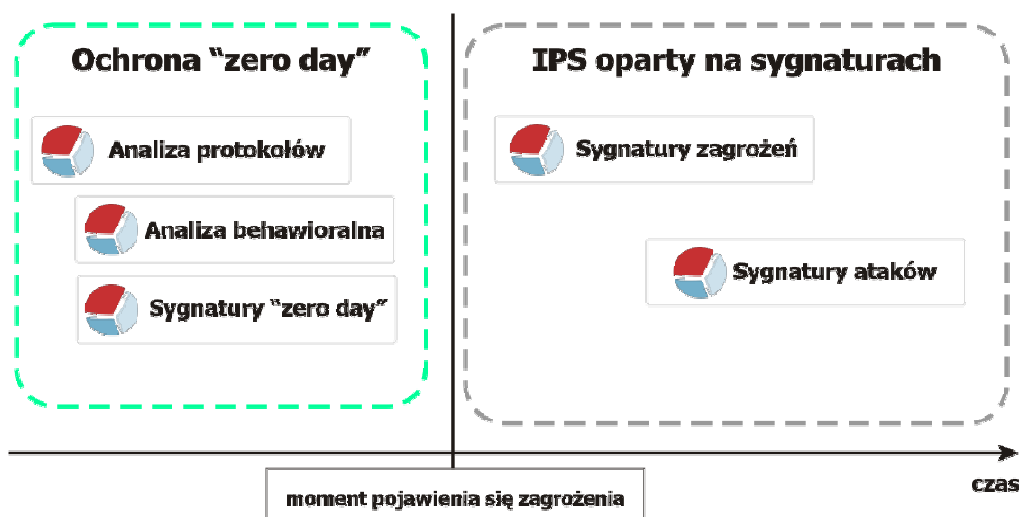


OCHRONA PROAKTYWNA W IPS NETASQ

NETASQ oferuje kompletną ochronę „dnia zerowego”, czyli ochronę nie tylko przed znanymi zagrożeniami, ale przede wszystkim przed tymi, które jeszcze nie zostały sklasyfikowane i na które jeszcze nie ma sygnatur. Intrusion Prevention System o nazwie ASQ to unikalna technologia oferująca wszystkie funkcje bezpieczeństwa przy zachowaniu wysokiej wydajności dzięki analizie pakietów na poziomie jądra systemu operacyjnego o nazwie NS-BSD (NETASQ Secured BSD). Oprócz tradycyjnego firewalla i bazy sygnatur ataków, ruch na styku sieci jest skanowany przy zastosowaniu czterech uzupełniających się analiz:

- ✓ **Analiza protokołu**, która łączy inspekcję protokołu, wielokrotne skanowanie oraz badanie zgodności (normalizacja) w odniesieniu do standardów RFC.
- ✓ **Analiza behawioralna**: wykrywanie nietypowego zachowania, takiego jak skanowanie portów, flooding, Denial of Service itp.
- ✓ **Sygnatury kontekstowe**: ponad 30 baz sygnatur stanowiących zbiór reguł wykrywających ataki związane z konkretnym zidentyfikowanym protokołem
- ✓ **Wzorce wrażliwości aplikacji**: te sygnatury opierają się na skanowaniu w czasie rzeczywistym ruchu przechodzącego przez ASQ analizując go pod kątem podatności aplikacji na ataki i zagrożenia z zewnątrz sieci.

Wykres poniżej pokazuje, architekturę systemu IPS ASQ zapewniającą realną ochronę proaktywną oraz architekturę systemu IPS, która jest zależna od szybkości reakcji administratora i szybkości wydania aktualizacji sygnatur ataków producenta rozwiązania.



Takie połączenie metod analizy skutecznie zastępuje tysiące tradycyjnych sygnatur ataków.