

Whalebone Immunity

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.

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



Odstraňte
slepá místa

Zabezpečte síť proti hrozbám, které standardní systémy jako firewally, antiviry a EDR nevyřeší.



Správa a přehled
o DNS

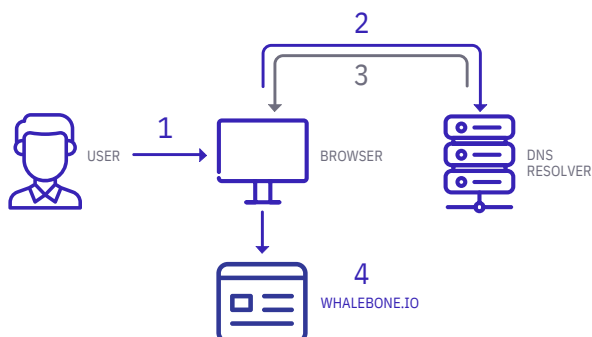
Správa a monitoring DNS překladu z jednoho místa.



Ochrana před širokou
škálou hrozeb

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

Komplexní zabezpečení DNS komunikace



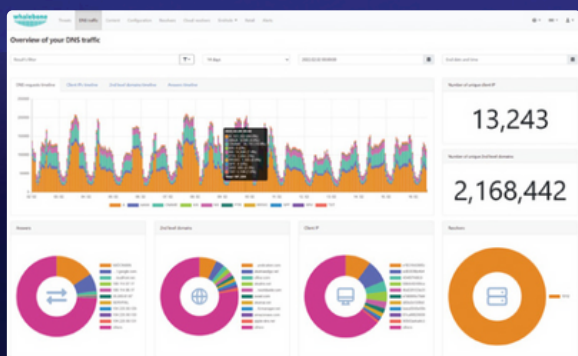
1. Chce navštívit whalebone.io
2. Jaká je IP adresa whalebone.io?
3. IP adresa whalebone.io je 88.86.121.135
4. Připojit se

Úplná kontrola nad DNS překladem a řízením přístupu

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.

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.



Viditelnost do DNS provozu, analýza a detekce anomálií

Správcí 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.

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.

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.

Identifikovatelnost na doménové jméno

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

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.

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.

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.

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.

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.

Cloud vs. on-premises resolver

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

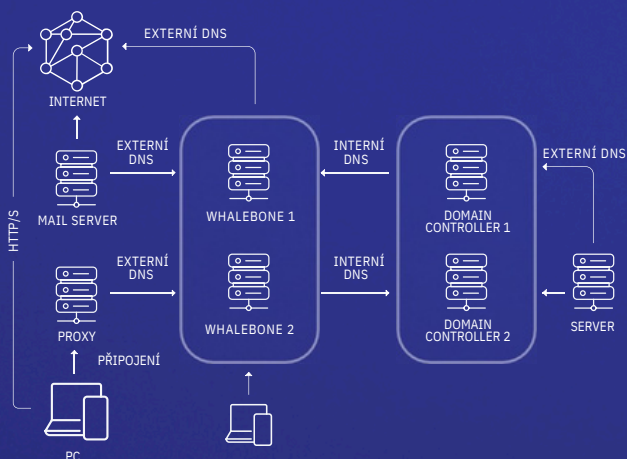
1. On-premise resolver by měl být implementován především za účelem získání úplného přehledu o komunikaci DNS až ke koncovým IP adresám a zvýšení zabezpečení DNSSEC validace.

2. 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.

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 resolversy nebo chce danou službu provozovat ve své interní síti).

	Cloud	On-premises
OCHRANA DNS PROVOZU	✓	✓
WEB MANAGEMENT	✓	✓
FULLTEXTOVÉ VYHLEDÁVÁNÍ V DNS	✓	✓
OBSAHOVÁ FILTRACE	✓	✓
VIDITELNOST LOCAL IP		✓
LOKÁLNÍ DNSSEC VALIDACE		✓
DNS FIREWALL (VČETNĚ OFFICE 365)		✓



Možnosti integrace

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

Dostupnost

Naše resolversy jsou navrženy tak, aby samotný DNS překlad byl zcela nezávislý na ostatních funkcích. I v případech, kdy jsou cloudové služby nedostupné, nebude DNS překlad nijak ovlivněn.

WHALEBONE'S KEY FEATURES

✓ Okamžité nasazení, nulové náklady na údržbu

Jediné, co je třeba nakonfigurovat, jsou DNS resolversy. Whalebone může pracovat samostatně na základě nakonfigurovaných zásad.

✓ Okamžitě viditelná hodnota

Během bezplatného zkušební období více než 50 % našich zákazníků identifikuje hrozbu, o které nevěděli a více než 50 % identifikuje uniklá citlivá data související se svou doménou.

✓ Zablokujte více hrozeb

Podle našich testů na datech poskytnutých AV-TESTem, přidání DNS vrstvy umožní identifikovat o 80% více hrozeb, než při použití pouze next-gen firewallu.

✓ Nezávislost na platformách

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

Jednoduše přeměrujte traffic z vaší sítě na resolversy Whalebone a zahajte bezplatnou zkušební verzi.

it@scenario.cz

Scenario s.r.o.
Pohraniční 1435/86, 703 00 Ostrava
tel.: +420 602 111 071
www.scenario.cz

scenario
Informační technologie • Marketing