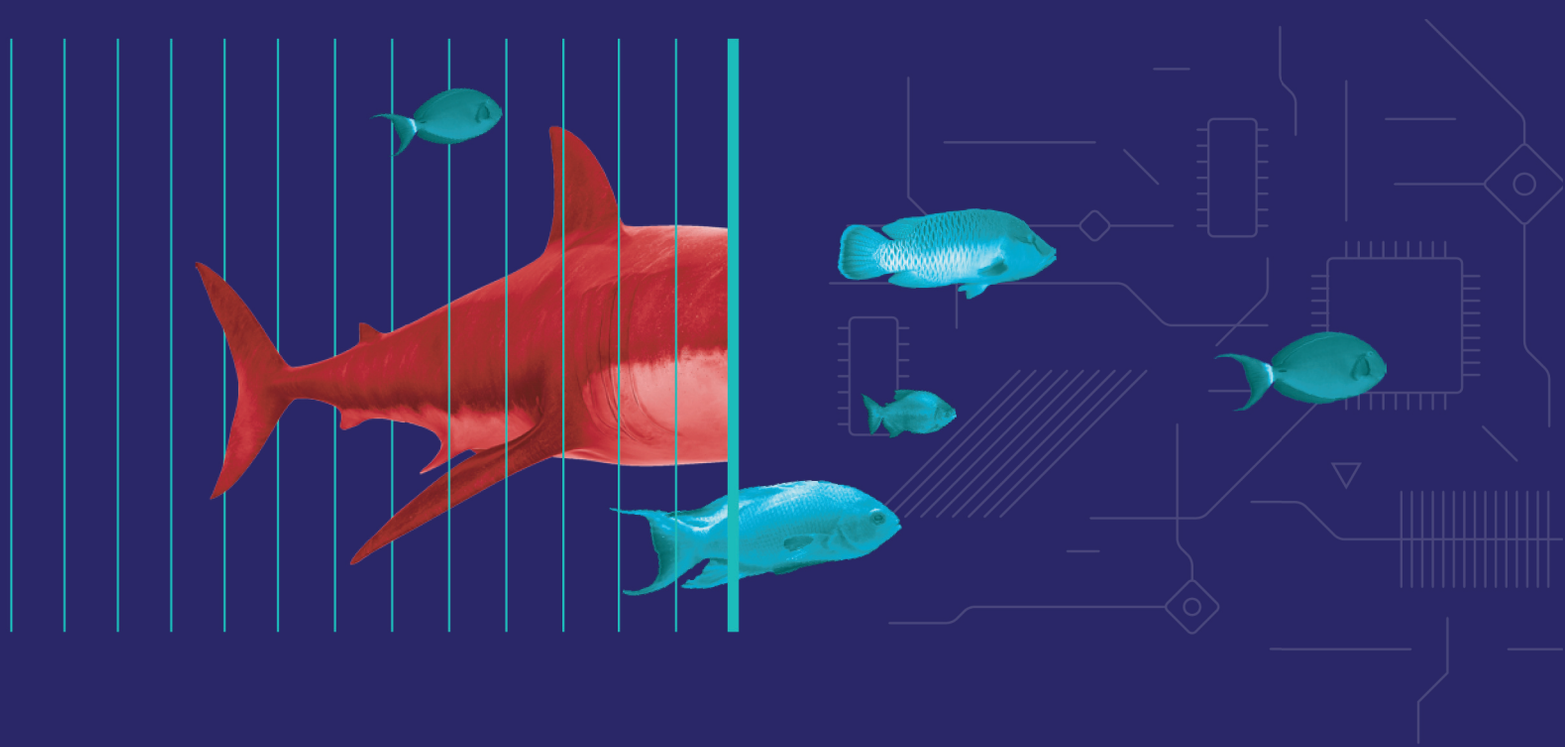
# Převezměte plnou kontrolu nad DNS provozem a zabezpečte slepé místo své sítě

whalebone

Whalebone poskytuje plnou kontrolu a ochranu nad DNS komunikací a překladem, bez ohledu na jejich velikost nebo složitost.

Většina organizací v rámci českého a slovenského trhu v současné době stále nedisponuje přímou kontrolou nad DNS překladem, nemonitoruje DNS provoz a ani tuto komunikaci nijak nezabezpečuje. Ve skutečnosti přitom více než 90% malware využívá v rámci svého životního cyklu právě DNS překlad.

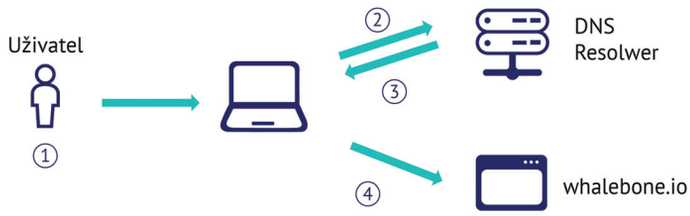


sales@whalebone.io

www.whalebone.io

# Klíčové benefity:

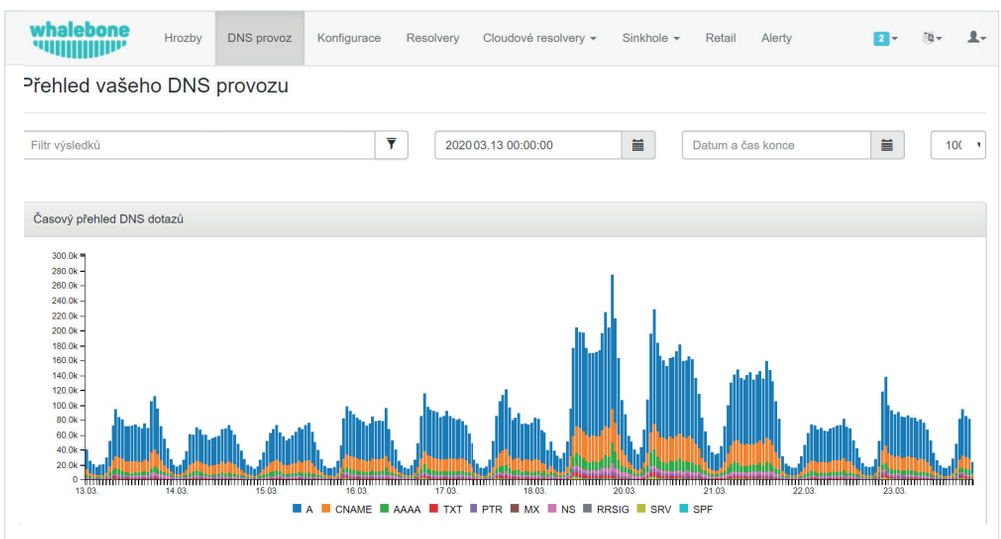
Díky Whalebone získáte schopnost řídit a monitorovat DNS překlad v interní síti z jednoho místa bez ohledu na použité aplikace. Současně tuto komunikaci zajistíte vůči hrozbám využívajícím zranitelnosti v DNS provozu. Nezáleží na tom, zda mluvíme o ochraně vůči kompromitaci e-mailové komunikace, ochraně vůči cíleným phishingovým kampaním nebo vůči škodlivému kódu na síťové úrovni.




1. Chce navštívit whalebone.io
2. Jaká je IP adresa whalebone.io?
3. IP adresa whalebone.io je 88.86.121.135
4. Vidí web whalebone.io

# Komplexní zabezpečení DNS komunikace a její využití v jednotlivých oblastech – use cases:

**1) Plná kontrola nad DNS překladem & řízení přístupu:** Whalebone poskytuje organizacím plnou kontrolu nad DNS překladem díky Whalebone resolver, které se doposud při překladu externích domén spoléhaly na svého internetového providera, u něhož se prováděl překlad. Díky Whalebone získají vlastní správu s možností řídit překlad jednotlivých domén od úrovně celé sítě přes jednotlivé segmenty až po úroveň koncových strojů včetně definování vlastních whitelistů a blacklistů.

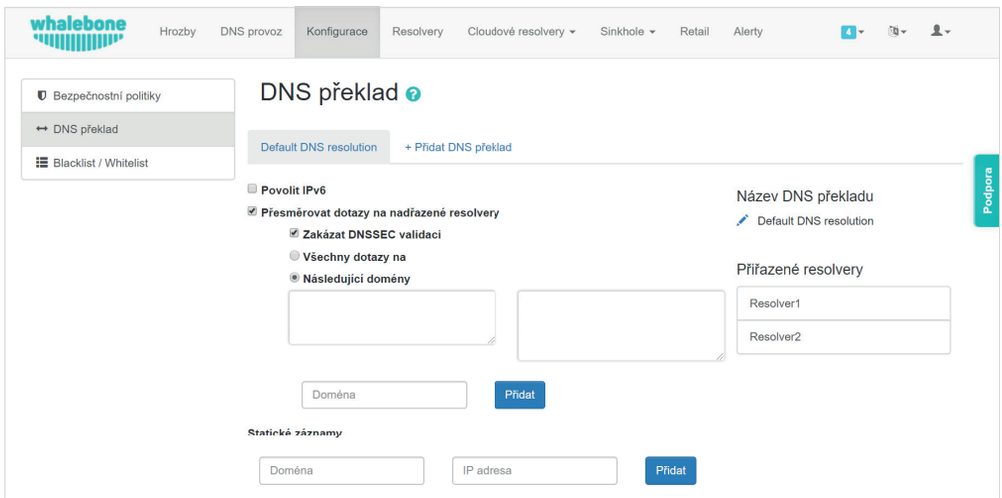



**2) Plná viditelnost DNS komunikace & analýza a detekce anomálií,** kterou dává řešení díky umístění Whalebone resolveru uvnitř sítě, ideálně mezi koncový stroj a doménový řadič s možností umístění od DMZ až před koncový stroj. Takové řešení dává administrátorům plnou viditelnost až na úroveň IP jednotlivých strojů a umožňuje identifikaci stroje s problémovou komunikací. Alerting zjednodušuje práci administrátorům díky nastavení upozornění na výskyt případných anomálií v DNS provozu pomocí předpřipravených šablon alertů zaměřených ať už na bezpečnostní incident, nebo provozní problémy v rámci infrastruktury Samozřejmostí je také možnost vytvoření custom alertů.

**3) Ochrana proti phishingovým kampaním se provádí několika způsoby.**
Whalebone Threat Intelligence databáze blokuje přístup na stránky s phishingem přímo v reálném čase, uživatel se tak na phishingové stránky vůbec nedostane.
Pokud jde o specifický phishing vytvořený přímo na danou organizaci a využívá doménu podobnou doméně zákazníka (např. na doménu „spolecnost.com“ použije útočník doménu „spolecnost.com“ s velkým „I“ namísto malého „L“), je možné i takové chování na úrovni DNS automaticky zachytit.

Pokud by k phishingu přece jen došlo, komplexní přehled DNS provozu umožňuje zjistit, které zařízení přeložilo podvodnou doménu, a tím dodá základní informace pro spuštění procesu změny přístupových údajů pro uživatele, jehož přístupové údaje mohly být kompromitovány.

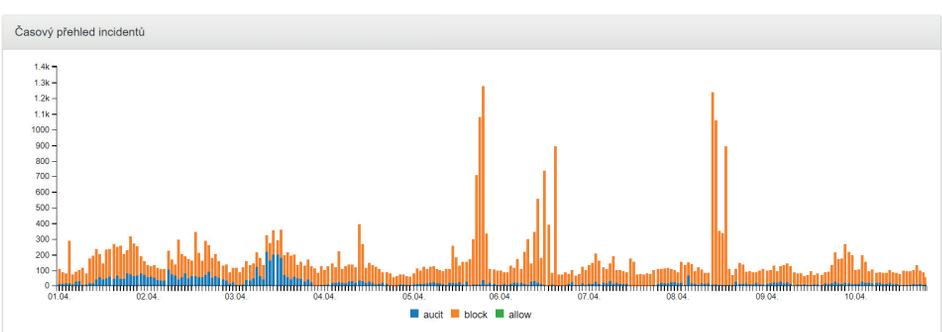
**4) DNS Firewall (pro Office 365, Skype for business a vybrané interní aplikace)** Microsoft pro službu Office 365 požaduje schopnost koncových bodů překládat externí domény a výjimku z filtrace na proxy. Tento požadavek často naruší bezpečnostní architekturu a bezpečnostní politiky.

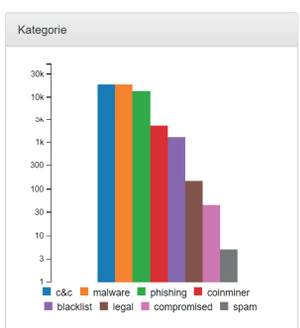


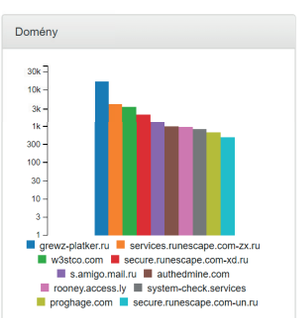

Tyto problémy řeší Whalebone jako DNS Firewall, který se využívá pro filtrování komunikace a domény patřící službám, jako jsou Office 365, Skype for Business nebo interní aplikace. Tyto domény jsou přímo překládané přes Whalebone, přičemž ostatní externí mohou být povoleny pouze přes webovou proxy. Tím se zachová původní záměr bezpečnostní politiky a bezpečnostní architektura zůstává nenarušená.

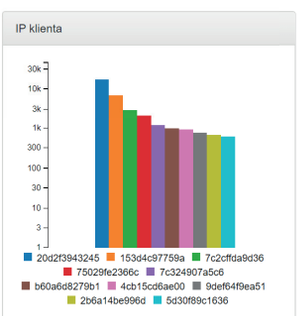
**5) DNSSEC validace je klíčová** pro zajištění integrity a autenticity odpovědí na DNS dotazy odcházející ze sítě. V některých případech se jedná o zcela zásadní podmínky ochrany provozu – zejména **pro zajištění důvěrné e-mailové komunikace s vybranými partnery.** Nezáleží na tom, zda jde o komunikaci vedení společnosti o strategických záležitostech s mateřskou organizací, pracovníky finančního oddělení při komunikaci s bankou, výzkumných pracovníků komunikujících s externími partnery či zaměstnance právního oddělení se zastupujícími advokáty. Validací DNSSEC zamezíte zneužití zranitelnosti SMTP protokolu vůči změně MX záznamu odpovědi, kterou mail server od odesílatele dostane při požadavku na IP adresu mail serveru přijímajícího elektronickou poštu a odeslání důvěrné komunikace útočníkovi.

**6) Ochrana proti škodlivému kódu a škodlivé komunikaci na úrovni sítě** je zajištěna díky blokování (změny odpovědi na blokační stránku Whalebone) pokusů o překlad problémové domény.
A to bez ohledu na to, ve které fázi životního cyklu škodlivého kódu se aktuálně nachází daný incident. Ať už jde o překlad domény známé šířením malwaru, nebo pokus o stažení části škodlivého kódu downloaderem či infektorem, anebo o komunikaci infikovaného stroje s Command & Control serverem.



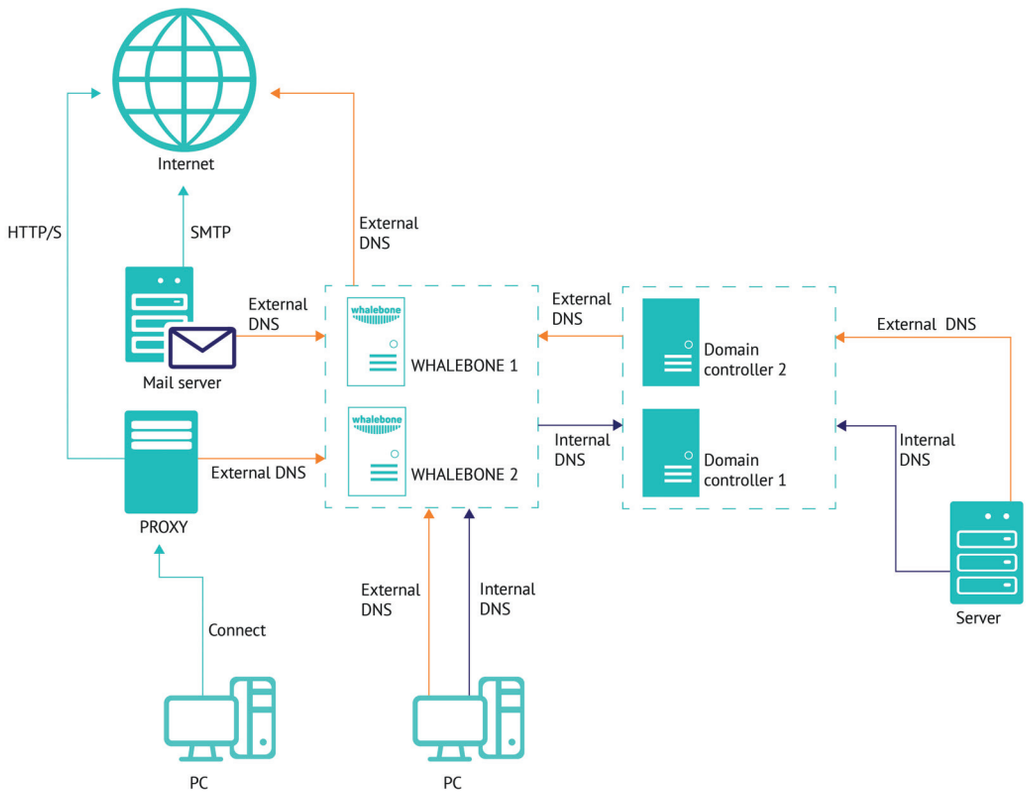

**7) Prevence proti DNS tunnelingu** je významnou částí zabezpečení DNS komunikace v oblasti ochrany proti škodlivému kódu, kdy malware pro svou komunikaci (např. s Command & Control serverem) použije pouze DNS překlad bez dalšího aplikačního protokolu. Aby škodlivý kód obešel standardní security technologie, jako jsou Next Generation Firewall (NGFW), webové proxy apod., svou komunikaci zakóduje (např. base64) a následně ji rozdělí a zasílá skrze standardní DNS dotazy. Na NGFW je viditelný pouze validní DNS provoz na relevantní nebo neznámé domény.

Současně je rozbíjení DNS tunelů důležité jako prevence vůči exfiltraci dat, při které je DNS tunneling možné zneužít pro vynesení citlivých dat.

**8) Alerting a & zjednodušení práce administrátorům** umožňuje administrátorům, aby své kapacity plně věnovali na svou primární činnost a řešili reálné incidenty, na které budou upozorněni real-time alertem. V případě akutního nedostatku kapacit je možné nastavit Whalebone na bezobslužný mód, který blokuje nežádoucí komunikaci na DNS a v pravidelných intervalech zasílá report o zaznamenaných a zablokovaných incidentech a konkrétních infikovaných zařízeních.

# Možnosti integrace

Řešení Whalebone bývá standardně integrované společně s různými provozními a bezpečnostními technologiemi, jako jsou Active Directory, provozní monitoring, helpdesk, SIEM, log management, Anomaly detection system, Honeypot, Endpoint security apod.




# Dostupnost

**Whalebone** resolvery jsou navržené tak, aby samotný DNS překlad byl zcela nezávislý na fungování ostatních funkcí. I v případě nedostupnosti některé nebo všech cloudových služeb nebude negativně ovlivněna funkce DNS překladu a tato kritická služba bude nadále fungovat.

# Cloudový vs. lokální resolver

Whalebone technologie podporuje možnost lokálního nasazení, stejně tak i využití cloudové služby.

- **Lokální resolver** je vhodné implementovat zejména kvůli získání plné viditelnosti do DNS komunikace až na úroveň IP adres koncových strojů a vyššímu zabezpečení DNSSEC validace.
- **Cloudový resolver** je vhodnější spíše pro menší společnosti, které chtějí plošně blokovat hrozby v celé síti a mít ve své společnosti přehled o DNS komunikaci, ale nemají vlastní infrastrukturu, na níž by řešení provozovaly, ani lidské zdroje, které by prováděly její správu.

Oba způsoby nasazení lze kombinovat v rámci jednoho multi-tenant účtu (např. větší organizace má vybrané pobočky nebo entity, které provádějí DNS překlad u poskytovatele, ale jejich centrála má vlastní resolvery, případně si chce danou službu provozovat v interní síti).

| | Cloud | On-premise |
|---|---|---|
| Ochrana DNS provozu | ✓ | ✓ |
| Web management | ✓ | ✓ |
| Fulltext vyhledávání v DNS provozu | ✓ | ✓ |
| Obsahová filtrace | ✓ | ✓ |
| Viditelnost lokálních IP | | ✓ |
| Lokální DNSSEC validace | | ✓ |
| DNS firewall (včetně Office 365) | | ✓ |

## Klíčové vlastnosti Whalebone

- **Okamžité nasazení.** Jediná věc, kterou je třeba konfigurovat, jsou DNS překladače.
- **Nulové nároky na správu.** Whalebone dokáže pracovat samostatně na základě nakonfigurovaných politik, v případě nedostatku interních kapacit zasílá automatizované reporty se zachycenými incidenty a hrozbami.
- **Absolutní dostupnost.** Je zahrnuta už v designu řešení, které navíc podporuje nasazení ve formě HA bez dopadu na cenu řešení.
- **Nezávislost na platformě.** Bez instalace agenta na koncový stroj funguje stejně pro všechny operační systémy.

## Reference

A1 O2 NTT Union Zdravotná Poisťovňa Union Pojišťovna ALD Automotive

LINET® Aero | VODOCHODY ROSTEX HYDRA®

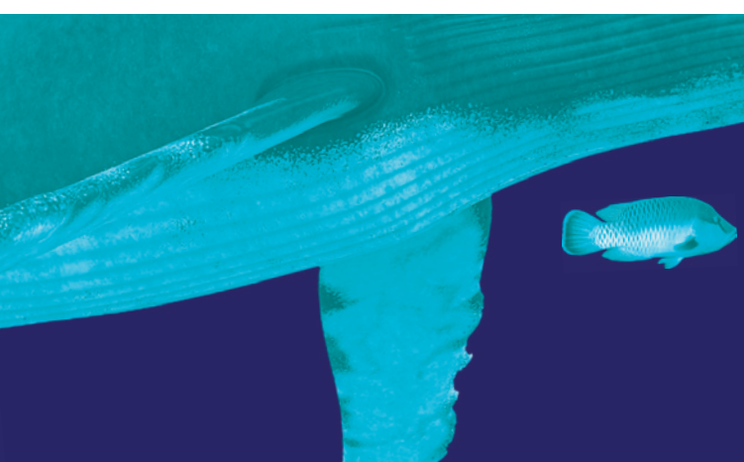
CZ SLOVALCO CHEMOSVIT PBS INDUSTRY

e.conomia GECO Slovenská poľnohospodárska univerzita Nitra

*„Poprvé v mé kariéře jsem zažil tak rychlou a bezproblémovou integraci bezpečnostní technologie do celé sítě."*

Aero | VODOCHODY

**Miloš Vodička**
Head of IT



## Kontaktujte nás

**sales@whalebone.io**

**Whalebone, s.r.o.,**
**Křenová 89/19, 602 00 Brno**