Forcepoint

KRÓTKI OPIS
ROZWIĄZANIA

Forcepoint ONE: Platforma chmurowa typu "wszystko w jednym" upraszcza zabezpieczenia dla pracowników hybrydowych

Przypadki użycia

- Zyskaj widoczność i kontrolę nad interakcjami pracowników hybrydowych z danymi w aplikacjach internetowych, chmurowych i prywatnych.
- Zapobiegaj nieuprawnionemu korzystaniu z wrażliwych danych dostępnych z zarządzanych lub niezarządzanych urządzeń.
- Kontroluj dostęp do treści internetowych wysokiego ryzyka.
- Zapewnij zdalny, szybki i bezpieczny dostęp do zasobów biznesowych i prywatnych aplikacji bez złożoności sieci VPN.

Rozwiązanie

- Jedna, ujednolicona platforma umożliwiająca zarządzanie jednym zestawem zasad we wszystkich aplikacjach, z jednej konsoli za pośrednictwem jednego agenta punktu końcowego.
- Usługa "wszystko w chmurze", która chroni dostęp i dane, łącząc Secure Web Gateway (SWG), Cloud Access Broker (CASB) i Zero Trust Network Access (ZTNA).
- Zintegrowana zaawansowana ochrona przed zagrożeniami i bezpieczeństwo danych, aby uniemożliwić atakującym dostęp do poufnych danych.
- Dodatkowe możliwości, takie jak RBI z CDR dla dostępu do sieci Zero Trust, CSPM do skanowania dzierżawców chmury publicznej pod kątem ryzykownych konfiguracji, Forcepoint Classification do tagowania danych i inne (szczegóły na str. 2).

Wynik

- **Uproszczony -** łączy zabezpieczenia aplikacji internetowych, chmurowych i prywatnych w jeden zestaw zasad, jedną konsolę i jednego agenta (z obsługą bezagentową).
- **Nowoczesne -** łączy zasady ZeroTrust z architekturą SASE i zaawansowanymi zabezpieczeniami, takimi jak Remote Browser Isolation i oczyszczanie pobieranych plików.
- **Wszędzie -** jest dostępny globalnie, z ponad 300 punktami obecności (PoP).
- **Niezawodny -** zapewnia 99,99% czasu działania od 2015 roku.
- **Szybkość -** wykorzystuje rozproszone wymuszanie i automatyczne skalowanie w celu wyeliminowania punktów zaporowych.

Złożone rozwiązania punktowe narażają Cię na ryzyko

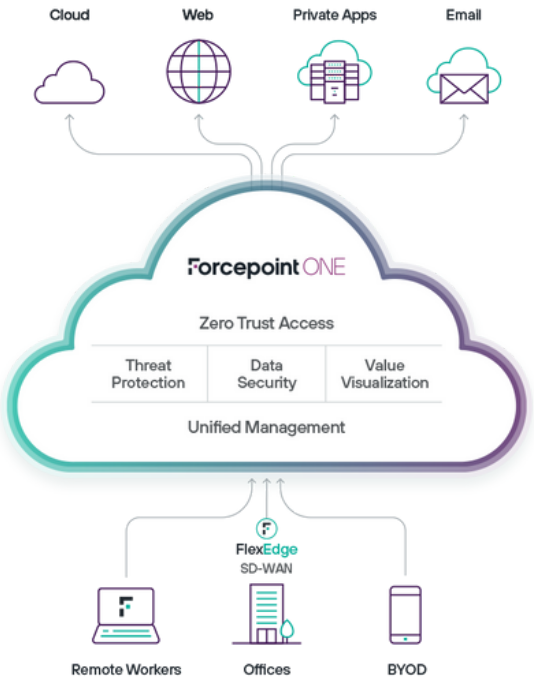
Bezpieczeństwo staje się coraz bardziej złożone. Gdy 75% pracowników pracuje zdalnie, granice między domem a biurem zacierają się. Dane są teraz wszędzie w witrynach internetowych, aplikacjach w chmurze i aplikacjach prywatnych.
Pracownicy zdalni, partnerzy i kontrahenci korzystający z niezarządzanych urządzeń i BYOD narażają Cię na niebezpieczeństwo. Urządzenia łączą się za pomocą starszych, powolnych sieci VPN. Nawet aplikacje służbowe, których używasz do współpracy lub komunikacji, zwiększają ryzyko. Złodzieje cybernetyczni i państwa narodowe zbliżają się do twoich danych i wykorzystują każdą sztuczkę, aby dostać się przez drzwi.

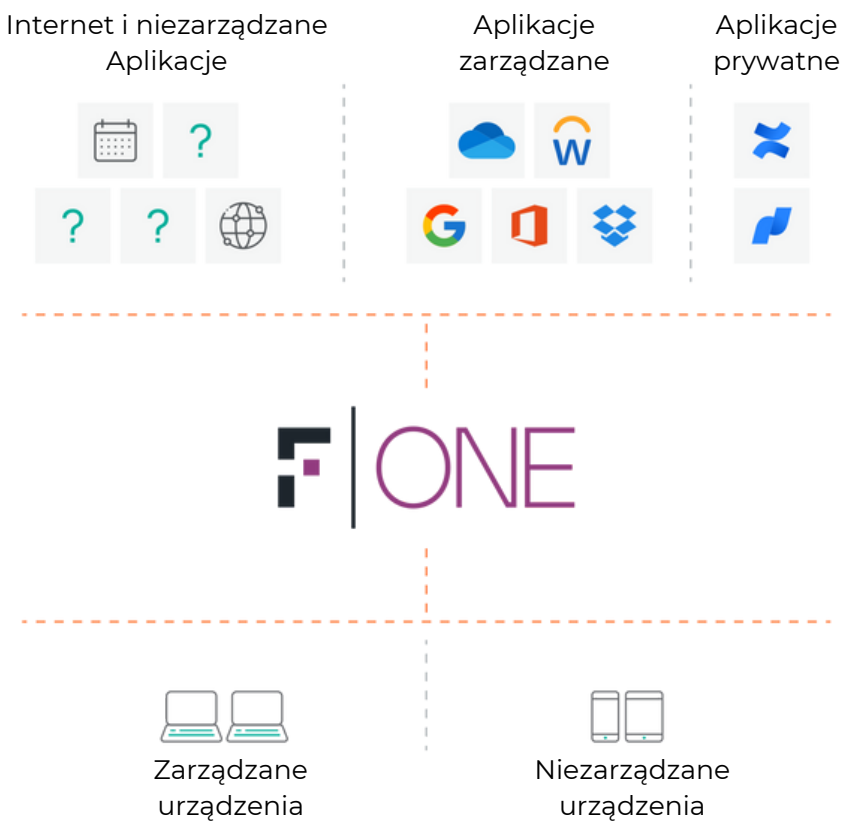
Stare portfolio produktów punktowych nie zostało do tego stworzone. Potrzebujesz prostszego podejścia.

Forcepoint ONE upraszcza bezpieczeństwo

Forcepoint ONE to kompleksowa platforma chmurowa, która sprawia, że bezpieczeństwo staje się proste. Możesz szybko wdrożyć Zero Trust i Security Service Edge (SSE, komponent bezpieczeństwa SASE), ponieważ ujednoliciliśmy kluczowe usługi bezpieczeństwa, w tym Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) i Zero Trust Network Access (ZTNA).

Koniec z rozdrobnionymi produktami. Dajemy Ci jedną platformę, jedną konsolę i jednego agenta z wieloma rozwiązaniami. Zyskaj widoczność, kontroluj dostęp i chroń dane w zarządzanych i niezarządzanych aplikacjach oraz na wszystkich urządzeniach, korzystając z jednego zestawu zasad bezpieczeństwa.





Zapewnij **całkowite bezpieczeństwo w chmurze** dla każdej interakcji

Natywne dla chmury funkcje Zero Trust Forcepoint ONE obejmują:

- **Ujednolicone bramy dostępu do sieci, chmury i prywatnych aplikacji.** Kontrola dostępu oparta na tożsamościach do aplikacji biznesowych zarządzanych w jednym miejscu dla SWG, CASB i ZTNA.
- **Bezagentowe zabezpieczenia DLP dla aplikacji chmurowych i prywatnych aplikacji.** Korzystaj z prywatnych aplikacji biznesowych z osobistych urządzeń, zachowując bezpieczeństwo wrażliwych danych.
- **Zintegrowana zaawansowana ochrona przed zagrożeniami i bezpieczeństwo danych.** Zapobiega utracie lub wyciekowi danych na wszystkich bramach i powstrzymuje hakerów przed dostaniem się do środka.
- **Dynamiczna skalowalność z globalnym dostępem.** 300 punktów PoP zbudowanych na AWS zapewnia szybką łączność o niskich opóźnieniach i 99,99% czasu pracy bez względu na to, gdzie pracujesz.

Ujednolicone zabezpieczenia dla aplikacji internetowych, chmurowych i prywatnych

- **Sieć:** SWG monitoruje i kontroluje interakcje z dowolną witryną internetową w oparciu o ryzyko i kategorię, blokując pobieranie złośliwego oprogramowania lub przesyłanie poufnych danych na osobiste udostępnianie plików i konta e-mail. Nasz ondevice SWG wymusza akceptowalne zasady użytkowania na zarządzanych urządzeniach znajdujących się w dowolnym miejscu.
- **Chmura:** CASB wymusza szczegółowy dostęp do firmowych aplikacji SaaS i danych z dowolnego urządzenia. CASB blokuje pobieranie wrażliwych danych i blokuje przesyłanie złośliwego oprogramowania w czasie rzeczywistym. Skanuje dane w spoczynku w popularnych SaaS i IaaS dla złośliwego oprogramowania i wrażliwych danych oraz środki zaradcze w razie potrzeby. CASB wykrywa ukryte aplikacje IT i kontroluje dostęp z dowolnego zarządzanego urządzenia.
- **Prywatne aplikacje:** ZTNA zabezpiecza i upraszcza dostęp do prywatnych aplikacji bez komplikacji i ryzyka związanego z VPN.

Wszechobecne bezpieczeństwo danych i ochrona przed zagrożeniami

- **Zapobieganie utracie danych (DLP):** Pliki i tekst są skanowane podczas przesyłania i pobierania w poszukiwaniu wrażliwych danych i odpowiednio blokowane, śledzone, szyfrowane lub redagowane. Ponad 190 wstępnie zdefiniowanych reguł DLP pomaga usprawnić zgodność z przepisami i zapewnia szybki czas uzyskania wartości. Łatwa integracja z Forcepoint Enterprise DLP zapewnia bezpieczeństwo danych wszędzie - na punktach końcowych, w sieci, w Internecie i w usługach w chmurze.
- **Skanowanie w poszukiwaniu złośliwego oprogramowania:** Pliki są skanowane podczas przesyłania i pobierania w poszukiwaniu złośliwego oprogramowania i blokowane po wykryciu.

Uproszczone egzekwowanie jednego zestawu zasad

- **Pojedyncza konsola zarządzania** do konfiguracji, monitorowania i raportowania.
- **Pojedynczy zestaw zasad logowania** do kontrolowania dostępu do aplikacji internetowych, chmurowych lub prywatnych w oparciu o lokalizację użytkownika, typ urządzenia, stan urządzenia, zachowanie użytkownika i grupę użytkowników. Parametry te pomagają zapobiegać przejęciom kont.
- **Pojedynczy zestaw zasad DLP** do kontrolowania pobierania i przesyłania poufnych danych i złośliwego oprogramowania dla zarządzanych aplikacji SaaS, aplikacji prywatnych i stron internetowych, a także dla danych przechowywanych w zarządzanych SaaS i IaaS.
- **Ujednolicony agent na urządzeniu** dla systemów Windows i MacOS do obsługi SWG, CASB i ZTNA dla aplikacji klienckich innych niż przeglądarka i kontroli shadow IT.
- **Ujednolicona analityka i wizualizacja wartości** zapewniająca szybki wgląd w zagrożenia bezpieczeństwa, ogólne wykorzystanie i wpływ kompleksowej platformy bezpieczeństwa w chmurze.

Dodatkowe funkcje dostępne w razie potrzeby

- **Cloud Security Posture Management (CSPM):** Skanuje ustawienia dzierżaw AWS, Azure i GCP pod kątem ryzykownych konfiguracji i zapewnia ręczne i zautomatyzowane środki zaradcze.
- **SaaS Security Posture Management (SSPM):** Skanuje ustawienia dzierżawy Salesforce, ServiceNow i Office 365 pod kątem ryzykownych konfiguracji oraz zapewnia ręczne i automatyczne środki zaradcze.
- **Remote Browser Isolation (RBI):** Chroni użytkownika przed złośliwym oprogramowaniem przenoszonym przez Internet na jego urządzeniu lokalnym, uruchamiając przeglądarkę w maszynie wirtualnej hostowanej w chmurze. Wykorzystuje CDR do oczyszczania plików pobranych podczas sesji RBI ze złośliwego oprogramowania lub obcych elementów.
- **Forcepoint Classification:** Klasyfikacja danych z sugestiami opartymi na sztucznej inteligencji w celu zwiększenia dokładności tagowania. Subskrypcje, które odblokowują prostotę

Subskrypcje, które odblokowują prostotę

Dostępne są roczne subskrypcje na użytkownika:

- **Edycja All-in-one** dla bezpieczeństwa sieci, chmury i aplikacji prywatnych.
- **Edycja Web-security** obejmuje bramę internetową oraz wbudowany CASB dla nieograniczonej liczby aplikacji w chmurze. Umożliwia klientom dodanie obsługi API dla aplikacji w chmurze oraz obsługi aplikacji prywatnych w późniejszym czasie.
- **Edycja ZTNA** chroni nieograniczoną liczbę aplikacji prywatnych.
- **Edycja CASB** chroni nieograniczoną liczbę aplikacji w chmurze inline obejmując interfejsy API dla 3 aplikacji z możliwością dodawania dodatkowych pakietów lub dedykowanych węzłów odpytywania API.
- **Wszystkie subskrypcje** obejmują scentralizowane zarządzanie chmurą. Ujednolicone polityki z funkcją zapobiegania utracie danych. Zautomatyzowany dostęp za pośrednictwem agenta wraz z kompleksowym raportowaniem.