Pięć unikatowych funkcji w UTM-ie firmy Check Point

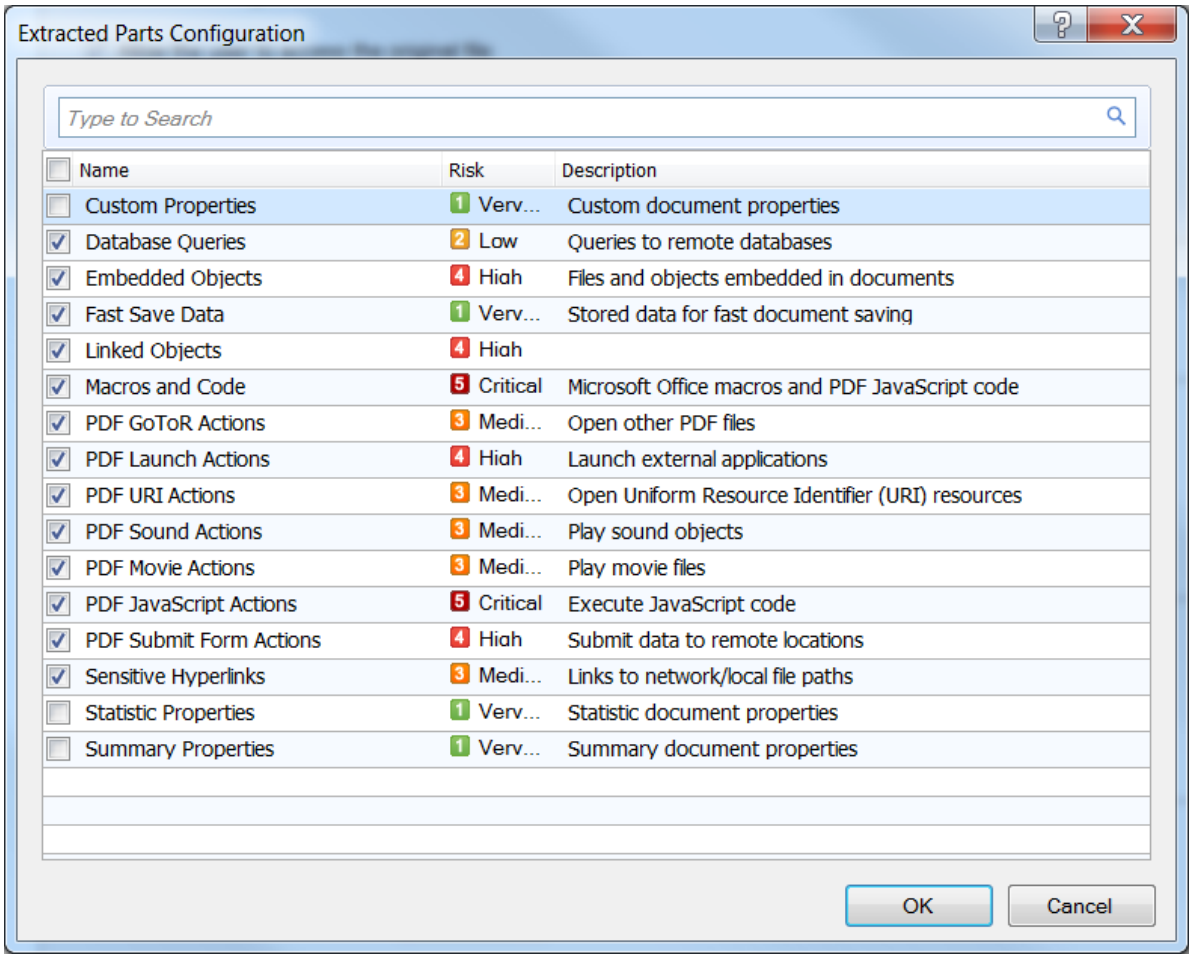
Obecnie rynek urządzeń brzegowych mocno się nasycił. Wraz ze zdrowym trendem wymiany klasycznych routerów na urządzenia firewall/UTM, wielu czołowych producentów wzbogaciło swoje oferty o urządzenia różnorakiej wydajności, oraz z możliwością w mniejszym lub większym stopniu wykupienia w nich interesujących usług. Skutkuje to z jednej strony elastyczną ofertą i walką o klienta, z drugiej zwiększa ilość informacji, którą karmią nas producenci i dystrybutorzy, przez co trudno przebrnąć nam do tych najbardziej kluczowych różnic. Bo prawda jest taka, że większość sprzętów firewall/UTM dysponuje bardzo podobnymi usługami, tworząc w ten sposób standard. Bo jakby nie patrzeć, urządzenie brzegowe nie obędzie się przecież bez IPS-a (Intrusion Prevention System), bez brzegowego antywirusa, systemów QoS (Quality of Service), czy zarządzania i obsługi tuneli VPN. Z doświadczenia zaś mogę dodać, że klienci decydują się na UTM-a głównie patrząc na takie rzeczy jak wydajność, wsparcie techniczne czy prostota interfejsu, co jest pokłosiem niewielkich różnic w oferowanych sprzętach. Oczywiście nie jest tak, że sprzęty niczym się nie wyróżniają. Ba, są takie, których funkcjonalności są innowacyjne i potrafią zwrócić na siebie uwagę. Takim, urządzeniem moim zdaniem dysponuje m. in. Check Point i o nim będzie ten artykuł.
Z góry zastrzegam, że to nie jest recenzja sprzętu, ani techniczna analiza. Bardziej wskazanie kilku ciekawych funkcji, które z jednej strony są dość unikatowe, z drugiej nie są jedynie fanaberią i przysłowiowym „zapychaczem”. Na pewno warto na nie zwrócić uwagę, gdy rozpatrujemy zakup rozwiązania firmy Check Point. Oto lista pięciu wybranych przeze mnie funkcji, które moim zdaniem czynią Check Point wyjątkowym:

1. Threat Emulation:

Sandboxy to dziś jedne z najskuteczniejszych zabezpieczeń wobec aktualnych zagrożeń, gdyż pozwalają na uruchamianie podejrzanych obiektów w odizolowanych strefach, by zanalizować ich zachowanie i prawdziwe zamiary, bez naruszania realnych zasobów. Podobnie jest i tutaj. Check Point Threat Emulation, analizuje zachowanie załączników poczty elektronicznej oraz pobieranych plików. Plik uruchamiany jest w bezpiecznym, odizolowanym środowisku, a analizie podlegają wszystkie wykonane przez ten plik operacje. Sandboxing nie jest obcy innym UTM-om (chociażby moduł „Breach Fighter" w StormShield). **Jednak Check Point wynosi sandboxing o poziom wyżej, m. in. dzięki Human Interaction Simulator, czyli emulacji zachowań ludzkich.** Co do takiego? Wyobraźcie sobie, że bardziej zaawansowane wirusy starają się ukrywać swoją tożsamość, poprzez analizę zachowań tego co dzieje się na komputerze ofiary, po to by wiedzieć czy faktycznie ma do czynienia z człowiekiem, a nie z programem ochronnym, udającym go (chcącym wirusa wykryć i zneutralizować). Organizacje tworzące złośliwe oprogramowanie współpracują z psychologami i socjologami, po to by ich wirusy mogły lepiej odróżniać człowieka od maszyny. Wyobraźmy sobie więc taką sytuację – wirus ukrywa się w dokumencie tekstowym (np. PDF). W tym momencie istotna jest wiedza, w jaki sposób czyta człowiek, a jak program. Program jest w stanie przelecieć tekst w ciągu sekundy. Człowiek będzie to robił znacznie wolniej. W dodatku przesuwanie kursora nie będzie jednostajne. Jeśli wirus „zobaczy" że owy sposób czytania jest „nie-ludzki", po prostu się nie uruchomi, albo wręcz dokona samozniszczenia, aby nie prowokować alertów w laboratoriach antywirusowych. **Check Point stworzył moduł sztucznej inteligencji, która ma za zadanie oszukiwać wirusa i jak najbardziej upodobnić swoje zachowanie do ludzkiego.** Wobec czego dochodzi tutaj do intrygującej batalii między psychologami stojącymi za emulacją zachowań, a psychologami którzy tworzą nowe formy ich wykrywania. Bo co jeśli np. w zarażonych dokumentach zaczną być nagle dołączane nagie fotki? Wtedy jeśli ktoś akurat nie zatrzyma wzroku choćby na moment, to opcje są trzy: albo jest ślepy, albo jest nastolatkiem z matką za plecami, albo właśnie

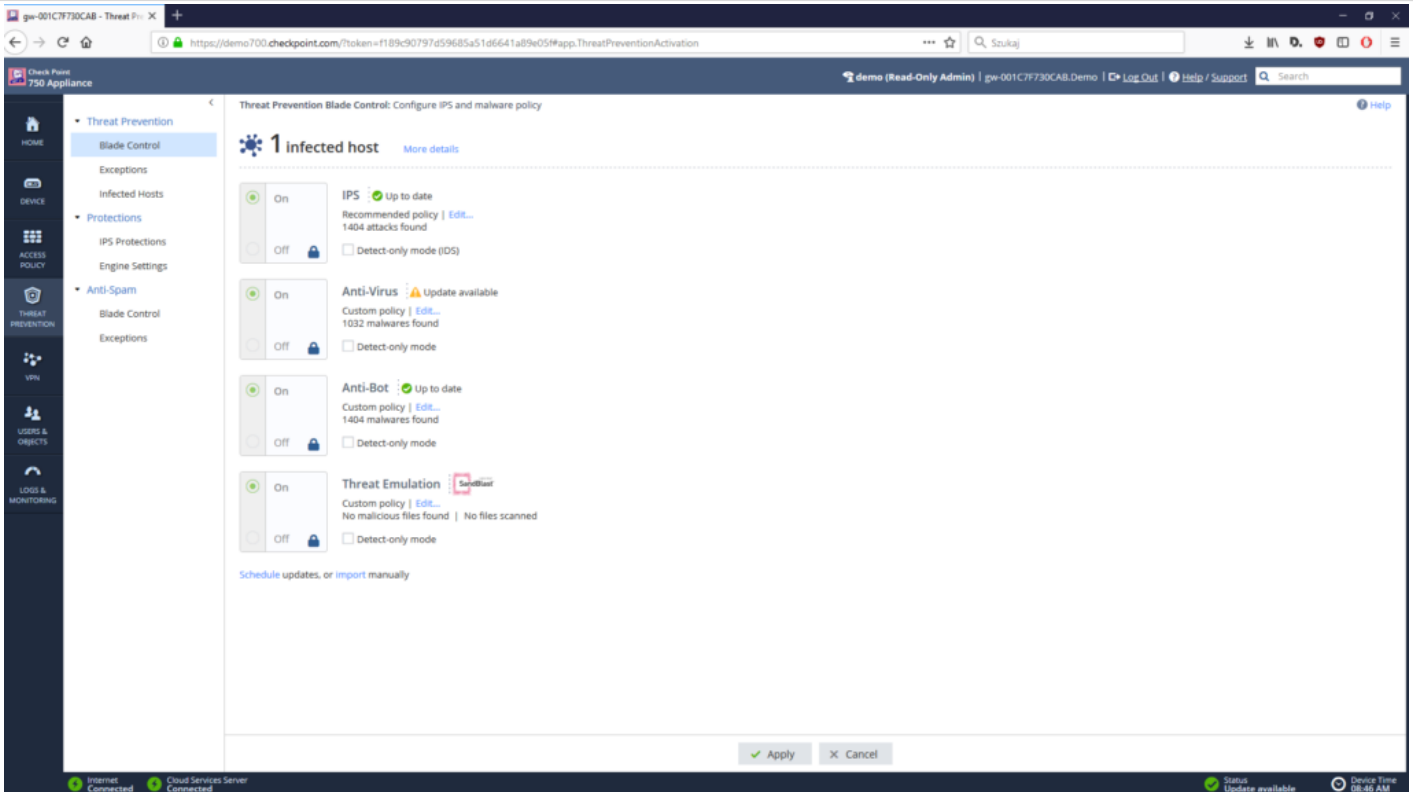
maszyną nieczułą na takie „dystrakcje"

2. Threat Extraction:



Wydaje się, że w obecnych czasach tylko pliki .txt, wydają się najbezpieczniejsze (co nie jest do końca prawdą). Dzisiaj wirusy mogą kryć się praktycznie wszędzie, a także lubią podszywać się pod inne pliki. Nasza czujność wystawiona jest na najwyższą próbę, a lęk przed otwarciem dokumentu może wpędzić niejedną księgową w paranoję. Z pomocą przychodzą technologię rozbrajające takie potencjalnie groźne obiekty. Taką technologią dysponuje Check Point. Threat Extraction usuwa z dokumentów (które są najczęściej wykorzystywane przy atakach) zawartość, która może zostać wykorzystana do ataku, taką jak: makra, elementy zagnieżdżone, łącza internetowe. Użytkownik otrzymuje zrekonstruowany plik, niestanowiący zagrożenia. Użytkownik, w uzasadnionych przypadkach samodzielnie może pobrać plik oryginalny. **Bardzo istotna jest ta rekonstrukcja – bo nie jest sztuką wyłącznie usunąć wszelkie dodatki z dokumentu, lecz również doprowadzić go do stanu, w którym będzie on nadal czytelny i w ogóle się uruchomi.**
Czyli innymi słowy księgowa otrzyma goły tekst, bez dodatków i będzie mogła w spokoju go rozpracować, bez ryzyka że zadzwoni do admina z pretensją, że plik jest zepsuty albo coś jej się nie otwiera

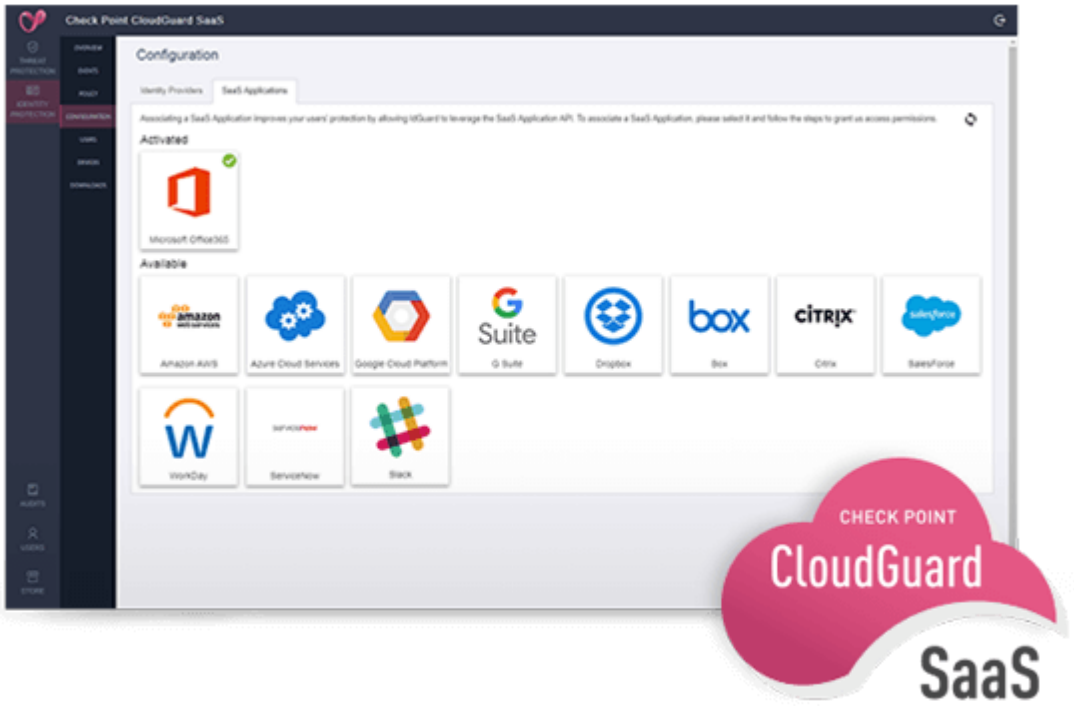
3. SMB Firewall:



Nie każdy z nas ma wystarczającą wiedzę, aby w ekspercki sposób konfigurować urządzenie brzegowe, a na domiar złego, każdy z producentów ma swoją wizję UI i API, przez co mając nawet odpowiednią wiedzę, tak czy owak musimy się nowo nabytego urządzenia nauczyć. Źle skonfigurowane urządzenie brzegowe, może przynieść więcej szkód niż pożytku, a nawet sparaliżować całą sieć. Daleko im więc do urządzeń typu „plug&play", acz dzięki specjalnej linii urządzeń SMB Firewall, konfiguracja i obsługa UTM-a nie będzie już taką katorgą. Czym ona jest? Ten typ urządzenia oferuje zarządzanie przez przeglądarkę, dostępne wszystkie funkcje ochrony oraz uproszczony interfejs administracyjny pozwolą na zabezpieczenie firmy nawet gdy nie posiada ona wykwalifikowanego specjalisty ds. bezpieczeństwa IT.

SMB Firewall to przede wszystkim dość uproszczony interfejs, pozwalający na prostą regulację, konfigurację i aktywację poszczególnych modułów. Wszystko w oparciu o przyjazną, graficzną formę – w głównej mierze suwaki, przyciski „włącz/wyłącz", czy pola wyboru. Wybieramy co nas interesuje, a resztą zajmie się Check Point w oparciu o optymalnie najlepsze konfiguracje. Oczywiście w każdej chwili możemy wybrać opcję manualnej i bardziej szczegółowej konfiguracji, o ile mamy wiedzę i czujemy się na siłach, by się za to zabrać. Dzięki temu Check Point staje się rozwiązaniem jak i dla sieciowych guru, jak i dla informatyków dopiero wkraczających w tematykę zaawansowanych urządzeń brzegowych.

4. Cloud Guard SaaS:



Chcemy, czy nie – co raz więcej producentów oprogramowań ulatnia się do chmury, by stamtąd oferować usługi do tej pory dostępne on-premise. Gartner – najbardziej prestiżowa firma analityczna rynku IT, wskazuje że w 2020 roku firmy z polityką anty-chmurową, będą tak rzadkie jak te bez internetu. Innymi słowy – dinozaury i odludki Choć usługi cloudowe nadal wzbudzają mieszane odczucia w kwestii bezpieczeństwa, nie oznacza to że jesteśmy kompletnie bezbronni. Inżynierowie Check Point wyszli naprzeciw trendom i stworzyli moduł, który chroni najbardziej popularne i jednocześnie narażone usługi chmurowe. Cloud Guard to w skrócie moduły ochronne Check Point przyłączone bezpośrednio do zasobów chmurowych, takich jak Office 365, Gmail, Dropbox, SalesForce, G Suite i wiele innych. Zarządzane są one z interfejsu WEB, czego pozytywnym efektem jest brak jakiegokolwiek obciążenia dotychczas wykorzystywanych zasobów. Warto tutaj wyróżnić szczegółowe analizy meta-danych i analizy językowe np. w e-mailach, które mają ochronić nas przed tzw. pshishingiem. Obejmuje dodatkową ochroną dane logowania, oraz monitoruje je, obejmuje także ochroną same pliki, chroniąc je w trybie rzeczywistym. **To oczywista reakcja na plagę wycieków danych, a usługi chmurowe stanowią wyjątkowo łakomy kąsek dla złodziejów.** Cenię więc adaptację i granie w otwarte karty – Check Point nie udaje, że wystarczy dziś chronić zasoby lokalne, albo że bezpieczeństwo usług chmurowych leży wyłącznie po stronie ich dostawców. Cloud nigdy nie będzie optymalnie najbezpieczniejszym miejscem, lecz i tak będziemy musieli z niego w mniejszym, lub większym stopniu korzystać. I dlatego musimy go objąć dodatkową ochroną. Im wcześniej, tym lepiej.

5. Compliance Blade:

Nawet jeśli udało nam się poprawnie skonfigurować nasze urządzenie brzegowe, wszystko działa i mamy wrażenie dobrze wykonanej roboty, tak w praktyce myślimy często bardzo życzeniowo.

Stosowny audyt (lub, co gorsza, realny atak) jest w stanie dopiero wykazać jak dobrze (lub nie) skonfigurowaliśmy nasze urządzenie. W przypadku Check Point, mamy w zestawie bardzo przyjemnego asystenta. Compliance Blade to unikalna funkcja, pozwalająca ocenić jakość konfiguracji oraz zgodność z wieloma powszechnie uznanymi standardami, takimi jak PCI DSS, SOX, NIST i wiele innych. Moduł analizuje konfigurację urządzenia pod kątem najlepszych praktyk i podpowiada na co należy zwrócić uwagę. Pozwala on na znalezienie i usunięcie błędów konfiguracyjnych zanim znajdą je inni. W łatwy sposób pozwala na podniesienie poziomu bezpieczeństwa organizacji. Nie musimy więc szukać po sieci i pytać po forach, co i jak należy skonfigurować aby było najbezpieczniej. **Innymi słowy – mamy do czynienia z kompleksowym, stałym audytem naszej konfiguracji i polityk, względem ogólnie przyjętych najlepszych praktyk i zasad bezpieczeństwa.** Jeśli nie mamy pewności co i jak skonfigurować, asystent wbudowany w Check Point po prostu nam o tym powie. Przyjemne, nieprawdaż?

Podsumowanie:

Podsumowując, Check Point osobiście intryguje mnie innowacyjnym, ale też adaptacyjnym podejściem do obecnych zagrożeń, oraz realiów rynkowych. Z jednej strony oferuje szerokie spektrum ułatwienia i skrócenia czasu potrzebnego na naukę, konfigurację i obsługę. Z drugiej, odpowiada na nowe trendy i co raz bardziej kreatywne metody ataków i infekcji ofiar przez złośliwe oprogramowanie.

Ps. Materiał powstał przy współpracy z Maciejem Mączką, inżynierem Check Point z firmy Clico. Za co mu gorąco dziękuję!

Ps. 2 Jeśli ktoś chce zobaczyć Check Point w akcji, można skorzystać z live demo, dostępnym na naszej stronie: http://pancernik.it/live-demo-firewall/

Autor: Karol Mondry

Źródła:

cioandleader.com
bleepingcomputer.com
checkpoint.com
wikipedia.org
pancernik.it