FireEye

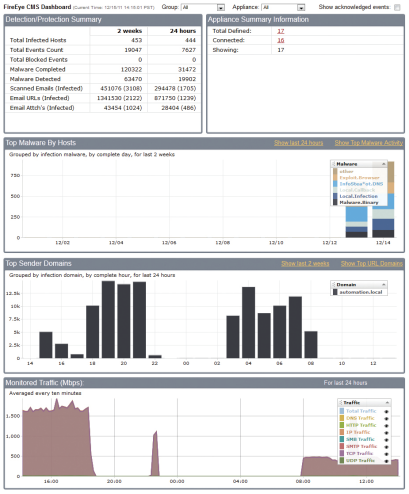
Specyfikacja urządzenia

Central Management System

Lokalna wymiana informacji o zagrożeniach.
Zunifikowane zarządzanie zainstalowanymi komponentami

Główne cechy:

- Urządzenie może być zainstalowane w 30 minut
- Idealne rozwiązanie dla Klientów używających 5 lub więcej urządzeń FireEye lub dla tych, którzy używają jednocześnie FireEye Web MPS, Email MPS, File MPS i/lub MAS
- Dostępne dwa modele do obsługi rosnącej liczby urządzeń
- Zoptymalizowane, scentralizowane zarządzanie wieloma urządzeniami FireEye skraca czas konfiguracji, uaktualnień oraz aktualizacji oprogramowania
- Panel kontrolny zapewnia podgląd na aktualny status ochrony przed zaawansowanymi, ukierunkowanymi atakami
- Znacznie przyspiesza przygotowanie raportów i audytów bezpieczeństwa



Panel kontrolny pokazuje postęp analizy plików oraz status zagrożenia

FireEye Central Management System™ (CMS) scala zarządzanie, raportowanie, przekaz informacji zbieranych przez FireEye Malware Protection System™ w jednym, łatwym do podłączenia urządzeniu sieciowym.

CMS umożliwia współdzielenie automatycznie generowanych przez urządzenia FireEye informacji o malware, w celu zablokowania zaawansowanego ataku wycelowanego w organizację. Pozwala także na centralne zarządzanie konfiguracją i raportowaniem.

Lokalna wymiana informacji o malware

Używając Virtual Execution (VX) engine™, urządzenia FireEye zapewniają ochronę przed zaawansowanym malware w czasie rzeczywistym. CMS pełni rolę centrum dystrybucji, które gwarantuje wszystkim instalacjom FireEye informacje o zaawansowanym, ukierunkowanym ataku, który został wykryty. Dodatkowo subskrybenci FireEye Malware Protection Cloud™ (MPC) mogą używać CMS do centralizacji wymiany informacji o wykrytym malware.

Przejrzysty panel kontroli bezpieczeństwa

CMS konsoliduje czynności i poprawia wiedzę o bieżącej sytuacji dzięki zunifikowanemu panelowi kontrolującemu bezpieczeństwo sieci. Panel ten umożliwia administratorom ocenę liczby zainfekowanych systemów w czasie rzeczywistym oraz daje możliwość poznania szczegółów każdej infekcji pomagając w ustaleniu kolejnych działań.

Zunifikowana analiza zaawansowanych ataków

Instalacja FireEye Web MPS, Email MPS, File MPS i Malware Analysis System ™ (MAS) razem z FireEye CMS umożliwia sporządzanie szczegółowych analiz dotyczących mieszanych zagrożeń, m.in. wskazywania spear phishingowych wiadomości email służących do dystrybucji złośliwych adresów URL. Specjaliści bezpieczeństwa IT zyskują narzędzie pozwalające zebrać wszystkie niezbędne informacje o mieszanym ataku, w celu zabezpieczenia organizacji przed zaawansowanymi i ukierunkowanymi atakami.

„Dla naszej uczelni, bezpieczeństwo użytkowników jest bardzo ważne. Dlatego też stosujemy wiele zabezpieczeń, m.in. antywirusy, firewalle i IPSy. Niestety zdalni użytkownicy są infekowani na zewnątrz naszej sieci. Zaniepokojeni rzeczywistością spear phishingu i ukierunkowanych ataków typu zero-day, zdajemy sobie sprawę, że tradycyjne formy ochrony bazujące na sygnaturach nie zapewniają dostatecznej ochrony przed dzisiejszymi exploitami i botnetami."

Systems and Server Manager, Liberal Arts College

Konsola i alerty

Wydarzenia zagrażające bezpieczeństwu mogą być wyszukiwane, filtrowane, a powiadomienia o bieżących próbach ataku wysyłane przez SMTP, SNMP, syslog, HTTP POST lub wyświetlane na konsoli CMS. Administratorzy mogą filtrować wydarzenia po incydentach, datach, adresach IP, a wyświetlane wyniki są dostosowane do zakresu uprawnień danego administratora. Powiadomienia mogą być również wysyłane do innych narzędzi SIEM, na przykład ArcSight, Nitro Security, Splunk i RSA.

Z poziomu konsoli CMS, administratorzy mogą kliknąć na wybrane wydarzenie i zostaną przekierowani do odpowiedniego urządzenia FireEye, by zobaczyć i ocenić segment sieci, który był celem ataku.

Centralna konfiguracja i aktualizacje

FireEye CMS zapewnia dynamiczną konfigurację dla sprawnego działania wszystkich instalacji. Ustawienia mogą być określone centralnie, a następnie odpowiednio rozdysponowane. Administratorzy mają możliwość zdalnie konfigurować pojedyncze urządzenie lub grupę urządzeń.

Aktualizacje mogą być instalowane we wszystkich zarządzanych urządzeniach jednocześnie gwarantując najnowsze standardy bezpieczeństwa. Także upgrade silnika VX dokonywany jest za pomocą jednego kliknięcia.

Skonsolidowane miejsce przechowywania oraz szczegółowe raporty

Dzięki CMS duże, kontrolowane organizacje mogą generować szczegółowe raporty. CMS zapewnia także możliwość zbierania i przechowywania informacji o incydentach, które mogą być wykorzystane w audytach potrzebnych do wypełnienia długoterminowych wymogów bezpieczeństwa danych.

FireEye CMS zapewnia odpowiednie narzędzia do generowania raportów dotyczących określonych typów zagrożeń. Klienci mogą również zobaczyć podsumowanie działania, na przykład najczęściej infekowane hosty, czy najgroźniejsze incydenty związane z malware i wywołaniami zwrotnymi wraz z ich geograficzną lokalizacją. Szersze spojrzenie lepiej ukazuje postęp w obniżaniu liczby zainfekowanych systemów.

Specyfikacja techniczna

	CMS 4310	CMS 7300
Obudowa	1U Rack	1U Rack
Waga	13,6 kg	13,6 kg
Wymiary (szer. x głęb. x wys. cm)	43,7 x 65,0 x 4,3	43,7 x 65,0 x 4,3
Mocowanie	19-calowy Rack	19-calowy Rack
Porty do zarządzania	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Porty do monitorowania	-	-
AC input voltage	Auto-switching 100~240 V AC Full Range	Auto-switching 100~240 V AC Full Range
AC input current	8,5-6,0 A	9,5-7,2 A
Zasilanie/RAID	Dual 700W / 3 SAS HDD in HW RAID 5	Dual 700W / 3 SAS HDD in HW RAID 5
Częstotliwość	50-60 Hz	50-60 Hz
Temp. pracy	10°C - 35°C	10°C - 35°C

UWAGA: niektóre parametry techniczne mogą różnić się w zależności od rodzaju ruchu i konfiguracji systemu