

## **IBM RealSecure Server Sensor jako narzędzie wspierające zgodność z wymogami regulacyjnymi i zapobiegające utracie danych**



---

## Najważniejsze cechy produktu

---

- *Aplikacja zorientowana na problematykę zgodności z wymogami regulacyjnymi, dzięki czemu upraszcza i wspomaga realizację procedur w tym zakresie*
- *Zawiera mechanizmy zapobiegania utracie danych i ochrony prewencyjnej, jednocześnie wspierając egzekwowanie zasad dotyczących bezpieczeństwa serwerów w przedsiębiorstwie*
- *Pomaga utrzymać integralność systemów, poufność danych oraz zgodność polityki bezpieczeństwa z normami wewnętrznymi i zewnętrznymi*
- *Chroni systemy operacyjne i aplikacje przed znanymi i nieznanymi zagrożeniami za pomocą zintegrowanej zapory oraz systemu zapobiegania włamaniom zorientowanego na analizę podatności*
- *Współpracuje z różnymi systemami operacyjnymi i platformami sieciowymi, w tym: Windows, AIX, HP-UX i Solaris*
- *Zawiera mechanizmy kontrolne umożliwiające ochronę przed zagrożeniami wewnętrznymi*
- *Płynnie współpracuje z istniejącą infrastrukturą informatyczną w celu utrzymania niezakłóconego przepływu danych*

### **Pomaga chronić serwery przed zagrożeniami wewnętrznymi i zewnętrznymi, jednocześnie wspomagając przestrzeganie wymogów regulacyjnych**

Najcenniejsze zasoby Twojej firmy są przedmiotem ataku. Coraz częściej to wewnętrzni użytkownicy naruszają reguły bezpieczeństwa przedsiębiorstwa, a wraz z rozwojem – niewykrywalnych przez tradycyjne technologie zabezpieczeń – technik hakerskich stanowią rosnące zagrożenie dla bezpieczeństwa serwerów. Jednocześnie ustawodawcy kładą coraz większy nacisk na konieczność monitorowania dostępu do serwerów. Jak nigdy dotąd, bezpieczeństwo serwerów ma absolutnie podstawowe znaczenie dla bieżącej działalności biznesowej, integralności danych i zdolności wypełniania wymagań regulacyjnych.

Aplikacja IBM RealSecure® Server Sensor aktywnie wspiera działania w kierunku przestrzegania wymogów ustawowych, chroniąc przedsiębiorstwo jako całość. W celu zwalczania zagrożeń o różnym charakterze program łączy kilka technologii zabezpieczeń w jednego wielowarstwowego agenta. Aplikacja chroni kluczowe systemy biznesowe i dane przed atakami z wewnątrz firmy i z otoczenia, pomagając wypełniać restrykcyjne normy w zakresie kontroli i stosowania się do branżowych regulacji. Ponadto system zaprojektowano pod kątem łatwości obsługi oraz współpracy z różnymi systemami operacyjnymi i platformami.

### **RealSecure Server Sensor pomaga utrzymać/poprawić stopień przestrzegania wymogów regulacyjnych**

Aplikacja RealSecure Server Sensor ułatwia przedsiębiorstwom ścisłe egzekwowanie zasad dotyczących zabezpieczeń, które pozwalają zachować poufność danych i funkcjonalność kluczowych systemów. Dzięki funkcjom centralnego zarządzania zasadami kontroli systemu operacyjnego program zabezpiecza przed podatnościami powstałymi na skutek błędów w konstrukcji lub wdrożeniu innych aplikacji. Ponadto system wymusza jednorodne zasady kontroli dla wszystkich krytycznych serwerów przez monitorowanie zdarzeń logowania, podwyższania uprawnień i innych działań na poziomie systemowym realizowane za pomocą następujących rozwiązań technicznych i procesów:

- *Monitorowanie integralności plików – monitorowanie aspektów „kto”, „co”, „kiedy” i „gdzie” dla najważniejszych plików, w tym kluczowych binarnych plików systemowych i plików konfiguracyjnych*
- *Egzekwowanie zasad dostępu do sieci – konfigurowanie ograniczeń w zakresie portów i adresów IP dla ruchu przychodzącego do serwera*
- *Wykrywanie i kontrola włamań na poziomie aplikacji – wykrywanie ataków lub niedozwolonych działań na poziomie aplikacji oraz podejmowanie odpowiednich interwencji*
- *Monitorowanie i prowadzenie dziennika zdarzeń dotyczących systemu operacyjnego – śledzenie prób dodawania/modyfikowania użytkowników i grup oraz podwyższania uprawnień; może obejmować analizę ataków*

## Zapobieganie utracie danych za pomocą wielowarstwowego systemu ochrony prewencyjnej

Bezpieczeństwo serwera to podstawowy składnik strategii zapobiegania utracie danych obowiązującej w przedsiębiorstwie. Wielowarstwowa technologia zabezpieczeń zastosowana w aplikacji RealSecure Server Sensor skutecznie chroni przed zagrożeniami zarówno z wewnątrz, jak i z otoczenia firmy. Obecnie ataki hybrydowe i wyrafinowani cyberprzestępcy są w stanie przełamać konwencjonalne systemy obronne. W związku z taką różnorodnością ataków żadne indywidualne rozwiązania nie zapewnią kompletnej ochrony serwerów. Zaawansowany wielopoziomowy system zabezpieczeń oferowany przez IBM Internet Security Systems™ (ISS) umożliwia powstrzymanie ataków zanim zdążą one spowodować szkody i naruszyć poufność danych. Dzięki rozbudowanej, wielowarstwowej ochronie realizowanej przez jednego agenta system RealSecure Server Sensor jest zdecydowanie łatwiejszy w obsłudze niż pakiet różnych, niepowiązanych z sobą rozwiązań.

Aplikacja RealSecure Server Sensor zawiera następujące moduły zabezpieczeń:

- **Zapora** – blokuje nieuprawnionym osobom i programom dostęp do portów i adresów IP, zapobiegając zjawiskom preparowania adresów IP i przejmowania końcówek sieci
- **System zapobiegania włamaniom (IPS)** – zapobiega znanym i nieznanym atakom, wykorzystując funkcje analizy sygnatur i protokołów
- **Zapobieganie wykorzystywaniu przypadków przepełnienia bufora (BOEP)** – rozpoznaje i blokuje szkodliwy kod atakujący luki w zabezpieczeniach bufora pamięci (system Windows)

- **Ochrona aplikacji internetowych** – zabezpiecza aplikacje WWW działające na serwerach internetowych Apache i IIS przez kontrolowanie ruchu szyfrowanego protokołem SSL (tylko systemy Windows i Solaris)
- **Technologia IBM Virtual Patch®** – automatycznie stosuje mechanizmy ochrony luk w zabezpieczeniach do czasu zainstalowania poprawek dostarczonych przez producenta sprzętu/oprogramowania

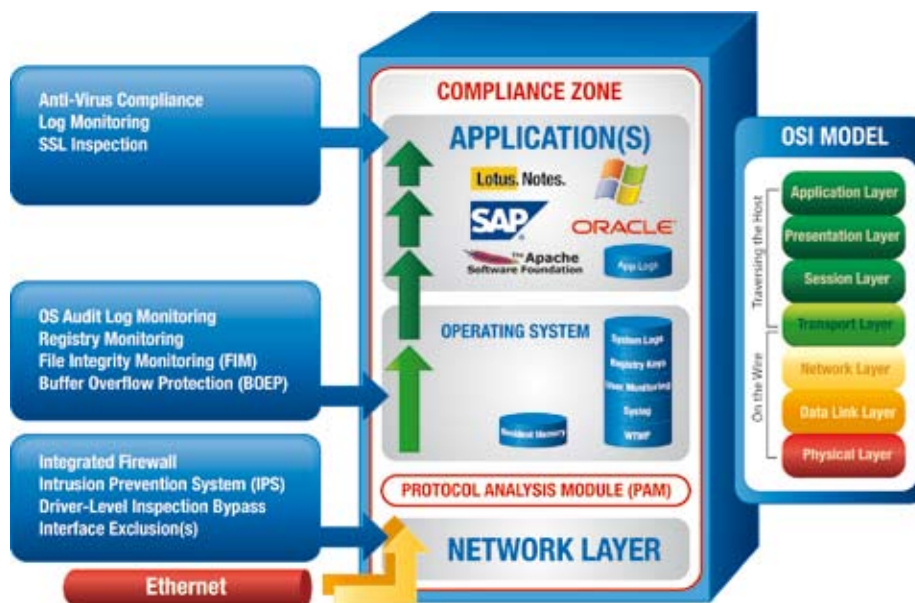
## Aplikacja RealSecure Server Sensor współpracuje z różnymi systemami operacyjnymi

Większość przedsiębiorstw korzysta ze środowisk informatycznych o wielu platformach serwerowych, dlatego nie są zainteresowane systemami zabezpieczeń obejmującymi jedynie fragment całej infrastruktury. Oprogramowanie RealSecure Server Sensor opracowano pod kątem możliwości współdziałania z róż-

norodnymi platformami, w tym z nowymi i starszymi wersjami systemów Microsoft® Windows®, Solaris, IBM AIX® i HP-UX. System zabezpieczeń obejmujący swoim zasięgiem wszystkie systemy operacyjne jest łatwiejszy w instalacji, zarządzaniu i utrzymaniu, co przekłada się na niższy całkowity koszt użytkowania.

## Aplikacja RealSecure Server Sensor została opracowana pod kątem łatwości obsługi

Centralnie zarządzana przez system IBM SiteProtector™, aplikacja RealSecure Server Sensor płynnie współpracuje z istniejącą infrastrukturą informatyczną przedsiębiorstwa. Dzięki ściśtemu współdziałaniu z usługą Active Directory umożliwia zarządzanie zasadami, monitorowanie zdarzeń i generowanie raportów przez grupy użytkowników. Aplikacja została tak skonstruowana, żeby mieć minimalny wpływ na wykorzystanie zasobów serwera oraz nie ingerować w wiarygodny ruch.



RealSecure Server Sensor — wielowarstwowa ochrona przed wewnętrznymi i zewnętrznymi zagrożeniami

## **IBM ISS – niezawodność dzięki zapleczu badawczemu**

Aplikacja RealSecure Server Sensor korzysta ze stałego wsparcia ze strony wewnętrznego zespołu badawczo-rozwojowego X-Force® działającego w ramach IBM Internet Security Systems. Gromadzone przez ten zespół informacje analityczne w zakresie zagrożeń i luk w zabezpieczeniach, które cieszą się uznaniem na całym świecie, na bieżąco są uwzględniane w aplikacji. Pozwala to eliminować pojawiające się zagrożenia, zwiększając poziom niezawodności i efektywności rozwiązania.

Ponadto w celu wzmocnienia skuteczności ochrony oferowanej przez aplikację RealSecure Server Sensor dział IBM ISS prowadzi globalne centrum operacyjne (GTOC) zajmujące się śledzeniem poziomu zagrożeń internetowych na całym świecie. Gdy tylko pojawi się nowy typ zagrożenia, analitycy centrum są jednymi z pierwszych, którzy się o tym dowiadują, i mogą ostrzec użytkowników rozwiązań Proventia.

## **Więcej informacji**

Aby dowiedzieć się, jak wielopoziomowy system zabezpieczeń RealSecure Server Sensor pomaga chronić kluczowe serwery przedsiębiorstwa przed zagrożeniami z Internetu oraz zapewnić przestrzeganie wymogów regulacyjnych lub aby zamówić demonstrację możliwości systemu w siedzibie firmy, odwiedź stronę [ibm.com/services/us/iss](http://ibm.com/services/us/iss) oraz [ibm.com/pl/services/security.html](http://ibm.com/pl/services/security.html) lub skontaktuj się z zespołem IBM ISS: [iss@pl.ibm.com](mailto:iss@pl.ibm.com).



### **© IBM Polska Sp. z o.o.**

Wiśniowy Business Park  
ul. 1 Sierpnia 8  
02-134 Warszawa  
tel. +48 22 878 6777  
fax: +48 22 878 6888

Strona główna IBM Polska znajduje się pod adresem: [ibm.com/pl](http://ibm.com/pl)

Wyprodukowano w Polsce  
Wszelkie prawa zastrzeżone  
IBM i logo IBM są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach. Proventia, Virtual Patch i X-Force są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Internet Security Systems, Inc. w Stanach Zjednoczonych i/lub innych krajach. Internet Security Systems, Inc. jest w pełni zależną filią International Business Machines Corporation.

Microsoft i Windows są znakami towarowymi lub zastrzeżonymi znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach.

Linux to zastrzeżony znak towarowy p. Linusa Torvaldsa w Stanach Zjednoczonych i/lub innych krajach.

Nazwy innych firm, produktów lub usług mogą być ich znakami towarowymi lub znakami usługowymi.

Zawarte w tym dokumencie informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, opublikowanych przez nich materiałów lub z innych źródeł dostępnych publicznie. Sieciowy system operacyjny (czasami określane również skrótowo mianem „system operacyjny”) został sprawdzony pod kątem współpracy z aplikacją i potwierdzono, że będzie z nią współdziałał. Pytania dotyczące funkcjonalności takich produktów należy kierować do ich producentów.

Wszystkie dane pomiarowe zawarte w niniejszej publikacji uzyskano w określonym środowisku roboczym i warunkach opisanych powyżej. Pełnią one wyłącznie rolę ilustracyjną. Wyniki uzyskane w innych środowiskach mogą się różnić. Klienci powinni przeprowadzić własne testy.

1. Dotyczy wyłącznie systemów operacyjnych Windows i Linux