Firemon

Zarządzanie złożonymi sieciami od chmury do lokalnych instalacji wymaga elastyczności i automatyzacji. Wraz z ewolucją biznesu, aby sprostać dzisiejszym wymaganiom, potrzebne są inteligentne rozwiązania. FireMon zapewnia pełną widoczność i kontrolę całego sieciowego środowisku IT, aby zautomatyzować zmiany zasad, zgodność i zminimalizować ryzyko związane z politykami. Od czasu stworzenia pierwszego w historii rozwiązania NSPM w 2004 roku, FireMon pomógł ponad 1700 klientom w prawie 70 krajach zabezpieczyć ich sieci. Oto narzędzia, których używamy do rozwiązywania problemów naszych klientów.

Czym jest Firemon?

FireMon dostarcza rozwiązania do zarządzania bezpieczeństwem, które umożliwiają organizacjom proaktywne działanie w obszarze monitorowanie zdarzeń w sieci i odpowiadanie reagowanie. Koncentrując się na zapewnieniu zaawansowanej widoczności, pomiarów, oceny i usprawnień procesów bezpieczeństwa, produkty FireMon pomagają wykrywać obszary podatności, słabe punkty oraz pomagają znaleźć właściwe rozwiązania w zakresie poprawy poziomu ochrony sieci przed próbami kompromitacji systemów bezpieczeństwa.

Problemy nowoczesnego przedsiębiorstwa

Wzrastająca złożoność sieci, wynikająca z ciągłego napływu usług chmurowych, nowych urządzeń i aplikacji, stanowi zniechęcające wyzwanie dla zarządzania politykami i zasadami zapór ogniowych. Typowe środowisko przedsiębiorstwa posiada miliony reguł, a jedna prosta pomyłka w konfiguracji może prowadzić do poważnych konsekwencji, takich jak naruszenia zgodności, przerwy w działaniu i wycieku danych.

Główne funkcje Firemon:

Kontrola polityk: Umożliwia definiowanie, zarządzanie i monitorowanie zasad bezpieczeństwa w infrastrukturze sieciowej.

Automatyzacja zmian: Pomaga w automatyzacji procesu wprowadzania zmian w politykach bezpieczeństwa, z minimalizacją ryzyka błędów.

Analiza ruchu w politykach: Zapewnia szczegółowe raporty dotyczące ruchu sieciowego, identyfikując potencjalne zagrożenia i anomalie.

Śledzenie wydajności: Monitoruje wydajność sieci oraz identyfikuje obszary wymagające optymalizacji.

Sprawdzanie zgodności: Przeprowadza skanowanie infrastruktury w celu sprawdzenia zgodności z politykami bezpieczeństwa i regulacjami.

Analiza ryzyka: Ocenia ryzyko związane z konfiguracją zabezpieczeń, identyfikując potencjalne luki w zabezpieczeniach.

Zarządzanie wieloma platformami: Integruje się z różnymi platformami i urządzeniami zabezpieczającymi w celu centralizacji zarządzania.

Generowanie raportów: Tworzy szczegółowe raporty dotyczące zdarzeń bezpieczeństwa oraz analizy skuteczności polityk.

Platforma FireMon składa się z kilku modułów funkcjonalnych:

Security Manager – System wspierający zarządzanie politykami bezpieczeństwa na urządzeniach bezpieczeństwa.

Policy Planner – Moduł wspierający zarzadzania politykami bezpieczeństwa poprzez planowanie polityk na urządzenia bezpieczeństwa

Policy Optimizer – Moduł wspierający zarządzanie politykami bezpieczeństwa poprzez optymalizację polityk bezpieczeństwa na urządzeniach bezpieczeństwa (recertyfikacja polityk bezpieczeństwa)

Risk Analyzer –Wsparcie analizy ryzyka związanej z infrastrukturą sieciową organizacji

Immediate Insight - System umożliwiający analizę zdarzeń, posiadający funkcjonalność BigData, w celu wsparcia analityki śledczej i przyspieszenia procesu reakcji na incydenty..

Global Policy Controller (GPC) - zapewnia połączenie potrzeb biznesowych w kontekście zasobów sieciowych i zapewnia automatyzację alokacji polityk bezpieczeństwa niezbędnych do prawidłowego dostępu za pomocą istniejącej infrastruktury

Dlaczego powinienem wybrać Firemon?

Sprawdzona wydajność w skali przedsiębiorstwa: FireMon Security Manager, Asset Manager i Cloud Defense zostały stworzone, aby sprostać potrzebom największych organizacji. Nasze rozwiązanie Security Manager NSPM zostało zaprojektowane specjalnie z myślą o złożoności polityk, z którymi borykają się przedsiębiorstwa, ze zweryfikowaną obsługą 15 000 urządzeń i ponad 25 milionami reguł. Asset Manager i Cloud Defense to oferty SaaS z niemal nieograniczonymi możliwościami rozbudowy, które mogą obsługiwać dowolne środowisko.

Funkcje zaprojektowane dla złożonych środowisk: Wszystkie rozwiązania FireMon zostały zaprojektowane tak, aby idealnie wpasować się w środowisko organizacji i oferować narzędzia, które ułatwiają zarządzanie. Wszystkie produkty oferują elastyczne, oparte na API i natywne integracje, które obsługują wiele różnych technologii bezpieczeństwa, w tym SIEM, SOAR, ITSM i skanery ryzyka.

Kompletne rozwiązanie: Nasze podejście oparte na wynikach zapewnia wszystko, czego potrzebujesz do realizacji zadań. Security Manager to jedyne rozwiązanie NSPM, które oferuje solidne zarządzanie ryzykiem, automatyzację zmian, przeglądy cyklu życia reguł i raportowanie zgodności w ramach jednej platformy, która obsługuje urządzenia w dowolnym miejscu w sieci, od środowisk lokalnych po chmurę. W połączeniu z Asset Manager i Cloud Defense, organizacje mogą włączyć wykrywanie urządzeń i CSPM od jednego dostawcy.

Podsumowanie:

FireMon to kompleksowe rozwiązanie do zarządzania politykami bezpieczeństwa sieciowego. Oferuje centralne kontrolowanie, analizę ryzyka, optymalizację polityk, automatyzację procesów oraz monitorowanie zmian, umożliwiając organizacjom skuteczne zarządzanie cyberzagrożeniami, spełnianie norm bezpieczeństwa i szybką reakcję na incydenty. FireMon pomaga w zabezpieczaniu infrastruktury sieciowej, a także optymalizuje wykorzystanie zasobów, co jest kluczowe dla skutecznej obrony przed zagrożeniami w dynamicznym środowisku IT.