A background image showing a laptop on a desk with a circular gauge overlay. The gauge has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office environment.

## Wyzwania w zakresie zabezpieczeń wirtualizacji

Koordinacja zabezpieczeń



### Ochrona serwerowa maszyn wirtualnych

*Dokument White Paper firmy Trend Micro  
Sierpień 2009*

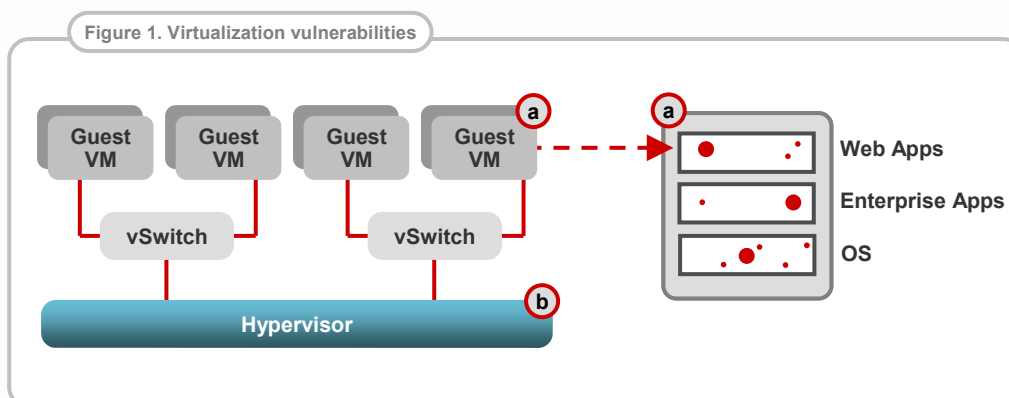
## I. WPROWADZENIE

Wirtualizacja daje organizacjom możliwość zwiększenia wydajności i oszczędności oraz uzyskiwania dodatkowych korzyści związanych z bardziej ekologicznymi, skonsolidowanymi centrami danych, większą skalowalnością oraz szybszym działaniem zasobów. Niestety zalety wirtualizacji są niwelowane przez zwiększone ryzyko zagrożeń, ponieważ systemy wirtualne w centrach danych są narażone, obok szeregu problemów w zakresie ochrony zasobów informatycznych, na takie same problemy, jakie występują w przypadku serwerów fizycznych. Organizacja musi sama ocenić, które mechanizmy zabezpieczeń będą najlepiej chronić zarówno serwery fizyczne, jak i serwery wirtualne — szczególnie w odniesieniu do sposobu wpływu architektury zwirtualizowanej na projektowanie i wdrażanie aplikacji o kluczowym znaczeniu oraz zarządzanie nimi.

Firma Trend Micro oferuje skuteczne rozwiązania, które pozwalają stawić czoła tym wyzwaniom. Dzięki innowacyjnym technologiom uzyskanym w wyniku przejęcia firmy Third Brigade oraz naszemu wieloletniemu doświadczeniu na rynku zabezpieczeń opracowaliśmy skoordynowane rozwiązanie do bezpośredniego wdrożenia, obejmujące systemy wykrywania włamań i zapobiegania im, zapórę oraz funkcje monitorowania spójności, kontroli dziennika, a także ochrony przed złośliwym oprogramowaniem. Architektura tego rozwiązania umożliwia korzystanie z najnowszych funkcji dodawanych przez producentów platform wirtualizacji, na przykład niedawno wprowadzonej na rynek platformy VMware vSphere™ 4, oferującej dostęp do interfejsów API VMware VMsafe™. Zapewniamy niezbędny poziom ochrony aplikacji o kluczowym znaczeniu w środowiskach zwirtualizowanych. W niniejszym dokumencie omówiono skoordynowane rozwiązanie firmy Trend Micro w zakresie ochrony serwerowej maszyn wirtualnych.

## II. WYZWANIA W ZAKRESIE ZABEZPIECZEŃ WIRTUALIZACJI

Wirtualny system zarządzający aplikacjami internetowymi i aplikacji przedsiębiorstwa korzysta z tego samego systemu operacyjnego co system fizyczny. Najważniejszym zagrożeniem dla takich systemów wirtualnych są złośliwe programy, które zdalnie wykorzystują luki w tych systemach i aplikacjach (rys. 1a), chociaż istnieją także luki wykorzystywane do ataku w obszarze hypervisor systemu (rys. 1b).



Producenci systemów wirtualnych pracują nad dalszym uproszczeniem konsoli usług, np. w środowisku VMware ESXi, co umożliwi znaczne ograniczenie ewentualnego obszaru narażenia na atak. Większości luk obszaru hypervisor nie będzie można wykorzystać zdalnie, ponieważ obszar hypervisor nie zawiera usług stanowiących zakończenie protokołów zdalnych. Luki te będą zwykle wykorzystywane przez złośliwe oprogramowanie atakujące maszynę wirtualną (VM). Jednym z najlepszych sposobów ochrony luk w zabezpieczeniach obszaru hypervisor jest blokowanie instalacji złośliwego oprogramowania w środowisku wirtualnym.

Dynamiczny charakter środowisk zwirtualizowanych stawia nowe wyzwania przed systemami wykrywania włamań i zapobiegania im (IDS/IPS). Maszyny wirtualne można szybko przywracać do poprzedniego stanu oraz łatwo przenosić między serwerami fizycznymi, jednak z tego względu trudno jest osiągnąć i utrzymać spójne zabezpieczenia.

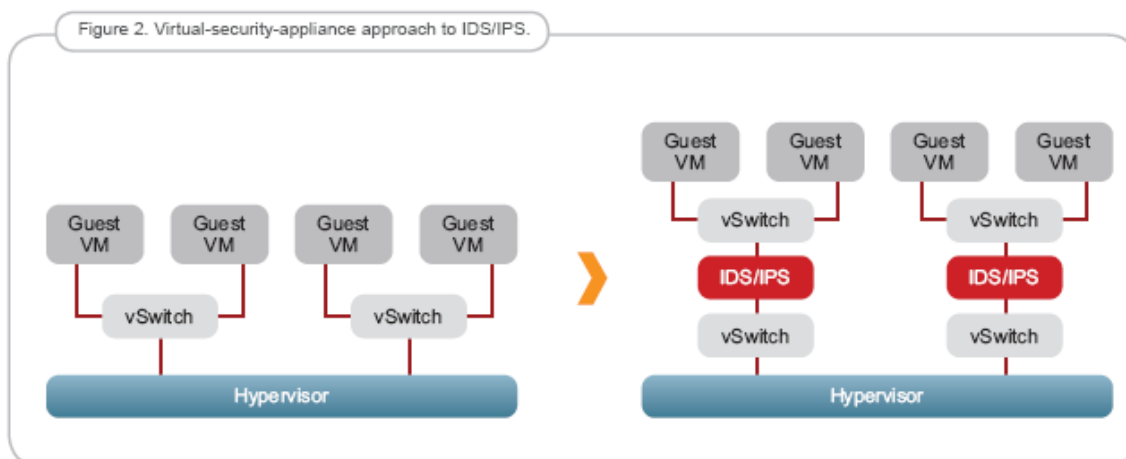
W celu uzyskania efektywnego rozwiązania w zakresie zabezpieczeń należy trzymać się tych samych zasad co w przypadku ochrony fizycznych zasobów informatycznych. Jedną z tych zasad jest „dogłębna ochrona”, która jest podstawowym wymogiem zabezpieczeń organizacji z zanikającymi granicami zabezpieczeń w ich infrastrukturze informatycznej. Zasada ta jest obsługiwana przez najlepsze rozwiązania branżowe, a organizacje takie jak Jericho Forum uwzględniają ją w swoich zaleceniach dotyczących zabezpieczeń. Wirtualizacja jeszcze bardziej uwypukliła problem zanikających granic zabezpieczeń i potrzeby wdrażania najlepszych rozwiązań z zakresu bezpieczeństwa. Przyczyną tego jest brak możliwości stosowania zabezpieczeń w odniesieniu do ataków występujących między maszynami wirtualnymi w obrębie jednego systemu fizycznego. W takim przypadku niezbędne jest zastosowanie najlepszych rozwiązań. Inne zasady zaprezentowane na forum to między innymi:

- Zakres i poziom ochrony powinien być właściwie dobrany do zasobu.
- Zabezpieczenia powinny wspomagać prężność działania firmy i być ekonomiczne.
- Zapory nadal mogą stanowić podstawową ochronę sieci, jednak poszczególne systemy i dane powinny mieć własne systemy ochrony.
- Ogólnie: im bliżej zasobu znajduje się zabezpieczenie, tym łatwiej jest taki zasób chronić.

Jeśli powyższe zasady odniesiemy do zwirtualizowanego centrum danych, dostrzeżemy konieczność wdrożenia bezpośrednio na serwerze fizycznym pewnych mechanizmów, które umożliwią ochronę systemów wirtualnych. Zgodnie z takim podejściem będą to zabezpieczenia wirtualizacji umożliwiające ochronę w jak najbliższym otoczeniu zasobu.

### III. OBECNE ROZWIĄZANIA W DZIEDZINIE ZABEZPIECZEŃ WIRTUALIZACJI

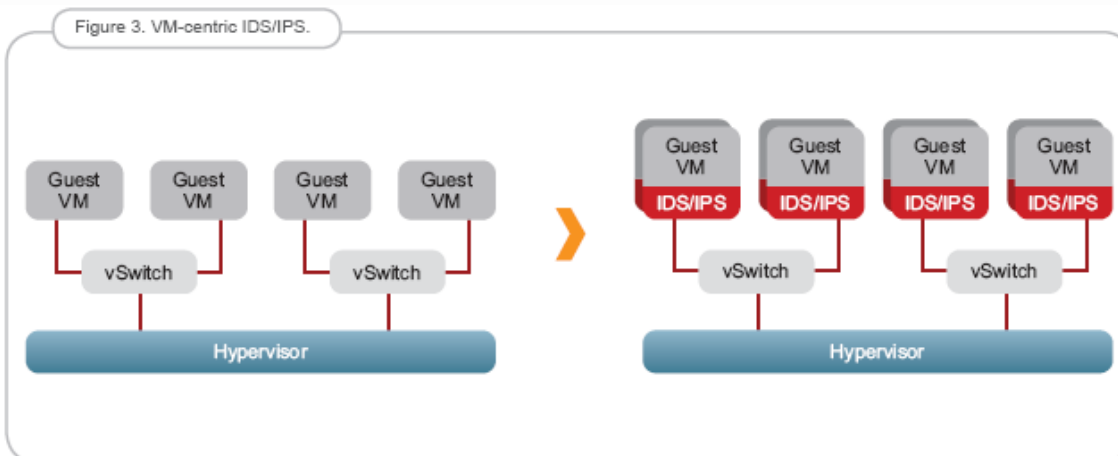
Poza powszechnie stosowanymi zabezpieczeniami przeznaczonymi dla interfejsów API program VMware VMsafe istnieją dwa rozwiązania ochrony maszyn wirtualnych. Pierwszym z nich jest zastosowanie zabezpieczenia w środowisku wirtualnym do monitorowania ruchu między przełącznikami wirtualnymi (vSwitch) a co najmniej jedną maszyną wirtualną (rys. 2).



Zabezpieczenie wirtualne zapewnia ochronę IDS/IPS przed atakami inicjowanymi z sieci, ma jednak szereg ograniczeń:

- **Ruch sieciowy między maszynami wirtualnymi** — zabezpieczenia wirtualne muszą znajdować się przed przełącznikiem wirtualnym i nie chronią przed atakami występującymi między dwiema maszynami wirtualnymi w obrębie jednego przełącznika.
- **Mobilność** — jeśli do przeniesienia maszyny wirtualnej z jednego serwera fizycznego na drugi jest używane takie narzędzie jak VMware VMotion™, zostaje utracony kontekst zabezpieczeń. Konieczne jest skonfigurowanie klastrowania zabezpieczeń wirtualnych dla każdego potencjalnego miejsca docelowego maszyny wirtualnej, dzięki czemu można zapobiec negatywnemu wpływowi na wydajność.
- **Brak przejrzystości** — architektura sieci wirtualnej przy dodawaniu zabezpieczeń wirtualnych musi ulec zmianie, dlatego ma to wpływ na administrowanie istniejącym systemem i na jego wydajność.
- **Wąskie gardła wydajności** — zabezpieczenie wirtualne musi przetwarzać cały ruch odbywający się między maszynami wirtualnymi a siecią, co może spowodować powstawanie wąskich gardeł wydajności.

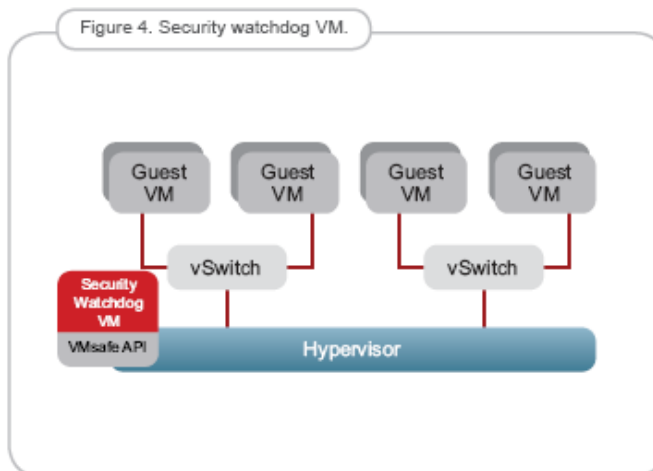
W przypadku drugiego rozwiązania tę samą funkcję IDS/IPS można wdrożyć na każdej maszynie wirtualnej (rys. 3).



W przeciwieństwie do metody zabezpieczeń wirtualnych podejścia ukierunkowanego na maszyny wirtualne nie cechują ograniczenia związane z ruchem sieciowym między maszynami wirtualnymi, mobilnością czy brakiem przejrzystości. Wprawdzie ta opcja wpływa na wydajność systemu, jednak jest rozproszona na maszynach wirtualnych w ramach danej infrastruktury informatycznej. Architektura ukierunkowana na maszyny wirtualne wymaga jednak wdrożenia na każdej maszynie wirtualnej agenta zabezpieczeń IDS/IPS. Procedurę tę można uprościć za pomocą różnych mechanizmów, na przykład szablonów, czyli — jak to określono w samouczku online „Working with Templates” opublikowanym przez firmę VMware — wdrażając wspólnego agenta zabezpieczeń na wszystkich maszynach wirtualnych. Dynamiczny charakter środowiska zwirtualizowanych może jednak powodować wprowadzanie maszyn wirtualnych w środowisku produkcyjnym bez zastosowania agenta zabezpieczeń.

## IV. STRAŻNICZA MASZYNA WIRTUALNA

Program VMware VMsafe umożliwia wdrożenie specjalnych maszyn wirtualnych z uprzywilejowanym dostępem do interfejsów API obszaru hypervisor. Dzięki temu można utworzyć specjalne narzędzie zabezpieczeń w postaci strażniczej maszyny wirtualnej, wspomnianej w raporcie pod tytułem „Radically Transforming Security and Management in a Virtualized World: Concepts” firmy Gartner. Strażnicza maszyna wirtualna stanowi nową metodę wdrażania zabezpieczeń w środowisku wirtualnym (rys. 4).



Funkcje strażnicze wykorzystują interfejsy API z możliwością samoobserwacji do uzyskiwania dostępu do uprzywilejowanych informacji poszczególnych maszyn wirtualnych, w tym do informacji o ich pamięci, stanie i ruchu sieciowym. Eliminuje to wszelkie ograniczenia związane z ruchem sieciowym między maszynami wirtualnymi oraz przejrzystością zabezpieczeń wirtualnych w przypadku filtrowania IDS/IPS, ponieważ cały ruch sieciowy w obrębie serwera jest widoczny bez zmieniania konfiguracji sieci wirtualnej. W przypadku filtrowania IDS/IPS na strażniczych maszynach wirtualnych należy jednak liczyć się z pewnym wpływem na mobilność i wydajność.

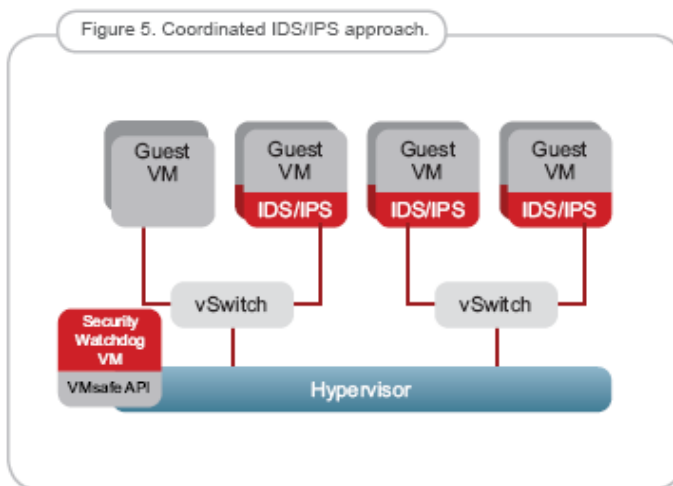
Na strażniczych maszynach wirtualnych można zastosować szeroką gamę funkcji zabezpieczeń, w tym zabezpieczenie antywirusowe, szyfrowanie, zaporę, IDS/IPS oraz funkcję sprawdzania spójności systemu. Zabezpieczenia wirtualne są konfigurowane tak, aby korzystały z tych interfejsów API. Dotyczy to także technologii ukierunkowanych na maszyny wirtualne, które również zostaną przeprojektowane tak, aby działały na strażniczych maszynach wirtualnych. W takich środowiskach będzie jednak wymagana pewna elastyczność, ponieważ:

- Pewne funkcje zabezpieczeń można uzyskać wyłącznie przy użyciu agentów w środowiskach ukierunkowanych na maszyny wirtualne, na przykład w odniesieniu do obsługi ruchu szyfrowanego czy uzyskiwania dostępu do pewnych informacji o stanie w czasie rzeczywistym.
- Trzeba znaleźć kompromis między wdrażaniem rozwiązania za pośrednictwem strażniczej maszyny wirtualnej a wdrażaniem agenta w środowisku ukierunkowanym na maszyny wirtualne.
- Niezbędne interfejsy API z możliwością samoobserwacji są opracowywane i publikowane etapami w miarę rozbudowy funkcji strażniczej maszyny wirtualnej.

W celu uzyskania inteligentnych i oszczędnych opcji zabezpieczeń ograniczających występowanie wąskich gardeł wydajności i zapewniających nadmiarową kontrolę wymagane jest skoordynowane rozwiązanie zapewniające korzyści zarówno płynące z zastosowania środowiska ukierunkowanego na maszyny wirtualne, jak i wynikające z zastosowania interfejsów API z możliwością samoobserwacji. Firma Trend Micro oferuje rozwiązanie spełniające to wymaganie.

## V. SKOORDYNOWANE ROZWIĄZANIE W ZAKRESIE ZABEZPIECZEŃ

Nasze skoordynowane rozwiązanie ochrony środowisk zwirtualizowanych składa się z agenta w technologii ukierunkowanej na maszyny wirtualne z możliwością wdrożenia na poszczególnych maszynach wirtualnych oraz ze strażniczej maszyny wirtualnej wdrożonej w celu ochrony wielu maszyn wirtualnych. Dzięki takiej architekturze wszelkie zasoby informatyczne o kluczowym znaczeniu — maszyny wirtualne — mogą być chronione przez wdrożenie



oprogramowania bezpośrednio na tych zasobach, podczas gdy pozostałe zasoby o mniejszym znaczeniu mogą być chronione przez strażniczą maszynę wirtualną (rys. 5).

## ZINTEGROWANE ROZWIĄZANIE

Nasze skoordynowane rozwiązanie obejmuje sześć aspektów. Przyjrzyjmy się im w dalszej części tego dokumentu.

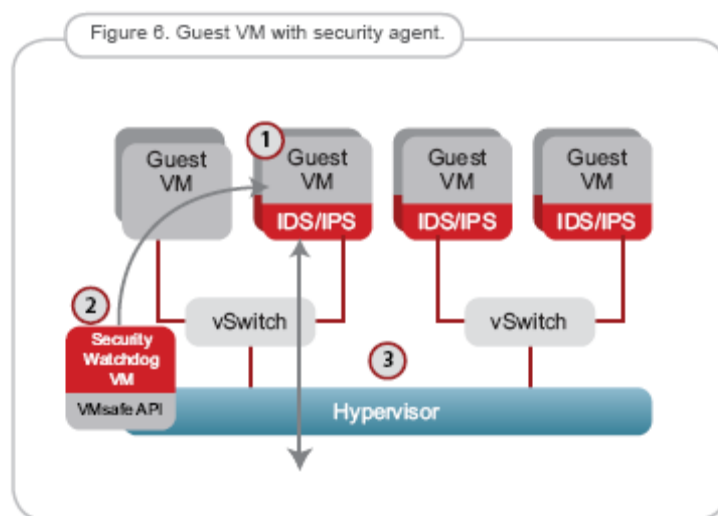
- Koordynacja systemów wykrywania włamań i zapobiegania im
- Integracja zarządzania wirtualizacją
- Zarządzanie korporacyjne
- Kompleksowa funkcjonalność IDS/IPS
- Wiele architektur wirtualizacji
- Modele licencjonowania oprogramowania

## KOORDYNACJA SYSTEMÓW WYKRYWANIA WŁAMAŃ I ZAPOBIEGANIA IM

Kolejność koordynacji przedstawia się następująco:

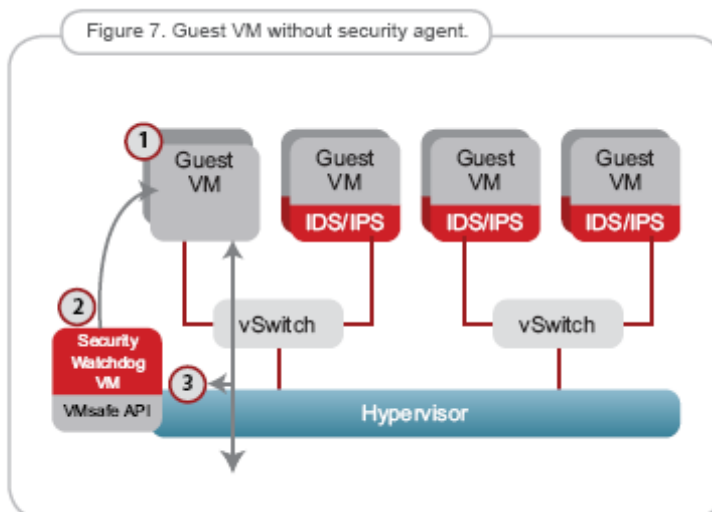
- Strażnicza maszyna wirtualna zostaje powiadomiona o włączeniu maszyny wirtualnej.
- Jeśli strażnicza maszyna wirtualna wykryje agenta zabezpieczeń na maszynie wirtualnej-gościu lub konieczność wdrożenia takiego agenta, sprawdza poprawność wersji i konfiguracji zabezpieczeń wdrożonego oprogramowania i w razie potrzeby aktualizuje konfigurację.
- W wyniku tego maszyna wirtualna-gość zyskuje aktualną ochronę i może się komunikować w obrębie sieci, kierując ruch bezpośrednio z obszaru hypervisor do maszyny wirtualnej.

Na rysunku 6 poniżej przedstawiono koordynację między strażniczą maszyną wirtualną a agentem w technologii ukierunkowanej na maszyny wirtualne.



Jak już wspomniano, agent zabezpieczeń nie musi być zainstalowany na wszystkich maszynach wirtualnych. Na rys. 7 przedstawiono koordynację w sytuacji, gdy maszyna wirtualna-gość została wdrożona bez agenta.

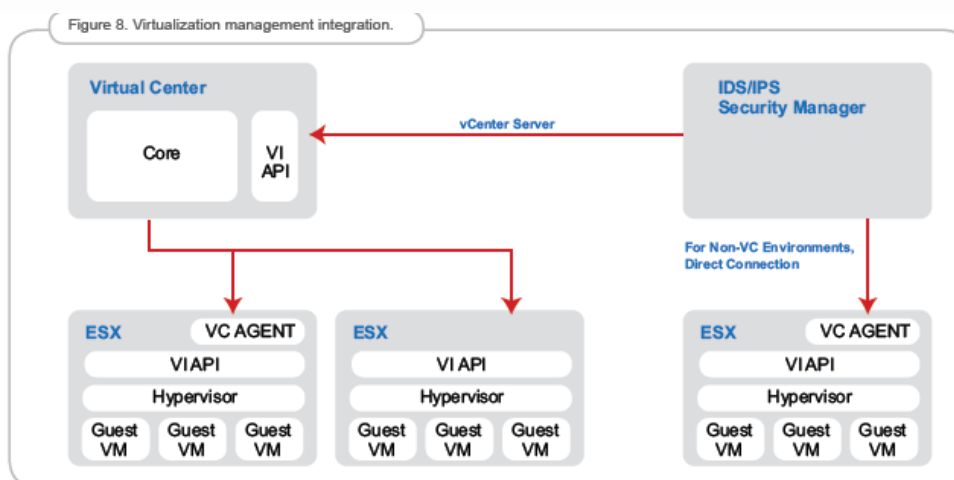
- Po uruchomieniu maszyny wirtualnej-gościa jest powiadamiana strażnicza maszyna wirtualna.
- Jeśli maszyna wirtualna-gość nie wymaga wdrożenia agenta, strażnicza maszyna wirtualna sprawdza konfigurację gościa i stosuje odpowiednie filtrowanie IDS/IPS.
- Dane przepływają od strażniczej maszyny wirtualnej przez interfejsy API programu VMsafe z zastosowanym filtrowaniem IDS/IPS.



Zaletą takiej architektury jest brak znacznych opóźnień ruchu kierowanego do maszyn wirtualnych przy użyciu wdrożonego agenta zabezpieczeń IDS/IPS, ponieważ ruch ten jest kierowany bezpośrednio z obszaru hypervisor do maszyny wirtualnej-gościa. Ruch kierowany do maszyn wirtualnych bez wdrożonego agenta może być przetwarzany centralnie przez strażniczą maszynę wirtualną przy minimalnym wpływie na wydajność.

## INTEGRACJA ZARZĄDZANIA WIRTUALIZACJĄ

Platformy wirtualizacji zwykle obejmują scentralizowany system zarządzania wdrażaniem hostów fizycznych i maszyn wirtualnych, na przykład VMware vCenter Server. Funkcja zarządzania zabezpieczeniami systemu IDS/IPS łączy się z tym systemem zarządzania wirtualizacją w celu uzyskania konfiguracji hostów i maszyn wirtualnych (rys. 8).



Następnie przy użyciu podobnej struktury można wyświetlić układ systemów w oknie menedżera zabezpieczeń IDS/IPS w celu łatwego i efektywnego zarządzania hostami fizycznymi i maszynami wirtualnymi (rys. 9).

## ZARZĄDZANIE KORPORACYJNE

Systemy IDS/IPS klasy korporacyjnej zapewniają scentralizowane zarządzanie zabezpieczeniami zintegrowane z zarządzaniem wirtualizacją. Funkcja ta definiuje i rozpowszechnia zasady do składników egzekwowania systemu IDS/IPS i gromadzi zdarzenia wykonywane przez te składniki, na przykład zdarzenia wykrycia ataków i zapobiegania im. Pozostałe elementy scentralizowanego zarządzania zabezpieczeniami w rozproszonym systemie IDS/IPS:

- Skalowalność zarządzania — składnik zarządzania powinien obsługiwać wirtualizację wielu maszyn wirtualnych w celu zapewnienia skalowalnego wdrożenia i wysokiej dostępności.
- Punkty integracji — np. usługi syslog i usługi sieci Web umożliwiające integrację funkcji IDS/IPS z innymi elementami zabezpieczeń korporacyjnych, w tym informacje o zabezpieczeniach czy systemy zarządzania zdarzeniami (SIEM).
- Pomocnicze funkcje zabezpieczeń — np. oparta na rolach kontrola dostępu i historia inspekcji działań administratora.
- Oceny zewnętrzne, np. ocena Common Criteria for Information Technology Security Evaluation — pomagają w weryfikacji szeregu parametrów zabezpieczeń.

## KOMPLEKSOWA FUNKCJONALNOŚĆ IDS/IPS

Chociaż funkcja analizy ruchu sieciowego jest używana zarówno w przypadku zabezpieczeń wirtualnych, jak i agentów w technologii ukierunkowanej na maszyny wirtualne, wytyczne „NIST Guide to Intrusion Detection and Prevention Systems” określają oparte na hostach systemy wykrywania włamań i zapobiegania im przy użyciu następujących kryteriów:

- Analiza kodu
- Analiza ruchu sieciowego — zaawansowana kontrola pakietów i kontrola protokołu aplikacji
- Filtrowanie ruchu sieciowego — zapora
- Monitorowanie systemu plików
- Analiza dziennika
- Monitorowanie konfiguracji sieci

W celu zapewnienia spójnych zabezpieczeń każdy z tych obszarów wymaga także koordynacji między agentami w technologii ukierunkowanej na maszyny wirtualne a strażniczymi maszynami wirtualnymi.

Figure 9. Hosts and virtual machines.



## **WIELE PLATFORM WIRTUALIZACJI**

Wprawdzie VMware jest czołową marką na rynku, lecz istnieją też platformy wirtualizacji opracowane przez innych producentów, m.in. Microsoft Windows Server Virtualization i Citrix XenServer. Funkcje strażniczej maszyny wirtualnej będą się różnić w zależności od platformy, jednak skoordynowane rozwiązanie firmy Trend Micro będzie skuteczne na każdej z nich.

## **MODELE LICENCJONOWANIA OPROGRAMOWANIA**

Przejęcie do środowisk zwirtualizowanych spowodowało większy nacisk na zagadnienia licencjonowania oprogramowania, ponieważ wirtualizacja znacząco wpłynęła na sposób udostępniania oprogramowania, podobnie jak kiedyś oprogramowanie zrewolucjonizowało korzystanie ze sprzętu. Organizacje oczekują rozszerzenia licencji z powodu szerszego wykorzystania oprogramowania dzięki odpowiedniej, korzystnej finansowo ofercie. Ponieważ organizacje stosują skoordynowane rozwiązanie do systemów IDS/IPS, wymagane są elastyczne i przyszłościowe wersje licencji dostosowanych zarówno do środowisk fizycznych, jak i środowisk wirtualnych. Dotyczy to m.in. możliwości nabycia licencji dla agentów IDS/IPS dla poszczególnych maszyn wirtualnych, a także licencji na funkcję IDS/IPS dla nieograniczonej liczby maszyn wirtualnych na serwerze fizycznym. Mechanizmy zarządzania licencjami powinny zapewnić organizacjom nieskomplikowane śledzenie wykorzystania licencji w dynamicznym środowisku wirtualnym.

## **VI. PODSUMOWANIE**

Wiele problemów charakterystycznych dla środowisk fizycznych dotyczy też wirtualnej infrastruktury informatycznej, tak więc środowiska wieloprocessorowe, architektury wielordzeniowe i oprogramowanie do wirtualizacji wymagają odpowiednich mechanizmów bezpieczeństwa. Ponadto wirtualne zasoby informatyczne na platformach wirtualizacji mogą być obecnie i w przyszłości chronione przez funkcje z możliwością samoobserwacji, takie jak interfejsy API programu VMsafe. Wdrażając skoordynowane rozwiązanie oraz oprogramowanie firmy Trend Micro w zakresie zabezpieczeń, można zapewnić optymalną ochronę wszystkich maszyn wirtualnych bez wąskich gardeł czy nadmiarowych narzędzi kontroli. Firma Trend Micro daje możliwość rozszerzenia środowiska wirtualnego na wszystkie używane systemy o kluczowym znaczeniu.

## **VII. DLACZEGO WARTO WYBRAĆ FIRMĘ TREND MICRO?**

Trend Micro zajmuje się zabezpieczeniami informacji od samego początku swojego istnienia, tj. od 20 lat. Firma uzyskuje roczne przychody rzędu 1 mld USD, zatrudnia ponad 1000 ekspertów do badania zagrożeń oraz 4000 pracowników na całym świecie. Ponadto firma dysponuje odpowiednią skalą i szybkością działania oraz unikatową infrastrukturą otoczenia sieciowego, służącą do zapewniania bezpieczeństwa informacji w firmach. Żadna inna firma nie jest w stanie dorównać ofercie firmy Trend Micro kierowanej do przedsiębiorstw. Dlatego tysiące przedsiębiorstw z całego świata zaufało firmie Trend Micro.

Ponieważ rośnie tempo powstawania zagrożeń, rośnie także ryzyko i koszty. Przedsiębiorstwa poszukują zabezpieczeń z możliwością skalowania, zarządzania i blokowania nowych zagrożeń. Tylko firma Trend Micro oferuje wyjątkowe połączenie natychmiastowej ochrony i prostoty obsługi.

Rozwiązanie Trend Micro Enterprise Security, oparte na innowacyjnej infrastrukturze Smart Protection Network, zapewnia natychmiastową ochronę, która jest ciągle aktualizowana, zamykając luki w zabezpieczeniach i zapobiegając awarii systemu. Produkty firmy Trend Micro gwarantują krótki czas zakupu, wdrożenia i zarządzania zabezpieczeniami. Dzięki rozwiązaniu Trend Micro Enterprise Security przedsiębiorstwa minimalizują czas wymagany do obsługi zabezpieczeń, obniżając tym samym ryzyko i koszty.

Aby uzyskać więcej informacji, można do nas zadzwonić lub odwiedzić naszą witrynę pod adresem <http://emea.trendmicro.com/emea/solutions/enterprise/security-solutions/virtualization/>

### VIII. LITERATURA

- Gartner, Radically Transforming Security and Management in a Virtualized World: Concepts, Neil MacDonald, 14 marca 2008
- Common Criteria for Information Technology Security Evaluation, [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)
- Jericho Forum, [www.jerichoforum.org/](http://www.jerichoforum.org/)
- NIST Guide to Intrusion Detection and Prevention Systems, <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- VMware, [www.vmware.com/overview/security/vmsafe.html](http://www.vmware.com/overview/security/vmsafe.html)
- Samouczek firmy VMware: „Working with Templates”, [www.vmware.com/support/vc13/doc/c13templateintro.html](http://www.vmware.com/support/vc13/doc/c13templateintro.html)
- VM World News, [www.vmware.com/vmworldnews/esx.html](http://www.vmware.com/vmworldnews/esx.html)

©2009 Trend Micro, Incorporated. Wszelkie prawa zastrzeżone. Trend Micro i logo t-ball są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Trend Micro Incorporated. Pozostałe nazwy firm i produktów mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. Informacje zawarte w niniejszym dokumencie mogą ulec zmianie bez powiadomienia. (WP01\_VirtSec\_080911PL)