**Cyberbezpieczeństwo bankowości. Jak zapewnić bezpieczną i zgodną migrację do chmury?**

**Gdy banki przenoszą dane i obciążenia do chmury, muszą upewnić się, że zasoby i dane w chmurze są zabezpieczone i zgodne z przepisami, takimi jak te wydane np. Przez Europejskie Stowarzyszenie Bankowe (EBA). Jednak nowoczesne wdrożenia chmurowe są niezwykle złożone i zazwyczaj obejmują wiele infrastruktur chmurowych. Mimo że dostawcy chmury publicznej inwestują znaczne wysiłki w bezpieczeństwo, to bank nadal jest odpowiedzialny za zapewnienie cyberbezpieczeństwa organizacji.**

 **Poniższy artykuł przedstawia prawdziwe studium przypadku dużego banku, ukazujące wyzwania z jakimi się mierzył oraz rozwiązania, które wykorzystał, aby wzmocnić swoje bezpieczeństwo.**

Jako że krajobraz cyberzagrożeń wciąż ewoluuje i staje się z roku na rok coraz bardziej niebezpieczny, ochrona infrastruktury informatycznej banku będzie stawać się coraz większym wyzwaniem. Osiągnięcie tego celu wiąże się z wieloma wyzwaniami, takimi jak:

l **Ujednolicone zarządzanie bezpieczeństwem** w chmurach i lokalnym centrum danych

l Wykrywanie i korygowanie **błędnych konfiguracji** w czasie rzeczywistym

l Usprawnienie i zapewnienie **zarządzania**

l Spełnianie rygorystycznych przepisów dotyczących **zgodności** i prywatności

**Jeden z południowoafrykańskich banków z tysiącami oddziałów,** rozszerza swoją chmurę Azure i AWS o ujednolicone rozwiązanie bezpieczeństwa natywne dla chmury.

**Głównymi wyzwaniami** banku są: **zarządzanie** i kontrola bezpieczeństwa z jednego miejsca, integracja z innymi systemami, łatwe tworzenie reguł i profili, skalowalność i konsolidacja.

**Rozwiązanie, które wybrał obejmuje** [CloudGuard Network Security](https://www.checkpoint.com/cloudguard/cloud-network-security/) firmy Check Point umożliwiający bezpieczną migrację ku chmurze, zapewniający bezpieczeństwo sieciowe i zapobieganie zagrożeniom oraz [CloudGuard Security Posture Management firmy Check Point w](https://www.checkpoint.com/cloudguard/cloud-security-posture-management/) celu zapewnienia zgodności chmury z przepisami. Bank zautomatyzował przepływy pracy związane z zarządzaniem środowiskiem wielochmurowym,

**Bank otrzymał jedno rozwiązanie bezpieczeństwa natywnego dla chmury** z pojedynczym zarządzaniem, obsługą wielu chmur (Azure, AWS, NSX…) oraz ujednoliconym zarządzaniem zabezpieczeniami i kontrolą stanu. Korzysta ze zautomatyzowanej zgodności **i najlepszych praktyk,** w tym egzekwowania bankowych ram zgodności, takich jak PCI DSS, NIST CSF/800-53 itp., wykrywania błędnych konfiguracji i egzekwowania zasad. Rozwiązanie zapewnia szybkie wyniki zgodności i alerty dzienników, a jego „builder” języka specyfikacji zarządzania (GSL) jest znacznie łatwiejszy w użyciu niż inne narzędzia na rynku.

Bank wykorzystuje **zapobieganie zagrożeniom w czasie rzeczywistym,** w tym emulację zagrożeń, ekstrakcję zagrożeń, zero-day, antywirus, rozwiązanie **antybot**, filtrowanie adresów URL, DLP, antyspam i tak dalej.

Ponadto osiągnął **wyższą wydajność i niższe koszty dzięki** niskim opóźnieniom dla aplikacji biznesowych, zarządzaniu i kontroli z jednego centralnego miejsca, łatwemu tworzeniu reguł i profili, łatwej integracji z innymi systemami. Całkowity koszt posiadania okazał się o 50% niższy niż w przypadku innych rozwiązań .

**Podsumowując**

Check Point umożliwia bankom dostarczanie klientom zaawansowanych usług cyfrowych z najwyższym poziomem bezpieczeństwa.

Przyjmując skonsolidowane podejście do bezpieczeństwa z **architekturą i usługami Check Point Infinity**, banki realizują prewencyjną ochronę przed zaawansowanymi atakami piątej generacji, osiągając jednocześnie **50% wzrost wydajności operacyjnej** i **20% redukcję kosztów bezpieczeństwa**.

Ta szeroka oferta rozwiązań i usług w zakresie cyberbezpieczeństwa firmy Check Pointumożliwia 6500 instytucjom finansowym na całym świecie sprostanie ich największym wyzwaniom.