# Przyspieszone odzyskiwanie danych po ransomware dzięki Usługom kopii zapasowych Dell PowerProtect

Odzyskiwanie danych po ataku oprogramowania wymuszającego okup w ciągu godzin, a nie dni

## Najważniejsze funkcje

Ataki oprogramowania wymuszającego okup stają się coraz częstsze, coraz bardziej zaawansowane i kosztowniejsze

- Brak możliwości szybkiego identyfikowania i przywracania niezainfekowanych kopii zapasowych lub plików
- Skażenie rozprzestrzeniło się i ponownie zainfekowało dane służące do odzyskiwania
- Utrata danych, niemożność odzyskania kompletnego zestawu danych
- Trudności w koordynowaniu organizacji reagowania na incydenty
- Wymagania dotyczące szybszego czasu RPO/RTO
- Kosztowne przestoje biznesowe prowadzące do utraty przychodów i utraty reputacji marki
- Grzywny prawne i regulacyjne z tytułu nieodpowiedniej ochrony danych

## Wyzwanie

Ransomware stanowi poważne zagrożenie dla każdego przedsiębiorstwa. Cyberataki występują często i mogą spowodować katastrofalne szkody. 79% organizacji obawia się, że w ciągu najbliższych 12 miesięcy dojdzie do destrukcyjnego ataku1. Firmy, które utracą swoje dane, są narażone na upadłość po katastrofie. Ataki oprogramowania wymuszającego okup nie tylko zdarzają się coraz częściej, ale też stały się bardziej zaawansowane technologicznie i kosztowne.

## Rozwiązanie

Szybkie, niezawodne odzyskiwanie eliminuje wszelkie powody, aby nawet pomyśleć o zapłaceniu okupu. Kiedy jednak dochodzi do incydentu bezpieczeństwa lub cyberataku, organizacje muszą zrozumieć promień wybuchu i przyczynę źródłową zanim przystąpią do odzyskiwania. Dzięki nieskazitelnym, odizolowanym migawkom obciążeń roboczych i maszyn wirtualnych dostępnym całodobowo, ciągłemu monitorowaniu anomalii związanych z użytkownikami i danymi, integracji z narzędziami zabezpieczającymi oraz automatycznemu odzyskiwaniu czystych danych możesz polepszyć stan bezpieczeństwa i zmienić ciężką przeprawę w możliwy do przetrwania incydent.

## Możliwości

**Dla wszystkich obciążeń roboczych:**

• Zapewnienie, że masz niezmienne, odizolowane kopie zapasowe dostępne 24x7

• Odzyskiwanie czystych danych lokalnie lub w chmurze z RPO/RTO liczonym w godzinach, a nie w dniach czy tygodniach

• Usługa Managed Data Detection and Response (MDDR) zapewnia całodobowe monitorowanie środowisk tworzenia kopii zapasowych w czasie rzeczywistym w trybie 24x7x365

• Z powodu przywracania obciążeń roboczych i maszyn wirtualnych w dowolnym regionie/koncie AWS przy użyciu danych z organizacji produkcyjnej oraz tworzenia licznych kopii tych danych i ich przechowywania w wielu miejscach narażasz swoją organizację na duże ryzyko.

**Szybkie odzyskiwanie danych po ataku ransomware dla kluczowych obciążeń:**

• Monitorowanie i proaktywne wykrywanie anomalii za pomocą algorytmów opartych na ML

• Orkiestracja działań reagowania i odzyskiwania danych za pośrednictwem integracji SIEM i SOAR

• Skanowanie migawek pod kątem złośliwego oprogramowania przed odzyskiwaniem i usuwanie zainfekowanych migawek i plików z kopii zapasowych

• Automatycznie odzyskać najnowszą czystą wersję każdego pliku w określonym przedziale czasu z kopii zapasowej złotego obrazu

## Ochrona

Pierwszym krokiem w zapobieganiu uszkodzeniom spowodowanym przez ransomware jest upewnienie się, że masz odizolowaną i niezmienną kopię danych. Usługi kopii zapasowych Dell PowerProtect oparte na wysoce odpornej infrastrukturze chmurowej uniemożliwiają oprogramowaniu wymuszającemu okup szyfrowanie danych kopii zapasowych. Architektura zgodna z modelem „zero trust”, obejmująca m.in. uwierzytelnianie wieloskładnikowe, szyfrowanie kopert i dostęp do oddzielnego konta, zapewnia, że oprogramowanie wymuszające okup nie może używać przechwyconych danych uwierzytelniających do środowiska podstawowego do ingerowania w środowisko kopii zapasowych ani w dane. Ponadto funkcje zapobiegające usuwaniu nadmiernych ilości danych i funkcje nietrwałego usuwania (kosza) zapewniają dodatkową warstwę zabezpieczeń, aby chronić kopie zapasowe przed usunięciem.

## Wykrywanie

Jak najszybsze wykrycie ataku ransomware może pomóc zespołom reagowania na incydenty i zapobiec rozprzestrzenianiu się zanieczyszczeń. Wchodzący w skład Usług kopii zapasowych Dell PowerProtect moduł przyspieszonego odzyskiwania danych po ataku oprogramowania wymuszającego okup stanowi centrum zarządzania bezpieczeństwem, które umożliwia monitorowanie stanu środowiska tworzenia kopii zapasowych. Dzięki dostępowi do informacji i wykrywaniu anomalii można szybko zidentyfikować nietypowe działania w całym środowisku i danych. Zapoznaj się z informacjami o lokalizacji, tożsamości i aktywności dla wszystkich prób dostępu użytkowników i interfejsów API. Wykrywanie anomalii za pomocą zastrzeżonych algorytmów ML, które dostarczają alerty dotyczące nietypowej aktywności danych (np. usuwania, szyfrowania itp.). Algorytm uczy się wzorców dla określonego środowiska tworzenia kopii zapasowych, więc nie wymaga konfiguracji ani dostrajania reguł. Używa również analiz opartych na entropii w celu zmniejszenia wyników fałszywie pozytywnych.

## na miejscu

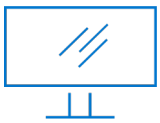
Gdy analityk bezpieczeństwa lub środowiska IT wykryje podejrzane zdarzenie lub co gorsza potwierdzi, że miał miejsce atak oprogramowania wymuszającego okup, krytyczne znaczenie ma szybkość reakcji. Chociaż istnieje wiele cennych narzędzi do zabezpieczania środowiska podstawowego, które mogą służyć do wykrywania ataków i koordynowania działań naprawczych, dane analityczne i informacje z dziennika zmian pochodzące z danych zapasowych (systemów tworzenia kopii zapasowych) usprawniają badania, reagowanie i czynności śledcze. Wchodzący w skład Usług kopii zapasowych Dell PowerProtect moduł przyspieszonego odzyskiwania danych po ataku oprogramowania wymuszającego okup zapewnia gotową, solidną integrację interfejsów API, co ułatwia dopasowanie rozwiązania do ogólnego ekosystemu zabezpieczeń. Koordynacja działań naprawczych przy użyciu rozwiązań SIEM i SOAR może znacznie skrócić średni czas reakcji (MTTR) poprzez automatyczne wykonywanie czynności, takich jak objęcie kwarantanną zainfekowanych systemów lub migawek czy też skanowanie kopii zapasowych pod kątem wskaźników wykrytych zagrożeń na podstawie wstępnie określonego instruktażu dotyczącego oprogramowania wymuszającego okup.

## Odzyskiwanie

Po początkowej fazie reakcji przychodzi ciężkie zadanie odzyskiwania. Dla wielu firm jest to proces ręczny i czasochłonny. Czas dostępu złośliwych podmiotów i oprogramowania wymuszającego okup do systemów organizacji może wynosić od tygodni do miesięcy, co utrudnia ustalenie, jak daleko należy się cofnąć, aby uzyskać czyste dane. Nawet po zidentyfikowaniu najlepszej migawki ukryte złośliwe oprogramowanie może spowodować ponowną infekcję. Jednak punkt odzyskiwania sprzed 2 tygodni nie jest akceptowany przez większość użytkowników biznesowych. Znalezienie i zweryfikowanie nowszych danych po incydencie wywołanym przez oprogramowanie wymuszające okup jest jednak zadaniem realizowanym ręcznie, żmudnym i często niewykonalnym.

Usługi kopii zapasowych Dell PowerProtect ułatwiają ten problem dzięki efektywnej architekturze tworzenia kopii zapasowych i zautomatyzowanym narzędziom przyspieszającym odzyskiwanie danych. Platforma chmurowa Usług kopii zapasowych Dell PowerProtect tworzy kopie zapasowe obciążeń roboczych bezpośrednio w chmurze, dzięki czemu są one gotowe do natychmiastowego odzyskania danych po ataku oprogramowania wymuszającego okup.

Moduł przyspieszonego odzyskiwania danych po ataku ransomware umożliwia bezpieczne odzyskiwanie danych dzięki zachowaniu higieny. Możesz skanować migawki w poszukiwaniu złośliwego oprogramowania i wskaźników wykrytych zagrożeń przy użyciu wbudowanego mechanizmu wykrywania wirusów albo za pomocą analizy zagrożeń na podstawie własnych dochodzeń śledczych lub źródeł danych wywiadowczych dotyczących zagrożeń. Skanowanie migawek przed odzyskiwaniem eliminuje ponowną infekcję.



Więcej informacji Dowiedz się więcej o Usługach kopii zapasowych PowerProtect

Kontakt z ekspertem firmy Dell Technologies