Dane aktualne na dzień: 24-10-2026 10:57

Link do produktu: https://sklepqnap.pl/qnap-licencja-adra-ndr-dla-qgd-1-rok-p-3049.html

# Qnap Licencja ADRA NDR dla QGD 1 rok

| | |
|---|---|
| Cena | **2 155,31 zł** |
| Dostępność | **Oczekujemy** |
| Numer katalogowy | **QNA_LSADRANDRGL1Y** |
| Kod producenta | **LS-ADRANDR-GL-1Y** |
| Kod EAN | **4711103082430** |
| Producent | **QNAP** |

## Opis produktu

## QNAP Licencja ADRA NDR dla QGD 1 rok

LS-ADRANDR-GL-1Y to roczna licencja służąca do aktywacji zaawansowanych funkcjonalności dla usługi ADRA NDR w przełącznikach PoE z funkcjami NDR, na potrzeby szybkiego wykrywania zagrożeń ze strony ukierunkowanego oprogramowania typu ransomware i innych, a także wczesnego ostrzegania przed nimi.

Cechy wyjątkowe **ADRA NDR**:

- Bez konieczności instalowania drogiego oprogramowania EDR dla każdego urządzenia końcowego — wystarczy przełącznik z ADRA NDR do wczesnego wykrywania potencjalnych zagrożeń na wszystkich urządzeniach końcowych.
- Po wychwyceniu podejrzanych działań przez funkcję Wykrywanie zagrożeń, Dogłębna analiza zagrożenia i Analiza korelacji zagrożenia określą typ ataku i ocenią związane z nim poziomy ryzyka.
- Automatycznie izolowane są tylko urządzenia objęte atakiem, co pomaga w powstrzymywaniu ataków złośliwego oprogramowania bez konieczności wyłączania całej sieci.
- Wdrożenie i obsługa oprogramowania ADRA NDR nie ma wpływu na wydajność sieci i istniejącą infrastrukturę.
- ADRA NDR zapewnia pulpit nawigacyjny oraz łatwy w obsłudze graficzny interfejs użytkownika do zarządzania, który pomaga pracownikom IT w szybkim wykrywaniu i analizowaniu potencjalnych zagrożeń.

Kompatybilne modele:

---

Podstawowe funkcje **przełącznika QNAP** dla rozwiązań biznesowych:

**Współczesne wyzwania IT: Ukryte ruchy poprzeczne są trudne do wykrycia**

W obliczu potencjalnych zagrożeń wokół nas, poleganie wyłącznie na sieciowych urządzeniach firewall (perymetrycznych) na obrzeżach sieci lokalnej nie zapewnia już wystarczającego bezpieczeństwa. Ochrona przed poprzecznym przemieszczaniem się złośliwego oprogramowania jest aktualnie bardzo ważna, ponieważ ukierunkowane oprogramowanie ransomware często występuje w sieci po cichu, zbierając cenne informacje i znajdując luki w infrastrukturze IT. Gdy ostatecznie się ujawni, działalność firmy zostanie zagrożona, ponieważ spowoduje to

nie tylko zaszyfrowanie danych, ale również znaczny czas i koszty związane z przywróceniem infrastruktury informatycznej i reputacji firmy.

**Szybko skanujące urządzenia ADRA NDR do ochrony przed zagrożeniami cybernetycznymi już są dostępne**

**QGD-1600P/1602P**, urządzenie do ochrony cybernetycznej, zapewnia rozwiązanie do wykrywania i reagowania w sieci (NDR), które precyzyjnie lokalizuje aktywność złośliwego oprogramowania w sieci lokalnej bez wpływu na wydajność. Zastosowany w urządzeniu **QGD-1600P/1602P** opatentowany mechanizm szybkiego skanowania wykrywa potencjalnie złośliwe działania na podstawie zestawu kryteriów i reaguje na te anomalie zgodnie ze zdefiniowanymi zasadami. Pozwala to znacznie zwiększyć bezpieczeństwo sieci bez wpływu na jej wydajność.

**Ochrona przed zagrożeniami za pomocą łatwego w obsłudze graficznego interfejsu użytkownika**

Oprogramowanie ADRA NDR oferuje przeglądowy pulpit nawigacyjny oraz łatwy w obsłudze graficzny interfejs użytkownika, który pomaga pracownikom IT skutecznie wykrywać i analizować zagrożenia sieciowe.

**Możliwość wdrażania rozwiązania ADRA NDR w zakładach i biurach**

Urządzenie **QGD-1600P/1602P ADRA NDR** jest przeznaczone do zastąpienia istniejących przełączników dostępowych, które są bezpośrednio podłączone do urządzeń końcowych, takich jak komputery, drukarki, kamery IP i inne podłączone urządzenia. Ta metoda wdrażania może skutecznie zmaksymalizować zakres ochrony zapewniany przez urządzenie do ochrony cybernetycznej. Po podłączeniu urządzenie **QGD-1600P/1602P** skanuje w poszukiwaniu anomalii do i z urządzeń końcowych i reaguje na wykryte nieprawidłowości.

**Możesz wyprzedzić działania cyberprzestępców w całym systemie**

Możliwość wdrożenia urządzenia do ochrony cybernetycznej QGD-1600P/1602P dla urządzeń o strategicznym znaczeniu, takich jak NAS. Aby uzyskać maksymalne zabezpieczenie przed większością typów zagrożeń, zaleca się instalację wielu **QGD-1600P/1602P** dla wszystkich urządzeń na poziomie przełącznika dostępu w celu szybkiego wykrycia złośliwego oprogramowania, takiego jak ukierunkowane oprogramowanie ransomware.