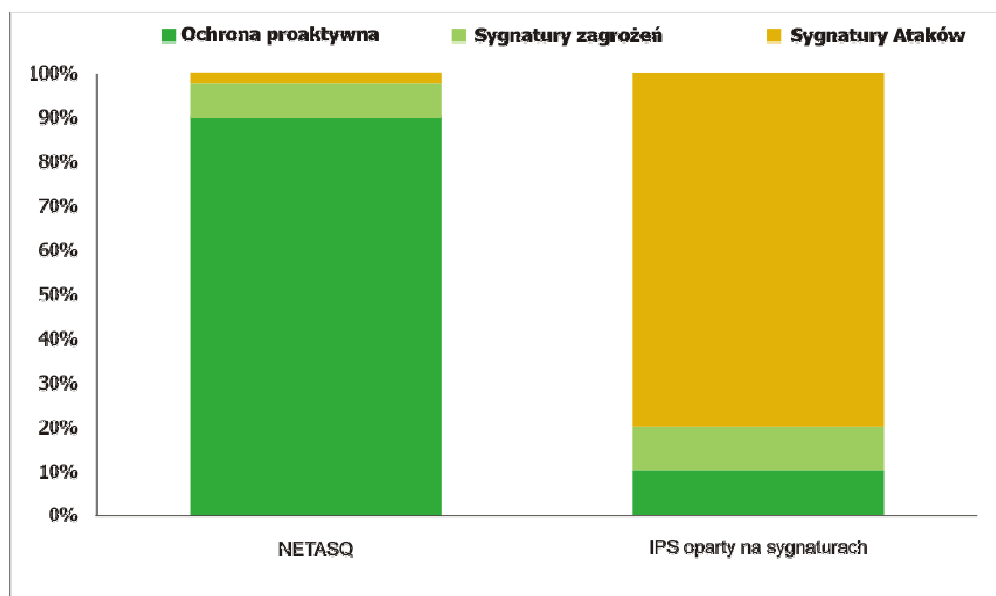


RÓŻNICE MIĘDZY TRADYCYJNYMI SYGNATURAMI A SYGNATURAMI KONTEKSTOWYMI

Podczas gdy w innych rozwiązaniach dla każdego nowego wariantu ataku potrzebna jest nowa sygnatura, ochrona pro aktywna NETASQ jest w stanie zapewnić ochronę niezależnie od szybkości reakcji administratora stanowiąc prawdziwą ochronę dnia zerowego. Dzięki temu NETASQ jest w stanie zablokować atak szybciej niż w innych przypadkach producent opublikuje odpowiednią aktualizację sygnatur. Wykres poniżej prezentuje przybliżony rozkład liczby ataków w zależności od kategorii analizy, której podlegają.

Ochrona NETASQ z większością zagrożeń radzi sobie przy wykorzystaniu analizy proaktywnej



Oznacza to, że większość nowych ataków jest rozpoznawana i blokowana bez konieczności tworzenia kolejnej sygnatury co znacznie poprawia wydajność pracy systemu IPS.

Sygnatury kontekstowe NETASQ to wysoko rozbudowane wersje tradycyjnych sygnatur:

- ✓ Większość sygnatur to sygnatury ochrony dnia zerowego. Jeden zbiór takich sygnatur, np. wzorec ataku typu SQL Injection, **zastępuje tysiące tradycyjnych sygnatur ataków.**
- ✓ Ponad 30 różnych baz danych użytych w kontekście konkretnego protokołu zdecydowanie zmniejsza liczbę sygnatur wykorzystywanych każdorazowo. Co ma znaczny wpływ na szybkość analizy ruchu w czasie rzeczywistym.

- ✓ Dzięki szerokiemu zakresowi analizowanych protokołów zaledwie kilka zbiorów danych jest porównywanych z dedykowaną bazą sygnatur.
- ✓ Każda baza sygnatur jest opracowywana przy użyciu algorytmu DAWG, który dzięki zastosowaniu analizy statystycznej znacznie poprawia szybkość jej przeszukiwania.
Wydajność skanowania nie jest bezpośrednio powiązana z liczbą sygnatur w bazie.

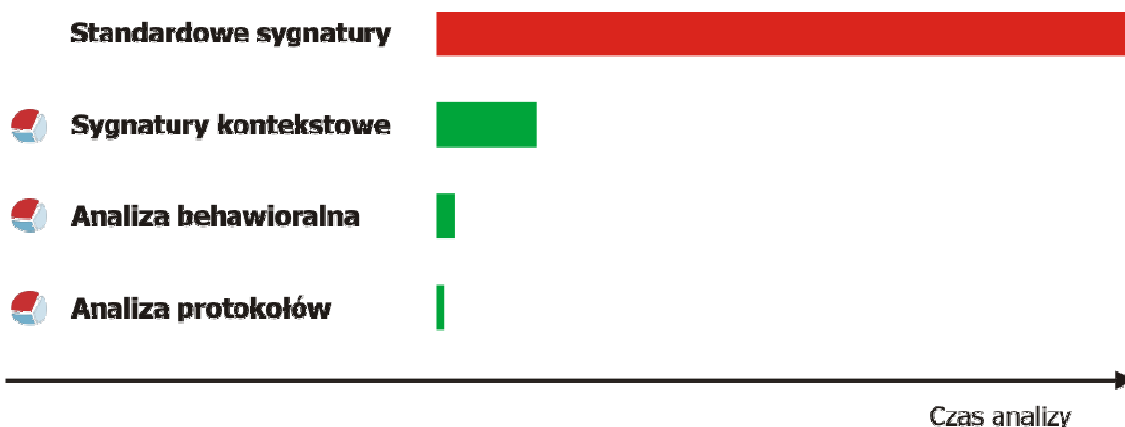
Silnik IPS firmy NETASQ jest integralną częścią systemu operacyjnego NETASQ Secured BSD - NGFW/UTM (Next Generation Firewall/Unified Threat Management). Silnik IPS analizuje i monitoruje połączenia TCP/IP. Zapobiega przechwyceniu ruchu i potrafi blokować próby odgadnięcia numeru sekwencyjnego pakietu TCP. Posiada wbudowaną ochronę przed atakami DoS w trakcie składania pakietów do pierwotnej postaci.

Poniżej znajduje się krótka lista form ochrony dnia zerowego zapewnianych przez silnik ASQ:

Ochrona dnia zerowego	Ochrona przed atakami Dos i DDOS
✓ Zapobieganie SQL injection	✓ Inteligentne zarządzanie połączeniem
✓ Wykrywanie i blokowanie ukrytych kanałów ICMP	✓ Konfigurowalne czyszczenie tablicy sesji, dostosowujące się automatycznie do nasilenia ruchu
✓ Zapobieganie XSS (cross-site scripting)	✓ Ochrona przed atakami polegającymi na ponownym składaniu fragmentów (rose attack)
✓ Wykrywanie i blokowanie mediów strumieniowych	✓ Zalewanie pakietami – flooding (ICMP/TCP/UDP)
✓ Ochrona połączeń VoIP	✓ Ataki oparte na niewielkich fragmentach IP / MTU
✓ Różne formy ochrony przed atakami typu Buffer Overflow	✓ Inne formy ataków DoS

NETASQ stale dodaje nowe formy ochrony by zapewnić najlepszą ochronę dnia zerowego.

Pod względem wydajności pracy technologie NETASQ IPS mogą pochwalić się dużo lepszymi wynikami.



W przypadku rozwiązań IPS opierających się jedynie na sygnaturach potrzebna jest nowa sygnatura dla każdego kolejnego zagrożenia. Połączenie technologii oferowane przez NETASQ sprawia, że liczba wzorców ataków jest nieistotna, gdyż większość form ochrony oferowanych przez NETASQ bazuje na analizie protokołu w warstwie jądra systemu operacyjnego.

Dla przykładu jedna sygnatura kontekstowa ochrony dnia zerowego firmy NETASQ przeciwko tzw. SQL injections odpowiada 1540 sygnaturom ataków.

Każdy zbiór sygnatur kontekstowych NETASQ może chronić przed setkami a nawet tysiącami zagrożeń. W przypadku systemu IPS opartego wyłącznie na sygnaturach ochrona taka wymagałaby odrębnej sygnatury dla każdego zagrożenia. Dzięki połączeniu różnych rodzajów analizy silnik IPS firmy NETASQ zapewnia pełną ochronę przed tysiącami zagrożeń już znanych jak i zagrożeniami, które dopiero się pojawiają.