SECFENSE

Secfense
User Access Security Broker (UASB)

Ochrona tożsamości użytkowników w dowolnej aplikacji web - aktywowana bez zaangażowania programistów czy ingerencji w kod oraz wolna od vendor-locka.

Secfense to rozwiązanie dostarczone w postaci fizycznego lub wirtualnego appliance, które pozwala zwiększyć bezpieczeństwo uwierzytelniania użytkowników oraz autoryzacji krytycznych operacji w dowolnej aplikacji webowej.

Istotą działania UASB jest tworzenie i egzekwowanie warstwy ochronnej w czasie rzeczywistym, bez modyfikacji chronionych aplikacji.

Architektura

UASB to, w uproszczeniu, serwer reverse proxy, który przejmuje ruch do aplikacji webowej i nakłada na nią warstwę ochronną zabezpieczającą kluczowe procesy.

Jednocześnie UASB stanowi szynę integracyjną dla modułów bezpieczeństwa, takich jak metody drugiego składnika uwierzytelniania (2FA). Każda metoda występuje w postaci niezależnego kontenera, zachowując pełną niezależność od chronionych aplikacji. Dzięki temu może być wymieniona w locie bez wpływu na działanie aplikacji.

Korzyści

Stworzenie spójnej, globalnej i uniezależnionej od rodzaju aplikacji polityki bezpieczeństwa kont pracowników, kontraktorów oraz klientów.

Ochrona przed skutkami phishingu, atakami man-in-the-middle czy kradzieżą sesji już zalogowanych użytkowników.

Integracja “w locie”, a w rezultacie brak kosztów związanych z pracami programistycznymi, problemów z integralnością oraz różnorodnością technologiczną chronionych aplikacji.

Zarządzanie dostępem uprzywilejowanych użytkowników do wrażliwych zasobów (potwierdzenie tożsamości przy określonych transakcjach lub autoryzacja transakcji przez osoby trzecie).

Zasady Działania

Centralnym elementem Secfense jest silnik, który umożliwia budowanie warstw ochronnych dla nieznanych wcześniej aplikacji, zarówno na poziomie protokołu HTTP(s), jak i w warstwach bliższych użytkownikowi (Document Object Model). W procesie uczenia do aplikacji docelowej wpuszczana jest sonda, która ma na celu przeskanowanie aplikacji pod kątem żądań (i odpowiedzi) związanych z uwierzytelnianiem użytkowników. To na tym etapie zbierane są wzorce ruchu sieciowego oraz interfejsu użytkownika. W większości przypadków proces uczenia jest automatyczny i trwa kilkanaście sekund. W przypadku wzorców nierozpoznanych automatycznie, administrator dokonuje ręcznego tuningu.

Po zastosowaniu wzorca w aplikacji aktywowana zostaje wybrana metoda 2FA. Podczas kolejnego logowania użytkownicy przypisani do polityki 2FA zobaczą komunikat o konieczności aktywacji drugiego składnika. Jest to możliwe dzięki przechwytywaniu żądań na poziomie interfejsu użytkownika oraz blokowaniu nieautoryzowanego ruchu w warstwie HTTP(s).

Użytkownik pozostaje w domenie chronionej aplikacji (nie zostaje przekierowany na zewnętrzny serwis), a sam proces rejestracji/użycia drugiego składnika sprawia wrażenie, jakby był integralną częścią chronionej aplikacji. Mechanizm ten działa zarówno dla aplikacji tradycyjnych (w których kod HTML renderowany jest całkowicie po stronie serwera), jak i tzw. SPA (Single-Page Apps).

Secfense nie analizuje i nie przechowuje haseł użytkowników, a wyłącznie nazwy użytkowników w kontekście danej aplikacji.

Integracja

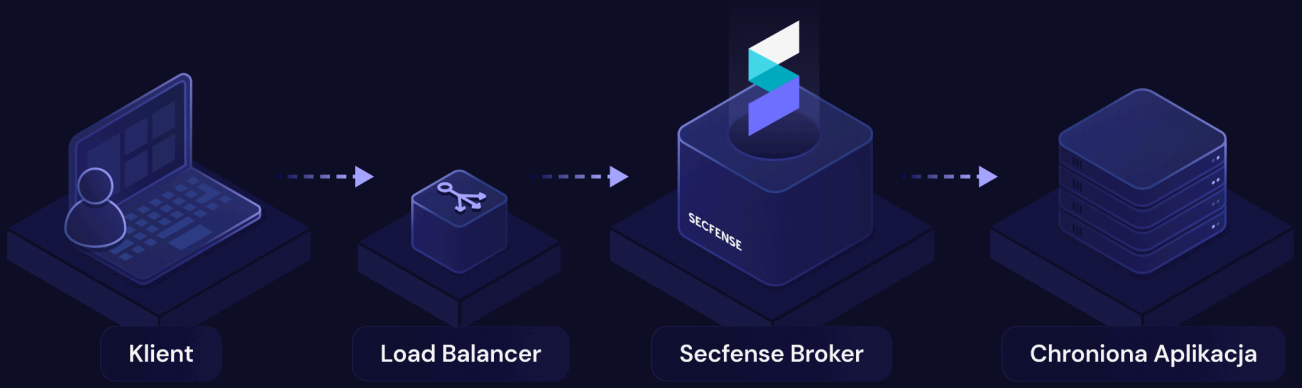
Secfense jest dostępny w postaci fizycznego lub wirtualnego appliance. Jest umieszczany pomiędzy użytkownikami a aplikacjami, tak aby mógł analizować i modyfikować ruch HTTP(s), najczęściej w pobliżu load balancera lub aplikacyjnego firewalla. W zależności od konfiguracji Secfense może terminować ruch SSL/TLS lub działać na ruchu odszyfrowanym przez inne urządzenia.

W celu zachowania poufności komunikacji Secfense nie nawiązuje połączeń z zewnętrznymi hostami ani nie przesyła danych telemetrycznych poza środowisko organizacji.

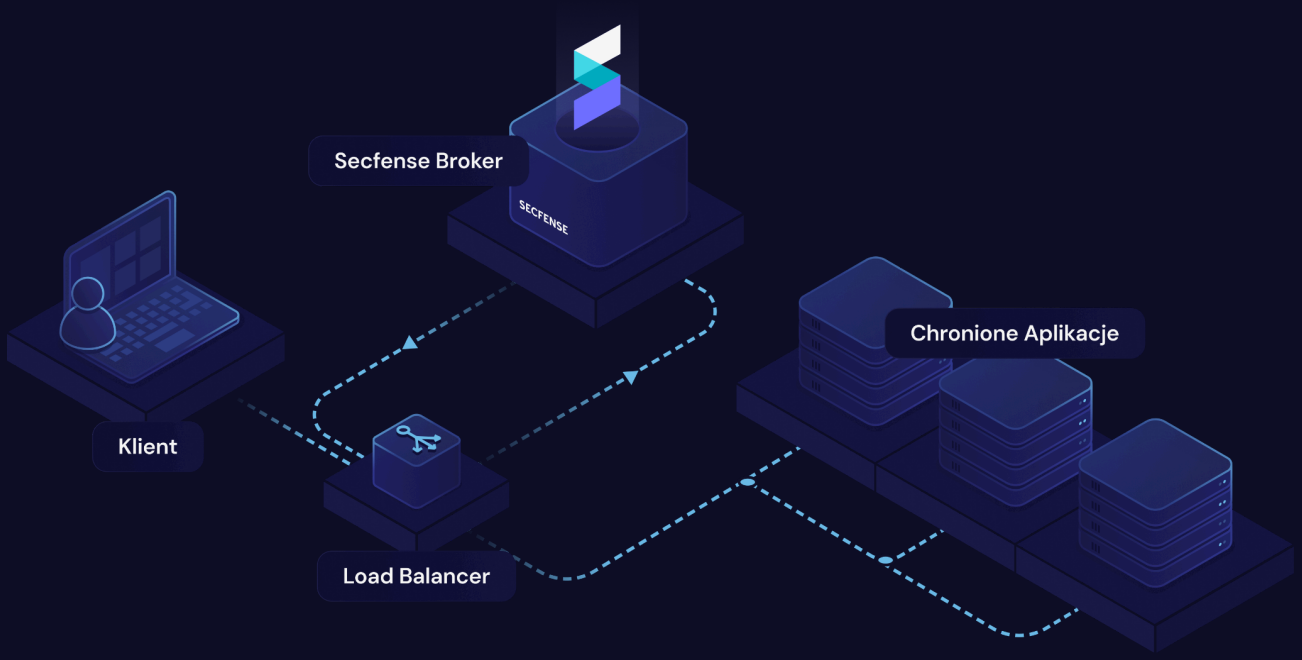
Warianty instalacji Secfense:

- **Inline** (Secfense terminujący SSL/TLS)

- **Inline** (Secfense pracujący na odszyfrowanym ruchu)



- **On a Stick** (Ruch z load balancera kierowany przez Secfense)



Mikroautoryzacje kluczowych transakcji

Mikroautoryzacje, umożliwiają zatrzymanie użytkownika w momencie próby dostępu do określonych zasobów lub wykonania konkretnej akcji w chronionych aplikacjach. W takich sytuacjach, Secfense przejmuje kontrolę, wymagając od użytkownika ponownego uwierzytelnienia (scenariusz 'OWNER') lub uzyskania autoryzacji od osoby trzeciej (scenariusz 'SUPERVISOR'). Ta warstwa ochronna, niezależna od chronionej aplikacji, jest szybko implementowana przez pośredniczącą warstwę Secfense.

W scenariuszu 'OWNER', mikroautoryzacja wprowadza dodatkowy poziom zabezpieczeń zgodnie z zasadą najmniejszych uprawnień, chroniąc przed atakami na aktywną sesję lub innymi zagrożeniami skierowanymi przeciwko zalogowanemu użytkownikowi, takimi jak phishing w czasie rzeczywistym czy malware. Natomiast w scenariuszu 'SUPERVISOR', mikroautoryzacja umożliwia kontrolę dostępu do szczególnie wrażliwych zasobów przez ograniczoną grupę zaufanych użytkowników. W obu przypadkach, mikroautoryzacja chroni wrażliwe zasoby przed niekontrolowanym eksportem, zapobiegając wyciekom poufnych danych przez interfejs aplikacji.

W praktyce, mikroautoryzacja jest najskuteczniejsza, gdy wykorzystuje metody minimalnie angażujące użytkownika, takie jak uwierzytelnianie oparte o U2F/FIDO2. Metody oparte na kodach jednorazowych, takie jak SMS czy TOTP, są mniej efektywne z powodu wymaganego większego zaangażowania użytkownika.

Wszystkie zdarzenia związane z mikroautoryzacjami są rejestrowane w dzienniku zdarzeń Secfense (lub przekazywane do zewnętrznego systemu logowania) i mogą być analizowane w celu wykrywania anomalii.

Full Site Protection

Full Site Protection, ogranicza dostęp do kluczowych części interfejsu aplikacji odpowiedzialnych za uwierzytelnianie. Dostęp jest możliwy tylko dla zaufanych użytkowników, sieci i komputerów. Mechanizm ten eliminuje zagrożenia pochodzące od niezaufanych użytkowników, automatycznych skanerów sieciowych i oraz skryptów wykrywających podatne usługi, odciętych od dostępu do chronionego serwisu.

W odróżnieniu od tradycyjnego MFA, Full Site Protection weryfikuje tożsamość użytkownika przed możliwością nawiązania połączenia z chronionym serwisem. Taka funkcjonalność jest kluczowa dla witryn wymagających dostępności w Internecie, takich jak strony logowania VPN, Outlook Web Access czy Netscaler Gateway. Są one szczególnie podatne na ataki typu zero-day, które mogą być wykorzystane przed wydaniem przez dostawcę odpowiednich poprawek bezpieczeństwa. Ataki te często stanowią pierwszy krok w penetracji infrastruktury IT, dlatego przestępcy intensywnie starają się wykryć i wykorzystać podatne serwisy przed ich zabezpieczeniem.

Full Site Protection nie tylko uniemożliwia automatyczne skanowanie podatności na chronionych serwisach, ale również skutecznie blokuje próby ich wykorzystania przez nieautoryzowanych użytkowników. Ogranicza to ryzyko ataków w okresie między opublikowaniem eksploitów a usunięciem podatności, dając administratorom czas na wdrożenie poprawek bezpieczeństwa bez presji natychmiastowego zagrożenia.

Full Site Protection chroni kluczowe elementy interfejsu aplikacji przed dostępem nieautoryzowanych użytkowników, zapewniając ochronę przed atakami zero-day i automatycznym skanowaniem podatności, jeszcze zanim użytkownik zdąży się zalogować.

SECFENSE

Skontaktuj się z nami

Jeśli masz jakiekolwiek pytania, skontaktuj się z nami bezpośrednio.

Email: sales@secfense.com

Więcej informacji:
www.secfense.com →