**Kaspersky Lab rozszerza ochronę dla maszyn wirtualnych**

**Kaspersky Lab wprowadza do sprzedaży Kaspersky Security for Virtualization 2.0, najnowszą wersję swojego rozwiązania do ochrony maszyn wirtualnych bazujących na platformie VMware. Dzięki integracji z nowymi funkcjami VMware vCloud Networking and Security produkt Kaspersky Lab oferuje dodatkowe funkcje wykrywania i ochrony przed zaawansowanymi atakami sieciowymi.**

Produkt zapewnia również znacznie ulepszoną ochronę antywirusową, wzbogaconą o obsługę chmury Kaspersky Security Network, dzięki której produkt otrzymuje w czasie rzeczywistym informacje o najnowszych zagrożeniach. Rezygnacja z modelu ochrony przy użyciu agenta sprawia, że Kaspersky Security for Virtualization 2.0 zapewnia równowagę między jakością ochrony a wydajnością sieci. Skanowanie całego ruchu sieciowego jest powierzane jednemu urządzeniu wirtualnemu, co sprawia, że firmy są w stanie maksymalnie wykorzystywać potencjał środowisk wirtualnych.

**Wgląd w zagrożenia komputerowe**

Narzędzia do wirtualizacji cieszą się rosnącym popytem w małych, średnich i dużych firmach. Niestety, w tym samym czasie firmy często zapominają, że maszyny wirtualne są narażone na cyberzagrożenia i potrzebują takiego samego poziomu ochrony jak standardowe stacje robocze.

W niektórych przypadkach firmy starają się rozwiązać ten problem za pomocą oprogramowania przeznaczonego do ochrony stacji roboczych i serwerów fizycznych. Dość powszechnym zjawiskiem jest uruchamianie kilkudziesięciu maszyn wirtualnych jednocześnie na tym samym serwerze fizycznym. Instalacja rozwiązań bezpieczeństwa na każdej maszynie wirtualnej z osobna może generować nadmierne obciążenie tego serwera. Problem ten jest szczególnie dotkliwy, gdy wykonywane są rutynowe czynności, takie jak aktualizacja baz sygnatur antywirusowych czy skanowanie na żądanie.

Zamiast stosowania na maszynach wirtualnych metod ochrony fizycznej, Kaspersky Lab proponuje wdrożenie rozwiązania bezpieczeństwa, które nie wykorzystuje agentów sieciowych, eliminuje potrzebę posiadania powielonych zasobów na każdej maszynie wirtualnej, pomaga w optymalizacji wydajności, redukuje koszty sprzętu i pobór energii, zapewniając jednocześnie szczegółowy rejestr zdarzeń związanych z bezpieczeństwem, spełniający nawet najsurowsze wymogi audytów zgodności.

*„Firmy coraz częściej rozumieją, że maszyny wirtualne muszą być chronione tak samo jak sprzęt fizyczny”* - powiedział Petr Merkulow, dyrektor ds. produktów, Kaspersky Lab. *„Z kolei Kaspersky Lab bacznie podąża za zapotrzebowaniem rynku i opracowuje rozwiązania, które sprostają tym oczekiwaniom. Możemy powiedzieć z przekonaniem, że najnowsza wersja Kaspersky Security for Virtualization 2.0 jest w pełni zgodna z aktualnym zapotrzebowaniem na ochronę maszyn wirtualnych przed rzeczywistymi zagrożeniami. Zapewniając, z poziomu jednej konsoli, administrację systemami fizycznymi i wirtualnymi, produkt doskonale pracuje w połączeniu z innymi rozwiązaniami biznesowymi Kaspersky Lab, gwarantując integralną ochronę kompletnej infrastruktury IT”.*

Warto również zauważyć, że Kaspersky Security for Virtualization 2.0 jest pierwszym rozwiązaniem integrującym się z VMware vCloud Ecosystem Framework – składnikiem VMware vCloud Networking and Security, który jest szeroko stosowany w nowoczesnej infrastrukturze informatycznej.

**Najważniejsze cechy produktu**

Kaspersky Security for Virtualization 2.0 posiada kilka cech, które gwarantują wydajną ochronę maszyn wirtualnych.

Przykładem może być **ochrona sieci**. Jest to narzędzie konieczne zarówno w sieciach fizycznych, jak i wirtualnych, służące do skanowania przychodzącego, wychodzącego i wewnętrznego ruchu sieciowego pod kątem prób wtargnięcia do sieci. Kaspersky Security for Virtualization 2.0 zawiera system ochrony przed włamaniami (IDS / IPS) i zapewnia w ten sposób bezpieczeństwo sieci wirtualnej. Jest to możliwe dzięki integracji z VMware vCloud Ecosystem Framework – części rozwiązania vCloud Networking and Security. Kaspersky Lab jest pierwszym producentem oprogramowania, który z powodzeniem zintegrował tę technologię z własnym produktem.

Ochrona przed szkodliwym oprogramowaniem z wykorzystaniem **Kaspersky Security Network** jest kolejną użyteczną funkcją, dostępną w Kaspersky Security for Virtualization 2.0. Złośliwe oprogramowanie stanowi jedno z najbardziej rozpowszechnionych zagrożeń dla systemów fizycznych i wirtualnych. Kaspersky Security for Virtualization 2.0 chroni przed szkodnikami system plików maszyny wirtualnej w czasie rzeczywistym przy użyciu chmury Kaspersky Security Network, która dostarcza informacje na temat pojawiających się zagrożeń, dzięki czemu natychmiast mogą zostać wdrożone odpowiednie środki ochrony.

Funkcja **współdzielonej pamięci podręcznej (Shared Cache)** poprawia wydajność ochrony. Stacje robocze na maszynach wirtualnych mogą zawierać kilka identycznych obiektów, np. plików systemowych. Skanowanie tych plików na każdej maszynie wirtualnej stwarza dodatkowe obciążenie serwera. Funkcja Shared Cache pozwala na uniknięcie takich sytuacji. Kiedy tylko produkt Kaspersky Security for Virtualization 2.0 przeskanuje plik na maszynie wirtualnej i stwierdzi, że jest on bezpieczny, werdykt ten zostanie zapisany w pamięci podręcznej aplikacji. Jeśli w przyszłości produkt Kaspersky Lab natknie się na podobny plik na innych maszynach wirtualnych, nie będzie marnował czasu na jego skanowanie, a jedynie użyje zapisanego wcześniej werdyktu.

Elastyczny model licencjonowania pozwala na szybkie zdefiniowanie odpowiedniej liczby licencji na oprogramowanie, niezbędnej do zapewnienia pełnej ochrony wirtualnej infrastruktury firmy. Właściciele centrów danych i usług infrastrukturalnych często mają kłopot z szacowaniem liczby aktywnych stacji roboczych i serwerów wirtualnych. Nowy model licencjonowania „na rdzeń” rozwiązuje ten problem - firmy mogą zakupić licencję na każdy rdzeń procesora, który zawiaduje maszynami wirtualnymi, co pozwala na objęcie licencjonowaniem dowolnej liczby maszyn wirtualnych.

Brak scentralizowanych narzędzi zarządzania może stać się problemem podczas zarządzania wieloskładnikową infrastrukturą informatyczną firmy. Dzięki modułowi Kaspersky Security Center specjaliści ds. IT mogą monitorować stan wszystkich chronionych firmowych stacji roboczych, zarówno fizycznych, jak i wirtualnych. Jest to szczególnie wygodne, gdy pozostałe węzły sieci firmowej również są chronione przez produkty i technologie Kaspersky Lab. Scentralizowane zarządzanie znacznie ułatwia ochronę maszyn wirtualnych i pomaga we wdrożeniu spójnych polityk bezpieczeństwa.

**Dostępność Kaspersky Security for Virtualization 2.0**

Produkt może być zakupiony jako odrębne rozwiązanie ochrony dla środowisk VMware lub zintegrowany w pełnym zestawie technologii Kaspersky Lab do ochrony punktów końcowych. W celu szczegółowego zapoznania się z dostępnością i ceną produktu prosimy o kontakt z Kaspersky Lab Polska ([sprzedaz@kaspersky.pl](http://mailto:sprzedaz@kaspersky.pl)).

Film demonstrujący sposób działania ochrony Kaspersky Lab dla środowisk wirtualnych jest dostępny na stronie <http://youtu.be/nqVd_IphSxw>.

Więcej informacji na temat produktu Kaspersky Security for Virtualization 2.0 znajduje się na stronie <http://www.kaspersky.pl/beready> przygotowanej przez ekspertów z Kaspersky Lab specjalnie z myślą o firmach. Witryna ta zawiera szczegółowe informacje na temat rozwiązań Kaspersky Lab dla biznesu, a także wiele porad, które mogą pomóc w stworzeniu skutecznej polityki bezpieczeństwa uwzględniającej systemy wirtualne, prywatne smartfony, tablety i laptopy pracowników.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.