FortiSIEM®

Zunifikowana korelacja zdarzeń i zarządzania ryzykiem dla nowoczesnych sieci

Bezpieczeństwo nie polega już tylko na ochronie informacji. Jest krytycznym czynnikiem utrzymania zaufania klientów i zabezpieczenia marki oraz reputacji organizacji.

Łatwe wprowadzenie zabezpieczeń i zgodności z przepisami

Przypadki naruszenia bezpieczeństwa mogą osłabić reputację przedsiębiorstwa i mieć istotny, negatywny wpływ na jego przychody. Zdobycie nowego klienta kosztuje nawet siedem razy więcej niżutrzymanie istniejącego. Do tego mogą pojawić się kary finansowe i prawne. W wypadku spółek publicznych może to oznaczać utrzymujące się osłabienie wartości ich akcji, a także pogorszenie relacji z dostawcami i akcjonariuszami. Na podstawie wszystkich tych czynników wiadomo, dlaczego coraz więcej zarządów podejmuje decyzje związane z bezpieczeństwem.

FortiSIEM jest kompleksowym skalowanym i holistycznym rozwiązaniem, począwszy od IoT do chmury, wyposażonym w opatentowane funkcje analityczne, dzięki którym można zarządzać bezpieczeństwem, wydajnością i zgodnością sieci z przepisami. Wszystkie te funkcje są dostępne w jednym widoku konsoli organizacji.

Zunifikowane funkcje analityczne NOC i SOC (opatentowane)

W firmie Fortinet opracowano architekturę, która umożliwia zunifikowane i skorelowane analizowanie danych pochodzących z różnych źródeł, jak np. dzienniki, metryki wydajności, SNMP Traps, alarmy bezpieczeństwa i zmiany konfiguracyjne. System FortSIEM przejmuje funkcje analityczne monitorowane tradycyjnie w oddzielnych magazynach — SOC i NOC — i łączy te dane w celu uzyskania bardziej holistycznego widoku danych zagrożenia dostępnych w organizacji. Każda część informacji jest zamieniana na zdarzenie, które jest najpierw analizowane, a następnie przekazywane do silnika opartego na zdarzeniach do obsługi wyszukiwania w czasie rzeczywistym, reguł, konsoli i zapytań ad-hoc.

Podstawowe informacje

- Zunifikowana analityka sieci w czasie rzeczywistym
- Jeden widok informatyczny
- Obsługa wielu profili użytkowników
- Gotowość do obsługi MSP/MSSP
- Korelacja krzyżowa funkcji analitycznych NOC i SOC
- Spis zasobów z funkcją automatycznego uczenia
- Architektura chmury
- Gotowe funkcje bezpieczeństwa i zgodności z przepisami

PODSTAWOWE INFORMACJE

Dane z zewnętrznych systemów analizy zagrożeń (Threat Intelligence, TI) pochodzące z ze źródeł otwartych (open source), komercyjnych i systemów klientów można łatwo zintegrować w środowisku Threat Intelligence systemu FortSIEM. Taka unifikacja różnorodnych źródeł danych pozwala na szybkie tworzenie kompleksowych konsol i raportów w celu błyskawicznego identyfikowania głównych przyczyn zagrożeń i podejmowania czynności naprawczych i ograniczania ryzyka.

Korelacja zdarzeń rozproszonych w czasie rzeczywistym (opatentowana)

Korelacja zdarzeń rozproszonych jest poważnym problemem, ponieważ wiele węzłów sieci musi udostępniać częściowo swój stan w czasie rzeczywistym w celu wyzwolenia reguły. Choć wielu dostawców systemów SIEM oferuje funkcje gromadzenia danych rozproszonych i wyszukiwania rozproszonego, firma Fortinet jako jedyna oferuje silnik korelacji zdarzeń rozproszonych czasu rzeczywistego. Złożone wzorce zdarzeń można wykrywać na bieżąco z niewielkim opóźnieniem. Dzięki temu opatentowanemu algorytmowi system FortSIEM obsługuje wiele reguł w czasie rzeczywistym przy dużym natężeniu zdarzeń w celu rozszerzenia ram czasowych wykrywania.

Automatyczne wykrywanie infrastruktury w czasie rzeczywistym i silnik wykrywania aplikacji (CMDB)

Do szybkiego rozwiązywania problemów potrzeba kontekstu infrastruktury. Większość dostawców funkcji analizy dzienników i systemów SIEM wymaga, aby administrator wprowadzał kontekst ręcznie. W ten sposób podawane dane szybko tracą ważność i są podatne na ludzkie błędy. W firmie Fortinet opracowano inteligentny silnik, który umożliwia proste wykrywanie i odwzorowanie topologii infrastruktury zarówno fizycznej, jak i wirtualnej, znajdującej się fizycznie u klienta i w chmurze publicznej/prywatnej na podstawie danych uwierzytelniających, bez uprzedniej wiedzy na temat występowania urządzeń czy aplikacji.
Wykrywanie jest zarówno szerokie (obejmuje duża liczbę dostawców poziomu 1/2/3), jak i głębokie (obejmuje system, sprzęt, oprogramowanie, uruchomione usługi, aplikacje, pamięci masowe, użytkowników, konfigurację sieci, topologię i relacje między urządzeniami). Wykrywanie można uruchomić na żądanie lub w sposób zaplanowany w celu odkrywania (w czasie rzeczywistym) zmian infrastruktury i zgłaszanie nowo wykrytych urządzeń i aplikacji. Jest to istotna część funkcji zarządzania zgodnością z przepisami, którą system FortSIEM spełnia w sposób unikatowy. Aktualna centralna baza danych zarządzania (Centralized Management Database, CMDB) umożliwia zaawansowane analizowanie zdarzeń z uwzględnieniem kontekstu przy użyciu obiektów CMDB w warunkach wyszukiwania.

Dynamiczne odwzorowanie tożsamości użytkowników

Krytycznym kontekstem do analizy dzienników jest połączenie tożsamości sieciowej (adres IP, adres MAC) z tożsamością użytkownika (nazwa użytkownika, pełna nazwa, rola w organizacji). Te informacje podlegają ciągłym zmianom, ponieważ użytkownicy uzyskują nowe adresu przez usługę DHCP lub VPN.
W firmie Fortinet opracowano metodę dynamicznego odwzorowania tożsamości użytkowników. W pierwszej kolejności wykrywa się użytkowników i ich role z repozytoriów klienta, jak np. Microsoft Active Directory i Open LDAP lub z repozytoriów jednokrotnego logowania (SSO) w chmurze, jak np. OKTA. Wykrywanie nowych użytkowników można uruchomić na żądanie lub w sposób zaplanowany.
Jednocześnie identyfikuje się tożsamość sieciową na podstawie ważnych zdarzeń sieciowych, jak np. zdarzenia translacji sieciowej zapory firewall, logowania do usługi Active Directory, logowania do sieci VPN, WLAN, dzienniki rejestracji agenta hosta itd. Po połączeniu tożsamości użytkowników, tożsamości sieciowej i danych geograficznych w rozproszonej bazie danych czasu rzeczywistego umiejscowionej w pamięci system FortSIEM może utworzyć dziennik audytu dynamicznej tożsamości użytkownika. Umożliwia to tworzenie strategii lub badanie na podstawie tożsamości użytkownika zamiast adresów IP, co pozwala z kolei na błyskawiczne rozwiązywanie problemów.

Elastyczne i szybkie środowisko analizowania dziennika klienta (opatentowane)

Skuteczne analizowanie dzienników wymaga zastosowania niestandardowych skryptów, te są z kolei wolne, zwłaszcza w wypadku dzienników o dużej pojemności jak np. Active Directory, dzienniki zapory firewall itd. Kod skompilowany jest z kolei szybszy, ale nie jest na tyle elastyczny, ponieważ wymaga przygotowania kolejnych wersji. W firmie Fortinet opracowano język analizy zdarzeń oparty na XML o funkcjonalności zbliżonej do języków programowania wysokiego poziomu, i jednocześnie łatwy do modyfikowania; w celu zapewnienia wysokiej skuteczności można go kompilować w trakcie pracy. Wszystkie analizatory składni FortiSIEM przewyższają parametrami większość ofert konkurencji dzięki zastosowaniu tego opatentowanego rozwiązania i pozwalają na analizę ponad 10k zdarzeń/s na węzeł.

Hybrydowa architektura bazy danych — wykorzystanie strukturalnych i niestrukturalnych danych wejściowych

System FortiSIEM wykorzystuje dwa różne źródła informacji — dane wykryte są danymi strukturalnymi przeznaczonymi dla tradycyjnej, relacyjnej bazy danych, a dzienniki, metryki wydajności itp. są danymi niestrukturalnymi, które wymagają bazy danych innej niż SQL. W firmie Fortinet opracowano hybrydowe podejście, w którym dane są przechowywane w optymalizowanych bazach danych o unikatowej logice warstwy biznesowej, zapewniając kompleksową, pojedynczą warstwę abstrakcji bazy danych.
Użytkownik może wyszukiwać zdarzenia (przechowywane w bazie danych innej niż SQL) przy użyciu obiektów CMDB (przechowywanych w relacyjnej bazie danych). Takie podejście pozwala na wykorzystanie mocy i zalet obu baz danych.

PODSTAWOWE INFORMACJE

Integracja danych dotyczących zagrożeń na dużą skalę

Klienci mogą subskrybować wiele źródeł zewnętrznych danych dotyczących zagrożeń służących do zarządzania potencjalnymi zagrożeniami w sieci. Dane dotyczące zagrożeń mogą być bardzo obszerne, zawierając często miliony adresów IP, domen złośliwego oprogramowania, znaczników hash i adresów URL, a te wszystkie informacje szybko tracą ważność, ponieważ witryny i domeny złośliwego oprogramowania są szybko zamykane i otwierane od nowa. Jest to poważne wyzwanie dotyczące mocy obliczeniowej użytkowników danych dotyczących zagrożeń. W firmie Fortinet opracowano własne algorytmy. które umożliwiają szybkie pozyskiwanie tak dużej ilości informacji ze źródła, a następnie skuteczne jej rozproszenie między węzłami FortiSIEM i oszacowanie w czasie rzeczywistym z szybkością wyższą niż u konkurencji (ponad 10k zdarzeń/s na węzeł).

Gotowość obsługi dużych przedsiębiorstw i dostawców usług zarządzanych — architektura wielu użytkowników

W firmie Fortinet opracowano dostosowywaną architekturę wielu profili użytkowników, dzięki której przedsiębiorstwa i dostawcy usług mogą zarządzać wieloma domenami fizycznymi/logicznymi i nakładającymi się systemami z poziomu jednej konsoli. W takim środowisku można bardzo łatwo skorelować informacje między domenami fizycznymi i logicznymi, a także poszczególnymi sieciami klienta. Dla każdej z nich można łatwo tworzyć unikatowe raporty, reguły i konsole, przy jednoczesnej możliwości wdrażania ich w szerokiej gamie raportowanych domen i klientów. Dla poszczególnych domen lub klientów można wdrożyć strategie archiwizowania zdarzeń.

FUNKCJE

Kontekst operacyjny w czasie rzeczywistym do szybkiej analizy bezpieczeństwa

- Stale aktualizowany i dokładny kontekst urządzenia — konfiguracja, zainstalowane oprogramowanie i poprawki, uruchomione usługi
- Analiza wydajności systemu i oprogramowania na podstawie kontekstowych danych relacji wewnętrznych do szybkiego segregowania problemów związanych z bezpieczeństwem
- Kontekst użytkownika, w czasie rzeczywistym, wraz z dziennikami audytu z adresami IP, zmianami tożsamości użytkownika, kontekst danych lokalizacji fizycznej i geograficznej
- Wykrywanie nieautoryzowanych urządzeń sieciowych i aplikacji, zmian konfiguracji

Gotowe raporty zgodności z przepisami

- Gotowe, wstępnie zdefiniowane raporty do obsługi wymogów związanych z audytem i zarządzaniem zgodnością z przepisami — PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls

Monitorowanie wydajności

- Monitorowanie podstawowych/często używanych metryk systemu
- Poziom systemu poprzez SNMP, WMI, PowerShell
- Poziom aplikacji poprzez JMX, WMI, PowerShell
- Monitorowanie wirtualizacji dla VMware, HyperV — poziom gościa, hosta, puli zasobów i klastra
- Monitorowanie wykorzystania pamięci masowej, wydajności — EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain
- Specjalizowane monitorowanie wydajności aplikacji
- Microsoft Active Directory i Exchange przez WMI i Powershell
- Bazy danych — Oracle, MS SQL, MySQL przez JDBC
- Infrastruktura VoIP przez IPSLA, SNMP, CDR/CMR
- Analiza przepływu i wydajności aplikacji — Netflow, SFlow, Cisco AVC, NBAR
- Możliwość dodawania metryk klienta
- Metryki podstawowe i wykrywanie znaczących odchyłek

Monitorowanie zmian konfiguracji w czasie rzeczywistym

- Gromadzenie plików konfiguracji sieci, przechowywanych w repozytorium ze śledzeniem wersji
- Gromadzenie zainstalowanych wersji oprogramowania, przechowywanych w repozytorium ze śledzeniem wersji
- Automatyczne wykrywanie zmian w konfiguracji sieci i zainstalowanym oprogramowaniu
- Automatyczne wykrywanie zmian plików/folderów — system Windows i Linux — dane szczegółowe kto i co
- Automatyczne wykrywanie zmian względem zatwierdzonego pliku konfiguracji
- Automatyczne wykrywanie zmian w rejestrze systemu Windows przez agenta FortiSIEM dla systemu Windows

FUNKCJE

Kontekst urządzenia i aplikacji

- Urządzenia sieciowe, w tym przełączniki, routery, urządzenia bezprzewodowej sieci LAN
- Urządzenia zabezpieczające — zapory sieciowe firewall, IPS sieciowe, bramy WWW/email, ochrona przed złośliwym oprogramowaniem, skanery słabych punktów sieci
- Serwery, jak np. Windows, Linux, AIX, HP UX
- Usługi infrastruktury, jak np. DNS, DHCP, DFS, AAA, kontrolery domen, VoIP
- Aplikacje mające styczność z użytkownikami, jak np. serwery WWW, serwery aplikacji, email, bazy danych
- Urządzenia pamięci masowej, jak np. NetApp, EMC, Isilon, Data Domain
- Aplikacje chmurowe, jak np. AWS, Box.com, Okta, Sales-force.com
- Infrastruktura chmury, jak np. AWS
- Urządzenia środowiskowe, jak np. UPS, klimatyzacje, osprzęt urządzeń
- Infrastruktura wirtualizacji, jak np. VMware ESX, Microsoft HyperVScalable i elastyczne gromadzenie dzienników

Skalowane i elastyczne gromadzenie dzienników

- Dzienniki bezpieczeństwa gromadzenia, analizowania, normalizac-ji, indeksowania i przechowywania w każdym punkcie (ponad 10k zdarzeń/s na węzeł)
- Gotowa obsługa szerokiej gamy interfejsów API systemów bezpieczeństwa i dostawców — zarówno fizycznych, jak i chmurowych
- Agenci systemu Windows zapewniają skalowane i wydajne gromadzenie zdarzeń, łącznie z monitorowaniem integralności plików, zmian w zainstalowanym oprogramowaniu i zmian w rejestrze systemu
- Agenci systemu Linux do monitorowania integralności plików
- Modyfikowanie analizatorów składni z poziomu graficznego interfejsu użytkownika i ponowne wdrożenie w działającym systemie, bez przestoju i utraty zdarzeń
- Tworzenie nowych analizatorów składni (szablonów XML) w zintegrowanym środowisku do tworzenia analizatorów, udostępnianie użytkownikom przy użyciu funkcji importu/eksportu
- Bezpieczne i niezawodne gromadzenie zdarzeń od użytkowników i urządzeń znajdujących się w dowolnym miejscu

Zarządzanie powiadomieniami i incydentami

- Środowisko powiadomień o incydentach na podstawie reguł
- Możliwość wyzwalania skryptu naprawczego po wystąpieniu określonego incydentu
- Integracja API z zewnętrznymi systemami obsługi kart problemów — ServiceNow, ConnectWise i Remedy
- Wbudowany system obsługi kart problemów

Rozbudowane i konfigurowane konsole

- Konfigurowane konsole czasu rzeczywistego, wraz z prezentacją mierników KPI
- Raporty z możliwością udostępniania i analiza między organizacjami i użytkownikami
- Kolory pomagają w identyfikowaniu krytycznych problemów
- Szybkość — aktualizacja na podstawie obliczeń w pamięci
- Specjalizowane, warstwowe konsole do obsługi usług biznesowych, wirtualizowanej infrastruktury i specjalizowanych aplikacji

Integracja z zewnętrznymi systemami obsługi zagrożeń

- Interfejsy API do integracji z zewnętrznymi systemami obsługi zagrożeń — domenami złośliwego oprogramowania, adresów IP, URL, znaczników hash, węzłów sieci Tor
- Wbudowana integracja popularnych inteligentnych źródeł zagrożeń — ThreatStream, CyberArk, SANS, Zeus
- Technologia obsługi dużych zbiorów danych dotyczących zagrożeń — przyrostowe pobieranie i udostępnianie w klastrze, dopasowywanie wzorca w czasie rzeczywistym do ruchu sieciowego

Wydajna i skalowana analiza

- Wyszukiwanie zdarzeń na bieżąco — bez konieczności indeksowania
- Wyszukiwanie z klawiatury i wyszukiwanie na podstawie analizowanych atrybutów zdarzenia
- Wyszukiwanie zdarzeń historycznych — zapytania podobne do SQL z logicznymi warunkami filtrowania, grupowanie według właściwych agregacji, filtry na dzień, dopasowania do wyrażeń regularnych, obliczone wyrażenia — interfejs graficzny i API
- Wyzwalanie na podstawie złożonych wzorców zdarzeń w czasie rzeczywistym
- Użycie wykrytych obiektów CMDB i użytkowników/tożsamości oraz danych lokalizacji w wyszukiwaniu i regułach
- Planowanie harmonogramu raportów i dostarczanie wyników w wiadomości email do osób odpowiedzialnych
- Wyszukiwanie zdarzeń w całej organizacji lub do poziomu fizycznej lub logicznej domeny raportowanej
- Dynamiczne listy obserwacji w celu śledzenia krytycznych użytkowników naruszających — z możliwością użycia listy śledzenia w każdej regule raportowania
- Skalowanie zbiorów danych analizy poprzez dodanie węzłów roboczych (Worker) bez przestoju
- Priorytetowanie raportowania incydentów można wdrożyć poprzez krytyczną usługę biznesową

Ustalenie danych bazowych i statystyczne wykrywanie nieprawidłowości

- Podstawowe zachowanie punktu końcowego/serwera/użytkownika — rozdzielczość do godzin w ciągu dnia tygodnia roboczego/weekendu
- Wysoka elastyczność — można wyznaczyć dane podstawowe dla dowolnego zestawu kluczy i metryk
- Wbudowane i dostosowywane wyzwalanie na podstawie statystycznych nieprawidłowości

Integracja z zewnętrznymi systemami

- Integracja z dowolną witryną zewnętrzną w celu wyszukiwania adresów IP
- Integracja API z zewnętrznymi systemami analizy zagrożeń
- 2-kierunkowa integracja API z systemami pomocy technicznej — bezproblemowa, gotowa obsługa systemów ServiceNow, ConnectWise i Remedy
- 2-kierunkowa integracja API z zewnętrzną bazą CMDB — bezproblemowa, gotowa obsługa systemów ServiceNow i ConnectWise
- Obsługa Kafka w celu integracji z zaawansowanym rapor-towaniem analitycznym — tj. ELK, Tableau i Hadoop
- Interfejs API do integracji z systemami konfigurowania usług
- Interfejs API do dodawania organizacji, tworzenia danych uwierzytelniających, wykrywania wyzwolenia, modyfikowania zdarzeń monitorowania

FUNKCJE

Proste i elastyczne administrowanie

- Internetowy graficzny interfejs użytkownika
- Wydajna kontrola dostępu na podstawie ról w celu ograniczenia dostępu do interfejsu graficznego i danych na różnych poziomach
- Cała komunikacja wewnątrzmodułowa jest chroniona protokołem HTTPS
- Pełny dziennik audytu aktywności użytkowników systemu FortiSIEM
- Łatwe aktualizowanie oprogramowania przy minimalnym przestoju i utracie zdarzeń
- Łatwe aktualizowanie bazy wiedzy FortiSIEM (analizatory składni, reguły, raporty)
- Archiwizacja na podstawie reguł
- Mieszanie danych logowania w momencie weryfikacji niezaprzeczalności i integralności
- Elastyczne uwierzytelnianie użytkowników — lokalne, zewnętrzne poprzez Microsoft AD i OpenLDAP, chmurowe SSO/SAML poprzez Okta
- Możliwość zalogowania do serwera zdalnego poza maszyną „Collector" z poziomu graficznego interfejsu użytkownika FortiSIEM poprzez zdalny tunel SSH

Łatwo skalowana architektura wirtualna

- Dostępna jako maszyny wirtualne do wdrożenia fizycznego i w chmurze publicznej/prywatnej na następujących platformach „hypervisor" — VMware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure
- Skalowanie zbioru danych poprzez wdrożenie maszyn wirtualnych „Collector"
- Maszyny „Collector" mogą buforować zdarzenia, gdy nie jest dostępne połączenie z chmurą FortiSIEM
- Skalowanie analizy zbioru danych poprzez wdrożenie maszyn wirtualnych „Worker"
- Wbudowana architektura z rozkładem obciążenia do zbierania zdarzeń z lokalizacji zdalnych poprzez maszyny „Collector"

Centrum obsługi zagrożeń poprzez sygnalizowanie

- Instancje FortiSIEM wysyłają dane na temat stanu i zanonimizowane incydenty do chmury FortiSIEM
- Korelacja krzyżowa między wieloma instancjami FortiSIEM pozwala na identyfikację wyłaniających się trendów i rozwoju złośliwego oprogramowania

Monitorowanie dostępności

- Monitorowanie stanu roboczego systemu (włączony/wyłączony) — poprzez ping, SNMP, WMI, analizę czasu aktywności, interfejs krytyczny, proces i usługę krytyczną, zmianę stanu BGP/OSPF/EIGRP, włączenie/wyłączenie portu pamięci masowej
- Modelowanie dostępności usługi poprzez syntetyczne monitorowanie transakcji — ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, śledzenie trasy i dla zwykłych portów TCP/UDP
- Monitorowanie sprzętu i środowiska
- Kalendarz konserwacji do planowania okien czasowych konserwacji
- Obliczenie SLA — uwzględnienie normalnych godzin pracy i czasu po godzinach

SPECYFIKACJE

Agenci Windows FortiSIEM

W firmie Fortinet opracowano skuteczną technologię zbierania informacji bez pośrednictwa agentów. Niektóre informacje, jak np. dane monitorowania integralności plików, są zbyt drogie, by je zbierać zdalnie. System FortiSIEM łączy technologię bez użycia agentów z nowo opracowanymi wysokowydajnymi agentami w celu znaczącego wsparcia zbierania danych.

	TECHNOLOGIA BEZ UŻYCIA AGENTÓW	AGENT PODSTAWOWY	AGENT ZAAWANSOWANY
Bez użycia agentów			
Wykrywanie	•		
Monitorowanie wydajności	•		
System zbierania (o niskiej wydajności), dzienniki aplikacji i bezpieczeństwa	•		
Agenci			
System zbierania (o wysokiej wydajności), dzienniki aplikacji i bezpieczeństwa		•	•
Zbieranie dzienników DNS, DHCP, DFS, IIS		•	•
Do 1800 zdarzeń/sekundę/serwer bezstratnie, małe opóźnienie		•	•

	TECHNOLOGIA BEZ UŻYCIA AGENTÓW	AGENT PODSTAWOWY	AGENT ZAAWANSOWANY
Maks. 500 agentów na menedżera agentów		•	•
Lokalna analiza składni i normalizacja czasu		•	•
Wykrywanie zainstalowanego oprogramowania			•
Monitorowanie zmian z rejestrze			•
Monitorowanie integralności plików			•
Monitorowanie pliku dziennika klienta			•
Monitorowanie wyprowadzania poleceń WMI			•
Monitorowanie wyprowadzania poleceń PowerShell			•

INFORMACJE NA TEMAT ZAMAWIANIA

Schemat licencjonowania

Licencje FortiSIEM zapewniają podstawową funkcjonalność wykrywania urządzeń sieciowych. Do urządzeń zalicza się przełączniki, routery, zapory sieciowe firewall, serwery itd. Każde monitorowane urządzenie wymaga licencji. Każda licencja obsługuje zbieranie i korelowanie danych, ostrzeganie i alarmowanie, raporty, funkcje analityczne, wyszukiwanie i zoptymalizowane repozytorium danych, i obejmuje 10 zdarzeń na sekundę (EPS). „EPS" jest miarą wydajności, która definiuje liczbę komunikatów lub zdarzeń generowanych na sekundę przez każde urządzenie. W razie potrzeby można zamówić dodatkowe EPS. Licencje są dostępne w wersji „Subscription" (Subskrypcja) lub „Perpetual" (Bezterminowa).

PRODUKT	SKU	OPIS
FortiSIEM All-In-One		
FortiSIEM All-In-One Perpetual License	FSM-AIO-BASE	Podstawowa, bezterminowa licencja na usługi monitorowania i bezpieczeństwa „wszystko w jednym". Zarządzanie maks. 50 urządzeniami i 500 EPS
	FSM-AIO-XXXX-UG	Dodaje XXXX urządzeń i XXXX EPS do licencji bezterminowej
FortiSIEM All-In-One Subscription License	FSM-AIO-BASE-DD	Podstawowa licencja subskrypcyjna na usługi monitorowania i bezpieczeństwa „wszystko w jednym". Zarządzanie maks. 50 urządzeniami i 500 EPS
	FSM-AIO-XXXX-UG-DD	Dodaje XXXX urządzeń i XXXX EPS do licencji subskrypcyjnej
FortiCare Support for FortiSIEM All-In-One License	FC[1-8]-10-FSM00-248-02-DD	Umowa FortiCare 24x7 (YYYY urządzeń)
FortiSIEM Windows Agent		
FortiSIEM Perpetual License for Basic Windows Agent	FSM-WIN-BASE	Podstawowa licencja bezterminowa na 50 podstawowych agentów Windows
	FSM-WIN-XXXX-UG	Dodaje XXXX podstawowych agentów Windows do licencji bezterminowej
FortiSIEM Subscription License for Basic Windows Agent	FSM-WIN-BASE-DD	Podstawowa licencja subskrypcyjna na 50 podstawowych agentów Windows
	FSM-WIN-XXXX-UG-DD	Dodaje XXXX podstawowych agentów Windows do licencji subskrypcyjnej
FortiSIEM Perpetual License for Advanced Windows Agent	FSM-WIN-ADV-BASE	Podstawowa licencja bezterminowa na 50 zaawansowanych agentów Windows
	FSM-WIN-ADV-XXXX-UG	Dodaje XXXX zaawansowanych agentów Windows do licencji bezterminowej
FortiSIEM Subscription License for Advanced Windows Agent	FSM-WIN-ADV-BASE-DD	Podstawowa licencja subskrypcyjna na 50 zaawansowanych agentów Windows
	FSM-WIN-ADV-XXXX-UG-DD	Dodaje XXXX zaawansowanych agentów Windows do licencji subskrypcyjnej
FortiCare Support for FortiSIEM Windows Agent License	FC[1-8]-10-FSM01-248-02-DD	Umowa FortiCare 24x7 (YYYY urządzeń)

UPRAWNIENIA FORTISIEM ALL-IN-ONE	PODSTAWA	POZIOMY AKTUALIZACJI (XXXX)						
	Podstawa	**100**	**250**	**450**	**950**	**1950**	**3950**	**4950**
Liczba urządzeń	50	100	250	450	950	1,950	3,950	4.950
Liczba EPS	500	1,000	2,500	4,500	9,500	19,500	39,500	49,500

UPRAWNIENIA FORTISIEM WINDOWS AGENT	PODSTAWA	POZIOMY AKTUALIZACJI (XXXX)						
	Podstawa	**100**	**250**	**450**	**950**	**1950**	**3950**	**4950**
Liczba agentów Windows	50	100	250	450	950	1,950	3,950	4.950

UPRAWNIENIA FORTICARE	OPCJE							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Liczba urządzeń (YYYY)	1–50	1–150	1–300	1–500	1–1,00	1–2,000	1–4,000	1–5,000

CENTRALA
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
Stany Zjednoczone
Tel: +1.408.235.7700
www.fortinet.com/sales

BIURO HANDLOWE EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel: +33.4.8987.0500

BIURO HANDLOWE APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel: +65.6395.2788

BIURO HANDLOWE AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Stany Zjednoczone
Tel: +1.954.368.9990

FST-PROD-DS-FSIEM
FSIEM-DAT-R2-201701