

FortiAnalyzer

Scentralizowane logowanie, analizy i raportowanie

Lepszy przegląd sieci dzięki platformom FortiAnalyzer

Platformy FortiAnalyzer łączą funkcje logowania, analizowania i raportowania pracy sieci w postaci pojedynczego systemu, oferującego poszerzoną wiedzę na temat zdarzeń z zakresu bezpieczeństwa w sieci. Urządzenia te są w stanie zapewnić instytucjom każdej wielkości scentralizowaną analizę zdarzeń z zakresu bezpieczeństwa, badanie śladów działań niedozwolonych, raportowanie, archiwizację treści, eksplorację danych, kwarantannę zainfekowanych plików oraz ocenę podatności zasobów. Technologie scentralizowanego gromadzenia, korelacji i analizy geograficznie i czasowo zróżnicowanych danych z zakresu bezpieczeństwa, pochodzących z urządzeń Fortinet pozwalają stworzyć uproszczony, skonsolidowany widok stanu bezpieczeństwa instytucji.

Rodzina produktów FortiAnalyzer pozwala zminimalizować zakres prac wymaganych w celu monitorowania i utrzymywania wdrożonych polityk oraz identyfikowania wzorców ataków. Te z kolei mogą być następnie wykorzystane do dostrojenia polityk w celu ochrony przed takimi atakami w przyszłości. Dodatkowo platformy FortiAnalyzer oferują funkcje gromadzenia szczegółowych danych, które mogą być stosowane w czasie analizy śledczej, w celu kontroli zgodności z normami i strategiami w aspekcie naruszeń bezpieczeństwa z zakresu prywatności i ujawnienia informacji.

Zarządzanie informacjami o zdarzeniach z zakresu bezpieczeństwa

Wzbogacenie infrastruktury bezpieczeństwa o platformy FortiAnalyzer, oferujące pojedynczy widok zdarzeń z zakresu bezpieczeństwa, treści zarchiwizowanych i oceny podatności zasobów, pozwoli Państwu zaoszczędzić wiele czasu. Platformy FortiAnalyzer akceptują szeroki zakres danych urządzeń Fortinet, w tym dane dotyczące ruchu, zdarzeń, wirusów, ataków oraz filtrowania treści i wiadomości e-mail. Rozwiązanie eliminuje konieczność ręcznego przeszukiwania wielu plików dziennika lub analizowania kilku konsol podczas przeprowadzania analizy śledczej lub audytu sieci. Centralne funkcje archiwizacji danych, kwarantanny plików i oceny podatności zasobów oferowane przez platformę FortiAnalyzer dodatkowo skracają czas, jaki użytkownik musi poświęcić na zarządzanie procesami bezpieczeństwa w swoim przedsiębiorstwie lub organizacji.

Zarządzanie punktami wrażliwymi

Wraz z premierą wersji FortiAnalyzerOS 4.0 rozwiązania Fortinet oferują zaawansowane funkcje skanowania zasobów w sieci, wykorzystujące zbiór sygnatur dynamicznych do oceny podatności zasobów, i wskazania sposobów usunięcia słabych punktów.

Lista dodatkowych możliwości obejmuje wykrywanie urządzeń, mapowanie, definiowanie i priorytetyzację zasobów oraz spersonalizowane raportowanie. Opcjonalna subskrypcja Vulnerability Management zapewnia częste aktualizacje opracowywane przez FortiGuard Labs, zawierające aktualne dane ze skanowania punktów wrażliwych, co pozwala z wyprzedzeniem reagować na zagrożenia.



Zalety systemu FortiAnalyzer

Platforma FortiAnalyzer oferuje możliwość kompleksowego przeglądu zabezpieczeń wraz z funkcjami granularnych raportów graficznych. Dzięki szerokiej skali działania mechanizmu gromadzenia danych można wyeliminować punkty dotąd pomijane w profilu bezpieczeństwa. Wyjątkowe narzędzia analizy śledczej stwarzają możliwość wykrycia, przeanalizowania i złagodzenia zagrożeń, zanim nastąpi penetracja systemu albo kradzież lub utrata danych.

Narzędzie analizy śledczej systemu FortiAnalyzer oferuje szczegółowe raporty czynności użytkownika, zaś narzędzie oceny podatności zasobów automatycznie wykrywa, rejestruje i ocenia stan zabezpieczeń serwerów i hostów w obrębie infrastruktury sieciowej.

Funkcje

Korzyści

Korelacja zdarzeń sieciowych

Administratorzy mają możliwość szybszego identyfikowania i reagowania na zagrożenia bezpieczeństwa w skali całej sieci.

Optymalizowane raporty graficzne

Raportowanie zdarzeń, czynności i tendencji notowanych na platformach FortiGate® oraz sprzęcie producentów zewnętrznych w skali całej sieci.

Skalowalna moc i wydajność

Modele rodziny FortiAnalyzer obsługują tysiące agentów FortiGate oraz FortiClient™.

Scentralizowane rejestrowanie wielu typów rekordów

Rejestracja obejmuje ruch sieciowy, zdarzenia systemowe, ataki, wirusy, zdarzenia z zakresu filtrowania sieci WWW oraz czynności i dane z komunikatorów internetowych.

Płynna integracja z portfolio produktów Fortinet

Ścisła integracja maksymalizuje wydajność i umożliwia zarządzanie zasobami FortiAnalyzer z poziomu interfejsów użytkownika FortiGate lub FortiManager™.

Specyfikacja techniczna	100C	400B	1000C	2000B	4000B
Platforma dedykowana	tak	tak	tak	tak	tak
Liczba portów Ethernet 10/100/1000	2	4	4	6	2 (+2 1GbE SFP)
Liczba portów Ethernet 10/100	1	0	0	0	0
Liczba dysków twardej	1 x 1 TB	1 X 500 GB 1 X 500 GB (opcja)	1 X 1 TB 3 X 1 TB (opcja)	2 X 1 TB 4 X 1 TB (opcja)	6 X 1 TB 3 X 1 TB (opcja)
Maksymalna pojemność dysku twardego	1 TB	500 GB (1 TB maks.)	1 TB (4 TB maks.)	2 TB (6 TB maks.)	6 TB (24 TB maks.)
Kontroler RAID / Tryb	nie	nie (tak 0,1 z opcjonalnym dyskiem)	nie (tak 0,1,10 z opcjonalnym dyskiem)	tak (0,1,5,10,50)	tak (0,1,5, 6,10,50, 60)
Liczba logów (RAID 0)	912, 680, 550	912, 680, 550	3, 865, 470, 566	5, 798, 205, 850	16, 384, 000, 000
Redundatny zasilacz w trybie Hot Swap	nie	nie	nie	tak	tak
Wydajność systemu					
Wydajność logowania	do 200	do 500	do 1000	do 3000	do 6000
Przepływność otrzymywanych danych	800 Kbps	2 Mbps	4 Mbps	12 Mbps	24 Mbps
Liczba licencjonowanych urządzeń sieciowych	100	200	2000	2000	2000
Liczba urządzeń FortiClient	100	2000	bez ograniczeń	bez ograniczeń	bez ograniczeń
Wspierane modele FortiGate	wszystkie modele	wszystkie modele	wszystkie modele	wszystkie modele	wszystkie modele
Wymiary					
Wysokość	44 mm	43 mm	43 mm	86 mm	175 mm
Szerokość	380 mm	438 mm	434 mm	443 mm	485 mm
Długość	160 mm	368 mm	627 mm	681 mm	690 mm
Waga	1,8 kg	4,5 kg	15,9 kg	26,1 kg	43 kg
Montaż w szafach rackowych	tak	tak	tak	tak	tak
Środowisko pracy					
Wymagane zasilanie	100-240 V, 50-60 Hz, 1,5 A	100-240 V, 50-60 Hz, 4,0 A	100-240 V, 50-60 Hz, 7,0 A	100-240 V, 50-60 Hz, 8,0 A	100-240 V, 50-60 Hz, 5,5-11,5 A/s
Zużycie energii	56 W	83 W	189 W	152 W	420 W dla 6 dysków
Emisja ciepła	190,4 BTU	283 BTU	643,6 BTU	519 BTU	1434 BTU (6 dysków) 2035 BTU (12 dysków)
Temperatura pracy	0-40°C	0-40°C	0-35°C	0-40°C	0-40°C
Temperatura przechowywania	-25-70°C				
Wilgotność	5 - 95% bez kondensacji				
Zgodność					
FCC Class A PArt 15, UL/CUL, C Tick, CE, VCCI					

Raporty graficzne

Systemy FortiAnalyzer dają administratorowi sieci lub zabezpieczeń wiedzę niezbędną do ochrony sieci, podaną w postaci kompleksowego zbioru standardowych raportów graficznych, oraz możliwość całkowicie elastycznego dostosowywania raportów niestandardowych. Wiedza z zakresu sieci może być archiwizowana, filtrowana i eksplorowana w celu zapewnienia zgodności z normami lub w związku z analizami.

Granularność informacji

Interfejs użytkownika FortiAnalyzer umożliwia administratorom wgląd w dane dziennika bezpieczeństwa, oferując dostęp do takiego poziomu szczegółowości raportu, jaki będzie niezbędny, aby zrozumieć aktualny stan sieci. Widoki historyczne lub czasu rzeczywistego pozwalają administratorom przeanalizować dziennik i informacje o zawartości oraz ruch sieciowy.

Centrala światowa
Fortinet Incorporated
 1090 Kifer Road, Sunnyvale, CA 94086 USA
 Tel.: +1-408-235-7700
 Fax: +1-408-235-7737
www.fortinet.com/sales

Biuro sprzedaży na Europę,
Bliski Wschód i Afrykę - Francja
Fortinet Incorporated
 120 rue Albert Caquot, 06560, Sophia Antipolis, Francja
 Tel.: +33-4-8987-0510
 Fax: +33-4-8987-0501

Autoryzowany Dystrybutor Rozwiązań
Fortinet w Polsce - Veracomp S.A.
 ul. Zawila 61, 30-390 Kraków
 Tel.: +48-12-25-25-555
 Fax: +48-12-25-25-500
www.veracomp.pl/fortinet

Copyright© 2006-2009 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate® oraz FortiGuard® to zastrzeżone znaki towarowe firmy Fortinet, Inc. Inne nazwy Fortinet użyte w dokumencie mogą również stanowić znaki towarowe firmy Fortinet. Wszelkie pozostałe nazwy produktów lub firm mogą stanowić znaki towarowe należące do odpowiednich właścicieli. Wyniki pomiarów wydajności przytoczone w niniejszym dokumencie zostały uzyskane w wewnętrznych testach laboratoryjnych w warunkach idealnych. Zmienne sieciowe, różne środowiska sieciowe oraz inne warunki mogą wpłynąć na wyniki wydajności. Firma Fortinet wyłącza wszelkie gwarancje, wyrażone wprost lub domyślnie, z wyłączeniem przypadków, kiedy firma Fortinet zawiera wiążącą umowę z kupującym, która wyraźnie gwarantuje, że określony produkt będzie funkcjonował w zgodności z wynikami pomiarów wydajności podanych w niniejszym dokumencie. W celu wyjaśnienia wątpliwości wszelkie takie gwarancje są ograniczone do pracy w takich samych warunkach idealnych jak w momencie wewnętrznych testów laboratoryjnych w firmie Fortinet. Firma Fortinet w pełni wyłącza wszelkie inne gwarancje. Firma Fortinet zastrzega sobie prawo do zmiany, modyfikacji, przeniesienia lub innego przekształcenia niniejszej publikacji bez powiadomienia, a moc obowiązującą będzie posiadać ostatnia wersja publikacji. Wybrane produkty Fortinet są licencjonowane na mocy patentu amerykańskiego nr 5.623.600.

Zaawansowane narzędzia analizy śledczej służą administratorom do śledzenia działań użytkowników na poziomie przesyłanych treści.

Podgląd dzienników w czasie rzeczywistym

Możliwość monitorowania sieci, ruchu i zdarzeń użytkowników w czasie rzeczywistym lub przeglądania zapisów historycznych pod kątem konkretnych zdarzeń stanowi efektywne narzędzie wglądu w zagrożenia bezpieczeństwa oraz problematykę wydajności i zachowania użytkowników.

Obsługiwane urządzenia

- Systemy FortiGate Multi-Threat Security
- Systemy FortiMail Messaging Security
- Pakiet FortiClient Endpoint Security Suite
- System FortiManager Centralized Management
- Dowolne urządzenia kompatybilne z Syslog