IBM Tivoli Endpoint Manager for Core Protection

Ochrona punktów końcowych przed szkodliwym oprogramowaniem i innymi zagrożeniami

Najważniejsze informacje

- W czasie rzeczywistym chroni punkty końcowe przed wirusami, końmi trojańskimi, oprogramowaniem szpiegującym, programami rootkit i innym szkodliwym oprogramowaniem.
- Do zapewnienia ochrony wykorzystuje takie metody, jak weryfikowanie reputacji plików i stron WWW, monitorowanie zachowania i osobisty firewall.
- Rozpoznaje środowiska zwirtualizowane i uwzględnia ich specyfikę, aby ograniczyć rywalizację o zasoby.
- Wykorzystuje czołowe rozwiązania techniczne firm IBM® oraz Trend Micro™ i udostępnia infrastrukturę zarządzania za pośrednictwem pojedynczej konsoli.

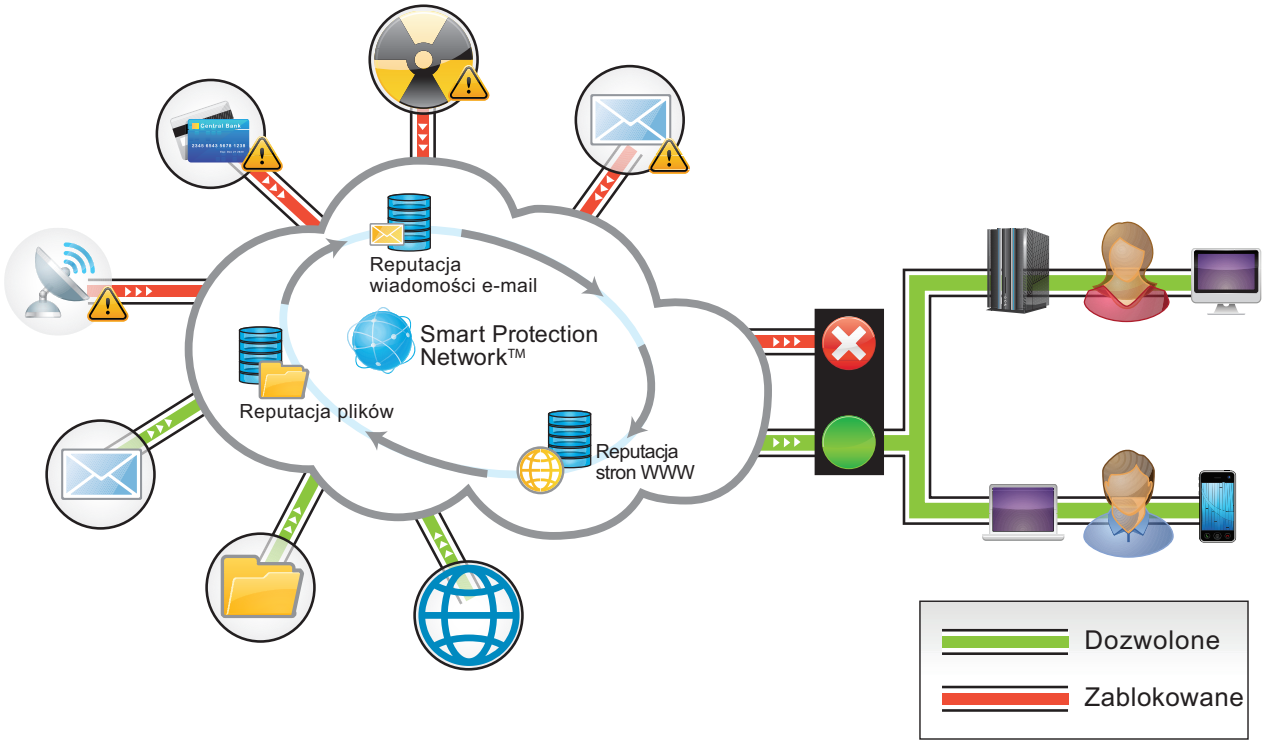
Rosnąca liczba i częstotliwość ataków dokonywanych z użyciem szkodliwego oprogramowania sprawia, że bieżąca ochrona punktów końcowych i danych staje się coraz trudniejsza. Nie jest to jednak jedyny aspekt zagrożenia. Ataki prowadzone są szybciej, a agresorzy wykorzystują słabe punkty zabezpieczeń natychmiast po ich odkryciu.

Organizacje zwykle przezornie wdrażają środki ochrony przed atakami, jednak środki te często same stają się częścią problemu, ponieważ złożone są z wielu skomplikowanych warstw, w których funkcjonują liczne produkty realizujące pojedyncze funkcje. Taki system ochrony nie jest w stanie odpowiednio szybko reagować na zagrożenie.

IBM Tivoli® Endpoint Manager for Core Protection stanowi zautomatyzowane, łatwe w użyciu rozwiązanie zdolne do wykrywania i usuwania szkodliwego oprogramowania zanim jeszcze zdoła ono wykorzystać słabe punkty zabezpieczeń. Za pośrednictwem pojedynczej konsoli udostępnia takie funkcje ochronne, jak wykrywanie i usuwanie szkodliwego oprogramowania, weryfikacja reputacji plików i stron WWW oraz osobisty firewall.

Wzmocniona ochrona rozproszonych punktów końcowych

Rozwiązanie proponowane przez IBM chroni fizyczne i wirtualne punkty końcowe przed szkodami wyrządzanymi przez wirusy, konie trojańskie, robaki, programy szpiegujące, programy rootkit i ataki pochodzące z sieci WWW — z uwzględnieniem ich najnowszych wariantów. Ogranicza ryzyko zakłóceń w działalności biznesowej, jakie mogą wystąpić w wyniku zainfekowania punktu końcowego, kradzieży tożsamości, utraty danych, przestoju sieci, spadku produktywności pracy i naruszeń formalnych norm bezpieczeństwa.



Tivoli Endpoint Manager for Core Protection powstrzymuje zagrożenia zanim zdołają się uaktywnić, w czasie rzeczywistym sprawdzając pliki, adresy URL i wiadomości e-mail pod kątem potencjalnej szkodliwości.

Tivoli Endpoint Manager for Core Protection weryfikuje informacje o zagrożeniach punktów końcowych z systemami Windows w dużej bazie danych stworzonej w chmurze przez firmę Trend Micro i stale aktualizowanej za pośrednictwem sieci Trend Micro Smart Protection Network™. Rozwiązanie — zapewniając niezbędną ochronę punktów końcowych z systemami Windows i Mac — dodatkowo w czasie rzeczywistym sprawdza, czy używane pliki lub adresy URL figurują w bazie danych jako potencjalnie szkodliwe.

Tivoli Endpoint Manager for Core Protection chroni zarówno stałe punkty końcowe podłączone do sieci lokalnej, jak i przenośne punkty końcowe podłączone do Internetu. Nieprzerwane monitorowanie przez agenty okazuje się być niezwykle skutecznym środkiem ochrony przenośnych punktów końcowych, które są szczególnie narażone na zagrożenia. Przykładowo, laptop używany na lotnisku może mieć zapewnioną ochronę „z chmury”, która będzie monitorować odbierane pliki i odwiedzane serwisy WWW.

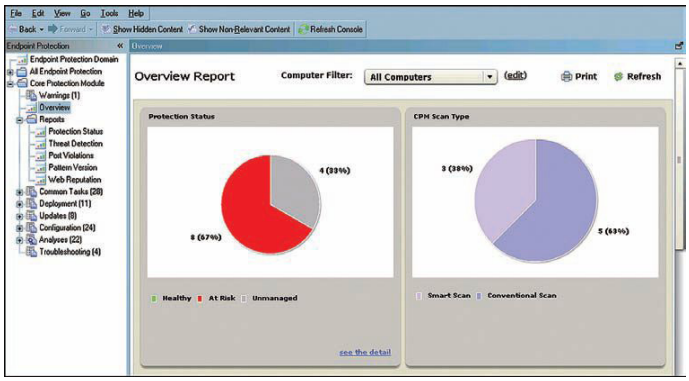
Skuteczna, przemyślana ochrona, która ogranicza ryzyko

Kluczem do skuteczności opisywanego rozwiązania jest jego zdolność do działania na wielu poziomach ochrony, w tym do powstrzymywania zagrożeń zanim zdołają uaktywnić się w chronionym systemie. Tivoli Endpoint Manager for Core Protection może przeglądać adresy URL w wiadomościach e-mail, sprawdzać, czy figurują w bazach danych o znanych zagrożeniach i w razie potrzeby blokować do nich dostęp. Takie środki stosowane na pierwszej linii obrony funkcjonują w oparciu o inne mechanizmy (patrz rys.), które w czasie rzeczywistym chronią infrastrukturę i punkty końcowe przed ewentualnymi próbami ataków. W rezultacie w ostatnio przeprowadzonych testach rozwiązanie Tivoli

Endpoint Manager for Core Protection przechwyciło 100 procent zagrożeń, podczas gdy drugie co do skuteczności rozwiązanie konkurencyjne przechwyciło zaledwie 77 procent z nich.*

Oto najważniejsze możliwości oferowane przez rozwiązanie IBM:

- **Wysoce skuteczna ochrona przed szkodliwym oprogramowaniem:** rozwiązanie chroni przed całą gamą szkodliwych programów i skanuje pocztę elektroniczną POP3 oraz foldery programu Microsoft Outlook w poszukiwaniu zagrożeń. Automatycznie oczyszcza punkty końcowe ze szkodliwego oprogramowania; usuwa także ukryte lub zablokowane procesy i wpisy w rejestrze.
- **Analiza reputacji plików:** dzięki możliwości natychmiastowego sprawdzenia danych w bazie prowadzonej w chmurze (obsługiwana jest także implementacja chmury prywatnej oferowanej przez firmę Trend Micro) rozwiązanie jest w stanie z wyprzedzeniem sprawdzić, czy plik jest bezpieczny, i zapobiec otwieraniu zainfekowanych dokumentów. Ogranicza pracochłonność zarządzania zabezpieczeniami i wpływ ochrony na wydajność punktów końcowych, a przy tym zapewnia bieżącą ochronę zarówno podczas pracy w sieci, jak i w trybie bez połączenia.
- **Analiza reputacji stron WWW:** ta funkcja automatycznie sprawdza, czy otwierane strony są bezpieczne, weryfikując adresy w bazie obejmującej miliony dynamicznie ocenianych serwisów WWW. Chroni punkty końcowe przed szkodliwym oprogramowaniem pochodzącym z sieci i kradzieżą danych, zaś całą organizację — przed spadkiem produktywności pracy personelu i utratą reputacji. Zapewnia ochronę w czasie rzeczywistym, niezależnie od typu połączenia, a dzięki synchronizacji w oparciu o chmurę może poprawić wydajność pracy w sieci WWW.
- **Monitorowanie zachowania:** rozwiązanie rozpoznaje podejrzane działania w systemie, takie jak użycie pamięci flash w celu dokonania zmian w rejestrze. W odpowiedzi na takie zdarzenie funkcja może zablokować potencjalnie szkodliwe działanie.



Innowacyjny graficzny interfejs użytkownika w przejrzysty sposób informuje administratorów o stanie zabezpieczeń i wskazuje potencjalnie zagrożone punkty końcowe.

Uproszczone zarządzanie punktami końcowymi dzięki przejrzystym informacjom

Tivoli Endpoint Manager for Core Protection usprawnia zarządzanie, udostępniając na jednej konsoli komplet informacji o stanie zabezpieczeń wszystkich punktów końcowych. Upraszcza i centralizuje zarządzanie fizycznymi i wirtualnymi punktami końcowymi i ułatwia podział zadań między administratorów dzięki szczegółowej strukturze ról administracyjnych.

Wykorzystanie infrastruktury oprogramowania Tivoli Endpoint Manager zapewnia wyższy poziom ochrony, gwarantując egzekwowanie strategii bezpieczeństwa; dba o to, aby usługi antywirusowe były zawsze zainstalowane, uruchomione i zaktualizowane. Scentralizowana, pojedyncza konsola pozwala na usprawnienie pracy i obniżenie kosztów zarządzania. Rozwiązanie IBM charakteryzuje się przy tym wyjątkową skalowalnością.

Zabezpieczenia dopasowane do potrzeb organizacji

Tivoli Endpoint Manager zaspokaja potrzeby charakterystyczne dla środowisk rozwijających się i ewoluujących. Do jego istotnych cech należy zaliczyć uwzględnienie przyszłościowych technologii, takich jak wirtualizacja stacji roboczych i przetwarzanie w chmurze, które usprawniają i upraszczają wdrożenia oraz zmniejszają pracochłonność utrzymania środowisk informatycznych.

- **Uwzględnianie wirtualizacji:** rozwiązanie IBM automatycznie rozpoznaje, czy agent działa na fizycznym, czy wirtualnym punkcie końcowym. Jest to szczególnie istotne w środowiskach, w których odbywa się właśnie etapowe przejście z komputerów stacjonarnych i laptopów na maszyny wirtualne. W przypadku wirtualnych punktów końcowych podejmowane są środki zapobiegające takim problemom, jak „sztorm antywirusowy", tj. współbieżne skanowania na dużej liczbie maszyn prowadzące do zablokowania sieci i punktów końcowych. Operacje skanowania i aktualizacje są szeregowane, co pozwala uniknąć konfliktów. Ponadto możliwe jest skrócenie czasu skanowania poprzez umieszczenie podstawowych obrazów maszyn i wcześniej przeskanowanych treści na „białej liście". Tivoli Endpoint Manager for Core Protection współdziała z rozwiązaniami wirtualizacyjnymi używanymi w organizacjach, takimi jak Citrix XenDesktop i VMware View, przyczyniając się do zwiększenia opłacalności bieżących inicjatyw wirtualizacyjnych.
- **Nieobciążające agenty:** Tivoli Endpoint Manager for Core Protection zużywa niewiele zasobów dzięki wykorzystaniu koncepcji przetwarzania w chmurze zarówno do realizacji zabezpieczeń, jak i zarządzania nimi. W tradycyjnych rozwiązaniach obszerne aktualizacje sygnatur wymagane do ochrony przed nowymi zagrożeniami mogą wydłużać instalację, przeciążać punkty końcowe i negatywnie wpływać na produktywność prac użytkowników. W przypadku rozwiązania IBM sygnatury są przechowywane w chmurze, przez co poszczególne punkty końcowe są mniej obciążone.

Inteligentna ochrona punktów końcowych

We współczesnym świecie oplecionym siecią połączeń i wypełnionym inteligentnymi urządzeniami kwestia zarządzania punktami końcowymi i ich odpowiedniego zabezpieczenia urasta do rangi priorytetu. Tivoli Endpoint Manager for Core Protection zapewnia bieżącą widoczność i ochronę punktów końcowych w czasie rzeczywistym. Stanowi łatwe w użyciu rozwiązanie, które zdolne jest do wykrywania i usuwania całej gamy szkodliwego oprogramowania zanim jeszcze wykorzysta ono słabe punkty w chronionych systemach. Wykorzystuje przy tym takie mechanizmy, jak analiza reputacji plików i stron WWW.

Wdrożenie innych produktów z rodziny Tivoli Endpoint Manager, w uzupełnieniu rozwiązania Tivoli Endpoint Manager for Core Protection, może przynieść organizacji znaczące korzyści. Na przykład ataki szkodliwego oprogramowania są zwykle skierowane na słabe punkty nieobjęte poprawkami. Tivoli Endpoint Manager oferuje kompleksowe funkcje zarządzania poprawkami, które usprawniają instalowanie na rozproszonych punktach końcowych poprawek do wielu różnych systemów operacyjnych i aplikacji. Przyspiesza dystrybucję poprawek i aktualizacji, nie zmniejszając w żaden sposób funkcjonalności punktów końcowych, nawet tych działających w sieciach o niskiej przepustowości lub bardzo rozległych geograficznie.

Kompleksowe rozwiązanie Tivoli Endpoint Manager integruje zarządzanie systemami z zapewnieniem bezpieczeństwa, oferując funkcje wspomagające obsługę słabych punktów zabezpieczeń, zarządzanie konfiguracją zabezpieczeń, wykrywanie zasobów, spisywanie zasobów, dystrybucję oprogramowania, wdrażanie systemów operacyjnych, analizę wykorzystania oprogramowania, czy raportowanie zgodności ze strategiami i normami bezpieczeństwa. Pojedyncza konsola Tivoli Endpoint Manager służy do zarządzania wszystkimi tymi funkcjami, także tymi udostępnianymi przez Tivoli Endpoint Manager for Core Protection. Takie kompleksowe rozwiązanie udostępnia wielostronne ujęcie środowiska zabezpieczeń punktów końcowych w całej organizacji.

Tivoli Endpoint Manager for Core Protection w skrócie

Wymagania serwera:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Wymagania konsoli:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Platformy obsługiwane przez agenta:

- Microsoft Windows, w tym XP, 2003, Vista, 2008, 2008 R2, 7, XP Embedded i Embedded Point-of-Sale
- Mac OS X

Więcej informacji

Aby uzyskać więcej informacji na temat rozwiązania IBM Tivoli Endpoint Manager for Core Protection należy skontaktować się z lokalnym przedstawicielem IBM lub Partnerem Handlowym IBM albo odwiedzić serwis WWW: ibm.com/tivoli/endpoint

Oprogramowanie IBM Tivoli

Oprogramowanie marki Tivoli oferowane przez IBM pomaga organizacjom w wydajnym i skutecznym zarządzaniu zasobami informatycznymi, zadaniami i procesami pod kątem spełniania stale zmieniających się wymagań biznesowych. Oferuje elastyczne i sprawne narzędzia do zarządzania usługami informatycznymi oraz przyczynia się do ograniczenia kosztów. Oferta Tivoli obejmuje oprogramowanie z dziedziny bezpieczeństwa, zapewnienia zgodności z przepisami i normami, zarządzania pamięcią masową, wydajnością, dostępnością konfiguracją, eksploatacją i cyklem życia środowisk informatycznych. Cenne zaplecze produktów Tivoli stanowią usługi, wsparcie i badania IBM.

Ponadto usługi finansowe oferowane przez IBM Global Financing umożliwiają efektywne zarządzanie płynnością, uniknięcie skutków starzenia się technologii, optymalizację całkowitych kosztów użytkowania i zwrotu z inwestycji. Oferowane przez IBM usługi w zakresie zagospodarowania zasobów — Global Asset Recovery Services — rozwiązują szereg problemów związanych z bezpieczeństwem środowiska naturalnego i pozwalają korzystać z nowych, energooszczędnych rozwiązań. Więcej informacji na temat oferty IBM Global Financing można znaleźć pod adresem: ibm.com/pl/financing

IBM Polska Sp. z o.o.
ul. 1 Sierpnia 8
02–134 Warszawa

tel. (+ 48 22) 878 67 77
faks (+ 48 22) 878 68 88
ibm.com/pl

Wyprodukowano w Polsce.

* „Trend Micro Enterprise Endpoint Comparative Report", AV-Test, styczeń 2011. http://us.trendmicro.com/us/trendwatch/core-technologies/ competitive-benchmarks/avtest/

Papier należy przetworzyć wtórnie