whalebone

Získejte plnou kontrolu nad DNS provozem a zabezpečte slepá místa své sítě

Panasonic O2 RPC Moravskoslezský kraj Železiarne Podbrezová Česká Zbrojovka Železničná spoločnosť Slovensko

Equa bank Union Pojišťovna ADASTRA ALD Automotive HBM Pharma ŽSR ZsVS

Whalebone Immunity poskytuje podnikovým sítím kontrolu a ochranu DNS komunikace bez ohledu na jejich velikost nebo složitost.

90 % malware potřebuje v průběhu svého životního cyklu DNS překlad, ale většina organizací stále nemá přímou kontrolu nad DNS provozem, který ani nijak nezabezpečuje.

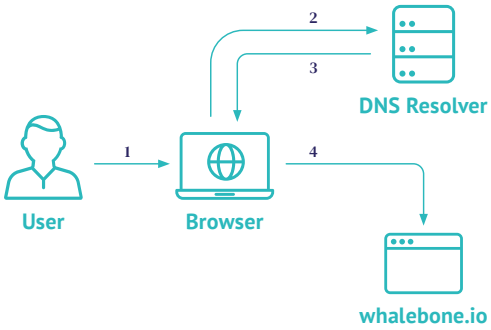
Hlavní výhody

Správa a monitoring DNS překladu z jednoho místa

Zabezpečení komunikace proti DNS hrozbám

Ochrana na síťové úrovni před podvodnými e-maily, cílenými phishingovými kampaněmi i malware

Komplexní zabezpečení DNS komunikace



1. Chce navštívit **whalebone.io**
2. Jaká je IP adresa whalebone.io?
3. IP adresa whalebone.io je 88.86.121.135
4. Připojit se

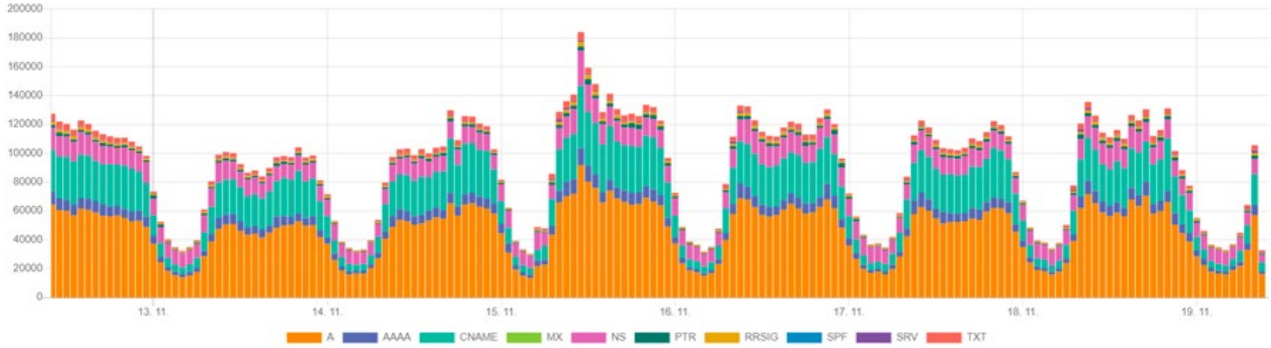
1 — Úplná kontrola nad DNS překladem a řízením přístupu

Díky Whalebone resolveru poskytuje Immunity plnou kontrolu nad DNS překladem organizacím, které se v tomto tradičně spoléhají na svého poskytovatele internetu. S Whalebone Immunity získáte možnost spravovat pravidla pro jednotlivé domény a nastavovat whitelisty a blacklisty pro celou síť nebo libovolný segment či jednotlivé zařízení, které si vyberete. Můžete také zadefinovat specifická pravidla filtrování obsahu, například blokování torrentů, obsahu pro dospělé nebo sociálních médií pro zvýšení produktivity týmu a snížení nároků na síťové zdroje.

2 — Whalebone Home Office Security

Immunity umožňuje správcům chránit zaměstnance, i když pracují mimo interní síť. Pomocí aplikace Home Office Security (HOS) mohou uživatelé pracovat z libovolného místa – z domova, letiště či kavárny – a mají stejnou úroveň zabezpečení, jako by byli v kanceláři. Aplikace HOS je nepřipraví o žádný prvek fungování Immunity. Je navíc součástí základního balíčku, za aplikaci neplatíte nic navíc.

Přehled vašeho DNS provozu

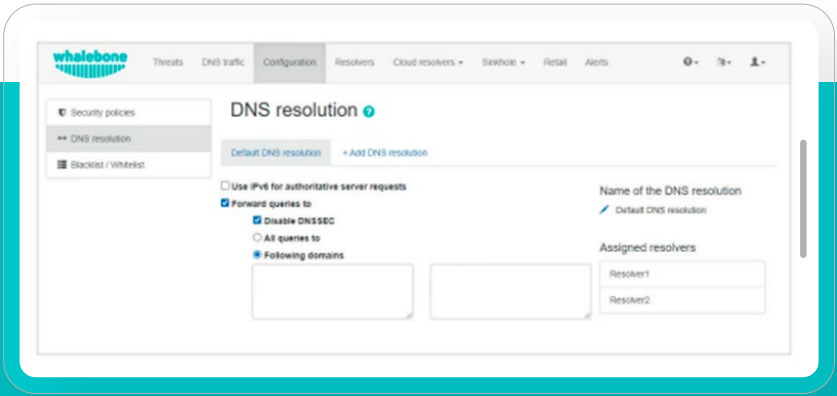


3 — Viditelnost do DNS provozu, analýza a detekce anomálií

Správci tak mají přehled až na úroveň IP jednotlivých zařízení a mohou být o krok napřed před útočníky, protože identifikují hrozby dříve, než reálně firmu ohrozí. Správcům navíc usnadňují práci přednastavené notifikace.

4 — Ochrana proti phishingu

Whalebone Threat Intelligence blokuje přístup k phishingovým webům v reálném čase, čímž účinně brání uživateli v ohrožení firemní sítě. Systém automaticky zachytí i domain spoofing a další cílené formy phishingových útoků. Když už k phishingu dojde, podrobný přehled provozu DNS umožňuje snadno identifikovat zařízení, které se pokusilo o přístup k podvodné doméně, a rychle zahájit proces změny přístupových údajů uživatelů, kteří mohli být ohroženi.



5 — DNS Firewall (pro Office 365, Skype pro firmy a vybrané interní aplikace)

Microsoft vyžaduje, aby koncové body využívající Office 365 dokázaly překládat externí domény přímo a na proxy serveru je pak potřeba vytvářet výjimky. Tento požadavek často narušuje bezpečnostní architekturu a zásady zabezpečení.

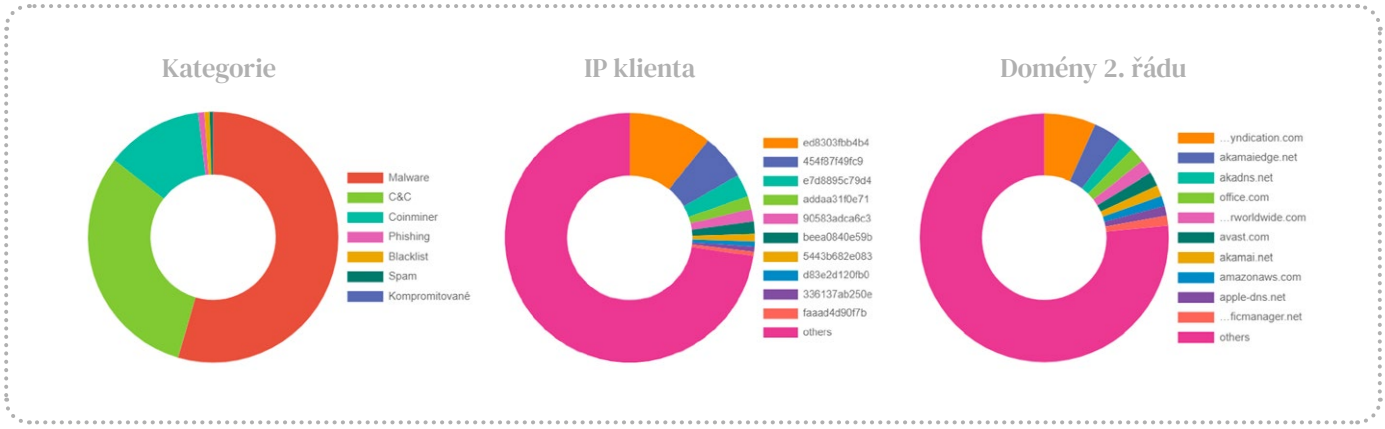
Whalebone tyto problémy řeší jako DNS firewall – filtruje komunikaci a domény služeb jako je Office 365, Skype pro firmy nebo interní aplikace. Tyto domény Whalebone obchází, zatímco ostatní externí domény lze povolit pouze prostřednictvím proxy serveru. Tím je zachován původní účel zásad zabezpečení a architektura zabezpečení zůstává nenarušena.

6 — DNSSEC validace

Ověřování DNSSEC umožňuje administrátorům snížit zranitelnost protokolu SMTP proti změně MX záznamu při přijímání nebo odesílání e-mailů. Tím se omezí riziko toho, že se citlivé údaje dostanou k útočníkovi.

7 — Ochrana proti škodlivému kódu a škodlivé komunikaci na síťové úrovni

Immunity to zajišťuje tak, že blokuje pokusy o překlad problematické domény. K tomu dochází bez ohledu na fázi životního cyklu infekce, ve které k danému incidentu došlo. To zahrnuje řešení domén známých šířením malwaru, pokusy o stažení části škodlivého kódu prostřednictvím downloaderu nebo infectoru a komunikaci infikovaných zařízení se servery Command & Control. Immunity také poskytuje ochranu proti cílenému i plošnému phishingu a spamovým kampaním.



8 — Ochrana proti DNS tunnelingu

Ochrana proti DNS tunnelingu je významným prvkem zabezpečení DNS. Různé rodiny malwaru používají tunelovací útoky k odcizení citlivých dat pro svá command & control centra.

9 — Alerty a zjednodušení práce správců

V případě, že správce nemá kapacitu na řešení konkrétního upozornění, Immunity může automaticky vynucovat zásady zabezpečení. Díky tomu se můžete zabývat pouze krátkým vyhodnocením automatických zpráv zasílaných e-mailem.

10 — Viditelnost na doménové jméno

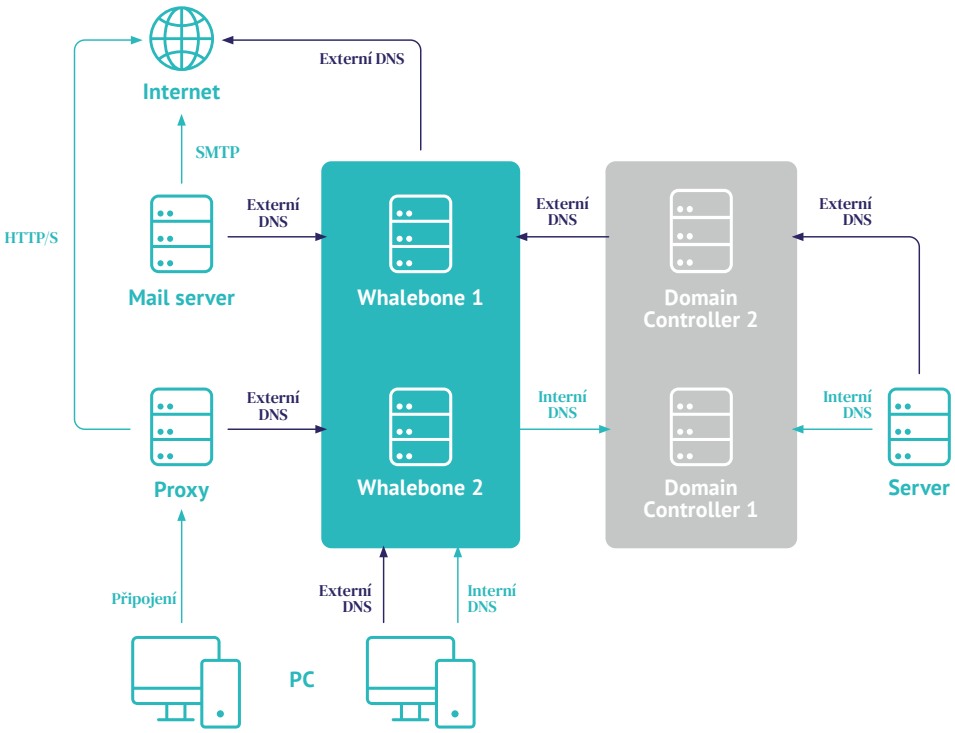
Immunity identifikuje doménové jméno zařízení, ze kterého došlo k zablokovanému bezpečnostnímu incidentu. To vám umožní rychle a efektivně odstranit vektor hrozby.

11 — Ochrana identity

Hackeři často na dark webu prodávají ukradená data, jako například hesla, kódy přístupových karet či další citlivé informace spojené s firemními doménami. Immunity vás upozorní na jakékoli nové úniky i na zasažená data z minulých let. Díky tomu budete moci podniknout kroky, které zabrání případným útokům.

Možnosti integrace

Whalebone Immunity je obvykle integrováno s různými provozními a bezpečnostními technologiemi včetně Active Directory, systémů pro monitorování provozu, helpdesku, SIEM, systémů pro správu logů, systémů detekce anomálií, Honeypotu, zabezpečení koncových bodů a http-proxy.



Dostupnost

Naše resolvery jsou navrženy tak, aby samotný DNS překlad byl zcela nezávislý na ostatních funkcích. I v případech, kdy jsou některé nebo všechny cloudové služby nedostupné, nebude DNS překlad nijak ovlivněn a bude fungovat i nadále.

Cloud vs. on-premise resolver

Technologie Whalebone podporují jak lokální nasazení, tak využití cloudových služeb.

- **On-premise resolver** by měl být implementován především za účelem získání úplného přehledu o komunikaci DNS až ke koncovým IP adresám a zvýšení zabezpečení DNSSEC validace.
- **Cloudový resolver** je vhodnější pro menší organizace, které chtějí blokovat hrozby v celé síti a mít přehled o komunikaci DNS ve své organizaci, ale nemají vlastní infrastrukturu, na které by mohlo Immunity běžet, ani lidské zdroje na jeho správu.

	Cloud	On-premise
Ochrana DNS provozu	✓	✓
Web management	✓	✓
Fulltextové vyhledávání v DNS provozu	✓	✓
Obsahová filtrace	✓	✓
Viditelnost k lokálním IP adresám		✓
Lokální DNSSEC validace		✓
DNS firewall (vč. Office 365)		✓

Oba způsoby nasazení lze kombinovat v rámci jednoho účtu (např. když větší organizace mají vybrané pobočky nebo subjekty, které provádějí překlad DNS u poskytovatele, ale jejich centrála má vlastní resolvery nebo chce danou službu provozovat ve své interní síti).

Klíčové funkce Whalebone

Okamžité nasazení

Jediné, co je třeba nakonfigurovat, jsou DNS resolvery.

Absolutní dostupnost

Whalebone může pracovat samostatně na základě nakonfigurovaných zásad a v případě nedostatečné interní kapacity odesílá **automatické zprávy o zachycených incidentech a hrozbách**.

Nulové náklady na údržbu

Whalebone **může pracovat samostatně** na základě nakonfigurovaných zásad. Navíc odesílá **automatické zprávy** o zachycených incidentech a hrozbách.

Nezávislost na platformách

V samotné síti **není pro koncové body nutná instalace agenta**; Immunity funguje stejné pro všechny operační systémy.

www.whalebone.io

Ochrana celé sítě ····· Home Office Security ····· Bezkonkurenční viditelnost