# Licencja LIC-GOLD-ZZ2Y07F

| | |
|---|---|
| Cena brutto | **4 758,99 zł** |
| Cena netto | **3 869,10 zł** |
| Numer katalogowy | **NUZYXBOLAS00060** |
| Kod producenta | **LIC-GOLD-ZZ2Y07F** |
| Data Act | **Zyxel - __ZYX%, __EDX%** |
| Uwaga | **Kosz zgodnie z zasadami recyklingu** |
| Czas trwania (pakiety gw.) | **2 lata** |
| Wersja | **Cyfrowa / do pobrania** |
| Pasuje do | **USG FLEX 500H** |

## Opis produktu

**Gold Security Pack 2YR USG FLEX 500H**

**Złoty pakiet bezpieczeństwa**

**Kompleksowa ochrona dostosowana do nowoczesnych sieci**
W dzisiejszym złożonym cyfrowym krajobrazie, Gold Security Pack oferuje przyszłościowe rozwiązanie zaprojektowane, aby zapobiegać mądrzej, reagować szybciej i zapewniać lepszą ochronę dla Twojej firmy. Ten kompleksowy pakiet zabezpieczeń jest dostosowany do zmieniających się potrzeb małych i średnich firm działających w środowiskach hybrydowych.

**Ochrona przed zaawansowanymi zagrożeniami**
Sandboxing zawiera wszystkie nieznane pliki lub wzorce użytkownika w izolacji, a następnie emuluje programy do uruchomienia i identyfikuje, czy są one złośliwe. Jeśli są złośliwe, Sandboxing zaktualizuje te nowe informacje o złośliwym oprogramowaniu za pomocą uczenia maszynowego Threat Intelligence.

**Kompletna ochrona sieci: wewnątrz i na zewnątrz**
Ochrona przed zagrożeniami zewnętrznymi przy jednoczesnym zachowaniu kontroli nad wewnętrznym wykorzystaniem sieci. Nasze wielowarstwowe podejście gwarantuje, że żadne luki nie zostaną ujawnione, zapewniając spokój ducha i pozwalając skupić się na podstawowych operacjach biznesowych.

**Ochrona przed złośliwym oprogramowaniem oparta na sztucznej inteligencji**
Ochrona przed złośliwym oprogramowaniem jest wzmocniona przez codzienną synchronizację za pomocą uczenia maszynowego Threat Intelligence, dzięki czemu ochrona przed złośliwym oprogramowaniem jest podnoszona z lokalnego zakresu do kompleksowego poziomu chmury z globalną synergią udostępniania. Cloud Query dodatkowo dodaje usługę sprawdzania hash w czasie rzeczywistym, zapewniając szybszą, lepszą i silniejszą ochronę przed złośliwym oprogramowaniem.

**Ochrona reputacji w czasie rzeczywistym**

- Reputacja IP
- Filtr zagrożeń DNS
- Filtr zagrożeń URL

Filtr reputacji poprawia skuteczność blokowania, ogranicza dostęp do złośliwych adresów IP / domen / adresów URL i blokuje dostęp z zagrożonych źródeł, zapewniając w ten sposób szczegółową ochronę przed stale ewoluującymi cyberzagrożeniami.

**Inteligentne filtrowanie sieci: Poza tradycyjnymi granicami**
Nasze zaawansowane filtrowanie stron internetowych łączy w sobie filtrowanie oparte na reputacji i kategoriach z dynamiczną

kategoryzacją treści. Ten potężny system analizuje nieznane strony internetowe, identyfikując niepożądane treści w różnych kategoriach. Nowy filtr treści DNS zwiększa możliwości inspekcji, skutecznie radząc sobie z wyzwaniami stawianymi przez strony internetowe z obsługą ESNI, w których tradycyjne filtrowanie adresów URL jest niewystarczające.

**Zwiększona kontrola: ponad 3700 aplikacji na wyciągnięcie ręki**
Nasz ulepszony patrol aplikacji oferuje teraz bardziej przejrzystą analizę skoncentrowaną na kliencie, natychmiastowe raportowanie i obszerną listę kategorii. Dzięki ponad 3700 skategoryzowanym aplikacjom, od antywirusów po sieci społecznościowe, zyskujesz kompleksową widoczność. Nowa strona monitorowania aplikacji w całej witrynie umożliwia natychmiastowe blokowanie, odblokowywanie i ograniczanie prędkości, umożliwiając użytkownikom Nebula efektywne zarządzanie i ochronę sieci dzięki możliwościom natychmiastowego działania.

**SecuReporter**
Wykorzystuje SecuReporter do dalszej analizy zagrożeń z funkcją korelacji, ułatwiając proaktywne śledzenie stanu sieci w celu zapobiegania kolejnym zagrożeniom. Scentralizowana widoczność działań sieciowych ułatwia zarządzanie wieloma klientami.

**Bezpieczne Wi-Fi**
Zapewnij taką samą kontrolę sieci bezprzewodowej, która może być stosowana w siedzibie głównej i innych zdalnych miejscach pracy. Łatwo i bezpiecznie rozszerzaj środowisko pracy tak, jakbyś był w biurze dzięki zastosowaniu bezpiecznego tunelowania.

**Wspólne wykrywanie i reagowanie**
Collaborative Detection & Response (CDR) identyfikuje zagrożenia w całej organizacji i tworzy reguły ochrony w oparciu o ich wagę. Zintegrowana analiza zagrożeń w chmurze wdraża te reguły, aby szybko blokować lub poddawać kwarantannie zagrożenia na brzegu sieci.

**Nebula Professional Pack**
Aby wzmocnić bezpieczeństwo sieci, wzmacniamy Zyxel Security Matrix w Nebula z naszymi zaporami ogniowymi w chmurze, zapewniając spokój ducha dzięki wspólnej obronie sieci i udostępnianiu piaskownicy. Uzyskaj szczegółowe raporty z dochodzeń, aktywny monitoring, wysoką widoczność działań sieciowych dzięki naszej ewoluującej ochronie bezpieczeństwa.