

Microsoft Forefront Security for Exchange Server

Wielosilnikowa ochrona przed najnowszymi zagrożeniami e-mail

Microsoft Forefront Security for Exchange Server zawiera kilka, stworzonych przez liderów branży bezpieczeństwa informatycznego, antywirusowych silników skanujących zintegrowanych w jednym rozwiązaniu, pozwalającym przedsiębiorstwom chronić ich środowiska pocztowe Exchange przed wirusami, robakami i spamem.

Microsoft Forefront Security for Exchange Server to jeden z kilku produktów rodziny rozwiązań Forefront firmy Microsoft. Ten wysoko ceniony produkt, który wcześniej był znany jako Microsoft Antigen for Exchange, a w swojej dziesiątej edycji został wydany pod marką Forefront, integruje rozmaite antywirusowe silniki skanujące, w celu zapewnienia wszechstronnej, wielowarstwowej ochrony serwerów wiadomości Exchange, przy jednoczesnej optymalizacji ich działania i uproszczeniu zarządzania bezpieczeństwem.

Wirusy rozsyłane drogą e-mailową pozostają największym zagrożeniem dla przedsiębiorstw z punktu widzenia straty czasu i spadku wydajności pracy.* Wirusy, robaki, spam i inne złośliwe oprogramowanie mogą paraliżować komunikację, zapychać zasoby serwerowe, wyłączać systemy – skutecznie uniemożliwiając pracę. I choć w 2006 roku niemal 97 procent przedsiębiorstw używało oprogramowania antywirusowego, to aż 65 procent z nich padło ofiarami ataków ze strony wirusów.*

Dlaczego? Jedną z przyczyn polega na tym, że firmy chcą zabezpieczyć najważniejsze swoje serwery przy pomocy tylko jednego antywirusowego silnika skanującego. Jeśli ten silnik szybko nie rozpozna zagrożenia, wirus błyskawicznie rozprzestrzeni się w organizacji, docierając do każdego punktu w sieci, chronionego przez to samo nieodporne narzędzie. Przesadnie restrykcyjne praktyki też mają swoje wady. Blokowanie całych wiadomości,

podczas gdy tylko ich część może stanowić zagrożenie, sprawia, że do użytkowników może nie dotrzeć ważna poczta. Skanowanie każdej wiadomości na każdym serwerze opóźnia jej doręczanie i powoduje marnowanie zasobów. Instalowanie i zarządzanie wieloma, niezintegrowanymi ze sobą programami antywirusowymi może przyprawić o zawrót głowy, zaś nadmiarowe skanowanie starych e-maili, bez względu na ich wiek, wyczerpuje zasoby serwerowe.

Wszystko to składa się na opóźnienia w dostarczaniu e-maili, słabszą ochronę pojedynczych elementów sieci, zwiększone koszty zarządzania i spadek wydajności.

Zwiększenie ochrony bez zwiększania wydatków

Microsoft Forefront Security for Exchange Server rozwiązuje te problemy, dostarczając wszechstronną, wielowarstwową ochronę przed wirusami, jednocześnie zapewniając szybkie tempo pracy serwera, poprzez optymalizację jego działania i uproszczenie zarządzania bezpieczeństwem systemów Exchange Server.

Wszechstronna ochrona przed najnowszymi zagrożeniami

W celu zwiększenia ochrony, Microsoft Forefront Security for Exchange Server dostarcza kilku silników antywirusowych, stworzonych przez liderów branży bezpieczeństwa informatycznego. Specjaliści z działu IT mogą jednocześnie uruchomić nawet pięć silników skanujących środowisko Exchange Server na kilku płaszczyznach. Kiedy jeden silnik zostanie wyłączony celem uaktualnienia, pozostałe kontynuują skanowanie poczty na serwerach Exchange 2007 Edge, Hub i Store – z pocztą przesyłaną przez urządzenie przenośne łącznie. Aktualizacje sygnatur dla wszystkich silników są szybkie i automatyczne, co pomaga obronić się przed najnowszymi zagrożeniami, jak tylko się pojawią.

W celu ochrony przed spamem, Forefront Security for Exchange Server wykorzystuje najlepsze filtry spamu i zawartości obecne w Exchange 2007 i umożliwia ich automatyczną aktualizację. Natomiast heurystyka i technologie filtrowania plików programu zabezpieczają korporacje przed coraz nowszymi zagrożeniami, wykrywając wirusy na podstawie ich zachowania i poprzez przechwytywanie niebezpiecznych plików, takich jak pliki wykonywalne, nawet jeśli rozszerzenia ich nazw zostały zmienione.

Optymalizacja działania, zapewniająca sprawne funkcjonowanie poczty

Forefront Security for Exchange Server jest zintegrowany z Exchange 2007, co pozwala uniknąć zbędnego powtarzania procesu filtrowania wiadomości, jeżeli przeszły już przez skanowanie na pierwszym serwerze. Po wyłączeniu niepotrzebnego skanowania poczta będzie przepływać szybciej, a serwery nie będą się zawieszać z powodu przeciążenia.

Aby usprawnić działanie serwerów Store, specjaliści IT mogą wybiórczo skanować skrzynki pocztowe celem wyszukiwania tylko najczęściej spotykanych wirusów. Takie przyrostowe skanowanie w tle uwalnia zasoby serwera od niepotrzebnego ponownego sprawdzania megabajtów starej poczty.

Uproszczone zarządzanie, odciążające specjalistów IT

Zautomatyzowane aktualizacje sygnatur i silników, migracja zabezpieczeń do serwerów Exchange 2007 oraz scentralizowane sterowanie i zarządzanie prowadzą do zwiększania wydajności i swobody działania. Forefront Security for Exchange Server może być centralnie konfigurowany, instalowany i aktualizowany w multiserwerowych środowiskach wykorzystujących konsolę Microsoft Forefront Server Security Management Console. Program obsługuje również Microsoft Operations Manager (MOM), w zakresie monitorowania serwerów Exchange całej korporacji.

Jak działa Microsoft Forefront Security for Exchange Server

Wszechstronna ochrona

- **Skanowanie kilkoma silnikami, brak pojedynczych punktów awarii.** Administratorzy mogą aplikować i zarządzać nawet pięcioma silnikami antywirusowymi jednocześnie oraz stosować różne ich kombinacje dla serwerów Exchange 2007 Transport (Edge i Hub) i Store (Mailbox/Folder Publiczny). Nawet jeśli jeden silnik jest wyłączony lub jeśli nie dostrzeże zagrożenia, e-mail zostanie przeskanowany również przez kolejne silniki, co eliminuje występowanie pojedynczych punktów awarii. Silniki skanujące dostarczane są przez takie firmy jak: Ahnlab, Authentium, CA, Kaspersky Labs, Norman Data Defense, Sophos oraz VirusBuster.
- **Doskonała ochrona antyspamowa.** Używając Forefront Security for Exchange Server można włączyć usługi antyspamowe w Exchange 2007, w tym IP Reputation Service, Intelligent Message Filters (IMF) do filtrowania zawartości oraz pliki sygnatur antyspamowych. Te antyspamowe narzędzia zostają włączone podczas instalacji i wielokrotnie w ciągu każdego dnia są automatycznie aktualizowane.
- **Warstwowa ochrona.** Administratorzy mogą zainstalować i włączyć skanowanie w różnych punktach kontrolnych, tak aby w przypadku awarii serwera Edge, e-mail został też przeskanowany na serwerze Hub. Ta warstwowa ochrona jest kluczowa w walce ze złośliwymi atakami jeszcze zanim uderzą one w sieć lub wydajność użytkowników końcowych.
- **Ochrona przed nowymi i ukrytymi zagrożeniami.** Dzięki wbudowanej technologii heurystycznej można zablokować złośliwy kod, bazujący na charakterystykach zachowań i skonfigurować zasady filtrowania plików, aby wyeliminować typy plików znane z przenoszenia wirusów (na przykład .exe), nawet jeśli rozszerzenia ich nazw zostały zmienione. Forefront Security for Exchange Server może też rozpakować i wybiórczo przepakować skompresowane załączniki, takie jak pliki .zip, już po usunięciu z nich zainfekowanych lub niechcianych elementów.
- **Walkę z nowymi zagrożeniami wspiera kilku dostawców skanerów AV.** Szanse na szybką reakcję na nowe ataki są duże większe. Dzięki Forefront Security for Exchange Server, kilku dostawców rozwiązań antywirusowych pracuje nad metodami blokowania najnowszych zagrożeń, a automatyczne pobieranie aktualizacji gwarantuje, że gdy tylko pierwszy dostawca opracuje rozwiązanie, natychmiast będzie ono dostępne.

Zoptymalizowane działanie

- **Ustawienia optymalizacji działania.** Serwery działają sprawniej, a poczta wydajniej, gdyż jest ona skanowana w pamięci (aby uniknąć buforowania danych na dysku) i wielotorowo (aby skanować kilka e-maili naraz). Układ sterowania Forefront Security for Exchange Server, pozwalający dynamicznie zarządzać liczbą silników używanych w danym procesie skanowania, pomaga specjalistom IT zachować równowagę pomiędzy płynnością działania serwera a poziomem zabezpieczenia.
- **Wydajniejsze skanowanie na serwerach Transport i Store.** Pozwala na wyeliminowanie zbędnego skanowania poczty. Przy pierwszym skanowaniu na serwerze Exchange 2007 Edge lub Hub do nagłówka każdego e-maila dołączana jest „pieczęć bezpieczeństwa” (antivirus stamp). Tak oznaczony e-mail jest dostarczany już bez ponownego skanowania, co oszczędza moce procesora w serwerze Hub lub Store. Ponownego skanowania poczty sprzed kilku tygodni lub miesięcy, też można zaniechać, ograniczając zakres skanowania w tle. Narastające skanowanie w tle może zostać zawężone tylko do wiadomości, które są najbardziej prawdopodobnymi nośnikami wirusów, czyli tych z ostatnich kilku dni.
- **Niezakłócony przepływ poczty podczas aktualizacji.** Sygnatury silników skanujących są aktualizowane na bieżąco, a podczas procesu aktualizacji przepływ poczty nie jest hamowany. Wielosilnikowe rozwiązanie Forefront Security for Exchange Server polega na tym, że jeżeli jeden silnik zostaje wyłączony celem przeprowadzenia aktualizacji, pozostałe są w pełnej gotowości do skanowania poczty.
- **Skuteczna obsługa środowisk klastrowych.** Dzięki Forefront Security for Exchange Server zarówno aktywne, jak i pasywne węzły mają aktualną konfigurację i sygnatury. Obsługa konfiguracji klastrowych zawiera Exchange 2007 CCR Clusters.

Uproszczone zarządzanie

- **Forefront Server Security Administrator.** Wbudowana konsola do zarządzania umożliwia pełne – zarówno lokalne, jak i zdalne – konfigurowanie Forefront Security for Exchange Server.
- **Zcentralizowana kontrola w przeglądarce.** Przy pomocy konsoli Microsoft Forefront Server Security Management Console, wbudowanej w Forefront Security for Exchange Server, można zdalnie i bezproblemowo zarządzać serwerami, generować wszechstronne raporty i odbierać sygnały alarmowe z całej infrastruktury. Ta działająca w oknie przeglądarki konsola umożliwia centralną

konfigurację, instalowanie i aktualizację wszystkich produktów zabezpieczających Forefront.

- **Automatyczne aktualizacje.** Aktualizacja silników skanowania przebiega bez pomocy specjalistów z działu IT. Microsoft na bieżąco monitoruje dostawców rozwiązań antywirusowych, oczekując od nich nowych sygnatur i aktualizacji silników. W ciągu kilku minut te aktualizacje zostają przetestowane w bazach danych o wirusach, zatwierdzone i wysłane do automatycznej aktualizacji za pośrednictwem systemów Forefront Security for Exchange Server lub Microsoft Forefront Server Security Management Console.
- **Ochrona migracji.** W trakcie migracji do Exchange 2007 chronione jest całe środowisko wiadomości. Nabywcy Forefront Security for Exchange Server, chcący zabezpieczyć serwery Exchange 2007 otrzymają również licencję na użytkowanie Microsoft Antigen for Exchange, Microsoft Antigen for SMTP Gateways oraz Antigen Spam Manager, aby móc chronić serwery Microsoft Exchange Server 2003 i Microsoft Exchange Server 2000.
- **Lokalizacja na 11 języków.** Program występuje w językach angielskim, niemieckim, francuskim, japońskim, włoskim, hiszpańskim, koreańskim, chińskim uproszczonym, chińskim tradycyjnym, portugalskim (Brazylia) lub rosyjskim.
- **Zintegrowany monitoring.** Pakiet do zarządzania Microsoft Operations Manager (MOM) umożliwia monitorowanie stanu środowisk Forefront Security for Exchange Server, co jest częścią praktyk związanych z zarządzaniem infrastrukturą IT.

Wymagania systemowe Microsoft Forefront Security for Exchange Server

Opisane elementy i funkcjonalności wymagają Windows Server® 2003, Microsoft Exchange Server 2007 (dla wcześniejszych wersji Exchange – program Microsoft Antigen), komputera opartego o architekturę x64, 512MB pamięci RAM na każdy serwer (zaleca się 1GB) i 300 MB przestrzeni dyskowej.

Forefront Security for Exchange Server obsługuje Exchange działający na Microsoft Cluster Servers.

Więcej informacji na temat Microsoft Forefront Security for Exchange Server można znaleźć w witrynie <http://www.microsoft.com/forefront>