FUDO

Monitoring, rejestracja i analiza zdalnych sesji dostępu do systemów informatycznych.

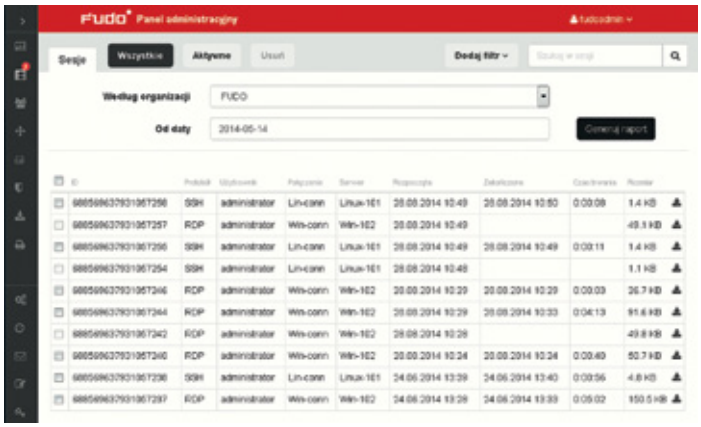
FUDO jest rozwiązaniem sprzętowo-programowym do stałego monitoringu, kontroli i rejestracji zdalnych sesji dostępu do systemów informatycznych. Aktywnie monitoruje ruch w sieci i rejestruje wszelkie sesje dostępu SSH, RDP, HTTP, HTTPS, MySQL, Oracle oraz VNC. FUDO pośredniczy w zestawianiu połączenia ze zdalnym zasobem i rejestruje wszelkie akcje użytkownika, włącznie z ruchem kursora myszy, danymi wprowadzanymi za pomocą klawiatury i przesyłanymi plikami. Umożliwia analizę zarówno sesji w czasie rzeczywistym jak archiwalnych. Podczas podglądu sesji na żywo, osoba nadzorująca może w każdej chwili ją zakończyć, wstrzymać lub włączyć się do niej, by pracować wspólnie ze zdalnym użytkownikiem. Wszystkie dane z sesji zapisywane są na urządzeniu FUDO w formie zaszyfrowanej oraz znakowane kryptograficznym znacznikiem czasu, dzięki czemu mogą stanowić dowód sądowy.

Korzyści wynikające z wdrożenia FUDO:

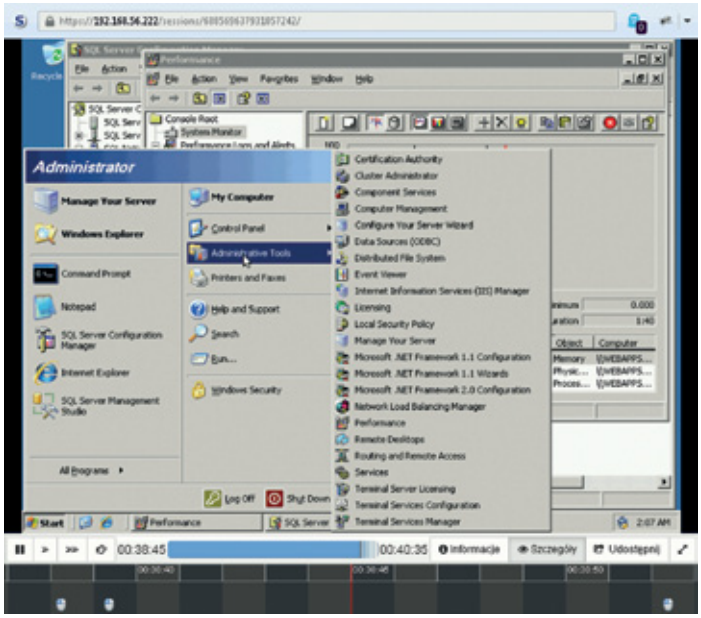
- Filmy wideo umożliwiają szybką analizę po włamaniu.
- Ochrona przed nadużyciami dzięki możliwości ingerencji oraz blokowania sesji zdalnych.
- Niezbite dowody nieuprawnionych działań w postaci podpisanych kryptograficznie i znakowanych czasem zapisów sesji.
- Ułatwienie pracy administratorów poprzez wykorzystanie nagrań sesji do celów szkoleniowych.
- Wdrożenie nie wymaga wprowadzenia żadnych zmian po stronie użytkowników oraz ingerencji po stronie serwerów.

Passus SA | ul. Wiktorska 63, 02-587 Warszawa | tel. +48 22 540 18 42 | e-mail: passus@passus.com.pl | www.passus.com.pl

Panel administracyjny z najważniejszymi informacjami.



Widok zarządzania sesjami pozwala na filtrowanie zapisanych sesji, podgląd sesji aktualnie trwających oraz pobranie zapisanych sesji dostępu.



Zapis sesji można obejrzeć za pomocą wbudowanego odtwarzacza, który pozwala na omijanie fragmentów bezczynności.

Monitoring

FUDO pozwala śledzić sesje dostępu z poziomu przeglądarki internetowej. Jedno kliknięcie uruchamia wewnętrzny odtwarzacz, bez konieczności instalacji dodatkowego oprogramowania. Podczas sesji terminalowych, prezentowany materiał jest w pełni aktywny i umożliwia np. kopiowanie tekstu z odtwarzacza do schowka. Rozwiązanie umożliwia współdzielenie sesji, dzięki czemu administrator jest w stanie wykonać wszystkie operacje tak, jak użytkownik. FUDO pozwala na udostępnienie podglądu z danej sesji osobom nieposiadającym konta w systemie. Wystarczy wysłać wygenerowany odnośnik do osób decyzyjnych, by te oceniły sytuację i zasugerowały podjęcie stosownych działań. W przypadku zauważenia niepokojących działań, FUDO daje możliwość chwilowego zablokowania sesji danego użytkownika, lub całkowitego zerwania połączenia i odebrania mu praw dostępu.

Rejestracja

Urządzenie FUDO wyposażono w pamięć masową o pojemności 20 terabajtów (z możliwością podpięcia dodatkowego zewnętrznego storage'u) umożliwiającą zapis i przechowywanie sesji. Cała przestrzeń w której składowane są dane jest zaszyfrowana. FUDO zapisuje cały materiał nie tylko jako film, wszystkie sesje zapisywane są bez modyfikacji jako pakiety sieciowe, które w razie potrzeby są podpisywane kryptograficznie i znakowane czasem przy użyciu kwalifikowanego certyfikatu. Dzięki temu zapis sesji może stanowić formalny materiał dowodowy w świetle polskiego prawa.

Analiza

Wbudowane narzędzia analityczne pozwalają na wyszukiwanie sesji, w ramach których wykonywane były określone komendy lub przesłany został określony tekst. Zakres wyszukiwania można zawężać do określonych systemów, użytkowników, protokołów czy też przedziałów czasowych. Można również zdefiniować zasady generowania raportów i wysyłania ich do wskazanych osób. Zapis sesji można obejrzeć za pomocą wbudowanego odtwarzacza, który pozwala na omijanie fragmentów bezczynności, odtwarzanie przyśpieszone lub bezpośrednie przechodzenie do wskazanego miejsca w sesji.

Architektura rozwiązania, scenariusze wdrożenia

FUDO to jedno samowystarczalne urządzenie. Nie wymaga instalacji dodatkowego oprogramowania, zarówno agentów na monitorowanych serwerach, jak i programów służących do audytu i analizy zapisanych sesji dostępu. Zarządzanie oraz odtwarzanie nagrań odbywa się za pomocą interfejsu www.

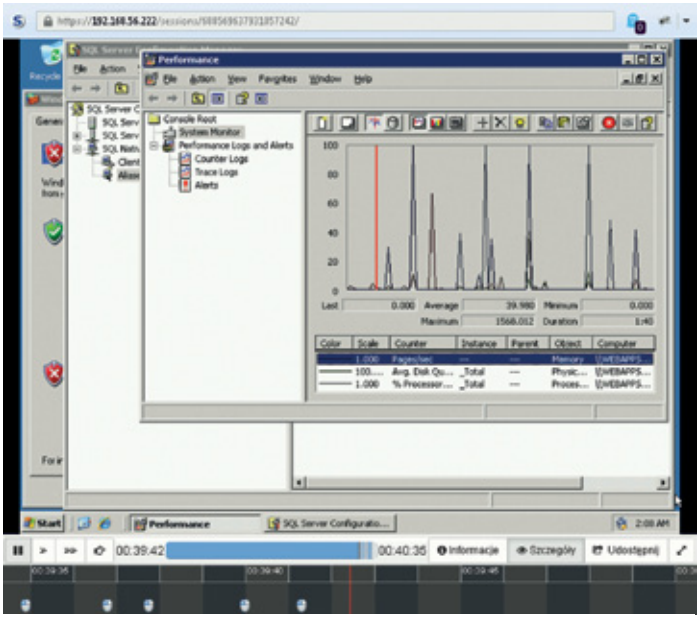
FUDO może działać w dwóch trybach instalacji:

- **Tryb transparentny** (mostu) - przez urządzenie FUDO przechodzą wszystkie połączenia pomiędzy użytkownikami a monitorowanymi serwerami. Zachowane są wszystkie oryginalne źródłowe i docelowe adresy IP i numery portów zdalnych połączeń.
- **Tryb pośrednika** - połączenia zdalne są przekazywane przez odpowiednio skonfigurowany router do urządzenia FUDO. Przez FUDO przechodzą tylko połączenia administracyjne, natomiast pozostały ruch jest kierowany bezpośrednio do serwera docelowego.

Mechanizmy bezpieczeństwa

Szyfrowanie danych - dane przechowywane na FUDO są szyfrowane za pomocą algorytmu AES-XTS, który wykorzystuje 256 bitowe klucze szyfrujące. Algorytm AES-XTS jest najefektywniejszym rozwiązaniem szyfrowania danych przechowywanych na napędach dyskowych. Klucze szyfrujące przechowywane są na dwóch modułach pamięci USB (pendrive). Wygenerowanie kluczy następuje przy pierwszym uruchomieniu urządzenia, podczas którego oba moduły pamięci USB muszą być podłączone.

Po zainicjowaniu kluczy i uruchomieniu FUDO, oba moduły pamięci USB mogą zostać odłączone od urządzenia i umieszczone w bezpiecznym miejscu. W codziennej eksploatacji, klucz szyfrujący wymagany jest jedynie podczas uruchamiania systemu. Jeśli procedury bezpieczeństwa na to pozwalają, jeden z kluczy może być stale podłączony do FUDO, dzięki czemu urządzenie będzie mogło uruchomić się samoczynnie



Zapis sesji może stanowić formalny materiał dowodowy w świetle polskiego prawa.

w sytuacji np. zaniku zasilania, lub ponownego uruchomienia po aktualizacji systemu.

Kopie zapasowe - FUDO posiada zaimplementowany mechanizm tworzenia kopii zapasowych danych, na zewnętrznych serwerach, przy wykorzystaniu protokołu.

Uprawnienia użytkowników - każdy obiekt modelu danych posiada przypisanych użytkowników, uprawnionych do zarządzania obiektem, w zakresie określonym rolą użytkownika.

Sandboxing - FUDO wykorzystuje mechanizm sandbox CAPSICUM, który separuje poszczególne połączenia na poziomie systemu operacyjnego FUDO. Ścisła kontrola przydzielonych zasobów systemowych i ograniczenie dostępu do informacji na temat systemu operacyjnego, zwiększają bezpieczeństwo oraz znacząco wpływają na stabilność systemu.

Konfiguracja klastrowa - FUDO może pracować w konfiguracji klastrowej. Układ klastrowy pracuje w trybie multi-master, w którym konfiguracja systemu (połączenia, serwery, sesje, etc.) synchronizowana jest na każdym z węzłów klastra.

Passus Spółka Akcyjna jest polskim integratorem i dostawcą wysoko specjalizowanych rozwiązań informatycznych obejmujących w szczególności:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT m.in. do wykrywania podatności, zabezpieczenia sieci, aplikacji oraz danych przed zaawansowanymi atakami oraz zagrożeniami wskutek nadużyć lub zaniedbań wewnętrznych;
- rozwiązania do projektowania, budowy i modernizacji wydajnych sieci WiFi w tym realizacji specjalistycznych projektów „pod klucz" (m.in. captive portal, lokalizacja zasobów, dostęp WiFi w środkach komunikacji i transportu).

Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Swedwood, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Bazując na własnych produktach i usługach oraz technologiach uznanych światowych producentów, Passus SA tworzy i wdraża rozwiązania, precyzyjnie dostosowane do wymagań klienta. Firma jest partnerem takich producentów jak: Riverbed, Core Security, GD Fidelis, Fluke Networks, Cisco, Invea-Tech oraz Qualys. Passus posiada także własny zespołów programistów i inżynierów realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń, w maju 2014 roku, zespół ten przygotował unikalne w skali światowej rozwiązanie umożliwiające identyfikację nadużyć i incydentów w oparciu o analizę ruchu sieciowego – Passus Security Anomaly Detector.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Zatrudnia blisko 30 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.: poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S (routing & switching), Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed Network and Application Performance Management Qualified Trainer oraz Fluke Networks Application Performance Appliance Certified Trainer.