Blocking's Page is whitelabeled and fully customizable by the ISP. Custom HTML, CSS and JavaScript code can be applied to the blocking page.

4.1.6 Content Filtering overview

The Content Filtering Overview page presents the attempts to resolve domain names that are tied to a category blocked by the active policies. In the same manner as with the Threats Overview, extensive filtering can be applied.



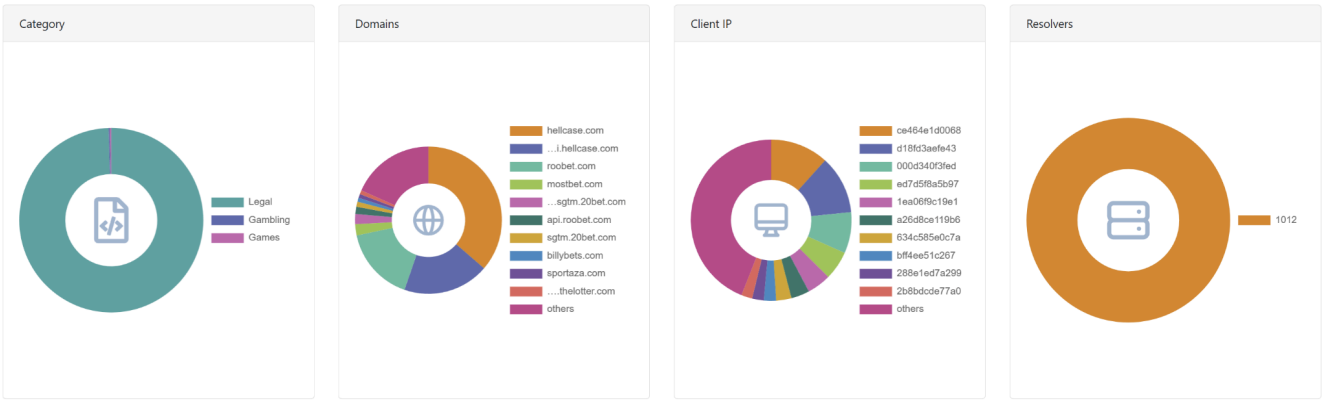


Figure 11: Content filtering dashboard

4.1.7 One-click Regulatory Blocking activation

Whalebone's solution provides the option to administrators to enable the blocking of legally required domains by using official blacklists (e.g. CSAM domains or illegal gambling).

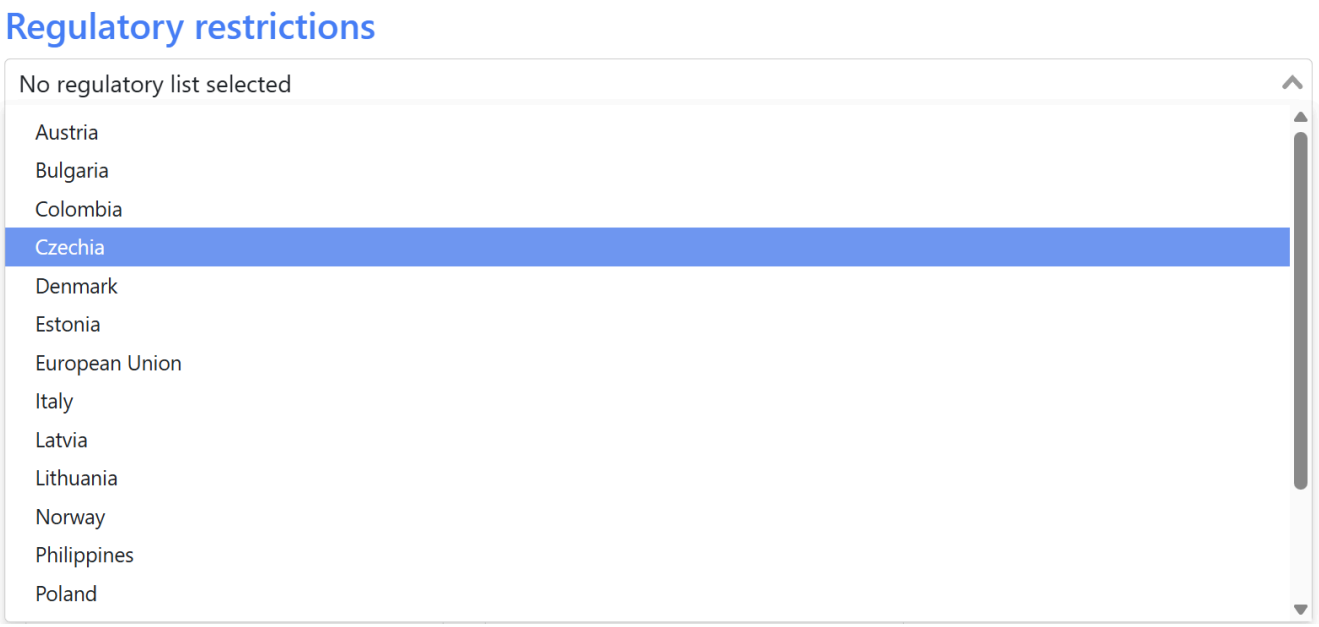


Figure 12: Domain regulatory restriction lists

4.1.8 DNS Traffic Overview

The DNS Traffic Overview page summarizes the traffic flow and its main properties. Several filters can be applied to the data that aid in the recognition of malicious behavior and the identification of suspicious events. Some examples of the filters regard the time of a query, the type of the DNS requests, the identity of the clients, and frequently queried domains.
Additionally, for each query, metadata can be previewed and further intelligence is provided via a single click.

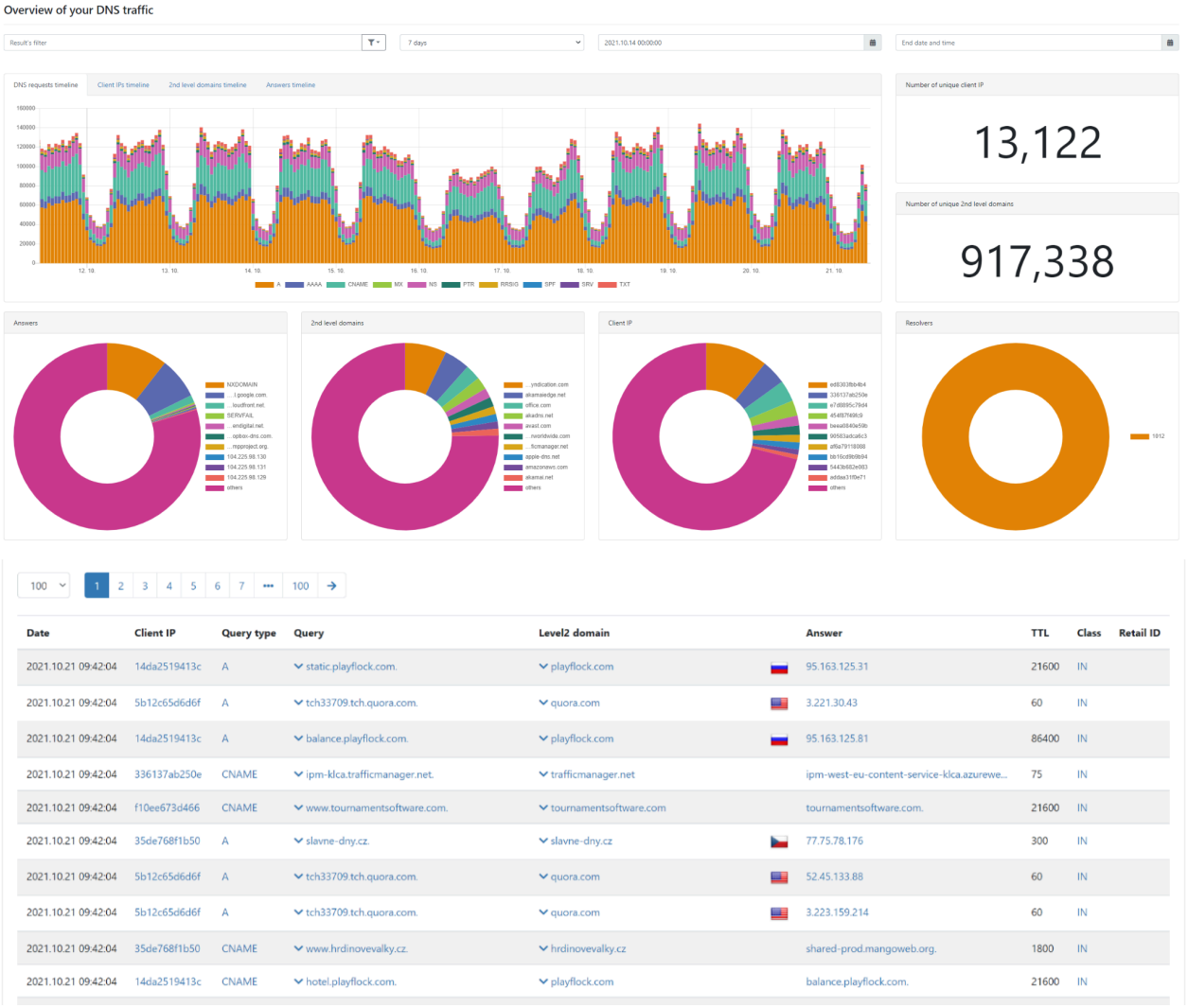


Figure 13: DNS traffic dashboard

4.1.9 Reporting and Alerting

4.1.9.1 Periodical reports

Whalebone Peacemaker is designed to work well without much intervention from the administrators. Even though some incidents should not be taken lightly and duly investigated based on their severity, some patterns become evident only in a longer time frame. For these purposes the admins are able to configure daily/weekly/bi-weekly reports that summarize the incidents and network traffic in a comprehensive pdf document.

Figure 14: Periodical report example

4.1.9.2 DNS traffic anomaly alerting

Some events in the network traffic do not pose a threat when isolated but when aggregated over a longer time period, might indicate a DDoS attack, an ongoing spam campaign or an active DGA malware. If proper actions are taken, customer complaints or blacklisting of entire IP segments can be predicted and avoided. Whalebone offers a variety of alerts that can be fine-tuned for each network with regards to its size, clients and history.

4.1.9.3 Security incident alerting

Whalebone Peacemaker can alert you in case a serious infection is found in your network. Incidents of C&C and DGA types are the most severe and if found on a piece of internal network hardware, can compromise the whole network and expose it to additional attacks.

4.1.9.4 Resolver health alerting

Uninterrupted service operation is crucial for any successful ISP. The resolver is able to alert the administrators in case of insufficient hardware resources (high CPU/RAM/HDD utilization), DNS resolution failure or a failed attempt to connect to Whalebone Cloud.

4.1.10 Service Line (Retail) Operator's View

The Service Line Operators are given access to an interactive interface from where they have access to the end-users' service details and the status of individual subscriptions. This view is only available for Peacemaker Profit type of deployment

Some of the functionalities that Operator's View supports are:

- Access to all End-users' details (the End-user's identifying information can be limited to internal identifiers or more detailed)
- Access to the configuration of end-users' devices
- Option to modify customers' whitelists and blacklists
- Option to change the reporting and alerting settings of the customers
- Option to change the per device filtering configuration
- Option to modify the subscription status of the end-users

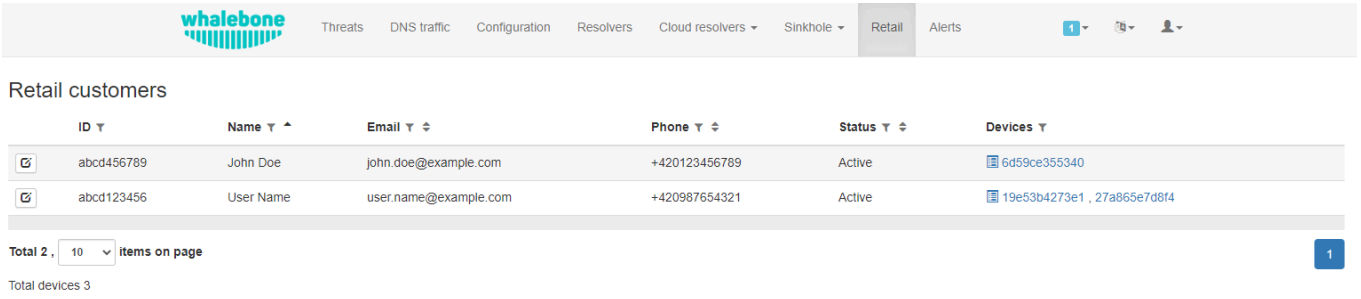


Figure 15: Service Line Operator's Main View

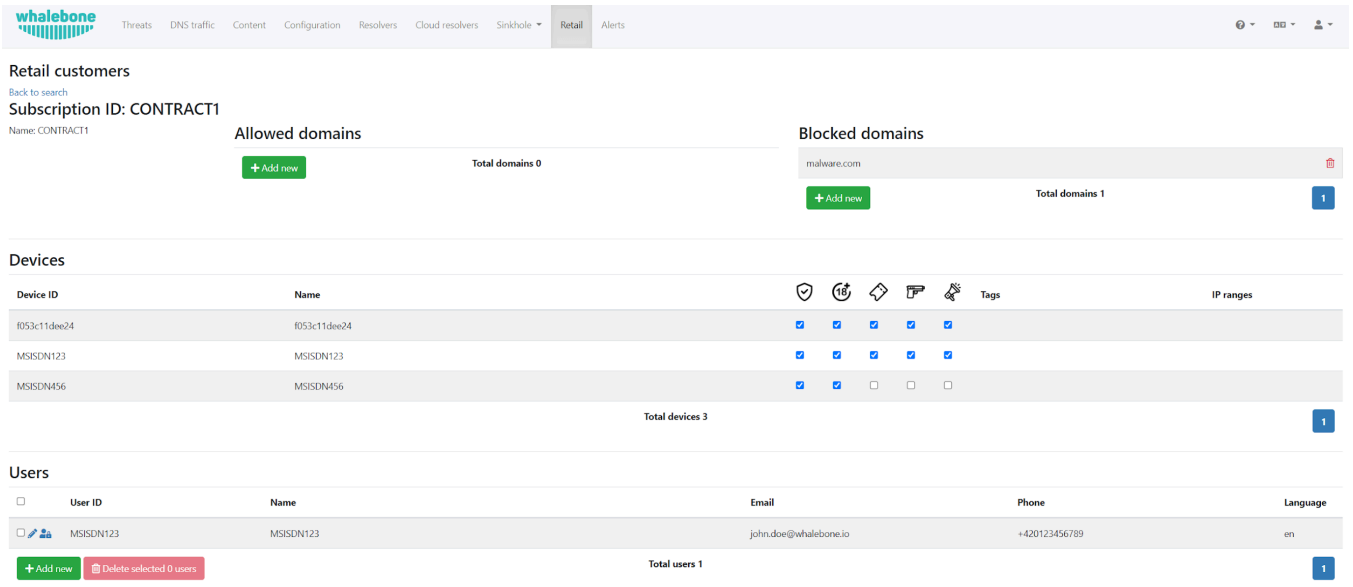


Figure 16: Service Line Operator - Edit Customer

4.1.11 Audit Trail

It is important to note that Whalebone provides an audit trail of all the actions that are taking place on the Administrator Portal. Access to this data can be achieved either through the API or from a dedicated view on the Administrator Portal.

4.1.12 Acquisition and retention features

Whalebone provides various possibilities on how to communicate with the customer, ensure successful acquisition and care for retention. ISPs can choose the most suitable mix of communication channels to comply with the particular business case. All of the communication paths are fully configurable and customizable in terms of visuals and copywriting. The provided acquisition and retention features are presented in the following sections.

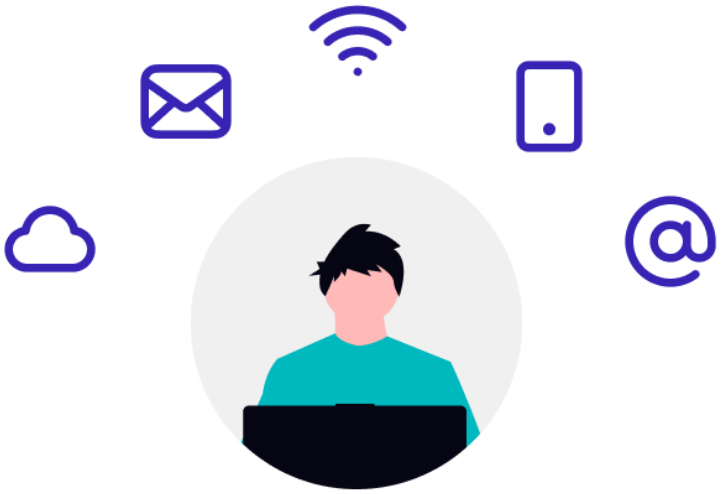


Figure 17: Acquisition and retention of customers

4.1.13 Data retention

As soon as Whalebone Peacemaker blocks a DNS request, the action is logged and immediately visible in the GUI. Logs of incidents are accessible for 90 days, while the logs of all DNS traffic are kept for 90 days. Upon request we are able to provide historical logs for up to 6 months in the past. After this period, all logs are deleted permanently.

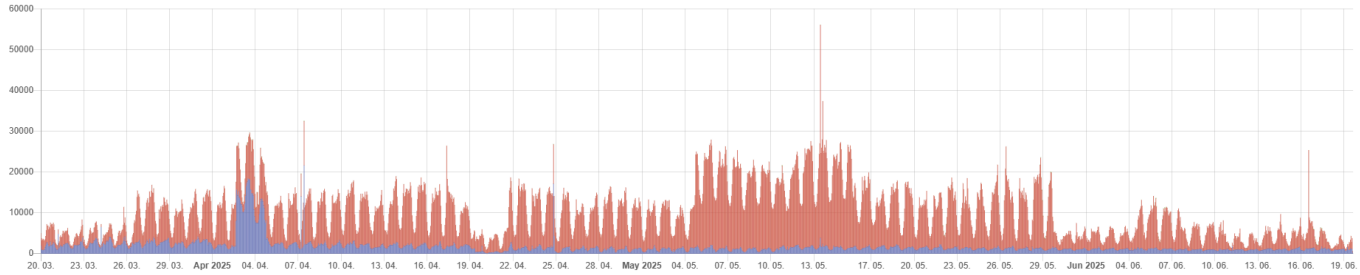


Figure 18: Data retention

4.2. End Customer Portal

The End Customer Portal is an end-user focused web interface that could be completely rebranded based on the ISP's default look and feel. It is designed as a single-page application (SPA) thus, it is convenient for integration to other applications. Some features that the portal provides are:

- Accessibility through Single sign-on (SSO) from the ISP's Customer Care portal and/or mobile application. Supported Single sign-on methods:
    - OAuth (OpenID)
    - Central Authentication Server (CAS / SAML)
- Ability to run on an ISP-specific domain (e.g., security.isp.com)

It is important to state that all the End Customer Portal's features are also available to the ISP through an API and can be integrated into existing applications and processes.

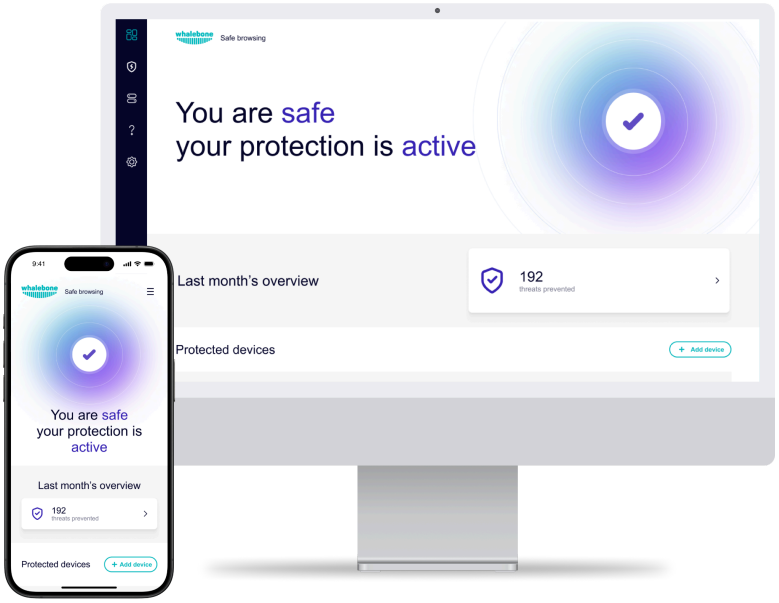


Figure 19: End Customer Portal dashboard – fully responsive

4.2.1 Security Filtering

Security filtering configuration allows the End-users to enable and disable filtering of particular threat categories. Individual pre-selected categories can be provided or all of them can be grouped under the term “Security”. The categories in End Customer Portal are presented at a higher level in order to keep the information simple and understandable for the End customer and not to overwhelm the End-user with technical details and various threat aspects.

Threat categories available for blocking and enabled by default are:

- Malicious domains – domains actively spreading malware, distributing variants of coin miners, ransomware and redirecting the End-user to exploit kits
- Malware activity – domains used by malware to coordinate their activity and communicate with botnet operators
- Phishing pages – websites trying to trick the End-user into entering sensitive information including the payment card details, passwords, etc. The phishing pages also include the general scamming schemes that try to sell non-existent or fraudulent products

The final decision depends on the product manager and the level of detail that they would like to provide. Internally, Whalebone has the following more granular categorization of domains:

- C&C (Command and Control): domains that facilitate botnet communication for coordination of their activity
- Malware: domains that host and distribute malware
- Phishing: domains aiming to trick End-users and extract sensitive information such as credit card details, login credentials etc.
- Blacklist: domains that are known to serve multiple nefarious purposes
- Exploit: domains that host code which aims in hijacking the End-users’ web browsers and spread malicious software
- Spam: domains that are linked with the spreading of spam email messages and scam offerings
- Compromised: legitimate domains that have been hacked and are temporarily used for malicious purposes
- Coinminer: domains linked with hijacking CPU resources and crypto mining activity

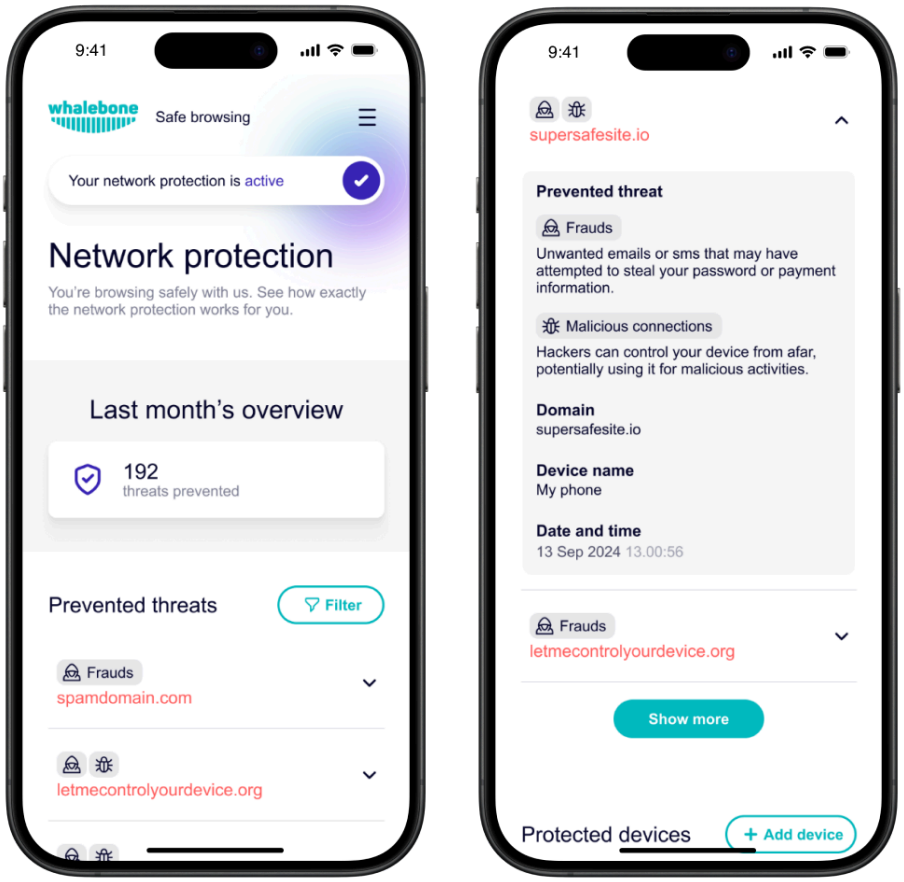


Figure 20: Security filtering setting - mobile app

4.2.2 Content Filtering / Parental Control

Content filtering uses the same filtering principles as the Security filtering, but applies different datasets to the end End-user traffic. The main goal of this feature is to protect end End-users (mainly children, thus Parental control) from the unwanted content hosted on the Internet websites. Blocking of the content goes usually without the possibility of bypassing the Blocking page, however this is a configurable parameter.

Configuration possibilities and examples
Different content categories are available for the access restriction configuration. Each category can be allowed or blocked. The entertainment category provides the possibility of extended configuration via scheduled access. As in the case of the security filtering, Whalebone's database consists of a more granular categorization of the domains. For a simpler End-user experience the following high-level categories are suggested:

- Adult – includes pornographic content and content destined for the adult audience only
- Entertainment – sites used for entertainment purposes, such as social networks, games, video streaming websites and similar.

    - Entertainment domains can be allowed during particular hours and days during the week.
- Crime – websites with content about illegal activities including violence, drugs, terrorism and other similar in nature
- Advertisement – domains used to deliver advertisement and tracking of End-user activity

An overview of the available categories is provided below:

- Sexual Content: sexual and pornographic material
- Gambling: games and activities involving betting money
- Weapons: guns and weapon-related sites
- Audio-video: audio and video streaming services
- Games: online games and gaming websites
- Chat: instant messaging and chatting applications
- Social-networks: social networking sites and applications
- Drugs: drug related websites including alcohol and tobacco
- Racism: content linked to racism and xenophobia
- Violence: explicit violence and gore
- Terrorism: domains linked to terrorism support
- Child Abuse: domains related to child pornography
- Advertisement: banners, context advertisements and other advertisements systems
- Tracking: web and email tracking systems
- Coinminers: domains connected to crypto-currency mining activities
- DNS over HTTPS: third party DNS over HTTPS endpoints
- Peer to Peer (P2P): domains that are used for the operation of peer-to-peer networks

4.2.3 Time-based Blocking

There is an option to configure content filtering categories to be actively blocked in a schedulable manner. The scheduling can be configured for specific days or hours of the day. An example use-case is a parental control scenario where the devices of the children are restricted access to social media websites after 10 p.m. during the week days.

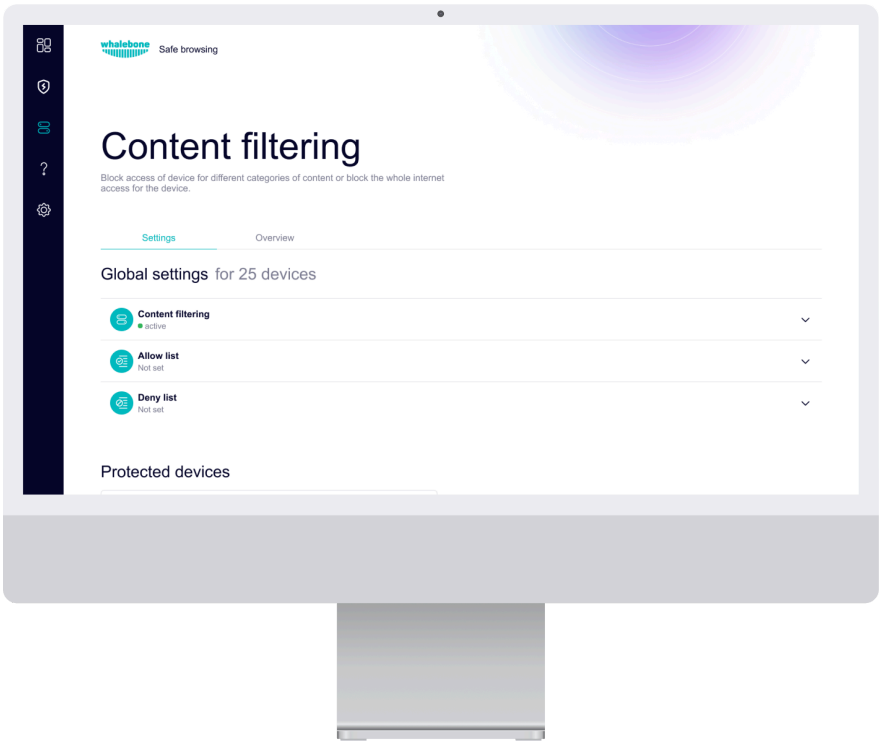


Figure 21: Parental / Content control

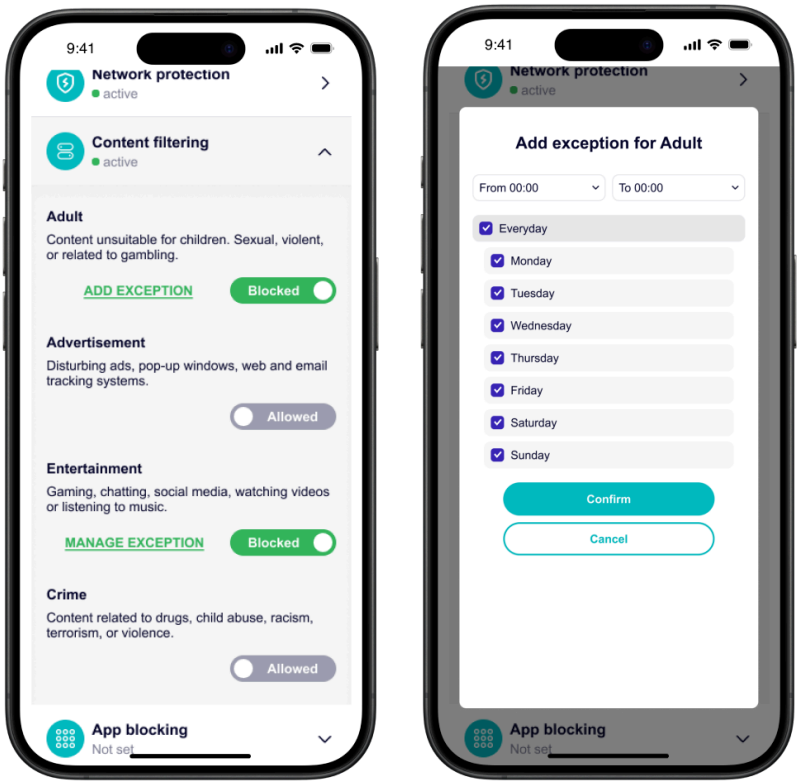


Figure 22: Parental / Content control management

Configuration examples and use cases:

- Parental Control configuration is individual and is assigned to each device (router, fixed connection line, etc.) individually.
    - Example: Peter is allowed to visit entertainment websites, but Julia is not.
- Parental Control management portal is available to chosen administrators that are assigned the proper permission roles. This is usually used for families and companies where only the chosen End-users should be able to modify the setting for all the devices.
    - Example: Family has licenses for each member, but parents have just Security filtering active and children have also Parental Control enabled. But the only one able to manage the settings is the father who is the main contact person.
    - Example: Company administrator sets the Content Filtering to the employees, but no other employee is able to disable the restriction.
- In case the End-user tries to visit the restricted category there are two multiple options how to respond, recommended setup (can be reconfigured as per ISP request) is as follows:
    - For Advertisement and tracking domains return a non-reachable destination (like 0.0.0.0) as this approach has the best End-user experience results. The pages are fast to load and their functionality does not break.
    - For other categories display a localized and ISP branded Blocking page explaining why the access to the particular domain has been restricted

4.2.4 Custom Allow / Deny lists

One of the End Customer Portal's major features is the ability to configure the filtering options, including custom deny and allow lists for every End-user, according to their own preferences. The ability to configure their own filtering presets gives the End-users significant power over the service's behavior. Additionally, the ability to configure the custom allow lists is a very efficient way to deal with any blocking that could be considered as a false positive by the End-user, without having to contact the support team.

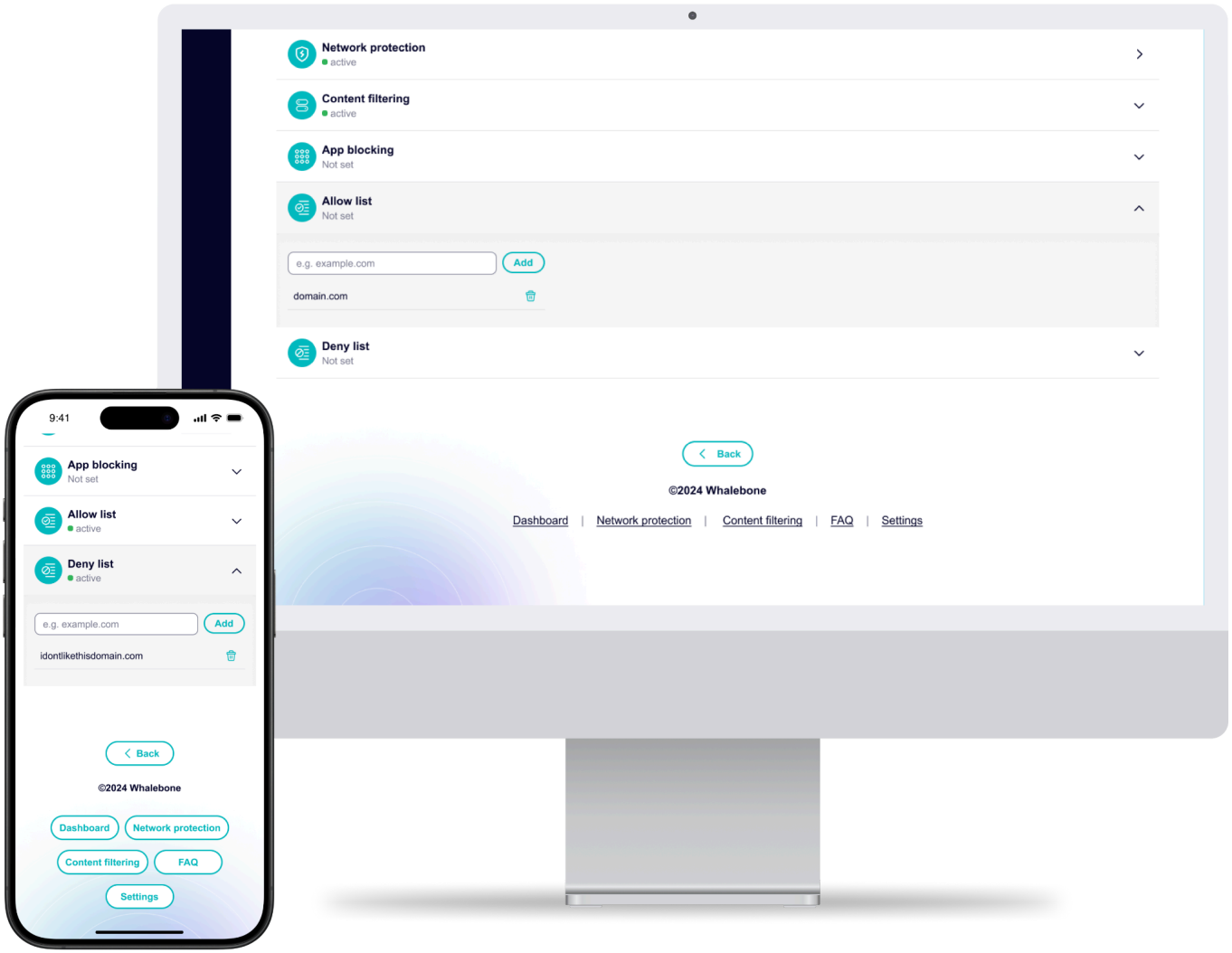


Figure 23: Individual allow/deny list setup

4.3 Blocking or pop-up page with single click purchase

A multitude of options (or a combination of these) is available for displaying on the Blocking page. Some examples are:

- Available “Continue anyway” button
- Direct purchase option during trial period (provided through the blocking page in the case of a security incident with a single click purchase)
- Number of threats currently in the net / number of blocked threats in the network in the last xx days

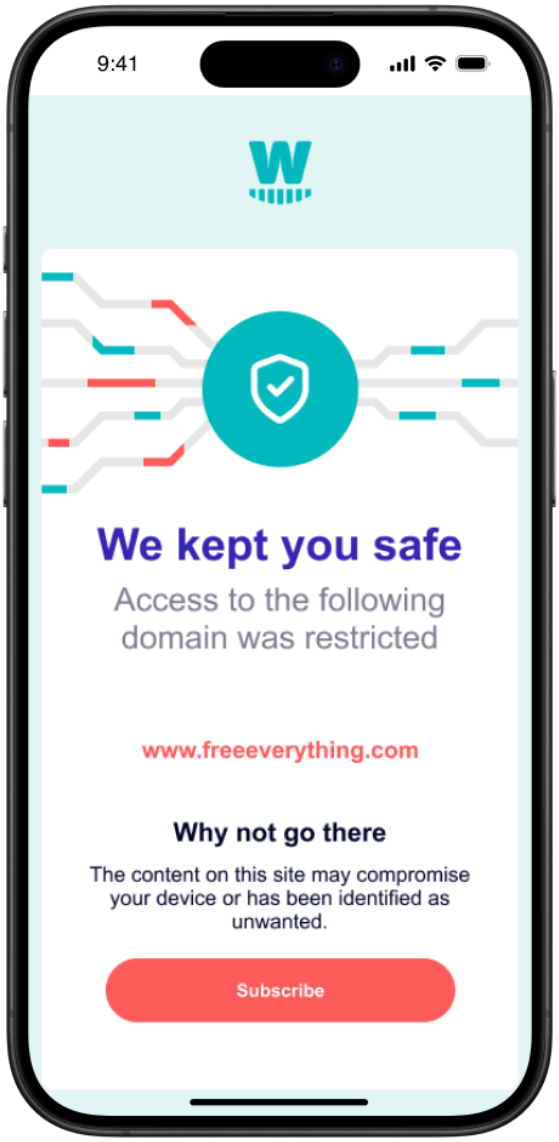


Figure 24: Blocking page

A Pop-up page can be displayed with various messages such as:

- Direct purchase capabilities during trial period
- Blocking page in case of a security incident with a single click to purchase
- Pop ups displayed during trial period *(European and national legal requirements considering Net neutrality shall be carefully considered)*
- Number of threats currently in the net / number of blocked threats in the network in the last xx days

4.4 API

Whalebone provides a robust API suite designed to facilitate seamless integration with external systems. The API enables access to extensive data collected by Whalebone's resolvers and supports both data retrieval and configuration management. The API documentation is organized into two main schemas: one for accessing event data and another for managing settings and configurations.

- Event Data Schema:
  Use this schema to retrieve incidents, DNS traffic data, and resolver metrics. It is ideal for monitoring, reporting, and integrating with business intelligence (BI) systems or ISP platforms. The schema supports advanced filtering, pagination, and efficient handling of large datasets.

- Configuration Schema:
  This schema allows you to configure resolvers, update policies, and manage allow/deny lists. It also provides endpoints to retrieve and update resolver settings, enabling automation and streamlined management of security policies.

- Retail API/Schema:
  The Retail API is tailored for ISP systems and BI services, enabling the ingestion of comprehensive End-user behavior and incident data. This rich dataset supports detailed analysis of individual End-user security exposure and overall behavioral trends. The API is extensively documented and includes an interactive online application for developers, offering both an overview and hands-on access to all available endpoints. The API provides options to create and set up subscriptions for different End-users to provide End-user experience of the configuration of their own policies. The full capabilities of the Retail API become apparent when working with large-scale, real-world datasets, such as tens of thousands of events. This allows service providers and analysts to leverage the API for advanced analytics, reporting, and security insights. API documentation and interactive tools are available here.

Authentication to the API is required for all End-users and is managed via an Access Key and Secret Key. These credentials can be generated and managed under the "API keys" section in the End-user account dropdown menu.

4.5 Multitenancy

Whalebone Peacemaker Profit service features advanced multitenancy, designed for organizations with complex structures and for ISPs aiming to deliver managed security services to SMBs or enterprise customers. Multitenancy enables ISPs to operate as managed service providers (MSPs), allowing them to manage larger customers and offer Whalebone's security products as an added-value service or as a standalone offering.

The multitenancy dashboard organizes managed tenants in a tree structure, supporting enterprises with multiple branches, ISPs with B2B customer bases, managed service providers, and business distributors. This structure ensures clear data separation between organizations while maintaining centralized and efficient configuration and management.

Permissions can be defined at the parent organization and inherited by child tenants. Roles include Owner (for organization management), Admin (for tenant configuration), and Viewer (for security analysts), supporting both broad oversight and delegated administration. This enables ISPs to grant their customers access to their own dashboards or manage all tenants centrally.

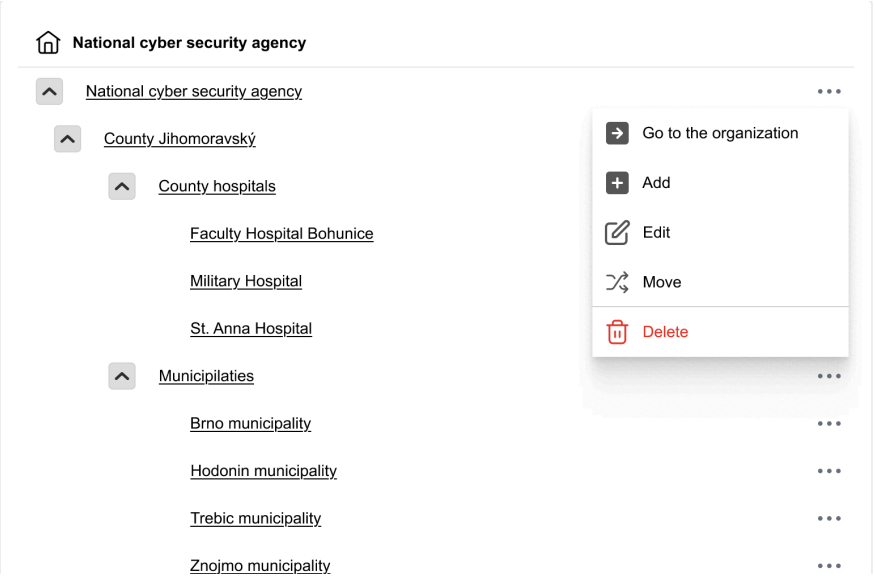


Figure 25: Multitenancy dashboard example

4.5.1 Use Case for ISPs

ISPs typically maintain separate accounts for each customer within the multitenancy dashboard. This enables them to provide or sell Whalebone's security product as an additional service on top of the internet connection. ISPs can manage security policies, monitor threats, and deliver value-added services efficiently. Multitenancy in Whalebone Peacemaker Profit thus empowers ISPs and large organizations to scale security management, streamline operations, and deliver tailored security services to diverse customer bases all from a single, unified platform.

4.6 Off-Net protection

Along with the main solution, Whalebone provides an end-point client that facilitates off the ISP's Network (Off-Net) protection. The purpose of this client is to securely communicate any traffic from End-users' devices that is not routed directly through the ISP's resolvers. Examples of this scenario are public hotspots or insecure Wi-fi networks in office environments. By using the Off-Net client, ISP's End-users can stay secure in any part of the world.

The foundations of Off-Net protection are the available mobile applications. These endpoint clients are able to initiate and preserve a secure connection to Whalebone's resolvers in the ISP's environment. In this way, the DNS traffic is filtered and the threats are cut off at the root.

Even though the connection is travelling through the public Internet, its confidentiality and integrity are ensured by using industry-standard TLS cryptography. Whalebone is in a place to guarantee the security of the connection as the solution incorporates the latest advancements in DNS technology. A prevalent example is the DNS over HTTPS (DoH) paradigm that is adopted from the mobile applications and via which the connection securely reaches the ISP's environment.

An overview of the Off-Net protection can be found in the following diagram:

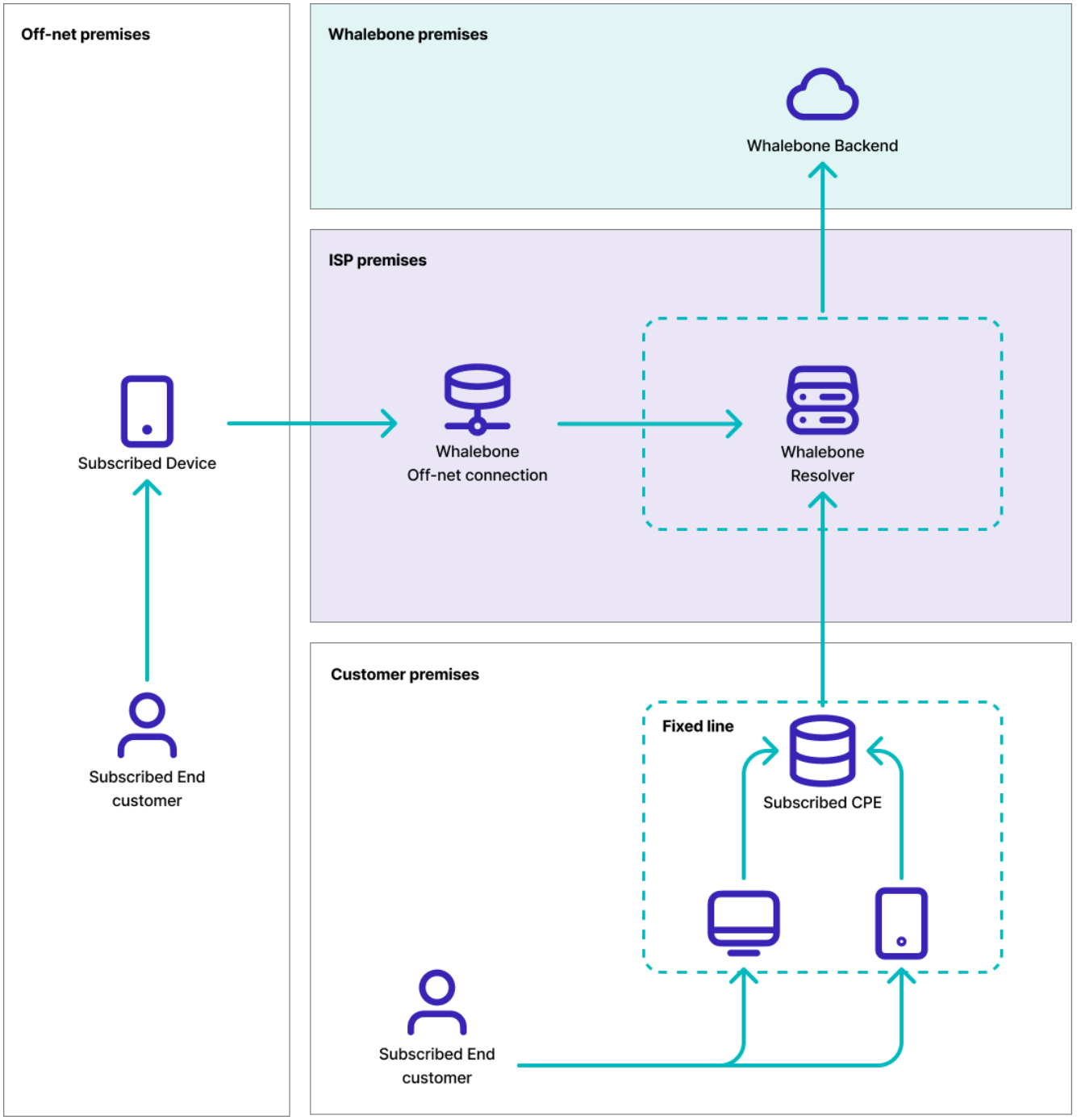


Figure 26: High-Level Deployment diagram

4.6.1. Deployment

Whalebone's Off-Net protection allows the ISP to choose between two types of deployment to the end customer.

The first option is to incorporate the **provided SDK** directly into one of the existing ISP's mobile application. This could be presented to the end-users as a new feature and could be seamlessly integrated. A multitude of modifications and adjustments are possible, as the ISP has complete control over the provided SDK and the way it interacts with the current application.

The second option could be to take advantage of the **standalone application** that is provided and branded by Whalebone. The application is designed in the Whalebone brand and the ISP is not able to label it with its own coloring schemes and copywriting. Available and supported is the application for iOS and Android.

Whalebone's Off-Net application has been built to be compatible with the majority of the versions of the most popular operating systems. As a result, it supports:

- iOS 13.4 and later
- Android 5.0 and later

4.6.2 How the Off-Net works

The Off-Net protection that Whalebone provides is utilizing a secure VPN connection that, unlike other off-the-shelf VPN solutions, Off-Net **tunnels only the DNS data**, while leaving the rest of the traffic to reach the Internet directly.

In this way, the end-users do not notice the difference when using the Off-Net protection, as there is no impact on the connection speed, stability and latency.

In more detail, the VPN profile that is installed on End-users‘ mobile devices connects directly to Whalebone's resolvers in the ISP's premises. This connection is initiated using a certificate that uniquely identifies the valid end-users to the ISP. When an End-user tries to connect to a domain, a new DNS over HTTPS request is being routed to the aforementioned infrastructure (step 1 in Figure 44). The answer is tunnelled back through the same connection without any additional delay (step 2 in Figure 44). This answer is filtered by Whalebone's product and thus malicious requests are prohibited from being resolved. As a result, the end-user enjoys the offered protection and can surf the Internet with peace of mind (step 3 in Figure 44).

The outcome of this process is, that even though the End-user could be on any hostile network environment around the world, both security and privacy are achieved and the integrity of the requests can be guaranteed by the cryptographic functions that are built in the process.

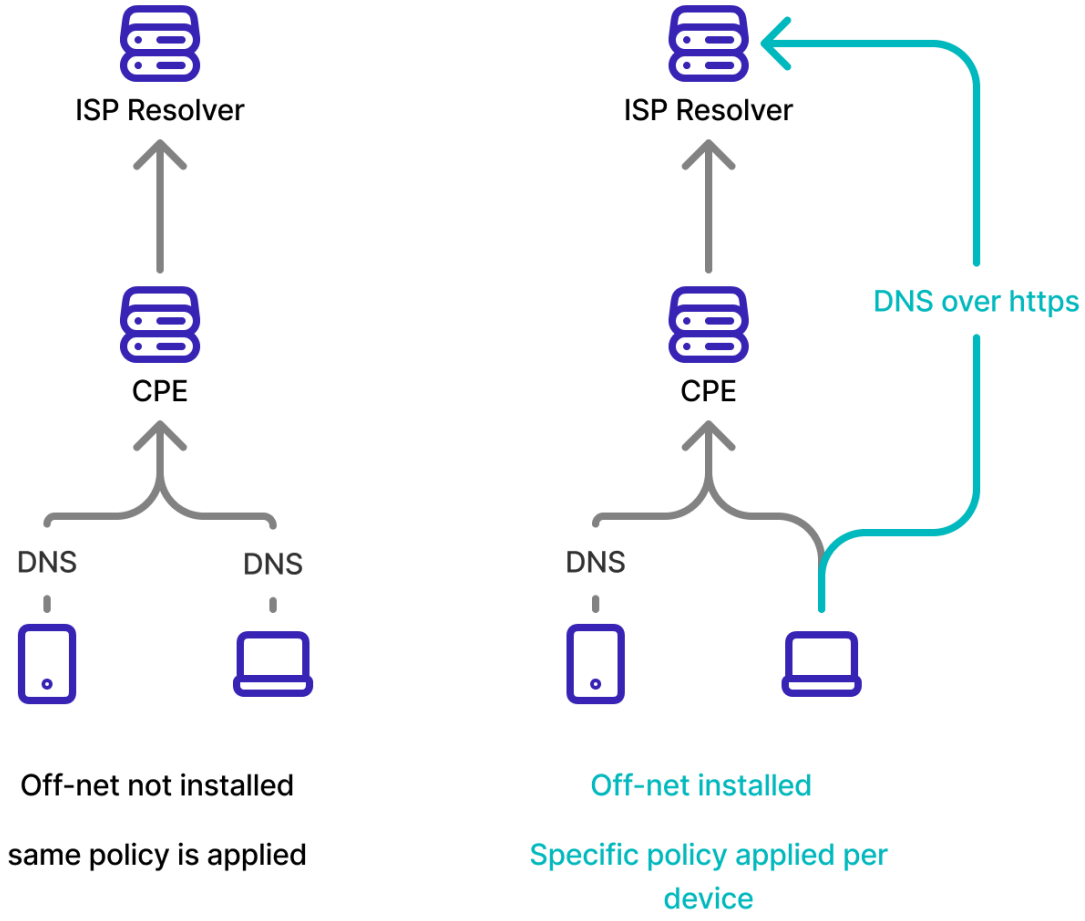


Figure 27: Overview of Off-Net Solution

4.6.3 VPN Connection Setup

In order to establish the new VPN connection, there is a procedure that is implemented in the SDK and the standalone application. The SDK version can be customized to any extent by the ISP.
For the connection to work and allow only legitimate End-users to utilize the ISP's security enhanced resolvers, custom VPN profiles are used. These profiles uniquely identify each End-user and allow the legitimate utilization of the resolvers.

In order to achieve this, during the first time that a End-user enables the service on their mobile devices, a
pairing takes place that generates a unique Application Token. This pairing, depending on the Telco's preferences can take place either on the End Customer Portal, that is provided by Whalebone, or in the case of the SDK integration directly in the ISP's backend. Following, the token is used to acquire a set of
Access and Secret Keys. These keys aid the process of the certificate generation and can be used to

issue newer certificates during the revocation process.

After this process has been completed, an End-user has an installed VPN profile on their device that facilitates the **mutual authentication** with the resolvers and protects the integrity and privacy of the subsequent connections.

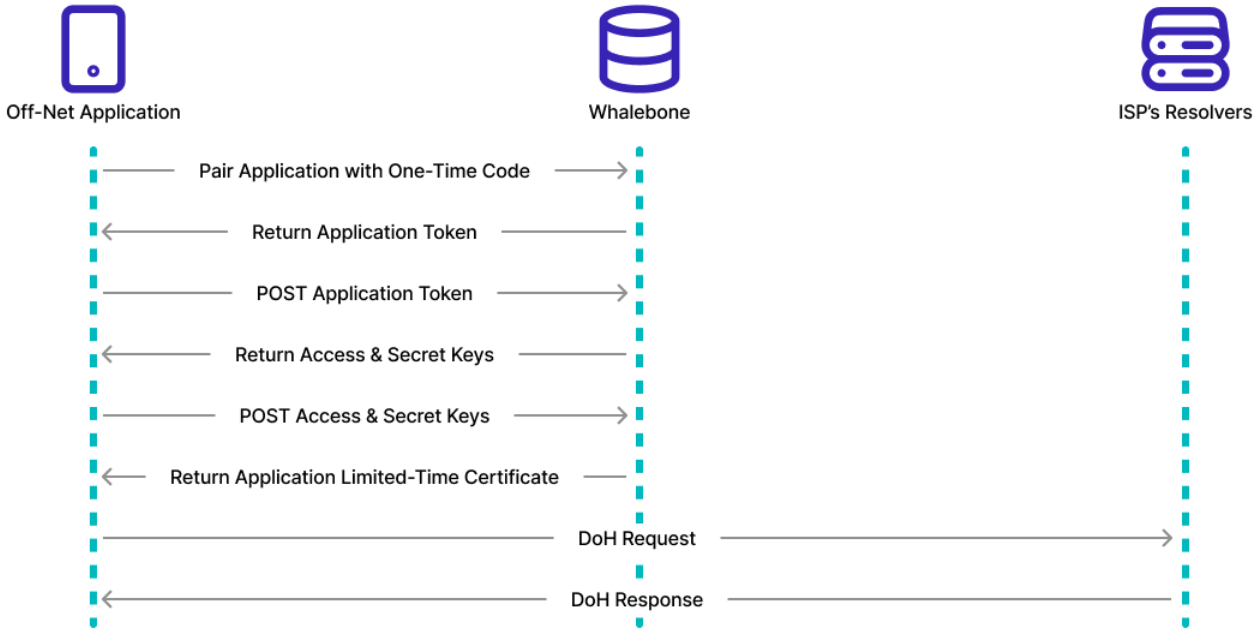


Figure 28: Sequence Diagram of the VPN Connection Setup

4.6.4 Device pairing with the subscription

During the pairing procedure, the End-user is asked to provide either a security PIN or scan a QR code. This functionality aids in the acquisition of the unique Application Token.

It is evident that if the SDK version is selected the end-users could be enrolled automatically without any additional steps. In this case the End-users would be seamlessly identified and would directly access
the security service.

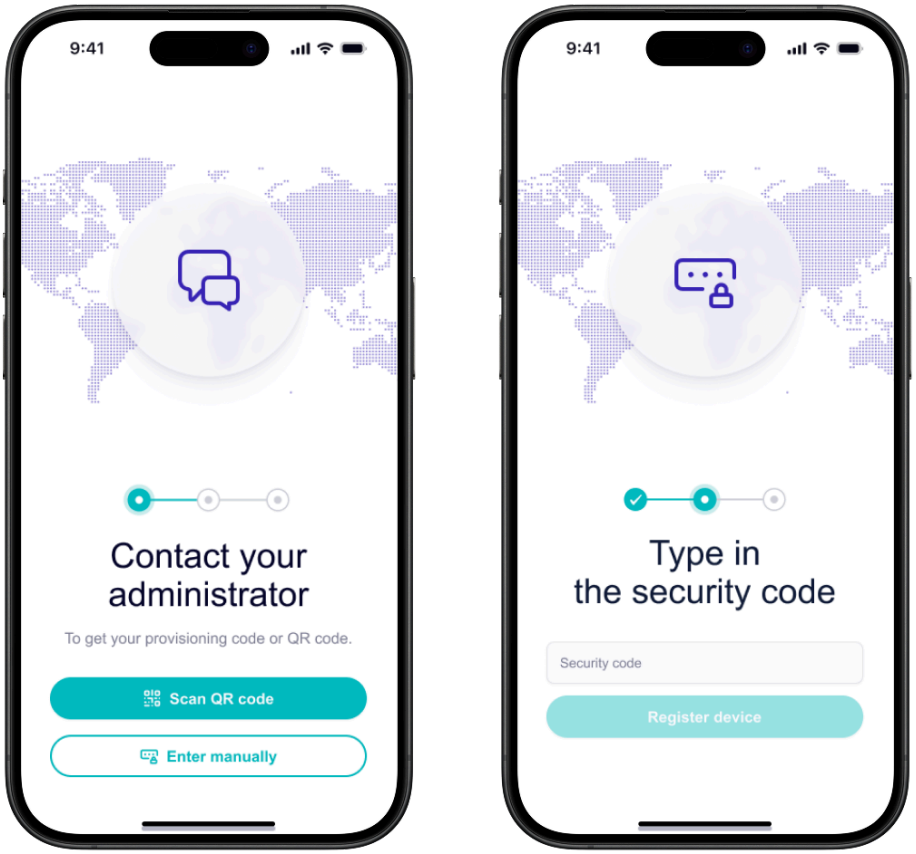


Figure 29: Off-Net Authentication in case of standalone app

4.6.5 Service Provisioning

In the main page of the Off-Net protection application, the End-user can enable or disable the service. The
end-users are only presented with an intuitive interface that allows them to enable and disable the service via a single click.

In a technical level, the enabling of the service can be translated as the initialization of the VPN connection that will filter only the DNS requests. The installation of the VPN profile is **a one-time operation**.

In the case of the SDK integration, the Telco may choose to present this option in a completely different way that could be considered as **“Single Click Protection”**.

The service enabling/disabling functionality in the standalone application can be depicted in the following figure:

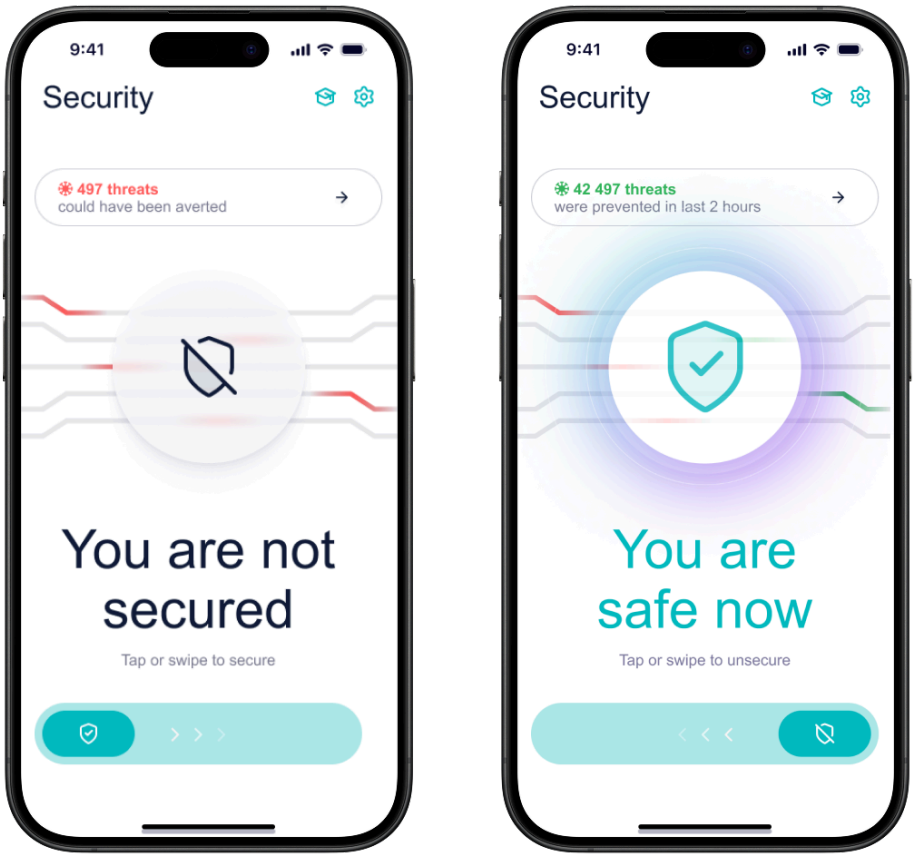


Figure 30: Service Enabling/Disabling

4.6.6 End-user Options

In the Whalebone's standalone application End-users are able to **fine-grain its behaviour** based on either the nature of the network they are connected to (mobile data or Wi-Fi) or its name (SSID that is present on each network).

The End-users are able to modify the application's behaviour in the space dimension by choosing the networks that they want the protection to have effect in. To elaborate, there is provided the option to automatically enable or disable the service according to the identified network's name. An example of this could be the case that the service is enabled on all the Wi-Fi networks that the device is connected to, except from the home network that is already protected by the ISPs or vice versa.

As a direct result, the End-users would be seamlessly using the existing ISP's application and would enjoy the security benefits of Whalebone's solution.

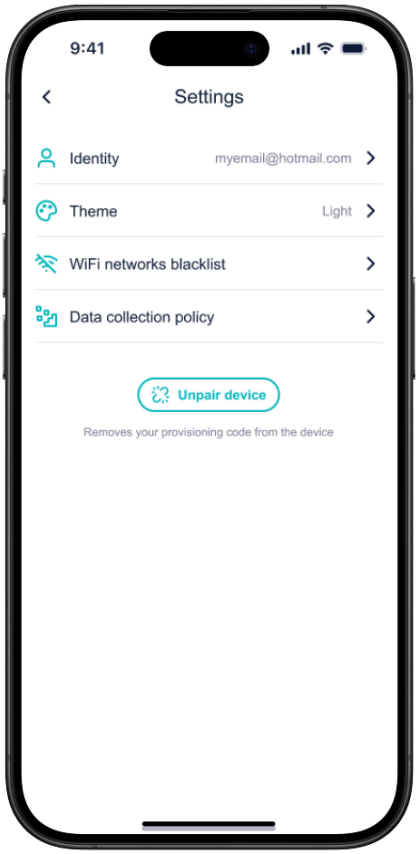


Figure 31: Settings Menu

5. Support

Two tiers of support are available. Basic and Premium support. Costs for each one are defined in the Contract. The tiers differ by their channels and SLA targets and are defined in the table in Chapter 1.2.

5.1 Areas covered by support

Support is provided for all technical matters and issues related to the product. Questions on setup, platform behavior, resolver configuration, resolver performance, resolver stability, API schemas and threat-intelligence-related issues.

5.2 Areas not covered by support

Customer's on-premise infrastructure

The provided support is delineated on the container-level of the Docker daemon of the underlying machine on which the Whalebone Resolver is running. Containers, images and their networking is covered by support, while the operating system, its configuration, version, packages, is not. The support also does not cover hardware-level maintenance (upgrading physical machines, scaling up or scaling down VMs).

Customers' network

The customer's network, its architecture, its maintenance and change management are out of scope of the support. Technical consultants may provide advice or answer questions about planned changes but the responsibility to carry out the changes and maintenance are on the Customer.

5.3 Support communication channels

The main communication channel with the support is the helpdesk, available at helpdesk.whalebone.io. Tickets in the helpdesk can be created via the following channels:

1. Anyone sending an email to the support inbox.
2. Users reporting malicious domains / false positives by clicking the buttons in the dashboards
3. Operators submitting a ticket via the help widget in the Admin Portal
4. Operators submitting a ticket via the helpdesk portal onSupport agents may also create the ticket manually based on communication with the customer.
5. The 24/7 hotline phone number (available for Premium support only)

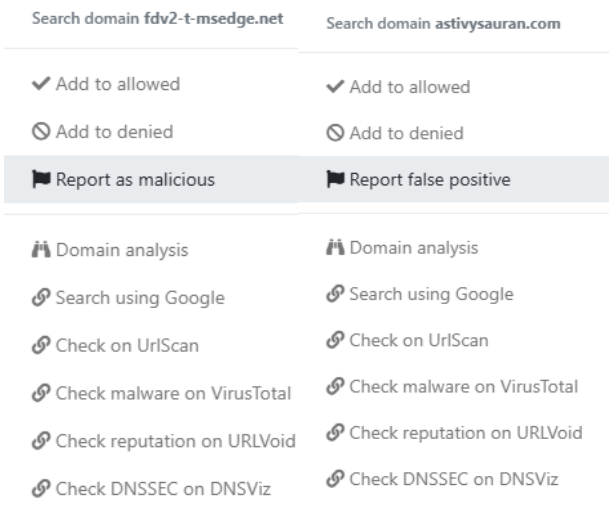


Figure 32: False positive/negative report

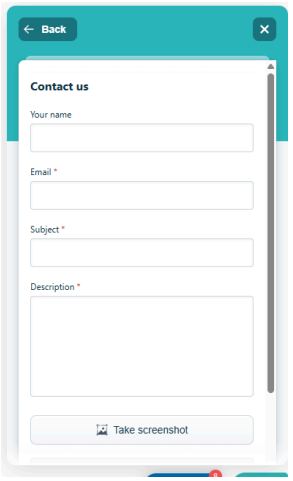


Figure 33: Contact form in administration portal

5.4 Ticket workflow

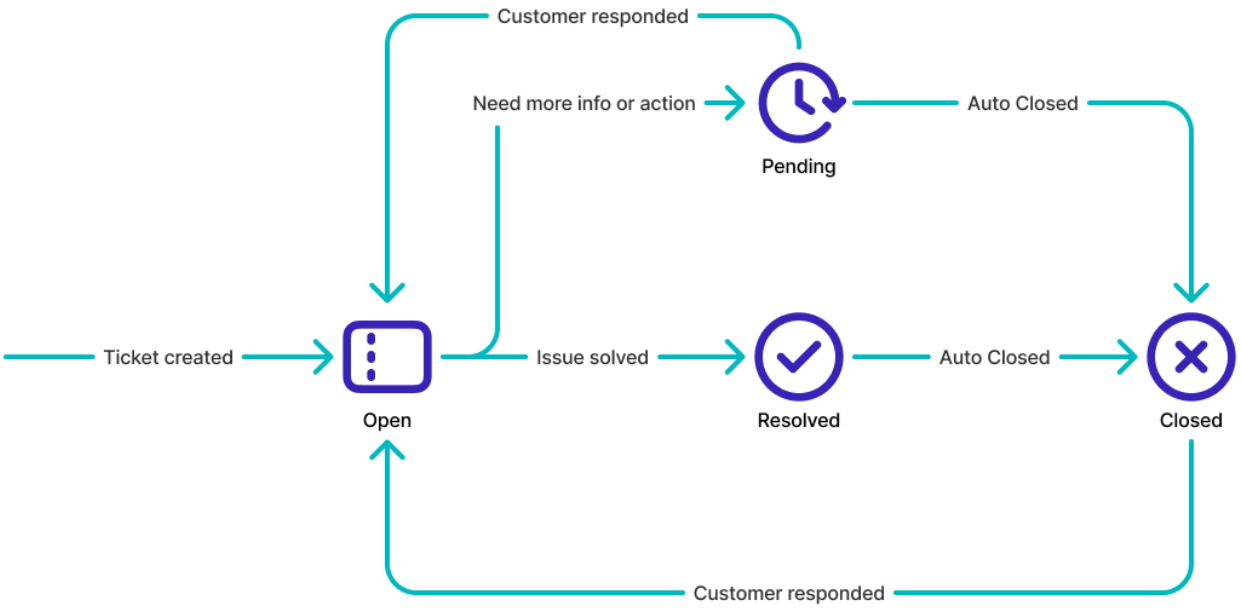


Figure 34: Ticket workflow diagram

- An open state represents a ticket which is awaiting Whalebone's response. SLA timers are running only while the ticket is in Open state.
- The pending status represents a state where Whalebone Support needs to gather more information or is waiting for some action on the customer's side.
- A pending ticket triggers a reminder to the customer after 7 days. Afterwards they are closed after 7 days of inactivity (total 14 days).
- The resolved ticket is automatically closed after 2 days.
- The customer can re-open tickets any time by replying to them (via email or platform)

Each ticket is classified by the Service Desk Agents as either a Service Request (SR), an Incident (IN), or a Change Request (CR) or a False Positive Report (FP). The ticket reporter does not have an option to change or choose the ticket type. Nevertheless throughout the course of communication with the reporter, the type may be changed.

Annex A: Available Reporting and Alerting Features

Property	Frequency	Medium	Availability
End-User Reports Summarizing Threats and Incidents	Regularly (e.g., weekly, bi-weekly, monthly)	Whalebone API	End Customer Portal
Business Reports Summarizing Traffic's Properties	As frequently as it is required	SMTP Server	Product Managers' Email
		Whalebone API	Administration Portal
Technical Reports Summarizing Traffic's Properties	As frequently as it is required	SMTP Server	ISP Operator's Email
Alerts to End-users	Upon Incident/ Subscription End	SMS Gateway	User's Mobile Phone
		SMTP Server	User's Email
		Whalebone API	User's Mobile Push Notification
Alerts to ISP Operators	Upon Incident/ Subscription End	SMTP Server	Operator's Email
		Whalebone API	Administrator Portal
		Slack Webhook	Compatible Slack Endpoint
		Webhook	Compatible Endpoints
		Syslog	Syslog Server

peacemaker@whalebone.io

Whalebone, s.r.o., Jezuitská 14/13 602
00 Brno, Czech Republic

Company ID: 05120403 VAT No.:
CZ05120403