Palo Alto Networks

Zabezpieczenia na miarę przyszłości

paloalto® NETWORKS

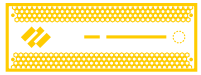
Palo Alto Networks to wiodący dostawca zabezpieczeń cybersecurity, który nie wymaga dokonania wyboru między ochroną przed bieżącymi atakami a przygotowaniem się na nowe zagrożenia. Chcemy zapewnić naszym klientom jedno i drugie, czyli bezpieczeństwo bez kompromisów teraz i w przyszłości.

W jaki sposób możemy zadbać o ochronę Państwa zasobów?

STRATA™
BY PALO ALTO NETWORKS

Strata

Już dziś możesz zabezpieczyć swoją firmę przed zagrożeniami, które pojawią się w przyszłości. Inteligentne zabezpieczenia sieci oferowane przez Palo Alto Networks chronią użytkowników, aplikacje i dane w każdym miejscu, gdzie rozciąga się sieć i środowisko IT naszych klientów.



Next-Generation Firewall

PA-Series

VM-Series

CN-Series

App-ID

Content-ID

User-ID

Device-ID

Panorama

DNS Security

Enterprise DLP

Threat Prevention

URL Filtering

WildFire

IoT Security

GlobalProtect

5G Security

SD-WAN

Firewalle nowej generacji

Fizyczne, wirtualne i chmurowe systemy ochrony

Możliwość konsolidacji wielu niezależnych od siebie zabezpieczeń w jednym prostym rozwiązaniu, które chroni sieć i pomaga w bezpiecznym przeprowadzeniu transformacji cyfrowej. Nasz pierwszy w branży firewall nowej generacji, wykorzystujący uczenie maszynowe, to najwyższej klasy spójny, zintegrowany, centralnie zarządzany system bezpieczeństwa sieciowego udostępniany w postaci platformy sprzętowej, wirtualnej, kontenerowej lub chmurowej, chroniący przed nieznanymi zagrożeniami.

Zapewnia widoczność i ochronę wszystkich elementów środowiska informatycznego, łącznie z systemami IoT, a dzięki automatycznym rekomendacjom polityk bezpieczeństwa zmniejsza liczbę błędów konfiguracyjnych. Warto zabezpieczyć swój kampus, chmurę hybrydową, oddziały przedsiębiorstwa i użytkowników mobilnych, wykorzystując rozwiązanie firmy, która dziewięciokrotnie znalazła się w kategorii liderów w raporcie firmy Gartner „Magic Quadrant".

Seria PA

Sprzętowy firewall nowej generacji

Sprzętowe firewalle nowej generacji serii PA zostały zbudowane z myślą o zwiększeniu wydajności mechanizmów bezpieczeństwa. Dzięki wielu szybkim interfejsom i architekturze platformy zapewniających maksymalną przepustowość, użytkownik zyskuje widoczność, bezpieczeństwo i kontrolę nad ruchem w sieci przedsiębiorstwa (łącznie z sieciami IoT i 5G), która obejmuje centra przetwarzania danych, obszar kampusu i oddziały firmy, instalacje przemysłowe i infrastrukturę mobilną 5G.

Seria VM

Wirtualny firewall nowej generacji

Wirtualne firewalle nowej generacji serii VM to idealne rozwiązanie dla środowisk, w których wdrożenie firewalli sprzętowych jest trudne lub niemożliwe. Udostępniają w formie maszyny wirtualnej wszystkie możliwości zapór Palo Alto Networks Next-Gen Firewall. Zapewniają bezpieczeństwo sieci w konfiguracji inline oraz ochronę przed zaawansowanymi zagrożeniami. W spójny sposób chronią chmury publiczne i prywatne, zwirtualizowane centra danych i zasoby w oddziałach firm.

Seria CN

Firewall nowej generacji w postaci kontenera

Firewalle nowej generacji serii CN udostępniają w formie kontenerów wszystkie możliwości zapór Palo Alto Networks Next-Gen Firewall. Pozwalają na maksymalne wykorzystanie mechanizmów kontroli bezpieczeństwa w środowiskach kontenerowych i uzyskanie kontekstu kontenerów, który można wykorzystać podczas tworzenia reguł bezpieczeństwa. Dzięki firewallowi serii CN usługi przeciwdziałania atakom i inne zaawansowane mechanizmy bezpieczeństwa sieci, np. IPS i filtrowanie adresów URL, mogą zostać zastosowane w odniesieniu do komunikacji sieciowej wychodzącej, przychodzącej lub poziomej między podami kontenerów, a także między aplikacjami kontenerowymi, maszynami wirtualnymi i serwerami fizycznymi.

App-ID

Funkcja identyfikacji aplikacji

App-ID™ to opatentowana technologia klasyfikowania ruchu w sieci, dostępna na firewallach Palo Alto Networks. Określa ona rodzaj aplikacji niezależnie od używanego przez nią portu, protokołu, szyfrowania SSH/SSL (w tym TLS 1.3 i HTTP/2) i innych złożonych technik, które mogą być stosowane w konkretnych przypadkach i zastosowaniach. Używane są różne mechanizmy klasyfikowania strumienia ruchu w sieci, umożliwiające poprawne zidentyfikowanie aplikacji, m.in. sygnatury aplikacji, dekodowanie protokołu aplikacji i heurystyka. Gdy aplikacja zostanie zidentyfikowana, sprawdzane są reguły bezpieczeństwa do niej przypisane i podejmowana jest decyzja o sposobie jej obsługi. Można na przykład aplikację zablokować lub zezwolić na jej uruchomienie ale przeskanować pod kątem zagrożeń oraz sprawdzić, czy nie występują przypadki przesyłania plików i przetwarzania danych bez upoważnienia. Można także kontrolować przepustowość komunikacji z wykorzystaniem mechanizmów QoS.

Zastąpienie reguł firewalla opartych na numerach portów przez reguły wykorzystujące technologię App-ID znacznie ogranicza ryzyko skutecznego ataku. Policy Optimizer – usługa dostępna w ramach systemu PAN-OS® działającego na firewallach Palo Alto Networks – wykorzystuje informacje o polityce bezpieczeństwa, budowie reguł i dane analityczne o połączeniach sieciowych gromadzone przez PAN-OS, aby podpowiedzieć i ułatwić przejście od dotychczasowych klasycznych reguł firewalla na mechanizmy kontrolne w oparciu o App-ID i w efekcie zwiększyć bezpieczeństwo sieci.

Content-ID

Mechanizm inspekcji treści

Mechanizm Content-ID™ wykorzystuje zaawansowane metody ochrony przed zagrożeniami umożliwiające pełną analizę dozwolonych połączeń, wykonując ją w ramach jednego przebiegu skanowania co minimalizuje wpływ na wydajność firewalla niezależnie od włączonych funkcji bezpieczeństwa. Zapory Palo Alto Networks Next-Gen Firewall korzystają z tej technologii i są w stanie zablokować próby wykorzystania luk w zabezpieczeniach, użycia malware, przepełnienia bufora i skanowania

portów, a także chronić sieć przed stosowanymi przez włamywaczy metodami omijania zabezpieczeń i maskowania ataków.

Nasze funkcje bezpieczeństwa wspierane usługami i narzędziami korzystającymi z zasobów w chmurze, takie jak Threat Prevention i URL Filtering, za pomocą technologii Content-ID zatrzymują połączenia nawiązywane przez złośliwe oprogramowanie, blokują dostęp do znanych serwisów umożliwiających pobranie szkodliwego oprogramowania i wyłudzenie cennych informacji (phishing sites) oraz ograniczają ryzyko związane z przesyłaniem wrażliwych danych i niedozwolonych typów plików. Content-ID umożliwia kompleksową ochronę przed zagrożeniami realizowaną z użyciem tylko jednego skanu połączenia sieciowego, co optymalizuje wydajność firewalli nowej generacji.

User-ID

Funkcja identyfikacji użytkowników

Technologia User-ID™ ułatwia definiowanie polityk bezpieczeństwa firewalli opartych o aplikacje dla specyficznych użytkowników i grup użytkowników, dla połączeń wychodzących i przychodzących. Na przykład, pozwala zapewnić dostęp do narzędzi takich jak SSH, telnet i FTP na standardowych portach jedynie pracownikom działu informatyki.

Reguły utworzone za pomocą technologii User-ID obowiązują niezależnie od miejsca pobytu użytkowników — tj. w centrali, w oddziałach oraz w domu — i rodzaju używanego przez nich urządzenia. Można uzyskać wgląd w działania aplikacji w kontekście użytkowników a nie tylko według adresów IP oraz generować raporty z tych działań. Można też wdrażać dla użytkowników systemy uwierzytelniania wieloskładnikowego (MFA) bez wprowadzania zmian w aplikacjach.

Technologia User-ID umożliwia zapobieganie wyciekowi poświadczeń użytkowników poza przedsiębiorstwo oraz uniemożliwia cyberprzestępcom ich wykorzystanie podczas ataku do rozpoznania i poruszania się wewnątrza zaatakowanej sieci. Mechanizm Dynamicznych Grup Użytkowników (ang. Dynamic Users Group - DUG) pozwala administratorom automatycznie modyfikować zasady dostępu użytkowników lub stosować uwierzytelnianie wieloskładnikowe, np. w razie wystąpienia oznak naruszenia bezpieczeństwa lub w związku z potrzebą nadania tymczasowego dostępu do sieci określonej grupie użytkowników (np. tymczasowym pracownikom lub pracownikom innych firm wykonujących pracę w naszej sieci).

Device-ID

Funkcja klasyfikacji urządzeń

Device-ID™ to nowy atrybut możliwy do użycia w konfiguracji zapory Palo Alto Next-Gen Firewall, który umożliwia administratorom tworzenie reguł na podstawie charakterystyki i typu urządzeń IoT komunikujących się poprzez firewall. Device-ID pomaga także znajdować powiązania między zdarzeniami bezpieczeństwa i urządzeniami podłączonymi do sieci oraz tworzyć reguły powiązane z urządzeniami (a nie z ich adresami IP lub lokalizacjami, które mogą się zmieniać).

Dzięki Device-ID nasze firewalle nowej generacji mogą dopuścić do sieci tylko te urządzenia IoT, które funkcjonują w sposób uznany jako prawidłowy, blokować urządzenia z przestarzałymi systemami operacyjnymi lub podatnościami, szybko określić zagrożenia dla poszczególnych urządzeń oraz wykorzystywać „urządzenie" jako warunek dopasowania w innych rodzajach reguł. Funkcję Device-ID można użyć w regułach dotyczących bezpieczeństwa, deszyfrowania, zapewniania jakości usług (QoS) i uwierzytelniania.

Funkcja ta jest dostępna na platformie zarządzania Panorama i na wszystkich firewallach Palo Alto Networks Next-Gen wykorzystujących uczenie maszynowe (z wyjątkiem serii VM-50 i CN) z systemem operacyjnym PAN-OS 10.0 lub nowszym.

Panorama

Platforma centralnego zarządzania

Panorama™ to rozwiązanie do centralnego zarządzania bezpieczeństwem sieci, przeznaczone do obsługi wszystkich firewalli Palo Alto Networks niezależnie od ich postaci i lokalizacji. Pozwala uprościć konfigurowanie i wdrażanie reguł bezpieczeństwa oraz zarządzanie nimi. Zapewnia wgląd w profil ruchu na podstawie logów przekazywanych przez firewalle oraz centralny dostęp do szczegółowych informacji o zawartości dzienników logów i wykrytych zagrożeniach na wszystkich zarządzanych zaporach Palo Alto Networks Next-Gen Firewall. Panorama zmniejsza pracochłonność zadań administracyjnych, ponieważ pomaga w zarządzaniu aktualizacjami, automatyzuje reagowanie na zagrożenia stosując reguły opisujące działania oraz wykorzystuje integrację z systemami innych firm poprzez swój interfejs API.

Specjaliści ds. bezpieczeństwa mogą uzyskać wgląd i kontrolę stanu bezpieczeństwa oraz konsolidować narzędzia i automatyzować ochronę sieci. Panorama zarządza regułami i dynamicznymi aktualizacjami zabezpieczeń. Pomaga przedsiębiorstwu dotrzymać kroku ciągle ewoluującym zagrożeniom sieciowym. Umożliwia uproszczenie operacji poprzez efektywne zarządzanie aktualizacjami oprogramowania oraz automatyzację aktualizacji definicji i reguł opisujących zagrożenia, co z kolei poprawia ogólny stan zabezpieczeń przedsiębiorstwa.

Za pomocą jednego rozwiązania do zarządzania firma może w pełni wykorzystywać możliwości firewalli, w które zainwestowała wcześniej, oraz dostępnych mechanizmów bezpieczeństwa wynikających z posiadanych subskrypcji. Wszystkie te dane i możliwości konfiguracji oraz administracji wieloma firewallami jednocześnie są dostępne z jednego miejsca.

DNS Security

Zapobieganie atakom opartym o protokół DNS

Osiemdziesiąt procent (80%) szkodliwego oprogramowania wykorzystuje protokół DNS podczas komunikacji command-and-control (C2) z serwerami kontrolowanymi przez cyberprzestępców. DNS jest również używany do wyprowadzania z zaatakowanej firmy cennych danych (ang. DNS tunneling). Cyberprzestępcy często używają połączeń DNS do ukrycia swoich działań, ponieważ natężenie ruchu sieciowego jest tak duże, że wiele przedsiębiorstw nie jest w stanie go odpowiednio monitorować, a w szczególności nie przykłada uwagi do tak podstawowego i niezbędnego protokołu jak DNS.

W celu zapewnienia ochrony przed zagrożeniami wykorzystującymi DNS potrzebne są wysokiej klasy mechanizmy wykrywania połączone z funkcjami analitycznymi, które zapewniają specjalistom ds. zabezpieczeń kontekst umożliwiający tworzenie reguł oraz szybkie i efektywne reagowanie na zagrożenia. Oferowana przez nas usługa DNS Security stosuje metody analizy predykcyjnej, uczenia maszynowego i automatyzacji, aby blokować ataki oparte na DNS. Ścisła integracja z firewallami nowej generacji pozwala zautomatyzować mechanizmy ochrony, uniemożliwia cyberprzestępcom obejście zabezpieczeń i eliminuje konieczność użycia odrębnych narzędzi oraz nie wymaga zmian w routingu DNS. Dzięki usłudze można sprawnie i proaktywnie wykrywać i zapobiegać użyciu szkodliwych domen w atakach oraz neutralizować zagrożenia związane z tunelowaniem DNS, a także szybko identyfikować i izolować zainfekowane urządzenia.

Funkcje raportowania dostępne w rozwiązaniu DNS Security zapewniają lepszy wgląd w zagrożenia oraz pełną widoczność ruchu w systemach DNS na poziomie makro, branży i organizacji. Mechanizmy ochrony DNS Security korzystają z usług i danych dostępnych z chmury aby zapewnić sobie praktycznie nieograniczone skalowanie wydajności i aktualność.

Przedsiębiorstwo zyskuje dostęp do nowego, ważnego punktu kontrolnego, z poziomu którego można powstrzymywać ataki oparte na DNS. Palo Alto Networks łączy najwyższej klasy funkcje wykrywania zagrożeń z funkcjami analitycznymi i bezpośrednim egzekwowaniem reguł niezbędnych do ochrony ruchu DNS w czasie rzeczywistym przez firewalle nowej generacji.

Enterprise Data Loss Prevention

Ochrona danych

Palo Alto Networks Enterprise Data Loss Prevention (DLP) to pierwsza w branży usługa zabezpieczająca dane udostępniana w chmurze, która wykrywa, monitoruje i chroni dane wrażliwe, takie jak informacje umożliwiające identyfikację osób oraz informacje stanowiące własność intelektualną, we wszystkich sieciach, chmurach i systemach użytkowników.

Usługa ochrony w chmurze i predefiniowane reguły zapewniają ochronę danych i zgodność z przepisami w sposób łatwy i spójny zarówno w środowiskach lokalnych, jak i systemach obsługujących pracowników zdalnych, a także w chmurze. Zintegrowana z istniejącymi punktami kontrolnymi w postaci firewalli firmy Palo Alto Networks usługa Enterprise DLP zapewnia aż trzykrotnie niższy całkowity koszt posiadania i utrzymania w porównaniu ze starszymi, skomplikowanymi produktami DLP. Jest również prostsza we wdrażaniu i utrzymaniu oraz eliminuje zapotrzebowanie na dodatkową infrastrukturę serwerową.

Threat Prevention

Zapobieganie atakom wykorzystującym luki w zabezpieczeniach, szkodliwe oprogramowanie i mechanizmy C2

Oferowana przez naszą firmę usługa Threat Prevention dla firewalli nowej generacji Palo Alto Networks pozwala, dzięki funkcjom IPS, automatycznie powstrzymywać ataki wykorzystujące znane luki w zabezpieczeniach po stronie klienta i serwera. Zapewnia bezpośrednią ochronę przed szkodliwym oprogramowaniem i blokowanie w czasie ataku komunikacji wychodzącej typu command-and-control (C2). Analizuje różne rodzaje ruchu w sieci pod kątem zagrożeń, niezależnie od portu, protokołu i metody szyfrowania.

Włączone w usługę Threat Prevention mechanizmy zapobiegania włamaniom (IPS) są oparte na dopasowywaniu sygnatur i wykrywaniu anomalii. Poza aktualizacjami sygnatur dostarczanymi przez Palo Alto Networks, możliwe jest także importowanie i stosowanie sygnatur i reguł w popularnych formatach, takich jak Snort i Suricata®.

Wykrywanie zagrożeń dotyczy wszystkich etapów życia cyberataku, nie tylko pierwszego kontaktu z siecią. Usługa Threat Prevention zapewnia wielowarstwową ochronę zgodną z modelem „Zero Trust".

Dzięki zastosowaniu jednolitego formatu sygnatur dla wszystkich zagrożeń możliwe jest wydajne przetwarzanie i przeprowadzenie analizy w ramach jednego zintegrowanego skanowania pakietów przez firewall. Eliminuje to nadmiarowe procesy typowe dla rozwiązań wykorzystujących wiele cykli skanowań tego samego połączenia i pakietów. Usługa Threat Prevention sprawdza każdy pakiet przechodzący przez firewalle Palo Alto Networks nowej generacji. Kontrolowane są sekwencje bajtów w nagłówkach pakietów i w ich zawartości. Na podstawie takiej analizy jesteśmy w stanie uzyskać ważne informacje o poszczególnych pakietach, do-

tyczące m.in. stosowanej aplikacji, źródła i miejsca docelowego połączenia oraz zgodności protokołu ze standardem RFC, a także pozwala to stwierdzić, czy w zawartości pakietu znajduje się szkodliwy kod lub exploit. Oprócz pojedynczych pakietów możemy także analizować kolejność przychodzących danych i sekwencje wielu pakietów, co pozwala wykryć próby użycia technik omijania i unikania zabezpieczeń i w efekcie zapobiec ich wykorzystaniu do przeprowadzenia ataku. Wszystkie opisane działania ochronne odbywają się w ramach jednego cyklu skanowania, więc ich wpływ na prędkość komunikacji sieciowej jest minimalny.

URL Filtering

Zapobieganie zagrożeniom związanym z niebezpiecznymi serwisami WWW i phishingiem

URL Filtering to rozwiązanie, które pozwala bezpiecznie korzystać z sieci web w związku z realizacją procesów biznesowych. Realizowana przez nasze firewalle nowej generacji i wspierana danymi o zagrożeniach z chmury usługa nie polega wyłącznie na podstawowym filtrowaniu komunikacji WWW — identyfikowanie zagrożeń odbywa się z wykorzystaniem analizy statycznej i uczenia maszynowego. Ataki wykorzystujące strony web, których celem jest wyłudzanie danych (phishing sites) oraz napisane w języku JavaScript, są wykrywane na bieżąco, w czasie liczonym w milisekundach.

Ponieważ codziennie pojawiają się tysiące nowych szkodliwych adresów URL, niebezpieczne strony WWW muszą być wykrywane natychmiast w celu zapewnienia ochrony przed atakami z Internetu. Automatyczne funkcje ochrony realizowane przez firewalle Palo Alto Networks blokują dostęp do szkodliwych serwisów rozpowszechniających szkodliwe oprogramowanie i wyłudzających dane logowania, dzięki czemu przedsiębiorstwo może uniknąć utraty danych. Rozszerzenie reguł firewalla o mechanizm URL Filtering zmniejsza ryzyko ataku, zwłaszcza że jest on zasilany ciągle aktualizowanymi informacjami o nowych zagrożeniach. Reguły firewalla oparte na aplikacjach i użytkownikach pozwalają uprościć złożone reguły bezpieczeństwa w komunikacji ze stronami WWW, a zatem ograniczyć ogólne koszty operacyjne.

Aby we właściwy sposób określić kategorie i współczynniki ryzyka, nasze narzędzia powiązane z usługą URL Filtering skanują serwisy WWW i analizują ich zawartość korzystając z algorytmów uczenia maszynowego w ramach analizy statycznej i dynamicznej. W efekcie możliwa jest klasyfikacja adresów URL jako niegroźne lub szkodliwe oraz ze względu na ich treść. Takie kategorie można łatwo uwzględnić w regułach firewalli, aby w pełni kontrolować komunikację WWW. Po wykryciu nowych adresów URL sklasyfikowanych jako szkodliwe lub należące do blokowanej kategorii mechanizm URL Filtering może natychmiast przerwać połączenie bez konieczności interwencji analityka bezpieczeństwa i administratora firewalla.

WildFire

Ochrona przed szkodliwym kodem

WildFire® to usługa chroniąca przed szkodliwym oprogramowaniem, w której zastosowano najbardziej zaawansowany na rynku, korzystający z możliwości obliczeniowych chmury mechanizm analizy zagrożeń i zapobiegania im, opracowany z myślą o trudnych do wykrycia, nieznanych wcześniej exploitach i rodzajach szkodliwego oprogramowania.

WildFire nie tylko wykorzystuje tradycyjne metody wykrywania nieznanych zagrożeń, lecz także łączy zalety wielu uzupełniających się technik o dużej precyzji i skuteczności, takich jak analiza dynamiczna i statyczna, uczenie maszynowe i analiza z wykorzystaniem serwerów fizycznych (bare-metal analysis). Usługa WildFire pozwala wprowadzać kolejne innowacyjne mechanizmy wykrywania zagrożeń bez utrudnień operacyjnych, które występują w tradycyjnych rozwiązaniach analizy opartych na czasowym buforowaniu analizowanego połączenia lub plików w wydzielonym środowisku, a następnie ich uwalnianiu. Specjaliści ds. zabezpieczeń mogą zaoszczędzić sporo czasu i zasobów dzięki szczegółowym informacjom na temat sposobów działania zidentyfikowanych zagrożeń, oznak naruszenia bezpieczeństwa oraz sposobów blokowania ataków.

Wykorzystując ciągle udoskonalane modele zagrożeń, WildFire udostępnia również innowacyjny mechanizm działający na firewallach w konfiguracji inline, który jest oparty na uczeniu maszynowym. Mechanizm ten działa na fizycznych i wirtualnych firewallach nowej generacji Palo Alto Networks. To nowatorskie, niewymagające sygnatur rozwiązanie chroni przed szkodliwym oprogramowaniem, takim jak nieznane wcześniej pliki wykonywalne oraz niebezpiecznymi atakami bezplikowymi opartymi na PowerShell. Ochrona jest realizowana w sposób całkowicie bezpośredni, z pominięciem etapu wysyłania i analizy danych w chmurze.

Z usługi WildFire korzysta największa w branży zabezpieczeń rzesza klientów i partnerów technologicznych, którzy wykorzystują analizę szkodliwego oprogramowania, zyskują informacje o zagrożeniach występujących w sieciach, na hostach i w środowiskach chmurowych. Gdy WildFire wykrywa nowy exploit lub szkodliwe oprogramowanie w środowisku jednego z subskrybentów, przekształca wyniki analizy w reguły ochrony, które automatycznie są rozsyłane i stają się dostępne dla innych subskrybentów na całym świecie. Cały proces realizowany jest w ciągu sekund od pierwszego wykrycia zagrożenia.

IoT Security

Zabezpieczenia urządzeń IoT dla przedsiębiorstw i służby zdrowia

IoT Security to najbardziej wszechstronne na rynku rozwiązanie do ochrony Internetu Rzeczy. Udostępnia na jednej platformie - firewallach Palo Alto Networks i w usłudze Prisma Access - funkcje wykrywania urządzeń IoT, ich klasyfikacji, zapobiegania zagrożeniom i wdrażania reguł rozpoznawania i ochrony opartych na uczeniu maszynowym. Jest to jedyny produkt, który wykorzystuje uczenie maszynowe w powiązaniu z technologią identyfikacji aplikacji App-ID i telemetrią opartą na danych gromadzonych przez firewalle pracujące w różnych środowiskach.

Umożliwia tworzenie profili wszystkich urządzeń, nawet tych wcześniej nieznanych i niezidentyfikowanych w sieci. Dokonuje także wykrywania zagrożeń i anomalii, oceny ryzyka, analizy luk w zabezpieczeniach oraz tworzy rekomendacje reguł bezpieczeństwa, które mogą być następnie wdrożone na firewallach nowej generacji Palo Alto Networks. Udostępnia wbudowane funkcje automatycznego i bezpośredniego zapobiegania atakom zamiast powszechnego w innych rozwiązaniach IoT podejścia opartego tylko na generowaniu alertów, co opóźnia tym samym moment faktycznego wyeliminowania zagrożenia. IoT Security chroni urządzenia IoT przed zagrożeniami, wykorzystaniem ich podatności i luk w zabezpieczeniach. Ponadto klientom z sektora służby zdrowia zapewnia większy zwrot z inwestycji w specjalizowane urządzenia medyczne i umożliwia lepszą obsługę pacjentów dzięki szczegółowej inwentaryzacji urządzeń w sieci, precyzyjnym informacjom dotyczącym ich wykorzystania oraz rozszerzonej ochronie.

Rozwiązanie IoT Security jest łatwe we wdrożeniu. Można je bezproblemowo zintegrować z dotychczasowymi platformami firewall Palo Alto Networks, co zmniejsza obciążenie zespołów odpowiedzialnych za infrastrukturę IoT, bezpieczeństwo i sieć. Specjalistom ds. zabezpieczeń produkt ten zapewnia inteligentną analizę danych o urządzeniach IoT, a ponadto pozwala na łatwą integrację z systemami zarządzania zasobami (CMMS/ITSM), kontroli dostępu do sieci (NAC) oraz zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), jak również z bazami danych informacji o urządzeniach specyficznych dla poszczególnych branż.

Rozwiązanie IoT Security może zostać z powodzeniem wykorzystane w przedsiębiorstwach, placówkach służby zdrowia, środowiskach ICS/SCADA, systemach zarządzania budynkami, w infrastrukturze inteligentnych miast, przemyśle naftowo-gazowym, przedsiębiorstwach użyteczności publicznej, transporcie, logistyce, itd.

GlobalProtect

Bezpieczeństwo użytkowników mobilnych

GlobalProtect™ zapewnia komunikację VPN i ochronę połączeń z urządzeń mobilnych i komputerów zdalnych. Rozszerza naszą najlepszą na rynku ochronę przed zagrożeniami na pracowników mobilnych niezależnie od miejsca, w którym się znajdują. Zabezpieczenie to jest wykorzystywane min. w rozwiązaniu Prisma Access w celu zapewnienia zdalnym użytkownikom szyfrowanego dostępu do sieci, zarówno bezagentowego, jak i z wykorzystaniem oprogramowania agenta.

Przedsiębiorstwo może rozszerzyć korporacyjne reguły kontroli dostępu na urządzenia niezarządzane, aplikacje w chmurze i w centrach danych. GlobalProtect umożliwia obsługę komunikacji VPN dla poszczególnych aplikacji mobilnych dzięki integracji z produktami do zarządzania mobilnością w przedsiębiorstwie, takimi jak AirWatch®, Microsoft Intune® i MobileIron®.

Aplikacja agenta GlobalProtect może także zbierać informacje o hoście, na którym działa. Następnie agent przesyła te informacje do bramy GlobalProtect po pomyślnym nawiązaniu połączenia VPN. Brama dopasowuje te informacje do zdefiniowanych profili HIP (ang. Host Information Profile) aby wymusić zastosowanie odpowiedniej polityki bezpieczeństwa dla łączącego się hosta i jego użytkownika. Zapewnia to realizację szczegółowych zabezpieczeń, które powodują, że zdalne hosty otwierające komunikację do zasobów firmowych są odpowiednio utrzymywane i przestrzegają standardów bezpieczeństwa, zanim uzyskają dostęp. Na przykład możliwe jest wymuszenie, aby zdalne urządzenia miały zainstalowaną minimalną wersję oprogramowania antywirusowego, zanim uzyskają dostęp do zasobów.

Rozwiązanie Prisma Access umożliwia pracownikom zdalnym dostęp do sieci w modelu „zero trust". Łączy kontrolę dostępu opartą na rolach (RBAC), pozwala nieprzerwanie monitorować jakość zdalnej pracy użytkowników (ang, Digital Experience Monitoring - DEM) oraz wykrywać zagrożenia realizując te zadania na jednej platformie chmurowej o dużej skalowalności, zapewniającej spójny, zdalny, bezpieczny dostęp każdemu użytkownikowi. Rozwiązanie Prisma Access wykorzystuje ponad 100 lokalizacji dostępowych dla użytkowników i oddziałów na całym świecie. Dzięki najlepszym na rynku poziomom usług (SLA) zapewnia wysoką dostępność, wydajną łączność oraz dostęp do aplikacji i usług z każdego miejsca na świecie. Umożliwia przedsiębiorstwom definiowanie i stosowanie szczegółowych reguł bezpieczeństwa, które ograniczają dostęp do usług i aplikacji na podstawie tożsamości, roli i lokalizacji użytkownika oraz stanu połączeń urządzenia. Regułami tymi można zarządzać z jednej konsoli.

Prisma Access konsoliduje ponad 10 produktów sieciowych i produktów zabezpieczających w formie jednej usługi z zaawansowanymi funkcjami zabezpieczeń. Funkcje te obejmują ochronę przed szkodliwym oprogramowaniem i wykrywanie exploitów, a także zapobieganie wykradaniu poświadczeń poprzez inspekcję całej komunikacji związanej z aplikacjami na wszystkich portach przez cały czas. Pozwala tworzyć i egzekwować bardziej skuteczne reguły bezpieczeństwa.

Zabezpieczenia przeznaczone dla sieci 5G

Bezpieczeństwo sieci 5G

Wiele przedsiębiorstw przeprowadza dziś transformację cyfrową. W celu dokonania dogłębnej transformacji opartej na koncepcji Przemysłu 4.0 będą one potrzebować nie tylko takich technologii jak chmura, automatyzacja, sztuczna inteligencja i IoT, lecz także sieci 5G. Technologia 5G sprawia, że firmy w większym stopniu korzystają z zalet chmury obliczeniowej i przetwarzania na brzegu sieci. Powstaje wysoce rozproszone środowisko obejmujące infrastrukturę, na którą składają się środowiska w wielu chmurach i produkty wielu dostawców.

Firma Palo Alto Networks oferuje rozwiązanie zabezpieczające opracowane specjalnie z myślą o sieciach 5G. Jest to najbardziej precyzyjne zabezpieczenie dla rdzenia sieci 5G działających w chmurze, rozproszonych chmurach i na brzegu sieci oraz dla korporacyjnych sieci 5G. W ramach tego rozwiązania dostępna jest prosta, ściśle zintegrowana platforma zabezpieczeń 5G, w której wykorzystano automatyzację, funkcje ochrony środowiska Kubernetes® oraz integrację z otwartymi interfejsami API w celu uproszczenia zarządzania. Zautomatyzowana analiza zagrożeń z wykorzystaniem uczenia maszynowego chroni przed atakami cyberprzestępców działając z szybkością dostosowaną do standardów sieci 5G. Zapobiega też znanym i nieznanym zagrożeniom w czasie rzeczywistym w sieciach 5G na skalę globalną. Na tej bazie możliwe jest oferowanie bezpiecznych rozwiązań sieciowych jako usług w sieci 5G, zabezpieczeń dla korporacyjnych sieci 5G oraz zabezpieczeń wielodostępowego środowiska realizującego przetwarzanie na brzegu sieci (ang. multi-access edge computing – MEC).

Rozwiązanie zabezpieczające przeznaczone dla sieci 5G jest obsługiwane na fizycznych firewallach serii PA-7000 i PA-5200, firewallach nowej generacji serii VM w postaci maszyn wirtualnych dla zwirtualizowanych wdrożeń 5G oraz firewallach nowej generacji serii CN przeznaczonych dla chmurowych wdrożeń kontenerowych 5G. Oznacza to, że jeśli firma używa już firewalli Palo Alto Networks, może nadal korzystać z tej samej platformy, aby zabezpieczyć infrastrukturę dostawcy usług 5G lub korporacyjną sieć 5G.

SD-WAN

Bezpieczna komunikacja między oddziałami

Subskrypcja SD-WAN dla firewalli nowej generacji Palo Alto Networks umożliwia firmie łatwe wdrożenie kompleksowej architektury sieci WAN sterowanej programowo, zawierającej połączone najlepsze na rynku funkcje zabezpieczeń i komunikację sieciową.

Dzięki integracji na jednej platformie firewalla nowej generacji mechanizmów bezpieczeństwa z elastycznym definiowaniem zasad realizacji połączeń sieciowych wykorzystującym rozpoznawanie aplikacji, przedsiębiorstwa obniżają koszty utrzymania infrastruktury, dostosowują swoje działanie do procesów transformacji cyfrowej i stopniowego, coraz szerszego wykorzystania zasobów i aplikacji korzystających z chmury.

Panorama - centralny system zarządzania polityką bezpieczeństwa a jednocześnie zasadami korzystania z różnych rodzajów połączeń sieciowych dostępnych w oddziałach oraz węzłach sieci firmy - upraszcza implementację, zarządzanie i utrzymanie rozbudowanych i rozproszonych środowisk. Wdrożenie SD-WAN jest dodatkowo ułatwione dzięki wyposażeniu firewalli w mechanizm automatycznego, bezobsługowego podłączenia do systemu centralnego zarządzania (ang. zero touch provisioning) i pobranie stamtąd konkretnej, dedykowanej polityki bezpieczeństwa i zasad komunikacji sieciowej bez udziału specjalisty sieciowego w miejscu wdrożenia.

PRISMA
BY PALO ALTO NETWORKS

Prisma

Prisma™ to najlepsza na rynku oferta zabezpieczeń środowisk chmurowych. Chcesz przyspieszyć transformację cyfrową w swojej firmie? Wykorzystaj specjalnie zaprojektowany pakiet produktów, aby już dziś zabezpieczyć chmurę przed zagrożeniami, które pojawią się w przyszłości.


Prisma SaaS


Prisma SD-WAN


Prisma Access


Prisma Cloud

Prisma Cloud

Platforma zabezpieczająca chmury publiczne

Prisma Cloud to kompleksowa platforma zabezpieczeń zbudowana z myślą o środowiskach chmurowych (ang. Cloud Native Security Platform — CNSP). Zawiera najszerszy na rynku zestaw zabezpieczeń i mechanizmów kontroli zgodności z regulacjami i wytycznymi dla wszystkich elementów technologii chmurowych, aplikacji i danych — zarówno w przypadku środowisk hybrydowych, jak i wielo-chmurowych.

Prisma Cloud chroni rodzime aplikacje chmurowe na hostach, w kontenerach, środowiskach bezserwerowych i rozwiązaniach PaaS („platform-as-a-service") działających na różnych platformach chmurowych. W dynamiczny sposób wykrywa wdrażane zasoby i dokonuje korelacji danych udostępnianych przez usługi chmurowe (konfiguracji zasobów, dzienników przepływu, dzienników audytowych, dzienników hostów i kontenerów itp.), aby uzyskać szczegółowe informacje o bezpieczeństwie i zgodności środowisk i aplikacji chmurowych. Wykorzystuje funkcje uczenia maszynowego do profilowania działań użytkowników, obciążeń i aplikacji, aby wcześnie wykrywać i zapobiec zaawansowanym cyberatakom.

Największa na rynku biblioteka procedur i reguł zgodności z wytycznymi bezpieczeństwa i regulacjami prawnymi znacznie upraszcza realizację zadań związanych z zachowaniem zgodności z przepisami. Jest to możliwe dzięki opcji udostępniania szczegółowego kontekstu obejmującego infrastrukturę, usługi PaaS, użytkowników, platformy programistyczne, dane i działanie aplikacji. Mechanizmy integracji Prisma Cloud z narzędziami do zarządzania zabezpieczeniami umożliwiają szybką, automatyczną reakcję na pojawienie się

zagrożeń i luk w zabezpieczeniach.

W celu zapewnienia bezpieczeństwa chmury przez cały cykl życia, rozwiązanie Prisma Cloud jest zintegrowane z narzędziami DevOps, co pozwala na zarządzanie lukami w zabezpieczeniach i kontrolę zgodności działania aplikacji z regułami i dobrymi praktykami. Wykorzystując bogaty zestaw wtyczek DevOps, obejmujących technologie IDEs, SCM, CI (ang. Continuous Implementation) i CD (ang. Continuous Delivery), specjaliści ds. zabezpieczeń i DevOps mogą zabezpieczyć infrastrukturę i aplikacje, w tym szablony, hosty, obrazy i funkcje infrastruktury w formie kodu (IaC) od początku tworzenia aplikacji do jej uruchomienia i utrzymania w środowisku produkcyjnym.

Prisma SaaS

Bezpieczeństwo aplikacji SaaS i kontrola ich zgodności z regulacjami dotyczącymi ochrony danych

Rozwiązanie Prisma SaaS umożliwia bezpieczne przejście na pracę z aplikacjami w chmurze dzięki opcjom monitorowania, mechanizmom zapewnienia zgodności z regulacjami oraz spójnym zabezpieczeniom aplikacji SaaS (Software-as-a-Service) i wrażliwych danych tam przetwarzanymi i przechowywanymi. Pozwala zminimalizować zakres wykorzystania niestandardowych i niedopuszczonych do użytku zasobów informatycznych, zabezpieczyć dostęp do korporacyjnych aplikacji SaaS, takich jak Microsoft 365™, Salesforce®, Google Workspace™, Slack® i Box, a także ograniczyć ryzyko naruszenia ochrony danych w chmurze.

Prisma SaaS zabezpiecza środowisko organizacji i jej dane przed zagrożeniami występującymi w chmurze, umożliwia bezpieczne korzystanie z aplikacji SaaS i pozwala bez ryzyka przechowywać dane wrażliwe w chmurze. Jako zintegrowana funkcja firewalli nowej generacji firmy Palo Alto Networks oraz dzięki połączeniu z zaawansowanym rozwiązaniem DLP, usługa ta jest ściśle powiązana z zabezpieczeniami obejmującymi całe przedsiębiorstwo. Dzięki uproszczonemu procesowi wdrażania przewyższa fragmentaryczne modele punktowych mechanizmów kontrolnych, takie jak CASB (Cloud Access Security Broker).

Prisma Access

Bezpieczeństwo użytkowników mobilnych zapewnione w chmurze

Usługa Prisma Access wprowadza nowy model ochrony sieci, który jest oparty na najbardziej kompleksowej w branży platformie udostępnianej w chmurze. Umożliwia on przedsiębiorstwom bezpieczną obsługę pracowników zdalnych. Starsze produkty do ochrony sieci nie zapewniają dostępu do wszystkich aplikacji ani ich nie chronią. Pozostawiają znaczne luki w zabezpieczeniach i nie pozwalają na pracę z dowolnego miejsca, która jest dziś koniecznością w wielu firmach. Prisma Access to jedyne rozwiązanie, które kontroluje ruch danych obejmujący wszystkie aplikacje, w tym przeglądarkowe, nie korzystające z przeglądarek web i szyfrowane za pomocą protokołów SSL/TLS, dwukierunkowo na wszystkich portach. Niezależnie od tego, czy chodzi o komunikację z Internetem, chmurą, centrum danych, czy też o komunikację między oddziałami. Zmniejsza to prawdopodobieństwo naruszenia i nieuprawnionego dostępu do danych o 45%.

Ponadto Prisma Access zapewnia większy zakres ochrony niż inne rozwiązania. Konsoliduje wiele produktów na jednej platformie, która obejmuje firewalla jako usługę (FWaaS), dostęp do sieci oparty na modelu „zero trust" (ZTNA), CASB, bezpieczną bramę internetową (SWG) i wiele innych elementów zarządzanych z jednej konsoli.

Rozwiązanie Prisma Access umożliwia pracownikom zdalnym dostęp do sieci stosując kontrolę dostępu opartą na rolach (RBAC), pozwala nieprzerwanie monitorować jakość zdalnej pracy użytkowników (ang, Digital Experience Monitoring - DEM) zapewniającej spójny, zdalny, bezpieczny dostęp każdemu użytkownikowi.

Rozwiązanie Prisma Access jest zbudowane na bazie sieci o dużej skalowalności. Wykorzystuje połączoną infrastrukturę platformy Amazon Web Services (AWS®) i Google Cloud Platform (GCP). Obejmuje ponad 100 punktów dostępu do usługi w 76 krajach. Dzięki temu Prisma Access zapewnia minimalne opóźnienia wsparte przez najlepsze w branży poziomy usług (SLA), co dla użytkowników oznacza wysoką jakość korzystania z usług.

Prisma SD-WAN

Optymalna komunikacja sieciowa i ochrona oddziałów przedsiębiorstw

Prisma SD-WAN to pierwsze na rynku rozwiązanie typu SD-WAN nowej generacji, które umożliwia ochronę oddziałów przedsiębiorstwa w chmurze. Przynosi zwrot z inwestycji na poziomie nawet 243%. Zapewnia znacznie większy komfort użytkowania w porównaniu ze starszymi i bardziej skomplikowanymi rozwiązaniami SD-WAN. Rozwiązanie Prisma SD-WAN jest oparte na regułach bezpieczeństwa z wykorzystaniem definicji aplikacji. Dzięki zastosowaniu uczenia maszynowego i automatyzacji upraszcza obsługę sieci i diagnozę problemów, jakie mogą w niej wystąpić.

Prisma SD-WAN wykorzystuje dedykowane platformy dostępowe w postaci urządzeń fizycznych lub maszyn wirtualnych dobieranych pod kątem wydajności i wyposażenia w interfejsy sieciowe.

Bezproblemowa integracja Prisma SD-WAN z Prisma Access pozwala na stworzenie najbardziej zaawansowanego na rynku, gotowego do użycia systemu SASE (ang. Secure Access Service Edge), zgodnego z wytycznymi firmy Gartner na temat przyszłości sieci komunikacyjnych współpracujących z przetwarzaniem danych w chmurze. Rozwiązanie SASE to połączenie sieci rozległych (WAN) i usług bezpieczeństwa sieci, takich jak CASB, FWaaS i Zero Trust, w jeden model usługowy dostarczany z chmury i w chmurze.

CORTEX®
BY PALO ALTO NETWORKS

Cortex

Cortex® to najbardziej wszechstronny na rynku pakiet produktów do obsługi operacji bezpieczeństwa. Udostępnia przedsiębiorstwom najlepsze funkcje zarządzania obszarami narażonymi na ataki, wykrywania zagrożeń i zapobiegania im, automatyzacji procesów i reagowania na incydenty.

AF AutoFocus

Cortex XDR

Cortex XSOAR

CRYPSIS™ A PALO ALTO NETWORKS COMPANY Crypsis

EXPANSE A PALO ALTO NETWORKS COMPANY Expanse

Cortex XDR

Rozbudowane funkcje wykrywania i reagowania

Cortex XDR™ to pierwsza w branży rozszerzona platforma wykrywania i przeciwdziałania zagrożeniom oraz reagowania na nie, która wykorzystuje różne źródła danych o bezpieczeństwie w celu powstrzymania zaawansowanych ataków. Pozwala przebić się przez szum informacyjny i skupić na realnych zagrożeniach, w czym pomagają funkcje inteligentnego grupowania alertów i oceny istotności incydentów. Zespoły SecOps mogą zmniejszyć złożoność infrastruktury bezpieczeństwa przedsiębiorstwa przez zastąpienie odrębnych, punktowych produktów jednolitą platformą przeznaczoną do zapobiegania zagrożeniom, ich wykrywania i analizy oraz odpowiedniego reagowania na incydenty bezpieczeństwa.

Cortex XDR automatycznie zabezpiecza urządzenia końcowe (hosty) blokując ataki na nie i precyzyjnie wykrywa zagrożenia w środowisku przedsiębiorstwa, analizując duże ilości różnorodnych danych z wykorzystaniem analizy behawioralnej, profilowania zachowania sieci i użytkowników, statycznej i dynamicznej analizy kodu, uczenia maszynowego. Tworzy pełny obraz każdego incydentu odtwarzając jego przebieg i pomaga znaleźć pierwotną przyczynę problemów, dzięki czemu proces analizy zagrożeń można zrealizować nawet ośmiokrotnie (8x) szybciej niż dotąd. Zaawansowane funkcje przeszukiwania danych gromadzonych przez agentów Cortex XDR umożliwiają pro-aktywne wyszukiwanie zagrożeń (ang. threat hunting). Produkt umożliwia izolowanie podejrzanych hostów podczas ich pogłębionej analizy, wykonywanie zdalnych połączeń typu live-terminal do urządzeń końcowych, uruchamianie własnych skryptów na stacjach i serwerach, zatrzymywanie podejrzanych procesów, blokowanie podejrzanych plików w kwarantannie, itd.

Cortex XDR obsługuje całą gamę systemów operacyjnych stosowanych przez przedsiębiorstwa (MS Windows, Apple Macos, Linux, Android), aby zapewnić jak najszersze pokrycie i funkcje bezpie-

czeństwa niezależnie od sposobu korzystania z zasobów firmy.

Ten wyjątkowy produkt upraszcza każdy etap operacji związanych z bezpieczeństwem, od określania priorytetów alertów po wykrywanie zagrożeń. Zmniejsza obciążenie wysokokwalifikowanych analityków bezpieczeństwa i znacznie skraca czas potrzebny na wykrywanie i analizę zagrożeń oraz odpowiednie reagowanie na nie. Ścisła integracja z firewallami nowej generacji skraca proces izolacji zagrożenia, co pozwala powstrzymać nawet najbardziej podstępne ataki, zanim spowodują poważne szkody.

Cortex XSOAR

Rozwiązanie do koordynacji i automatyzacji zabezpieczeń oraz reagowania na incydenty

Cortex™ XSOAR pozwala znacznie zwiększyć efektywność działania centrum operacji bezpieczeństwa SOC, dzięki zastosowaniu najbardziej wszechstronnej na rynku platformy koordynacji działań podczas obsługi incydentów bezpieczeństwa, automatyzacji i reagowania SOAR (ang. Security Orchestration, Automation and Response). Specjaliści ds. zabezpieczeń zyskują możliwość transformacji i optymalizacji praktycznie dowolnych powtarzalnych procesów i aspektów działań operacyjnych.

W rozwiązaniu zastosowano jednolite metody zarządzania incydentami, automatyzacji, współpracy w czasie rzeczywistym i zarządzania informacjami analitycznymi. Poszczególne zespoły reagowania mogą obsługiwać alerty pochodzące z wielu źródeł, standaryzować i automatycznie wykonywać procesy obsługi wg scenariuszy działań (ang. playbooks), podejmować kroki na podstawie analizy zagrożeń oraz automatyzować reakcje w każdym obszarze związanym z zabezpieczeniami. Według doświadczeń naszych klientów, czas reakcji na incydent można skrócić nawet o 90%, a liczbę alertów wymagających ręcznej interwencji analityka SOC zmniejszyć o 95%.

Cortex XSOAR pomaga zwiększyć także korzyści z używania innych produktów bezpieczeństwa w przedsiębiorstwie, dzięki ich integracji i koordynacji danych i czynności, w automatyczny sposób prowadząc działania podczas wystąpienia incydentu bezpieczeństwa lub dla jego zapobieżenia.

Otwartość i elastyczność platformy Cortex XSOAR umożliwia zastosowanie jej nie tylko w obszarze bezpieczeństwa IT, ale również wszędzie tam gdzie mamy do czynienia z powtarzalnymi, żmudnymi, nierzadko wykonywalnymi manualnie zadaniami - np. nadzór nad sieciami, w działaniach HR, administracji zasobami firmy, itp.

Moduł TIM (ang. Threat Intel Management) platformy Cortex XSOAR umożliwia centralne gromadzenie, zarządzanie i udostępnianie innym systemom atrybutów ataków, które pozwalają na ich szybką identyfikację (ang. Indicator of Compromise - IoC). Dzięki wbudowanym i ciągle aktualizowanym skryptom integracji ze źródłami wiedzy o zagrożeniach (ang. threat intel) - w tym z AutoFocus - oraz możliwości tworzenia własnych połączeń z takimi źródłami, działy bezpieczeństwa w przedsiębiorstwie zyskują wydajny, centralny zasób danych o atakach, który pozwala na wczesne ostrzeżenie o zagrożeniu i zminimalizowanie ryzyka jego wystąpienia.

AutoFocus

Kontekstowa informacja o zagrożeniach

Usługa kontekstowej analizy zagrożeń AutoFocus™ zapewnia bezpośredni dostęp do ogromnego repozytorium wiarygodnych informacji analitycznych, które można wykorzystywać podczas obsługi incydentów bezpieczeństwa oraz aby im zapobiegać.

Informacje te są gromadzone i obejmują największy w branży zestaw źródeł analitycznych dotyczących sieci, urządzeń końcowych i środowisk chmurowych, dzięki czemu klienci uzyskują wyjątkowy wgląd w najnowsze rzeczywiste zagrożenia. Informacje o zagrożeniach wzbogacane są o kontekst przygotowany przez zespół renomowanych specjalistów zespołu Unit 42 Palo Alto Networks. Analitycy bezpieczeństwa w przedsiębiorstwie, mogą zaoszczędzić sporo czasu podczas analizy incydentów i wyszukiwaniu zagrożeń dzięki informacjom udostępnianym przez AutoFocus, także za pośrednictwem interfejsu API.

Crypsis

Usługi reagowania na incydenty

Crypsis Group, spółka należąca do Palo Alto Networks, to zespół specjalistów świadczący usługi doradcze w dziedzinie cyberbezpieczeństwa oraz pomagający w analizie i postępowaniu po wystąpieniu incydentu.

Usługi Crypsis pomagają przedsiębiorstwom w tworzeniu i utrzymaniu bezpiecznego cyfrowego środowiska poprzez udostępnianie najwyższej jakości usług reagowania na incydenty, zarządzania ryzykiem i informatyki śledczej. Pomagamy naszym klientom w obronie przed groźnymi cyberatakami i reagowaniu na nie. Zespół Crypsis jest w stanie reagować na incydenty w skali globalnej. Ciągle wprowadzamy innowacje technologiczne i dysponujemy najwyższej klasy specjalistami w dziedzinie cyberbezpieczeństwa. Wszystko to sprawia, że nasze usługi pomagają firmom w walce z szybko ewoluującymi zagrożeniami.

Expanse

Zarządzanie obszarem narażonym na ataki

Expanse to zautomatyzowana platforma do identyfikacji i zarządzania obszarami narażonymi na ataki (ang. attack surface management – ASM). Udostępnia ona pełny i dokładny wykaz globalnych zasobów przedsiębiorstwa mających kontakt z Internetem oraz wykrywa błędy w konfiguracji środowiska IT firmy oraz w dostępie do zasobów organizacji. Znajdowanie problemów i eliminowanie ich przed pojawieniem się ataku z ich użyciem ma zasadnicze znaczenie dla zachowania integralności bezpieczeństwa firmy.

Expanse umożliwia ciągłe wykrywanie, ocenę i ograniczanie obszarów narażonych na ataki. Oznakowuje ryzykowne połączenia do zasobów, analizuje zagrożenia związane z dostawcami usług oraz ocenia bezpieczeństwo IT podczas potencjalnych fuzji i przejęć, bez konieczności instalacji agentów i dodatkowego oprogramowania.