Safetica ONE vs NXT

	safetica NXT	safetica ONE
Podstawowe informacje	**SaaS DLP nowej generacji** • Łatwe w użyciu, oparte na ryzyku rozwiązanie SaaS • Skupione na podstawowych scenariuszach bezpieczeństwa danych, maksymalnie uproszczone i zautomatyzowane w oparciu o najlepsze praktyki	**DLP dla średnich i dużych przedsiębiorstw - ochrona przed zagrożeniami wewnętrznymi** • Sprawdzone na rynku rozwiązanie klasy korporacyjnej • Obejmuje pełen zakres scenariuszy bezpieczeństwa z naciskiem na ochronę danych, audyt przestrzeni roboczej oraz optymalizację kosztów
Typowy klient	**50 - 500 użytkowników** • Ograniczona infrastruktura sprzętowa lub jej brak • Ograniczone zasoby ludzkie w zespole IT lub outsourcing usług informatycznych • Preferowany model SaaS - opłata za bezpieczeństwo danych jako usługa	**200 - 4 000 użytkowników** • Własna infrastruktura i preferowane wykorzystanie własnych zasobów • Własny zespół IT lub zespół ds. bezpieczeństwa • Środowisko wielodomenowe, potrzeba integracji z narzędziami bezpieczeństwa innych dostawców
Opcje wdrożenia	**SaaS w chmurze** • Usługa chmurowa działająca w oparciu o Microsoft Azure • Opcja samodzielnego zarządzania rozwiazaniem lub przez wyspecjalizowanego dostawcę usług IT • Wymaga zainstalowania Safetica Client na urządzeniach	**Elastyczne opcje wdrożenia** • System działający w środowisku lokalnym, zdalnym centrum danych lub w chmurze • Wymaga zainstalowania Safetica Client na urządzeniach
Administracja i konserwacja	**Maksymalna prostota i automatyzacja** • Proste ustawienia, większość konfiguracji wykorzystuje najlepsze praktyki (zalecenia) z zakresu bezpieczeństwa danych • Niski wpływ na zasoby administracyjne, dzięki automatycznemu wykrywaniu ryzyka • ~2-4h pracy administratora tygodniowo	**Zaawansowana konsola ustawień** • Granularne opcje konfiguracji • Zarządzanie i ustawienia zapewniające równowagę między bezpieczeństwem danych a produktywnością przedsiębiorstwa • ~8h+ pracy administratora tygodniowo

Safetica ONE vs NXT

	safetica NXT	safetica ONE
Czas wdrożenia	**Wdrożenie w ciągu kilku godzin** • Godziny na wdrożenie • Dni do tygodni na przeprowadzenie audytu bezpieczeństwa i skonfigurowanie wstępnych reguł ochrony	**Wdrożenie w ciągu kilku tygodni** • Tygodnie na wdrożenie i przeprowadzenie audytu bezpieczeństwa • Od tygodni do miesięcy na pełne skonfigurowanie
Modele licencji i płatności	**Subskrypcja na zasadzie pay-as-you-go** • Miesięczna lub roczna opłata abonamentowa płacona per użytkownik	**Licencja roczna** • Roczna, wieloletnia lub bezterminowa licencja oparta na liczbie punktów końcowych
Zakres przypadków użycia		
• **Wykrywanie danych wrażliwych**	Wykrywanie i klasyfikacja danych wrażliwych na podstawie treści	Klasyfikacja danych oparta na treści z technologią OCR i kontekście
• **Ochrona własności intelektualnej**	Prosta konfiguracja zasad DLP/ochrony	Granularna konfiguracja zasad DLP w celu zaspokojenia określonych potrzeb biznesowych
• **Zgodność z przepisami**	Szybka konfiguracja wykrywania danych wrażliwych/incydentów, dzięki wstępnie skonfigurowanym kategoriom danych (dane osobowe, finansowe i zdrowotne)	Niestandardowa konfiguracja wykrywania wrażliwych danych/zdarzeń dla szerokiego zakresu regulacji i standardów
• **Analiza (ryzyka) użytkowników i obszarów roboczych**	Informacje o poziomie ryzyka każdego zdarzenia i użytkownika	Szczegółowe informacje o zachowaniu użytkowników w przestrzeni roboczej, kontrola wykorzystania sprzętu i oprogramowania w celu optymalizacji kosztów
• **Kontrola stron internetowych/aplikacji**	Tylko kontrola wysyłania plików (jako część DLP - zarządzanie przepływem danych)	Pełna kontrola sieci i aplikacji z precyzyjną kategoryzacją
• **Zabezpieczone strefy**	Pojedyncza bezpieczna przestrzeń robocza z inteligentnym automatycznym wykrywaniem	Możliwość ustawienia i skonfigurowania wielu bezpiecznych stref