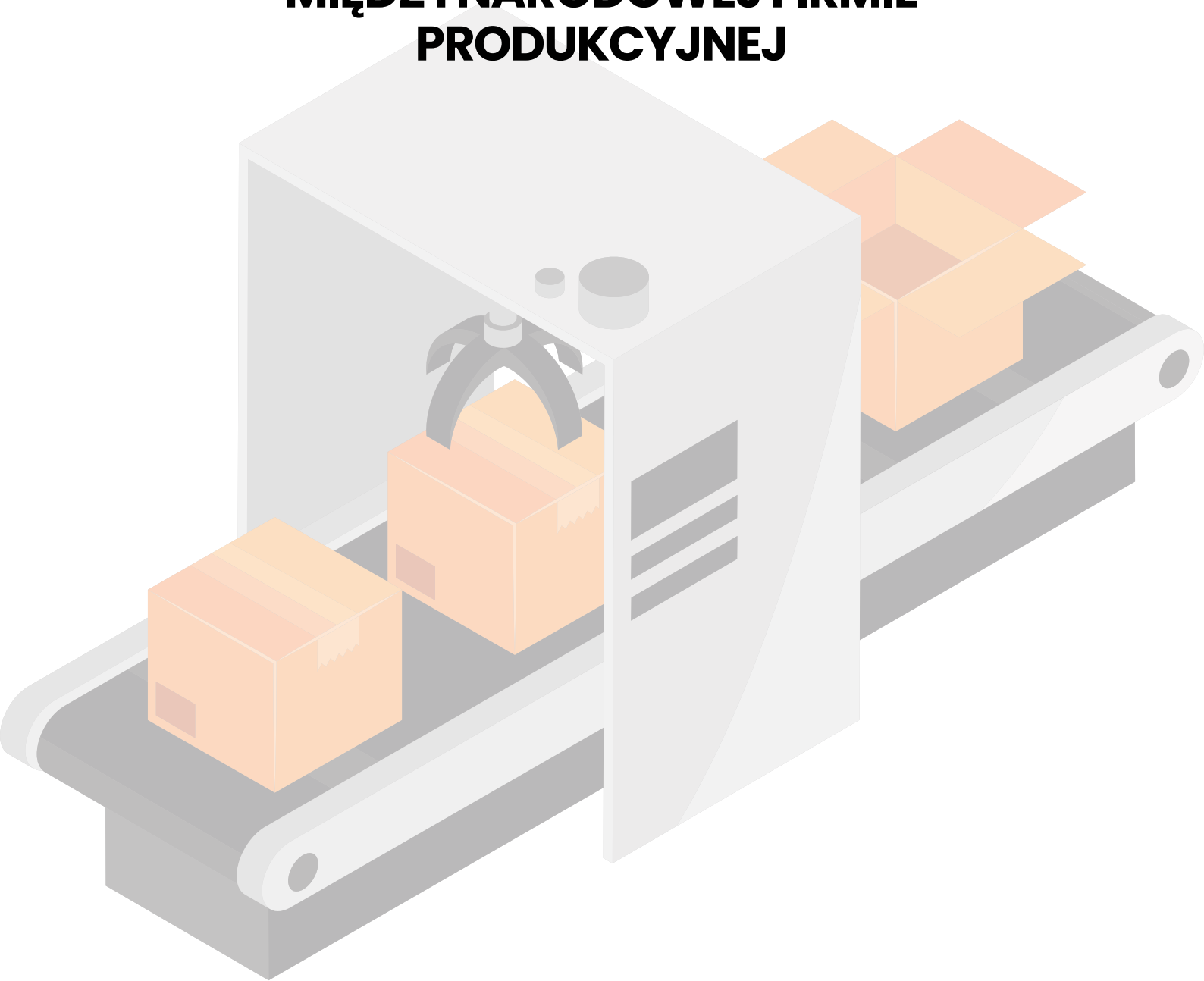
INTRATEL

veeam

OCHRONA INFRASTRUKTURY SERWEROWEJ PRZED ATAKAMI RANSOMWARE

JAK CHRONIĆ DANE W MIĘDZYNARODOWEJ FIRMIE PRODUKCYJNEJ



WPROWADZENIE

Współczesny świat biznesu jest coraz bardziej zależny od technologii informacyjnych. Digitalizacja procesów, chmura obliczeniowa i Big Data to tylko niektóre z trendów, które rewolucjonizują sposób prowadzenia działalności. Jednocześnie, wraz z rosnącą liczbą cyfrowych aktywów, wzrasta również ryzyko cyberataków. Firmy produkcyjne, ze względu na charakter swojej działalności, są szczególnie narażone na tego typu zagrożenia.

Niniejszy case study prezentuje rzeczywisty przypadek, w którym międzynarodowa firma produkcyjna doświadczyła poważnych konsekwencji ataku ransomware. Cyberprzestępcy, wykorzystując lukę w zabezpieczeniach, zaszyfrowali wszystkie pliki kopii zapasowych maszyn wirtualnych, uniemożliwiając przywrócenie danych i paraliżując kluczowe procesy biznesowe.

CO ZOSTAŁO ZAATAKOWANE?

W wyniku zaawansowanego ataku cybernetycznego, serwer fizyczny VMware ESXi, będący centralnym elementem infrastruktury IT klienta, został skompromitowany przez złośliwe oprogramowanie typu ransomware. Cyberprzestępcy, wykorzystując luki w zabezpieczeniach serwera, zyskali nieuprawniony dostęp do szerokiej gamy zasobów macierzowych podłączonych do środowiska VMware.

Wśród tych zasobów znalazł się krytyczny wolumen służący do przechowywania kopii zapasowych maszyn wirtualnych, zawierających cenne dane biznesowe. Po uzyskaniu kontroli nad tym wolumenem, atakujący przeprowadzili skoordynowaną akcję szyfrowania wszystkich plików znajdujących się na nim. Co więcej, ich działania nie ograniczyły się jedynie do tego konkretnego wolumenu. W wyniku eskalacji ataku, wszystkie wolumeny dostępne w środowisku VMware, w tym te zawierające dane produkcyjne, zostały zaszyfrowane, czyniąc je tym samym niedostępnymi dla uprawnionych użytkowników.

SKUTKI ATAKU

Skutki ataku ransomware okazały się dla naszego klienta katastrofalne. Cała infrastruktura produkcyjna oparta na maszynach wirtualnych została sparaliżowana. Cyberprzestępcy, szyfrując zarówno maszyny produkcyjne, jak i ich kopie zapasowe, pozbawili firmę dostępu do kluczowych danych biznesowych.

Utrata danych kopii zapasowych przechowywanych na dedykowanych macierzach była szczególnie dotkliwa. Mimo wdrożenia mechanizmu migawek na macierzach produkcyjnych, który umożliwił częściowe odzyskanie danych z maszyn wirtualnych, firma straciła bezpowrotnie historyczne kopie zapasowe, zawierające m.in. poprzednie wersje plików, konfiguracje systemów oraz dane archiwalne. To oznaczało konieczność rozpoczęcia wielu procesów od początku oraz ryzyko utraty cennych informacji, które mogły okazać się niezbędne w przyszłości.

ROZWIĄZANIE

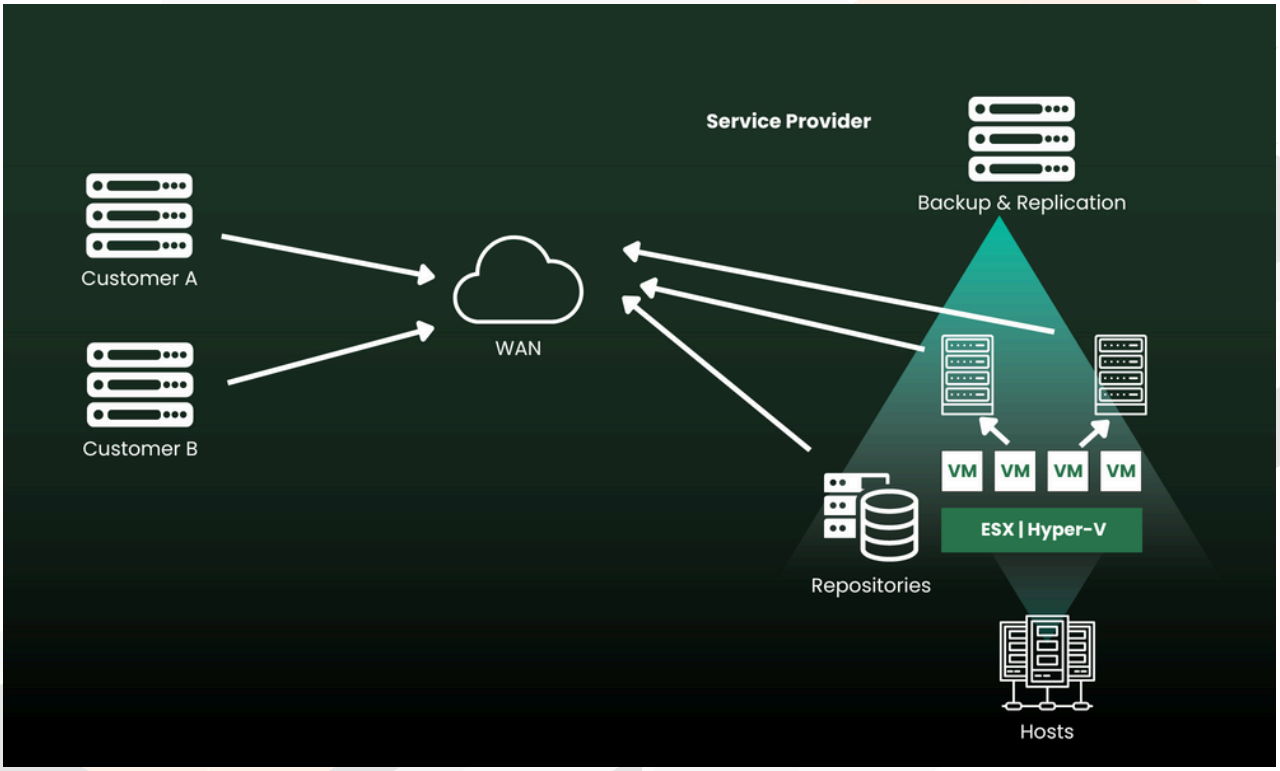
W obliczu poważnych konsekwencji ataku ransomware, firma Intratel zaproponowała kompleksowe rozwiązanie oparte na rozszerzeniu funkcjonalności platformy Veeam Backup&Replication. Celem było nie tylko przywrócenie ciągłości działania, ale przede wszystkim zapewnienie maksymalnej ochrony danych przed przyszłymi zagrożeniami.

VEEAM CLOUD CONNECT:

Aby zwiększyć odporność na ataki i zapewnić dodatkową warstwę bezpieczeństwa, wdrożono rozwiązanie Veeam Cloud Connect. Dzięki tej funkcji kopie zapasowe są replikowane w czasie rzeczywistym do bezpiecznego Data Center Intratel, zlokalizowanego poza infrastrukturą klienta. Proces replikacji jest niezwykle wydajny, ponieważ kopiowane są jedynie zmiany wprowadzone od ostatniego backupu, co minimalizuje zużycie przepustowości sieci i pojemności dyskowej. To rozwiązanie gwarantuje, że nawet w przypadku poważnych incydentów, takich jak całkowite zniszczenie lokalnej infrastruktury, klient ma dostęp do aktualnych kopii zapasowych, umożliwiających szybkie przywrócenie działania.

VEEAM HARDENED REPOSITORY:

Równolegle wdrożono funkcję Veeam Hardened Repository, która zapewnia najwyższy poziom bezpieczeństwa przechowywanych kopii zapasowych. Rozwiązanie to skutecznie uniemożliwia przypadkowe lub celowe usunięcie, nadpisanie lub modyfikację danych backupu. Dodatkową zaletą jest odporność na infekcje samego systemu operacyjnego serwera Veeam, co oznacza, że nawet w przypadku ataku na infrastrukturę wewnętrzną, kopie zapasowe pozostają nienaruszone.



Veeam Cloud Connect

IMPLEMENTACJA ROZWIĄZANIA BACKUPOWEGO

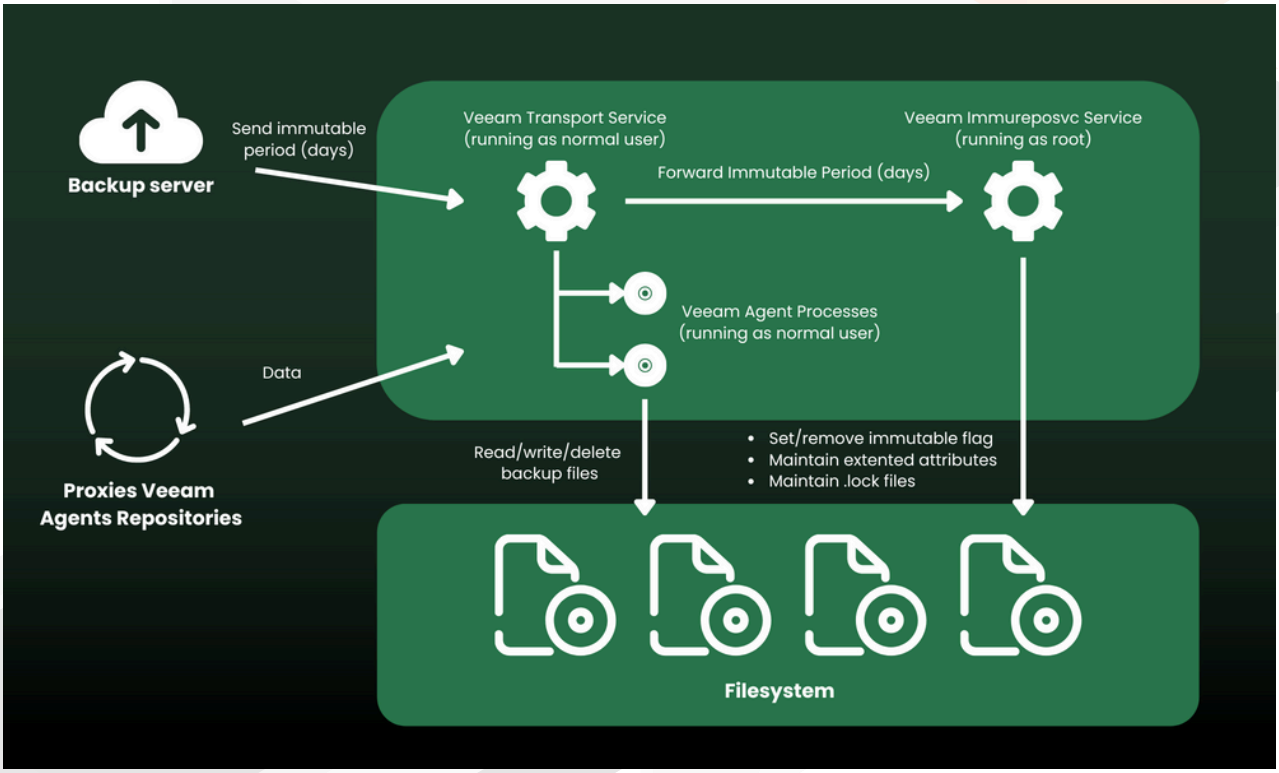
W ramach projektu wdrożenia zaawansowanego systemu backupowego, zrealizowano implementację kluczowych funkcjonalności Veeam, w tym Veeam Cloud Connect oraz Veeam Hardened Repository.

VEEAM CLOUD CONNECT:

Funkcjonalność Veeam Cloud Connect została wdrożona poprzez replikację codziennych kopii zapasowych klienta do bezpiecznego DataCenter Intratel. W tym celu wykorzystano dedykowaną infrastrukturę Intratel, pełniącą rolę zaufanego partnera Veeam Cloud Connect. Proces ten zapewnia nie tylko automatyczne tworzenie kopii zapasowych, ale także ich przechowywanie w zewnętrznym centrum danych, co znacząco podnosi poziom bezpieczeństwa i dostępności danych. Replikacja do DataCenter Intratel odbywa się w sposób całkowicie zautomatyzowany, z gwarancją integralności i poufności przechowywanych danych.

VEEAM HARDENED REPOSITORY:

Funkcjonalność Veeam Hardened Repository została zainstalowana na dedykowanym serwerze fizycznym, wyposażonym w lokalne dyski. W celu maksymalnego zabezpieczenia danych, system operacyjny tego serwera został dodatkowo zabezpieczony zgodnie z wytycznymi DISA STIG (Defense Information Systems Agency Security Technical Implementation Guides). Zastosowanie tych rygorystycznych wytycznych zapewnia ochronę danych i konfiguracji przed nieautoryzowanym dostępem, co jest kluczowe dla utrzymania wysokiego poziomu bezpieczeństwa. Dodatkowo, serwer został skonfigurowany tak, aby wszelkie operacje zapisu były nieodwracalne, co oznacza, że raz zapisane dane nie mogą zostać zmodyfikowane ani usunięte.



Veeam Hardened Repository

REZULTAT IMPLEMENTACJI

Wdrożenie zaawansowanych funkcjonalności Veeam Cloud Connect i Veeam Hardened Repository przyniosło klientowi szereg istotnych korzyści, które w znaczący sposób wpłynęły na bezpieczeństwo i efektywność zarządzania danymi.

1

Zwiększone Bezpieczeństwo Danych

Dzięki wdrożeniu Veeam Cloud Connect, kopie zapasowe są teraz przechowywane poza organizacją klienta w bezpiecznym DataCenter Intratel. Taka architektura przechowywania zapewnia wysoki poziom ochrony przed różnorodnymi zagrożeniami, w tym atakami ransomware. Dane są replikowane w sposób zautomatyzowany, co minimalizuje ryzyko ludzkich błędów i zapewnia integralność kopii zapasowych. Veeam Hardened Repository dodatkowo zabezpiecza te dane, czyniąc je odpornymi na modyfikacje i usunięcia, co jest kluczowe w walce z cyberatakami.

2

Szybsze Odzyskiwanie Danych

Jednym z kluczowych rezultatów wdrożenia jest znaczące skrócenie czasu potrzebnego na odzyskiwanie danych. W przypadku awarii maszyny wirtualnej, jej kopia zapasowa może zostać szybko i sprawnie przywrócona z bezpiecznego DataCenter Intratel. To oznacza minimalne przestoje w działalności operacyjnej klienta, co jest szczególnie ważne w środowiskach, gdzie ciągłość działania ma kluczowe znaczenie.

3

Większy Spokój Ducha

Wdrożenie nowoczesnych rozwiązań backupowych Veeam przekłada się również na większy spokój ducha klienta. Klient ma pewność, że jego dane są chronione na najwyższym poziomie i w razie potrzeby mogą zostać szybko przywrócone. Świadomość, że dane są bezpiecznie przechowywane i chronione przed wszelkimi zagrożeniami, pozwala klientowi skupić się na głównych aspektach swojej działalności, bez obaw o potencjalne straty danych.

Podsumowując, implementacja Veeam Cloud Connect i Veeam Hardened Repository znacząco podniosła poziom bezpieczeństwa danych, przyspieszyła proces odzyskiwania danych oraz zapewniła klientowi pewność, że jego zasoby są odpowiednio chronione i dostępne w każdej sytuacji awaryjnej.

WNIOSKI

Atak ransomware w firmie produkcyjnej uwidocznił krytyczną rolę, jaką odgrywa solidne zabezpieczenie infrastruktury serwerowej w ochronie kluczowych danych. Doświadczenie to podkreśliło, że tradycyjne metody ochrony są niewystarczające w obliczu współczesnych zagrożeń cybernetycznych, zwłaszcza w branżach, gdzie utrata danych może prowadzić do poważnych przestojów i strat finansowych.

Wdrożenie rozwiązań takich jak Veeam Cloud Connect i Veeam Hardened Repository okazało się kluczowe w znacznym podniesieniu poziomu bezpieczeństwa infrastruktury IT klienta. Dzięki Veeam Cloud Connect, dane zostały skutecznie zreplikowane do zewnętrznego, bezpiecznego DataCenter, co nie tylko zabezpiecza je przed utratą, ale także umożliwia szybkie odzyskanie w razie awarii. Natomiast Veeam Hardened Repository, dzięki zaawansowanym mechanizmom ochrony, gwarantuje, że dane są chronione przed nieautoryzowanym dostępem i nie mogą być zmodyfikowane ani usunięte, co jest kluczowe w kontekście ochrony przed ransomware.

Te zaawansowane rozwiązania nie tylko zwiększyły poziom bezpieczeństwa danych, ale także zapewniły firmie długoterminową ochronę przed przyszłymi atakami. Firma, która doświadczyła skutków ataku ransomware, zyskała teraz większą pewność, że jej zasoby są odpowiednio chronione. W efekcie, wdrożenie tych technologii stanowiło strategiczny krok w kierunku budowy odpornej na zagrożenia infrastruktury IT, która nie tylko chroni przed bieżącymi zagrożeniami, ale także jest przygotowana na przyszłe wyzwania.

DODATKOWE KORZYŚCI Z WDROŻENIA

1

Łatwość Obsługi

Jednym z kluczowych atutów wdrożonego rozwiązania jest jego intuicyjność. Veeam Backup & Replication zostało zaprojektowane z myślą o prostocie użytkowania, co znacząco ułatwia zarówno początkową konfigurację, jak i późniejsze zarządzanie systemem. Przyjazny interfejs użytkownika oraz przejrzysta dokumentacja sprawiają, że z rozwiązania mogą korzystać nie tylko specjaliści IT, ale także mniej zaawansowani użytkownicy, co redukuje czas i koszty związane z wdrożeniem oraz bieżącą obsługą.

2

Skalowalność

W miarę jak firma klienta się rozwija, rośnie również zapotrzebowanie na przestrzeń dyskową oraz zasoby do zarządzania danymi. Veeam Backup & Replication oferuje wysoką skalowalność, co pozwala na elastyczne dostosowanie systemu do rosnących potrzeb biznesu. Możliwość łatwego dodawania nowych zasobów i rozbudowy infrastruktury backupowej gwarantuje, że rozwiązanie będzie wspierać firmę na każdym etapie jej rozwoju, niezależnie od skali operacji.

3

Opłacalność

Veeam Backup & Replication to rozwiązanie, które oferuje doskonały stosunek wartości do ceny. Dzięki zaawansowanym funkcjonalnościom, takim jak Cloud Connect i Hardened Repository, klient otrzymuje kompleksowe narzędzie do zarządzania i ochrony danych, które minimalizuje ryzyko przestojów i utraty danych, jednocześnie optymalizując koszty operacyjne. Zdolność do skutecznej ochrony danych, szybkie odzyskiwanie i łatwość zarządzania sprawiają, że inwestycja w to rozwiązanie szybko się zwraca, przynosząc długoterminowe oszczędności.

PODSUMOWANIE

Oprócz zwiększonego bezpieczeństwa danych, wdrożenie Veeam Backup & Replication z funkcjonalnościami Cloud Connect i Hardened Repository przyniosło klientowi szereg dodatkowych korzyści, takich jak łatwość obsługi, możliwość skalowania wraz z rozwojem firmy oraz wysoka opłacalność inwestycji. Te cechy sprawiają, że rozwiązanie nie tylko spełnia, ale często przewyższa oczekiwania klientów, zapewniając stabilne i elastyczne wsparcie w zarządzaniu danymi.

DLACZEGO WARTO WYBRAĆ FIRMĘ INTRATEL?

Kluczowym czynnikiem sukcesu tego wdrożenia była współpraca z firmą Intratel, specjalistami w dziedzinie IT i ochrony danych. Dzięki wieloletniemu doświadczeniu oraz dogłębnej znajomości technologii Veeam, Intratel zapewnił profesjonalną implementację, dostosowaną do indywidualnych potrzeb klienta. Firma ta oferuje kompleksowe wsparcie na każdym etapie projektu – od analizy potrzeb, przez planowanie i wdrożenie, aż po bieżące zarządzanie i optymalizację systemu backupowego. Wybór Intratel to gwarancja, że wdrożenie zostanie przeprowadzone sprawnie, a zastosowane rozwiązania będą skutecznie chronić dane klienta, zapewniając jednocześnie elastyczność i skalowalność systemu w przyszłości.

SKONTAKTUJ SIĘ Z NAMI

Porozmawiajmy o rozwiązaniu dla Twojej firmy!

Mariusz Bakun
Architekt Rozwiązań
m.bakun@intratel.pl
tel. +605 237 228

Intratel Sp. z o.o.
Aleja Tysiąclecia
Państwa Polskiego 39A
15-111 Białystok