DELL Technologies

Krótki opis

CyberSense® dla Dell PowerProtect Cyber Recovery

Oparte na sztucznej inteligencji narzędzia analityczne i śledcze do wykrywania, diagnozowania i odzyskiwania danych po cyberatakach

ZALETY ROZWIĄZANIA CYBERSENSE

Rozwiązanie CyberSense® jest w pełni zintegrowane z rozwiązaniem magazynowym Dell PowerProtect Cyber Recovery.

- Automatyzuje regularne skanowanie danych kopii zapasowych, które sprawdza integralność danych i informuje o wykryciu podejrzanego zachowania.
- Bezpośrednio skanuje zawartość obrazów kopii zapasowych z aplikacji Dell Avamar, NetWorker, Commvault, NetBackup i PowerProtect Data Manager bez konieczności ponownego przywracania danych.
- Wykonuje dogłębną analizę pełnej zawartości przy każdym skanowaniu danych w celu wykrycia nawet najbardziej zaawansowanych ataków ransomware.
- Niestandardowe alerty dotyczące reguł YARA i sygnatur złośliwego oprogramowania w celu wykrywania znanych zachowań oprogramowania ransomware lub zachowań związanych z zagrożeniami wewnętrznymi.
- Inteligentniejsze i szybsze odzyskiwanie danych dzięki raportom śledczym po ataku zapewnia dogłębny wgląd w atak i listę ostatnich prawidłowych zestawów kopii zapasowych przed ich naruszeniem.

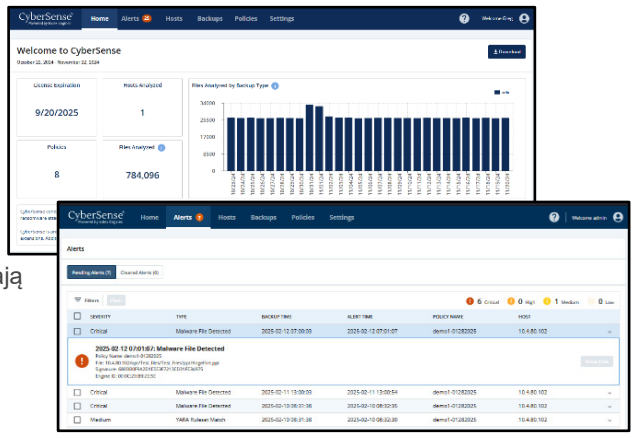
Rozwiązanie CyberSense wyróżnia się na tle innych metod analizy danych i daje większą pewność, że dane kopii zapasowej są integralne i można je szybko odzyskać po wystąpieniu ataku.

Ponieważ częstotliwość cyberataków nadal rośnie, a cyberprzestępcy działają w sposób coraz bardziej wyrafinowany, tradycyjne zabezpieczenia nie chronią już skutecznie danych przed cyberatakami.

Rozwiązanie **CyberSense®** wykrywa uszkodzenia danych po ataku z dokładnością na poziomie 99,99%* oraz umożliwia inteligentne i szybkie przywracanie danych. Rozwiązanie CyberSense, będące pierwszą linią odzyskiwania danych dla tysięcy organizacji na całym świecie, zapewnia integralność zasobów danych, w tym podstawowej infrastruktury, baz danych i kluczowych dokumentów, dając pewność, że dane są wolne od złośliwych uszkodzeń.

CyberSense skanuje kopie zapasowe danych w magazynie Cyber Recovery, obserwując, jak dane zmieniają się w czasie. Następnie wykorzystuje uczenie maszynowe i sztuczną inteligencję do wykrywania oznak uszkodzenia wskazujących na atak ransomware. Dane porównywane są z ponad 200 analizami opartymi na treści w celu znalezienia uszkodzenia z dokładnością do 99,99%*. Działania te pomagają chronić infrastrukturę i treści o znaczeniu krytycznym dla firmy. Rozwiązanie CyberSense wykrywa masowe usuwanie, szyfrowanie i inne podejrzane zmiany wynikające z zaawansowanych ataków w podstawowej infrastrukturze (w tym Active Directory, DNS itp.), rezpozytoriach i systemach plików oraz w bazach danych o znaczeniu krytycznym.

W przypadku wystąpienia podejrzanego zachowania rozwiązanie CyberSense udostępnia raporty śledcze po cyberataku, aby zdiagnozować jego zakres. Po wykryciu uszkodzenia danych dostępna jest lista ostatnich znanych prawidłowych zestawów danych kopii zapasowych, które umożliwiają szybkie, ukierunkowane odzyskiwanie, co pomaga ograniczyć przerwy w działalności i utratę danych, a tym samym ograniczyć koszt odzyskiwania danych.

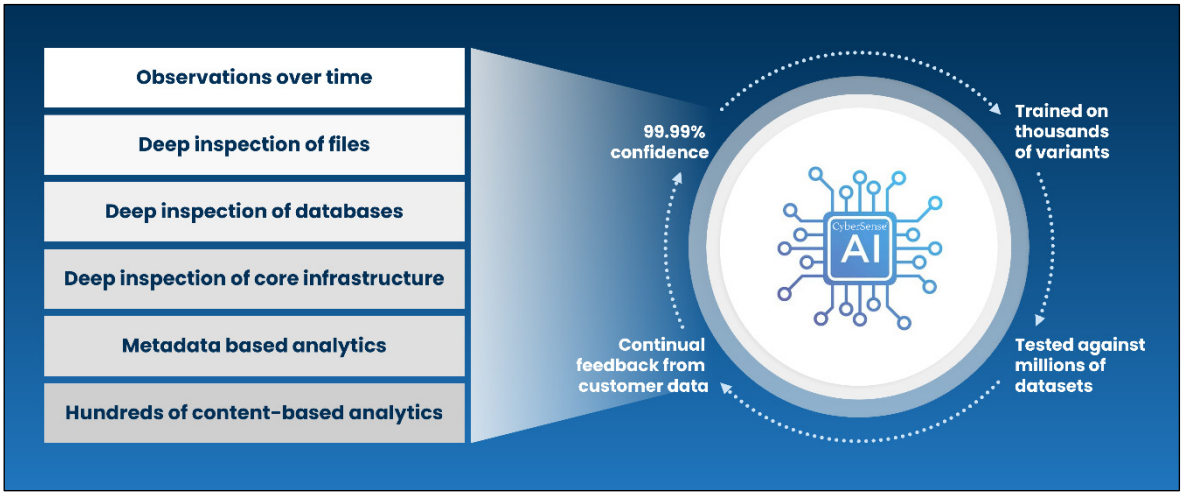


Przepływ pracy Cyber Recovery

CyberSense bezproblemowo integruje się z rozwiązaniem Dell PowerProtect Cyber Recovery, aktywnie monitorując pliki i bazy danych w celu wykrywania uszkodzeń spowodowanych oprogramowaniem ransomware na podstawie analizy integralności danych. Po zreplikowaniu danych do magazynu Cyber Recovery i zastosowaniu blokady retencji rozwiązanie CyberSense automatycznie inicjuje kompleksowe skanowanie danych kopii zapasowej, tworząc punkty obserwacyjne plików, baz danych i podstawowej infrastruktury z określonego okresu. Rozwiązanie CyberSense może skrupulatnie śledzić zmiany w plikach w czasie, skutecznie wykrywając uszkodzenia danych spowodowane przez nawet najbardziej zaawansowane zagrożenia cybernetyczne.

Pełna analiza treści

CyberSense to jedyny produkt na rynku, który umożliwia indeksowanie i analizę wszystkich chronionych danych oparte całkowicie na zawartości. Korzystając ze sztucznej inteligencji, CyberSense przeprowadza głęboką analizę wszystkich danych i z prawdopodobieństwem rzędu 99,99%* określa, czy dane są integralne czy też zostały uszkodzone przez oprogramowanie ransomware. Ta funkcja odróżnia CyberSense od innych rozwiązań, które zapewniają ogólny wgląd w dane i korzystają z analiz wykrywających oczywiste oznaki uszkodzenia na podstawie metadanych. Uszkodzenie na poziomie metadanych, na przykład zmiana rozszerzenia pliku na .encrypted lub radykalna zmiana rozmiaru pliku, nie jest trudne do wykrycia. Tego typu zagrożenia nie stanowią zaawansowanych ataków, które są obecnie przeprowadzane przez cyberprzestępców.



CyberSense wykracza poza rozwiązania oparte wyłącznie na metadanych i wykrywa uszkodzenie danych za pomocą analizy pełnej zawartości. Przeprowadza audyt plików i baz danych pod kątem zmian wskazujących na atak, w tym na pełne lub częściowe uszkodzenie plików. Tradycyjne analizy pomijają te zagrożenia, co prowadzi do fałszywego poczucia bezpieczeństwa. Na podstawie zmian w plikach, na podstawie plików dodanych lub usuniętych można ustawić niestandardowe alerty progowe. Można również wdrożyć niestandardowe reguły YARA i sygnatury złośliwego oprogramowania, aby wykrywać złośliwe oprogramowanie zarówno w przeszłych, jak i przyszłych kopiach zapasowych.

Obsługiwane typy danych

Rozwiązanie CyberSense generuje analizy na podstawie szerokiego zakresu typów danych. Obejmuje to podstawową infrastrukturę, taką jak DNS, LDAP, Active Directory, pliki bez struktury, np. dokumenty, umowy, własność intelektualna i bazy danych, w tym Oracle, DB2, SQL, PostgreSQL, Epic Caché itp.

Podsumowanie

CyberSense, w pełni zintegrowane z rozwiązaniem Dell PowerProtect Cyber Recovery, analizuje dane magazynu i wykrywa oparte na zachowaniu wskaźniki naruszenia i uszkodzenia. Rozwiązanie CyberSense umożliwia proaktywne zrozumienie zakresu trwającego cyberataku i wdrożenie planu szybkiej diagnostyki i odzyskiwania w celu ograniczenia przerwy w działalności i związanych z nią kosztów.

Dowiedz się więcej o rozwiązaniu Dell PowerProtect Cyber Recovery

Skontaktuj się z ekspertem firmy Dell Technologies

Więcej informacji o rozwiązaniu CyberSense

Dołącz do rozmowy, stosując hasztag #PowerProtect

* Na podstawie raportu „Index Engines' CyberSense Validated 99,99% Effective in Detecting Ransomware Corruption" opracowanego przez ESG na zlecenie Index Engines. Czerwiec 2024 r.

DELL Technologies