

Bitdefender GravityZone Email Security

Przedstawiamy GRAVITYZONE EMAIL SECURITY

Wielowarstwowa, oparta na chmurze ochrona poczty e-mail dla całej organizacji. Skuteczne zabezpieczenie usługi Office 365

Bitdefender GravityZone Email Security jest kompleksowym rozwiązaniem ochrony poczty elektronicznej, które spełnia wszystkie potrzeby w zakresie bezpieczeństwa. Zapewnia Twojej organizacji kompletną ochronę poczty e-mail znacznie wykraczającą poza złośliwe oprogramowanie i inne tradycyjne zagrożenia, takie jak spam, ataki phishingowe na szeroką skalę i niebezpieczne adresy URL. Powstrzymuje również najnowsze, ukierunkowane i złożone zagrożenia związane z pocztą elektroniczną, w tym oszustwa Business Email Compromise (BEC) i oszustwa CEO.

Nieźródlna ochrona przed zagrożeniami

Kompleksowy zestaw technologii zapewnia skuteczną ochronę przed znanymi, nieznanymi dotychczas i nowo powstałymi zagrożeniami dotyczącymi poczty elektronicznej.

Ochrona przed atakami metodą podszywania się pod CEO

Wykrywa zagrożenia niezawierające złośliwego oprogramowania, takie jak próby wyłudzenia danych uwierzytelniających i fałszywe wiadomości e-mail

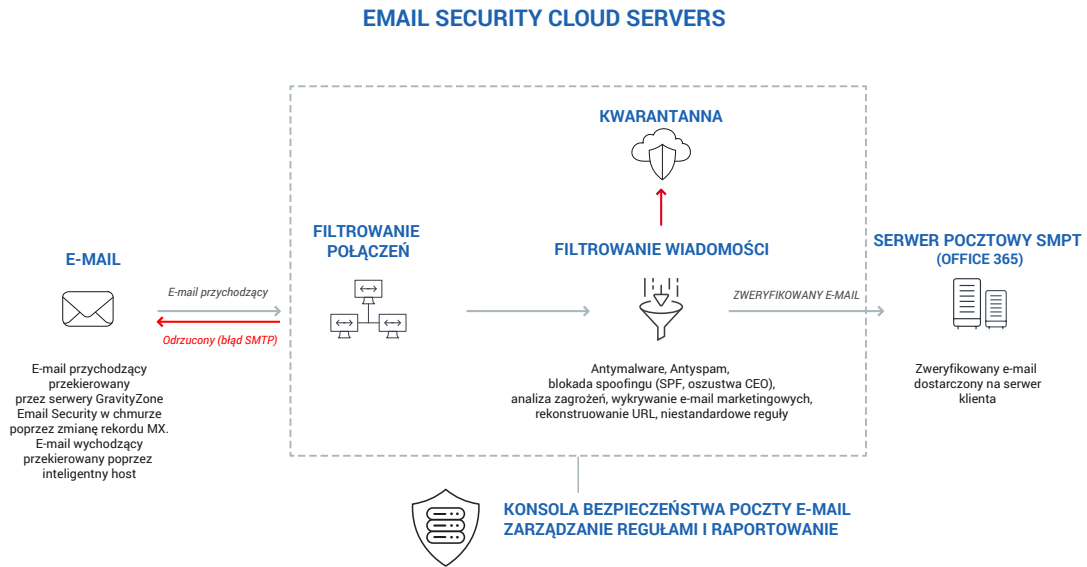
Połączenie wielu silników skanujących

Tradycyjne silniki AV oparte na sygnaturach wraz ze skanowaniem behawioralnym automatycznie wykrywają nowe techniki łączenia złośliwego oprogramowania

Jak to działa

- Tradycyjny mechanizm rozpoznawania schematów, atrybutów wiadomości i ich charakterystyk jest uzupełniony o analizę algorytmiczną, która zapewnia **najwyższą skuteczność wykrywania zagrożeń przy zachowaniu precyzji**.
- **Analiza behawioralna** obejmuje ponad 10 000 algorytmów analizujących ponad 130 zmiennych wyodrębnionych z każdej wiadomości e-mail.
- **Połączenie wielu silników antywirusowych opartych na sygnaturach i analizie behawioralnej** zapewnia ochronę przed wszystkimi rodzajami złośliwego oprogramowania, łącznie z zagrożeniami typu zero-day:
 - 99.999% skuteczność wykrywania spamu przy niemal zerowej liczbie fałszywych alarmów
 - 100% ochrona przed wirusami
- **Zaawansowany mechanizm reguł**, który pozwala administratorowi IT na dokładne dostosowanie sposobu przepływu poczty elektronicznej do i z organizacji. Mechanizm ten może sprawdzać wszystkie parametry wiadomości e-mail, w tym rozmiar, treść, załączniki, nagłówki, nadawców i odbiorców, oraz podejmować odpowiednie działania, takie jak dostarczenie, kwarantanna, kwarantanna obejmująca całą organizację, przekierowanie, powiadomienie lub odrzucenie.
- **GravityZone Email Security jest zarówno zaawansowanym rozwiązaniem bezpieczeństwa poczty e-mail, jak i w pełni opartym na chmurze silnikiem routingu** do zarządzania wiadomościami z wbudowanymi mechanizmami kwarantanny ogólnej lub indywidualnej. Głęboka kategoryzacja - rozróżnianie pomiędzy wiadomościami marketingowymi, podejrzanymi masowymi kampaniami mailingowymi i innymi - umożliwia tworzenie elastycznych reguł, które szczegółowo określają jak różne rodzaje wiadomości są przetwarzane i oznaczane.
- **Precyzyjne śledzenie wiadomości** jest niezbędne dla administratorów poczty elektronicznej, pozwalając im szybko sprawdzić, dlaczego wiadomość e-mail została dostarczona lub odrzucona, z uwzględnieniem nagłówek wiadomości i całej komunikacji ze zdalnym serwerem pocztowym.

GravityZone Email Security - architektura rozwiązania



Najważniejsze funkcje GravityZone Email Security

FUNKCJE OCHRONY

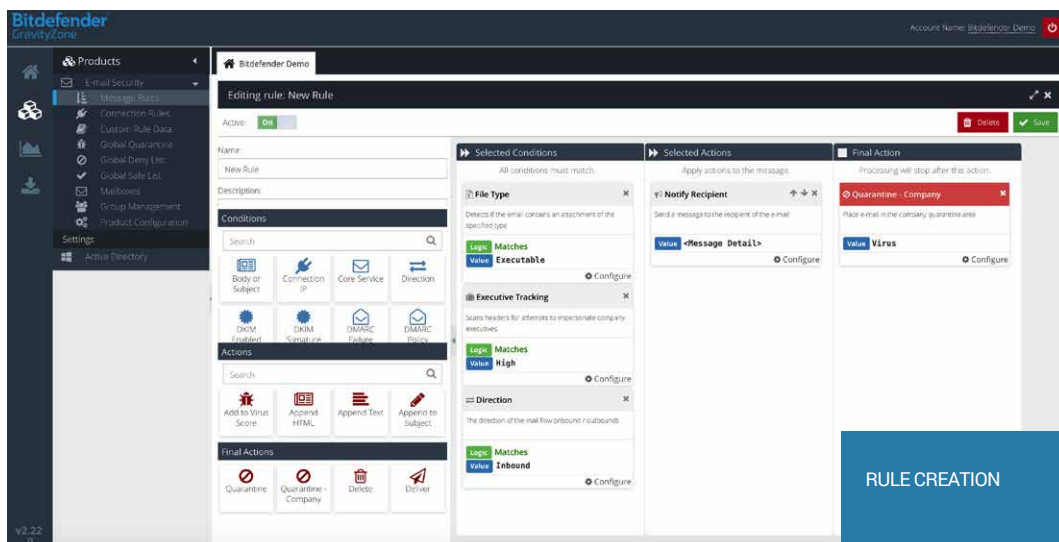
- Antyspam: Wielo-silnikowy mechanizm wykorzystuje kombinację technologii do wykrywania spamu jak również bardziej złożonych, ukierunkowanych ataków phishingowych i prób podszywania się.
- Anty-malware: Półłączenie wielu tradycyjnych silników antywirusowych opartych na sygnaturach i skanowania behawioralnego dla skutecznego wykrywania złośliwego oprogramowania.
- Ochrona w chwili kliknięcia (tzw. time-of-click): Przetwarza i rekonstruuje adresy URL w wiadomościach e-mail i zapewnia ochronę w momencie kliknięcia przy użyciu licznych funkcji analizy reputacji.
 - Opcje automatycznego przekierowania, naciśnięcia przycisku w celu przejścia dalej, blokowania w przypadku zagrożenia oraz pokazywania/ukrywania docelowego adresu URL.
 - Opcja skanowania linków w momencie dostarczenia wiadomości, jak również w chwili kliknięcia.
- Listy bezpiecznych i blokowanych nadawców: Umożliwia tworzenie list na poziomie całej firmy i/lub poszczególnych użytkowników.
- TLS / StartTLS:
 - Ustanawia szyfrowanie TLS i ogranicza komunikację z innymi serwerami pocztowymi, które nie obsługują protokołu TLS.
 - Opcja umożliwiająca użycie StartTLS z możliwością przejścia do trybu zwykłego tekstu, jeśli TLS nie jest obsługiwany przez serwer odbierający.
- Uwierzytelnianie poczty e-mail: Wsparcie SPF, DKIM i DMARC.
- Lista monitorowania kadry kierowniczej: Wykorzystanie danych zsynchronizowanych z Active Directory do automatycznego wykrywania prawdziwych nazwisk użytkowników w nagłówkach i polach adresowych e-maili w celu ochrony przed próbami podszywania się / atakami CEO.
- Domeny o podobnym brzmieniu:
 - Porównuje domenę nadawcy z prawdziwymi nazwami domen, aby zidentyfikować zbliżone domeny (które różnią się od właściwej) o jeden lub dwa znaki.
 - Chroni przed atakami wykorzystującymi metodę podszywania się / oszustwa CEO.
- Znaczniki tematu i nagłówki:
 - Dodawanie znaczników takich jak [ZEWNĘTRZNE] lub [MARKETING] do tematu wiadomości.
 - Dodawanie nagłówka HTML lub zwykłego tekstu do wiadomości przychodzących w celu ostrzeżenia użytkowników o potencjalnych zagrożeniach.
- Załączniki:
 - Sprawdzanie typu MIME załączanych plików i możliwość blokowania niebezpiecznych typów plików.
 - Wykrywanie archiwów chronionych hasłem.
- Listy słów kluczowych: Twórz nieograniczone listy słów kluczowych. Używaj reguł do analizowania wiadomości i podejmowania działań w oparciu o poufne lub wrażliwe treści.
- Kolejowanie poczty: Wiadomości e-mail są automatycznie umieszczane w kolejce na 7 dni w przypadku awarii lub przestoju głównej usługi/serwera(ów) poczty elektronicznej.
- Monitorowanie wolumenu wysyłanej poczty: Automatyczna ochrona przed próbami wysyłania dużej liczby wiadomości wychodzących, aby zapobiec trafieniu domeny Twojej organizacji na czarną listę.
- Zapobieganie atakom typu Directory Harvest Attack (DHA): Usuwanie wiadomości e-mail kierowanych na nieprawidłowe lub fałszywe adresy e-mail.

FUNKCJE OCHRONY

- Mechanizm reguł: Możliwość określenia ponad 20 kryteriów do kontroli dostarczania wiadomości e-mail i filtrowania ich w oparciu o rozmiar, słowa kluczowe, wartość spam score, czas, źródło, odbiorcę, rozmiar załącznika, nagłówki, atrybuty AD i wiele innych.
- Synchronizacja użytkowników: Usługa synchronizacji Active Directory zapewnia replikację zmian. W razie potrzeby można zastosować reguły oparte na przynależności do grup AD.
- Interfejs sieciowy: W pełni zarządzany i obsługiwany za pośrednictwem konsoli GravityZone Email Security.
- Administracja delegowana: Pozwala na ustanowienie wielu administratorów z różnymi poziomami dostępu.
- Kwarantanna: Opcja przenoszenia wiadomości do kwarantanny obejmującej całą firmę lub danego użytkownika.
- Przegląd wiadomości w kwarantannie: Wiadomości zbiorcze zawierają listę wszystkich e-maili danego użytkownika objętych kwarantanną i pozwalają na ich podgląd, odblokowanie lub zablokowanie.
- Klauzule wyłączenia odpowiedzialności: Dołączaj stopkę HTML i/lub zwykły tekst do wszystkich wychodzących wiadomości e-mail. Możesz ustawić różne stopki dla różnych domen.

FUNKCJE RAPORTOWANIA

- Widoczność w czasie rzeczywistym: Wykresy zapewniają szczegółowy wgląd w przepływ poczty przychodzącej i wychodzącej, jak również w uruchamianie reguł i podejmowane działania. Możliwość przechodzenia od wysokopoziomowych wykresów i diagramów do szczegółowych raportów.
- Kreator raportów: Administratorzy mogą tworzyć własne raporty w oparciu o dostępne nazwy pól i kryteria. Raporty mogą być zapisywane, a następnie eksportowane. Raporty z audytu mogą być przeszukiwane przy użyciu kryteriów takich jak: czas, użytkownik, adres nadawcy, temat, IP nadawcy, odbiorca, kierunek przepływu, działanie końcowe, nazwa reguły. Oznaczenie danego raportu jako "Ulubiony" dodaje go do obszaru szybkiego dostępu.
- Harmonogramy i powiadomienia: Połącz raporty z harmonogramami i korzystaj z opcji otrzymywania raportów, gdy tylko pojawi się określona treść (tryb alertów). Powiadomienia mogą dotyczyć reguł, działań, treści itp.
- Raporty głównych trendów: Wybór predefiniowanych raportów o trendach z wykresami i danymi tabelarycznymi. Raporty trendów mogą być eksportowane do formatu PDF i wysyłane pocztą elektroniczną do odbiorców.
- Wiele widoków: Analizuj i generuj raporty według czasu, użytkownika, adresu nadawcy, tematu, IP nadawcy, odbiorcy, kierunku przepływu, działania końcowego, nazwy reguły.
- Szczegółowy audyt (śledzenie wiadomości): Dokładny podgląd analizy poszczególnych wiadomości z podaniem konkretnej przyczyny dostarczenia lub odrzucenia wiadomości. Zawiera nagłówki e-maili i pełen przebieg komunikacji ze zdalnym serwerem pocztowym.
- Przechowywanie i automatyczna archiwizacja logów: Dane logów GravityZone Email Security są automatycznie archiwizowane po 90 dniach i dostępne do pobrania z konsoli przez okres kolejnych 12 miesięcy.



Message Rules

Priority	Direction	Rule Name	Final Action	Active	Act...
1	↔	Opportunistic TLS	Add Message Header	On	⋮
2	↔	Macro and VBA Detection	Add to Virus Score	Off	⋮
3	↔	Virus	Quarantine Company Only	On	⋮
4	↔	Spooled Messages	Add to Spam Score	On	⋮
5	↔	Executive Tracking	Quarantine Company Only	On	⋮
6	↔	Nearby Domain	Add to Spam Score	On	⋮
7	↔	CoreService Suspect	Add to Spam Score	On	⋮
8	↔	Script and Executable Files	Add to Spam Score	On	⋮
9	↔	Uniscam	Re-write URLS	On	⋮
10	↔	High Reputation Marketing	Prefix Text to Subject	On	⋮
11	↔	Medium Reputation Marketing	Prefix Text to Subject	On	⋮
12	↔	Low Reputation Marketing	Add to Spam Score	On	⋮
13	↔	SPF Fail		On	⋮
14	↔	Confirmed Phishing		On	⋮
15	↔	Confirmed Spam		On	⋮
16	↔	Possible Spam		On	⋮
17	↔	Deliver Inbound		On	⋮

TYPICAL MESSAGE RULESET

Top Final Rules

Rule Name	Frequency (Approximate)
Deliver Inbound	95
Isolated DMARC	85
Possible Spam	80
Confirmed Spam	75
Medium Reputation Marketing	35
(Default) DMARC Fail	15
Executive Tracking	10
Virus	5
Deliver Outbound	5
Script and Executable Files	5
Confirmed Phishing	5

RAPORT DOTYCZĄCY NAJWAŻNIEJSZYCH REGUŁ KOŃCOWYCH

WDROŻENIE

- Szybkie i łatwe wdrożenie: Przekieruj rekordy MX domeny do chmury GravityZone Email Security.
- Wsparcie dostawców pocztowych: Współpracuje z wszystkimi dostawcami usług poczty e-mail. Dostarczaj wiadomości do różnych operatorów e-mail w oparciu o członkostwo użytkownika w grupie AD - obsługa środowisk hybrydowych wykorzystujących Exchange on-premise oraz O365 Exchange Online lub Gmail.
- Zmień rekordy MX, aby przekierować przychodzące wiadomości e-mail za pomocą serwerów GravityZone Email Security w chmurze.
- Skonfiguruj hosty inteligentne, by przekierowywać wychodzące wiadomości e-mail przez serwery GravityZone Email Security w chmurze.

