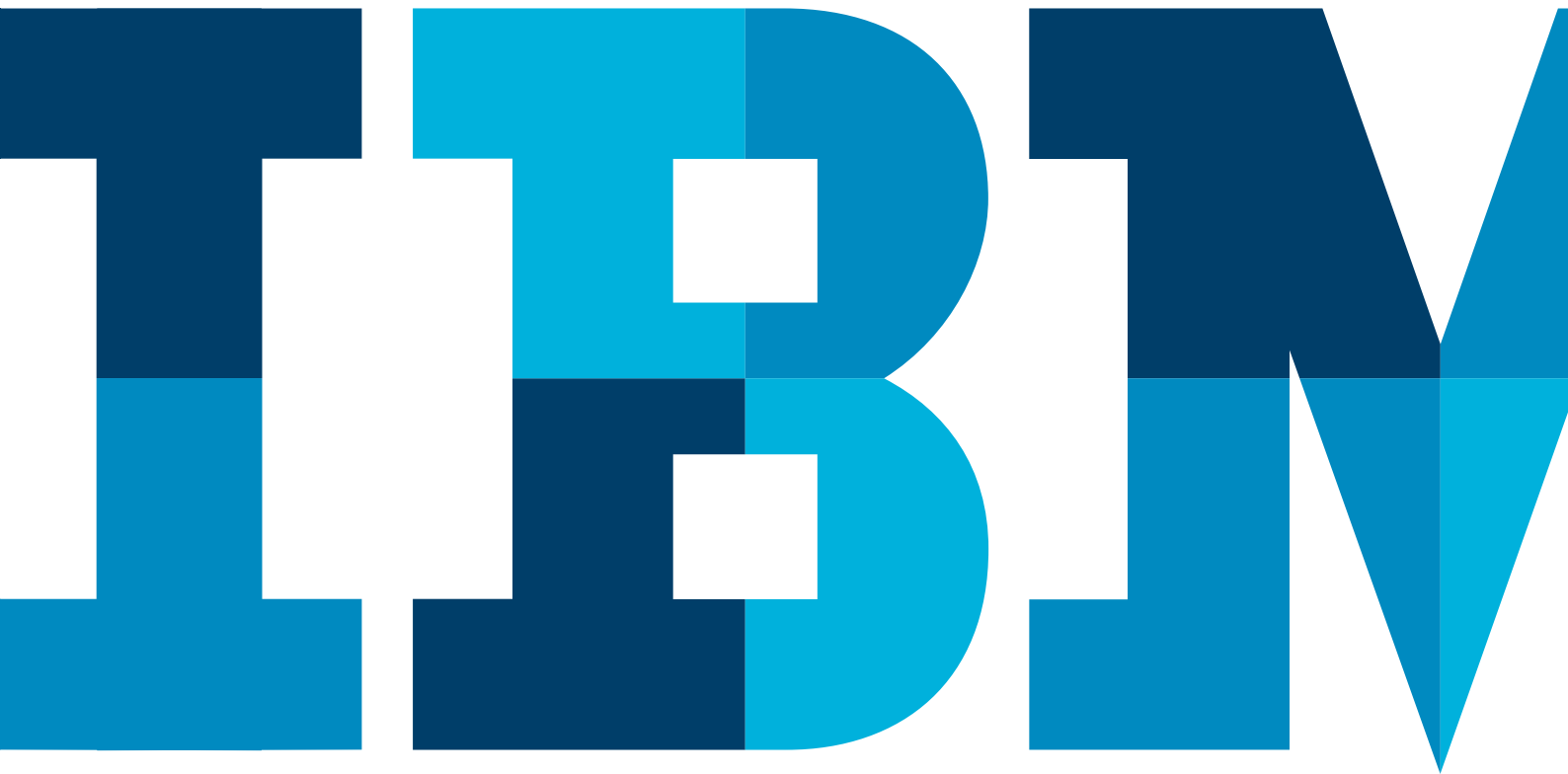


IBM

Think Integrated – strategia zintegrowana

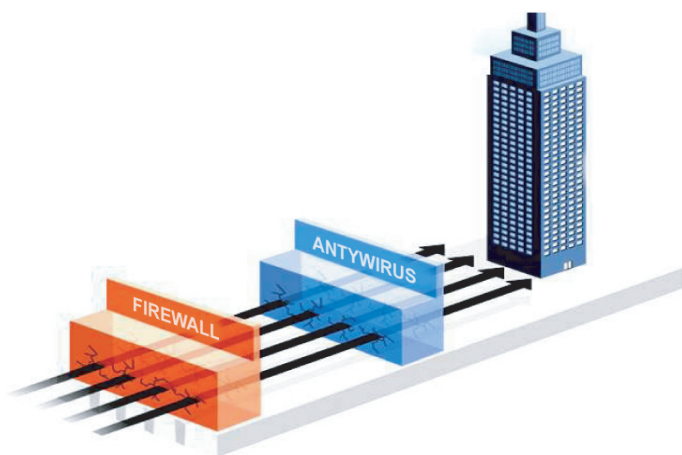
Monitorowanie zagrożeń i analizy bezpieczeństwa

*Inteligencja, integracja, wiedza. Najbardziej zaawansowana oferta produktów
i usług z dziedziny bezpieczeństwa korporacyjnego*



Tradycyjne zabezpieczenia można obejść

Nowa kategoria ataków – tzw. Advanced Persistent Threats – mają na celu uzyskanie stałego dostępu do niewrażliwych danych biznesowych. Ataki takie, realizowane przy wykorzystaniu najnowocześniejszych metodologii, mogą trwać dowolnie długo i są ściśle ukierunkowane. Nowe metody ataków znacznie osłabiły skuteczność tradycyjnych zabezpieczeń informatycznych, takich jak firewalle i oprogramowanie antywirusowe – a w niektórych przypadkach umożliwiają nawet ich całkowite obejście. Aby skutecznie zabezpieczyć współczesne przedsiębiorstwo, niezbędne jest wdrożenie zupełnie innej niż dotąd strategii bezpieczeństwa – opartej nie tylko na skutecznych rozwiązaniach technicznych, lecz również rygorystycznie przestrzeganych procesach, odpowiedniej strukturze organizacyjnej i kulturze zachowań. Odrębne, pojedyncze produkty chroniące granicę sieci nie są już wystarczające.



Nowy dział: IBM Security Systems Division

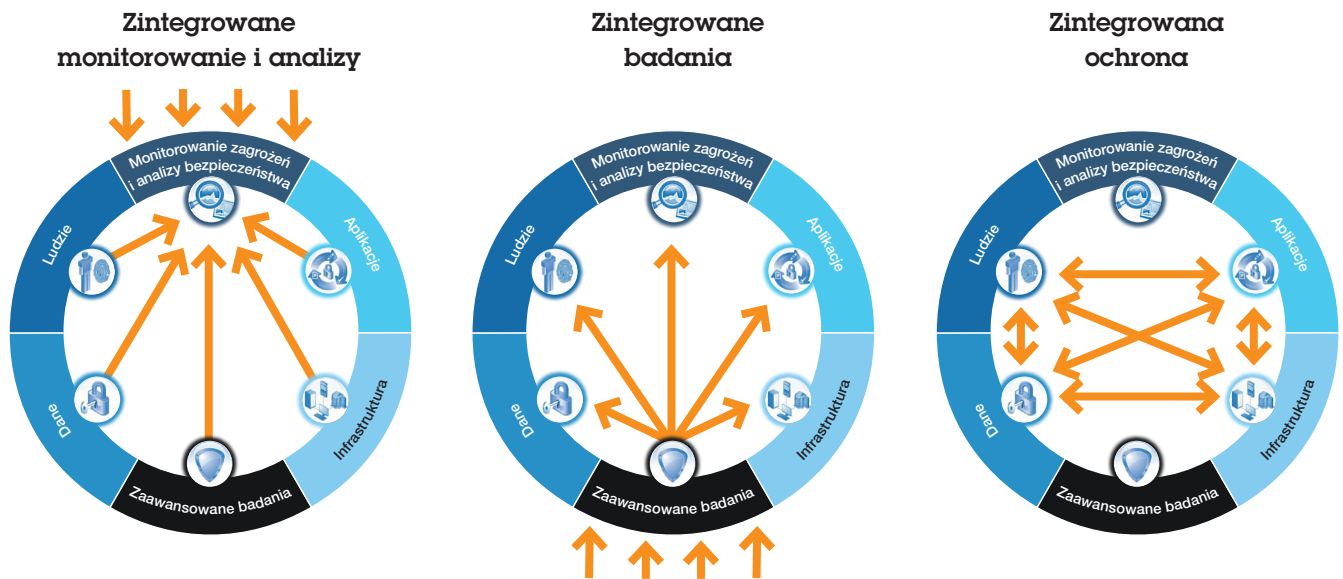
Na początku 2012 roku w IBM utworzony został dział Security Systems Division, którego zadaniem jest opracowanie zintegrowanej strategii i planów niezbędnych we współczesnym świecie pełnym coraz bardziej złożonych zagrożeń. Z myślą o zapewnieniu przedsiębiorstwom prawdziwej ochrony w dzisiejszym hiper-skomunikowanym środowisku biznesowym, wobec konieczności operowania na „dużych danych” oraz zacierania się granic między systemami wewnętrznymi a światem zewnętrznym, nowy dział IBM realizuje potrójną doktrynę: monitorowania i analizy (Intelligence), integracji (Integration) oraz wiedzy (Expertise). Rozwiązanie IBM wypełnia luki, jakie istnieją w strategiach wobec niego konkurencyjnych:



Architektura bezpieczeństwa IBM

Monitorowanie i analiza (Intelligence) – pierwszym składnikiem doktryny IBM jest monitorowanie zagrożeń i analiza bezpieczeństwa: przetwarzanie i badanie milionów zdarzeń w czasie rzeczywistym, w celu wykrywania, przewidywania zagrożeń i podejmowania środków zaradczych w wypadku naruszenia zabezpieczeń. Dzięki doświadczeniu i wiedzy specjalistycznej IBM powstał system, któremu pod tym względem nie dorównuje żaden inny.

Integracja (Integration) – drugim składnikiem doktryny jest integracja kompleksowej oferty IBM: rozwiązań do monitorowania i analiz, badań zespołu X-Force® oraz podstawowych technologii ochrony. Taka integracja eliminuje niepotrzebne bariery między różnymi obszarami ochrony, ułatwia sprawozdawczość, optymalizuje jakość analiz, upraszcza środowisko bezpieczeństwa i obniża koszty utrzymania odpowiednio wysokiego poziomu bezpieczeństwa.



Oto bardziej szczegółowa lista korzyści:

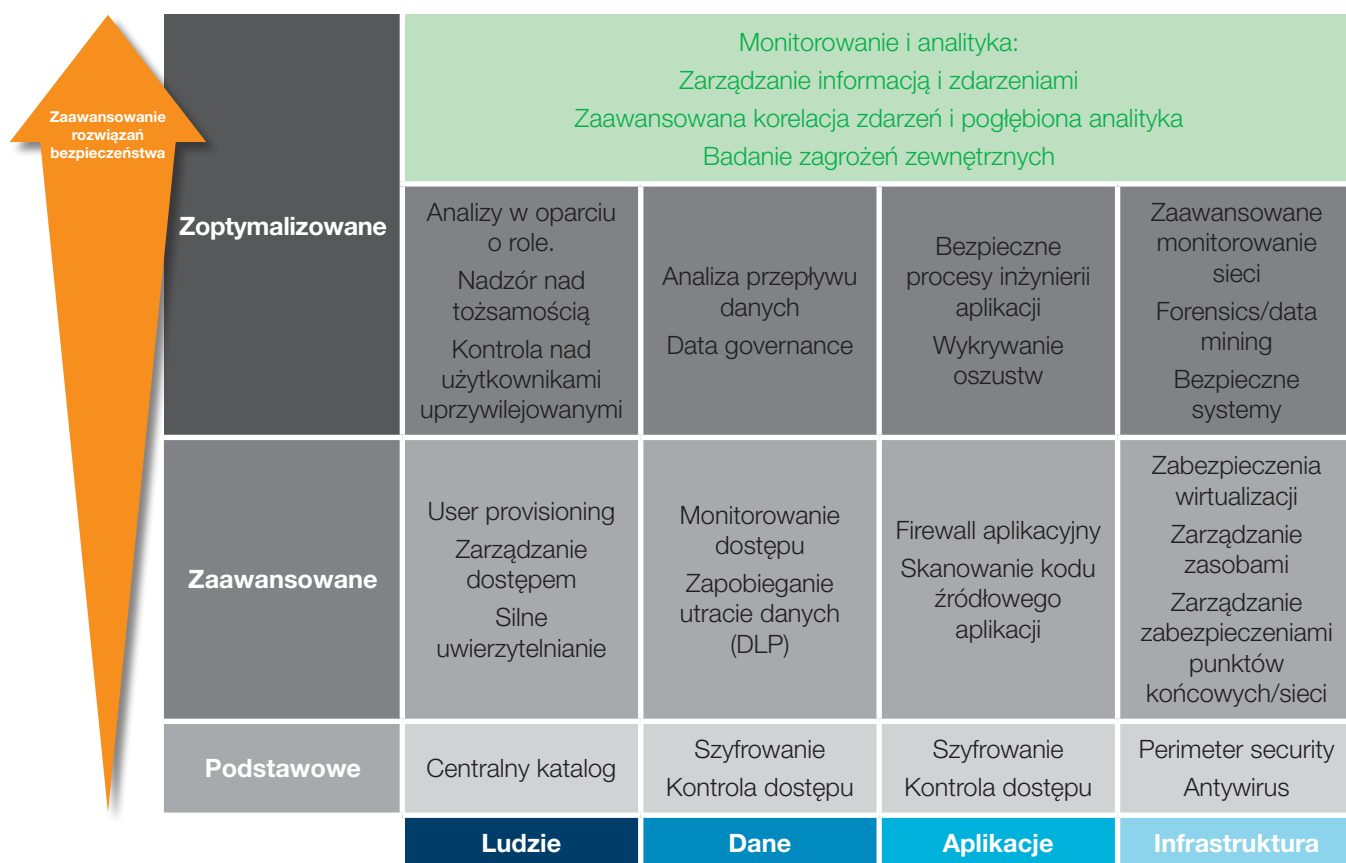
- Dostępność pełnych, kontekstowych informacji wewnętrznych i zewnętrznych potrzebnych do wykrywania i przewidywania naruszeń oraz podejmowania środków zaradczych.
- Automatyzacja aktualizacji urządzeń i oprogramowania w celu eliminacji wykrytych i zbadanych słabych punktów.
- Powiązanie uwierzytelniania i autoryzacji z podejrzanymi działaniami w bazie danych.
- Automatyzacja zapewnienia zgodności z przepisami i strategiami oraz oceny ryzyka.
- I wiele innych korzyści.

Wiedza specjalistyczna (Expertise) – IBM utrzymuje największą na świecie organizację zajmującą się badaniami oraz tworzeniem i wdrażaniem rozwiązań z dziedziny bezpieczeństwa korporacyjnego. W strukturach tej organizacji zatrudnionych jest ponad 15 000 naukowców, programistów i ekspertów. W jej skład wchodzi renomowany zespół badawczo-rozwojowy X-Force®, który prowadzi największą w branży bazę danych o słabych punktach zabezpieczeń, a także dziewięć ośrodków operacyjnych, dziewięć ośrodków badawczych IBM, jedenaście laboratoriów, w których powstaje oprogramowanie zabezpieczające, a także Institute for Advanced Security z oddziałami w Stanach Zjednoczonych, Europie i Azji Wschodniej. IBM monitoruje obecnie dziennie ponad 13 miliardów zdarzeń związanych z bezpieczeństwem na rzecz klientów w ponad 130 krajach. Tylko IBM dysponuje kadrami i wiedzą niezbędną, by pomóc każdej firmie w zbudowaniu zoptymalizowanych, zintegrowanych i inteligentnych mechanizmów bezpieczeństwa.

Chmura, platformy przenośne, wielkie zbiory (big data), serwisy społecznościowe: architektura bezpieczeństwa dla każdego środowiska

Nowoczesne środowiska prowadzenia biznesu stwarzają przedsiębiorstwom olbrzymie szanse, ale są też źródłem ryzyka. Przyjęta przez IBM zintegrowana, wszechstronna

strategia bezpieczeństwa uwzględnia wszystkie aspekty środowiska – ludzi, dane, aplikacje i infrastrukturę – oraz stanowi fundament dla implementacji nowych technologii znanych już teraz i takich, które dopiero powstaną. IBM jako jedyne przedsiębiorstwo na świecie oferuje tak szerokie spektrum znakomitych produktów i usług z dziedziny bezpieczeństwa korporacyjnego.



Czołowe produkty i usługi w każdym segmencie

Więcej informacji

Zapraszamy do kontaktu z przedstawicielem IBM:

ibm.com/planetwide



Na Twitterze: [@ibmsecurity](https://twitter.com/ibmsecurity)



Filmy: www.youtube.com/ibmsecuritysolutions



Institute for Advanced Security

Zapraszamy:

www.instituteforadvancedsecurity.com



© Copyright IBM Corporation 2012

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

Strona główna IBM znajduje się pod adresem:
ibm.com/pl/

Wydrukowano w Polsce
Wszelkie prawa zastrzeżone.

IBM, logo IBM, ibm.com i WebSphere są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach.

Pozostałe nazwy firm, produktów i usług mogą być znakami towarowymi lub znakami usług należącymi do innych podmiotów.
