ROZWIĄZANIA BROADCOM

Kompleksowa ochrona danych, informacji, dokumentów, aplikacji i infrastruktury IT

Oferta firmy Broadcom skierowana do dużych oraz średnich firm i instytucji zabezpiecza różne kanały komunikacji, która odbywa się przy pomocy poczty elektronicznej, protokołu http, chmury bez względu, czy mamy do czynienia z ruchem szyfrowanym czy nie.

Oferowane rozwiązania zapewniają:

ochronę przed wyciekiem informacji (DLP) - kompleksowe rozwiązanie do ochrony przed wyciekiem informacji działające w formie agentów na stacjach końcowych i jako moduł sieciowy. Chroni poufne informacje bez względu na ich format i kanał dystrybucji. Analizuje dane w spoczynku, dane w ruchu, dane w użyciu, wspiera również rozwiązania chmurowe.

ochronę stacji końcowych i serwerów - rozwiązania zabezpieczające przed wirusami, robakami, koniami trojańskimi, spywarem, adwarem, rootkitami i atakami typu zero-day. Ochroną objęte są stacje końcowe jak i fizyczne i wirtualne serwery aplikacji, bazy danych zlokalizowane w data center.

bezpieczeństwo komunikacji http - rozwiązania umożliwiające kontrolę nad ruchem w sieci poprzez uwierzytelnianie użytkowników, filtrowanie www, kontrolę i zapewnienie widoczności ruchu szyfrowanego SSL, buforowanie treści, zarządzanie pasmem, rozdzielanie strumienia uzupełnione o narzędzia zabezpieczające przed atakami wykorzystującymi przeglądarkę internetową poprzez wyeliminowanie aktywnej treści.

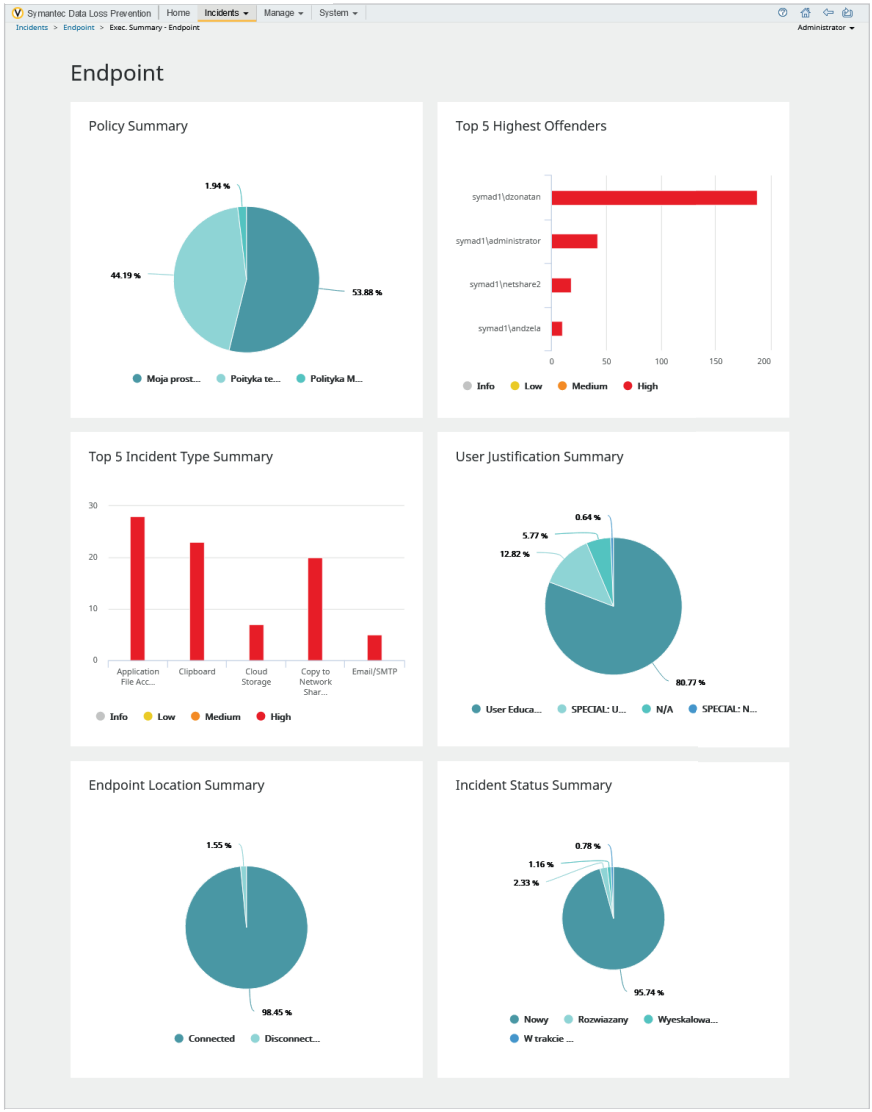
bezpieczeństwo komunikacji e-mail – rozwiązania umożliwiające zabezpieczenie wiadomości przychodzących i wychodzących, ochronę antyspamową i antywirusową w czasie rzeczywistym, zaawansowane filtrowanie treści, ochronę przed utratą danych oraz szyfrowanie komunikacji e-mail.

monitorowanie ruchu szyfrowanego - rozwiązanie do deszyfracji ruchu SSL umożliwiające podgląd i kontrolę wszystkich połączeń szyfrowanych, jakie nawiązują użytkownicy sieci z zewnętrznymi aplikacjami. Potrafi deszyfrować oraz ponownie zaszyfrować ruch SSL, dzięki czemu może dostarczać ruch do pasywnych oraz aktywnych (takich jak IPS, DLP) systemów analizy trzecich firm.

możliwość przeprowadzenia analiz powłamaniowych – rozwiązanie posiadające zaawansowane funkcje badania śladów w sieci i sprawnego reagowania na incydenty, dzięki czemu zespół bezpieczeństwa otrzymuje klarowne i zwięzłe odpowiedzi na kluczowe pytania zadawane po ataku typu kto to zrobił, w jaki sposób, kiedy, do jakich zasobów uzyskano dostęp.

OCHRONA PRZED WYCIEKIEM INFORMACJI/DLP

Rozwiązanie DLP firmy Broadcom wykrywa, monitoruje i chroni poufne dane niezależnie od miejsca ich przechowywania i sposobu użytkowania. Rozwiązanie ogranicza ryzyko utraty danych, chroni organizacje przed stratami finansowymi (GDPR/RODO), zapewnia zgodność z przepisami i procedurami bezpieczeństwa, równocześnie chroniąc dane klientów, wiarygodność marki i własność intelektualną. Działa zarówno w formie agentów na stacjach końcowych i jako moduł sieciowy.



Rozwiązanie DLP firmy Broadcom znajduje się w gronie liderów w raporcie Forrester: Unstructured Data Security Platforms, Q2 2021

DLP for Network

monitoruje łączność sieciową i wykrywa dane wrażliwe przesyłane z naruszeniem polityki bezpieczeństwa. W przypadku wykrycia naruszenia polityki wiadomości są kierowane do bramki szyfrującej, informacje poufne usuwane z postów na stronach www, wiadomości są kierowane do kwarantanny na bezpiecznym serwerze, a transmisje e-mail i www zostają zablokowane.

DLP for Endpoint

wykrywa dane poufne, niezależnie od tego, gdzie one się znajdują, oraz identyfikuje punkty końcowe o najwyższym stopniu ryzyka. Program aktywnie monitoruje też wiele sposobów, w jakie dane poufne mogą być wykorzystywane w punktach końcowych, oraz sygnalizuje wszelkie działania niezgodne z przyjętą polityką

BEZPIECZEŃSTWO STRON WWW

Przeglądarka internetowa jest jednym z głównych źródeł, wykorzystywanych do udanych ataków cybernetycznych. Stosowane są różnorodne techniki złośliwego oprogramowania i socjotechniki, aby nakłonić pracowników do odwiedzenia złośliwych stron internetowych i zainfekowania swoich urządzeń i sieci firmowych

Web Isolation

pozwala na ochronę przed atakami wykorzystującymi przeglądarkę internetową. Użytkownikowi korzystającemu z rozwiązania wyświetla się w oknie bezpieczna graficzna reprezentacja strony, do której się odwoływał. Dzięki temu pozbywamy się problemu z aktywną treścią w postaci JavaScriptu, CSS, czy podatności w samych obrazkach umieszczonych na stronie. Użytkownik może normalnie używać strony, a jednocześnie jego urządzenie jest chronione. Rozwiązanie jest dodatkiem do systemu proxy, z którym Web Isolation się integruje, niezależnie od producenta.

Proxy Secure Gateway (Proxy SG)

pozwala na szybkie kategoryzowanie stron www pod kątem dostarczanej zawartości oraz bezpieczeństwa, oraz nadawanie adresom URL odpowiedniej oceny od 1 do 10, która odzwierciedla poziom jego ryzyka. W połączeniu z geolokalizacją daje użytkownikom możliwość bardzo szczegółowej kontroli ruchu.

BEZPIECZEŃSTWO KOMUNIKACJI E-MAIL

Messaging Gateway

skutecznie reaguje na nowe zagrożenia pocztowe i oferuje ochronę przeciw spamowi i oprogramowaniu złośliwemu w czasie rzeczywistym, zaawansowaną ochronę przed zagrożeniami oraz technologie zapobiegania utracie danych. Integruje się z mechanizmem Symantec Content and Malware Analysis, aby zapewnić dodatkowe możliwości zaawansowanej ochrony przed zagrożeniami.

Desktop Email Encryption (PGP)

automatycznie szyfruje i odszyfrowuje wiadomości e-mail bezpośrednio między klientami. E-mail pozostaje zaszyfrowany na wewnętrznych serwerach pocztowych lub podczas wysyłania e-maili do chmury.

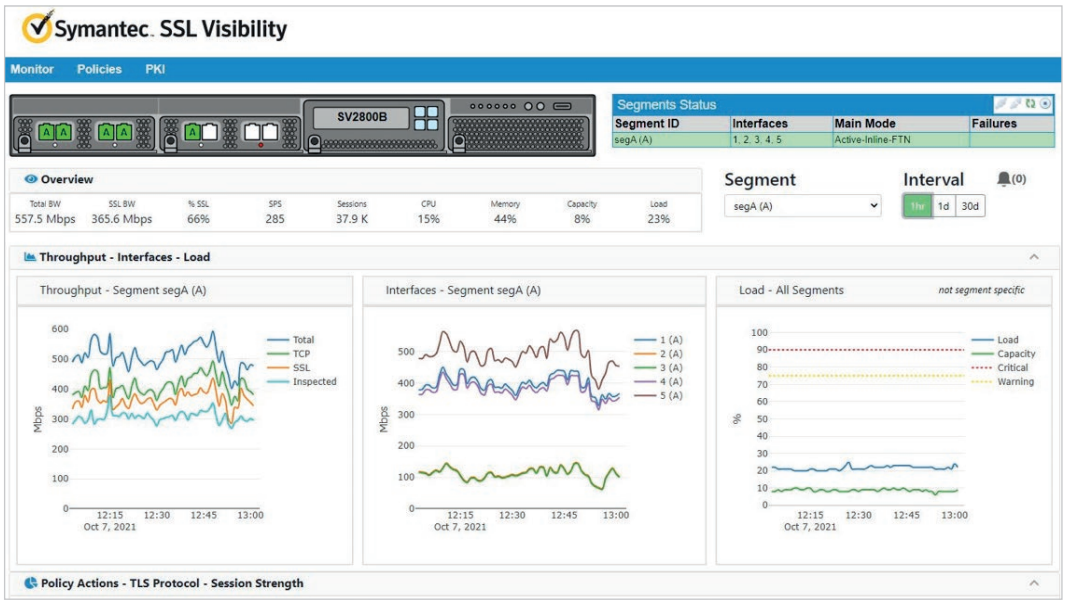
MONITOROWANIE RUCHU SZYFROWANEGO

Udział ruchu szyfrowanego SSL/TLS nieustannie wzrasta, co oznacza, że jego monitorowanie jest niezbędne, aby dostarczyć kompletnych informacji:

- systemom DLP aby mogły wychwytywać wycieki,
- systemom IDS/IPS, antymalware aby mogły chronić stacje robocze przed zagrożeniami typu malware czy ataki APT.

SSL Visibility (SSL-V)

rozpoznaje ruch SSL niezależnie od portu oraz aplikacji, a następnie deszyfruje go, w celu przesłania pakietów do analizy przez dowolny system – np. IPS, AV, sandbox, zaawansowanej analizy czy logowania. Dodatkowo możliwość kategoryzacji URL pozwala na budowanie polityk wyłączających z dekrypcji ruch traktowany jako poufny np. komunikacja z bankowością online, portalami związanymi z ochroną zdrowia itp.



SSL Visibility potrafi deszyfrować oraz ponownie zaszyfrować ruch SSL, dzięki czemu może dostarczać ruch do pasywnych oraz aktywnych (IPS, DLP) systemów analizy.

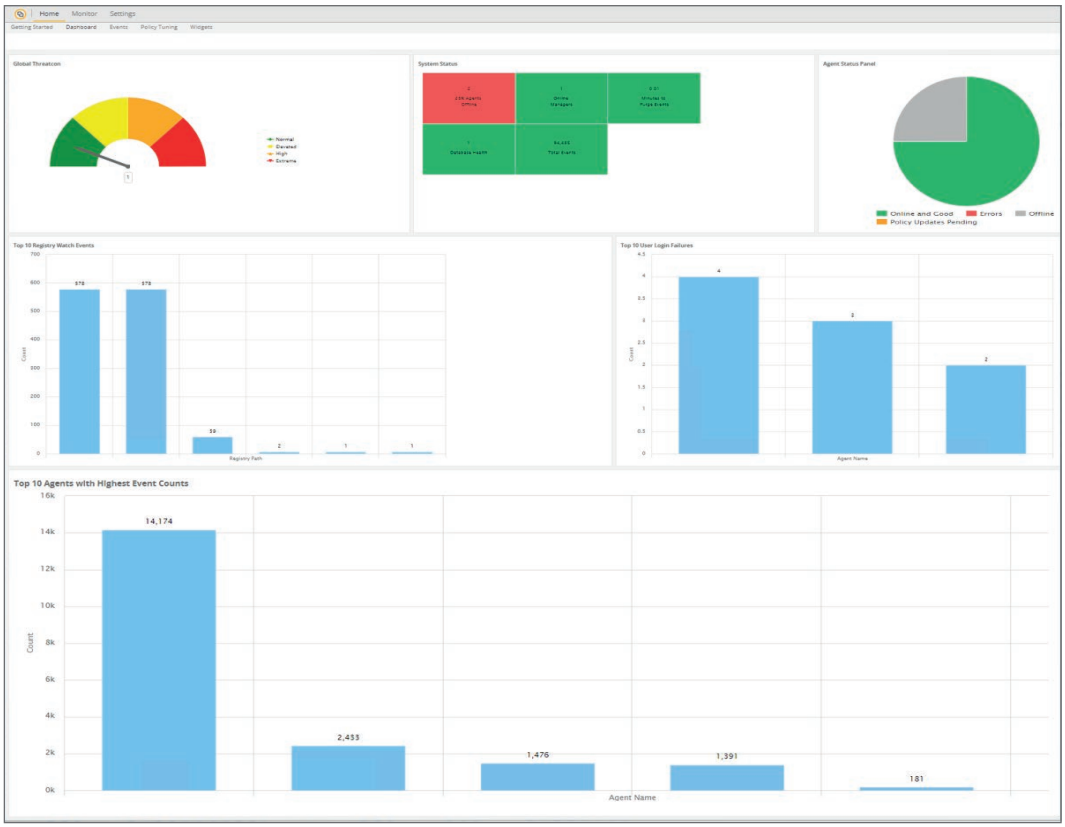
OCHRONA STACJI KOŃCOWYCH I SERWERÓW

Endpoint Protection (SEP)

powstrzymuje zaawansowane zagrożenia na stacjach końcowych przy użyciu nowoczesnych technologii - uczenia maszynowego, analizy reputacji plików oraz analizy behawioralnej prowadzonej w czasie rzeczywistym. Dzięki pojedynczej konsoli zarządzania i niewielkim agentom, które mogą integrować się z innymi produktami w obrębie infrastruktury bezpieczeństwa, rozwiązanie zapewnia ochronę punktów końcowych bez ograniczania ich wydajności.

Data Center Security (DCS)

zapewnia bezpieczeństwo serwerów w centrach danych, blokując ataki typu „zero-day" oraz ataki celowane przeciwko serwerom, umożliwia hardening systemów poprzez instalację łat w nowych i starszych systemach operacyjnych, kompleksowo chroni środowiska VMware.



Rozwiązanie Symantec Data Center Security (DCS) zapewnia bezpieczeństwo serwerów w centrach danych, m. in. ułatwiając instalację łat w starszych systemach operacyjnych.

ANALIZA ŚLEDCZA

Współczesne zaawansowane oprogramowanie złośliwe i ataki typu „zero-day" są w stanie ominąć tradycyjne technologie zabezpieczeń. W rezultacie organizacje godzą się z faktem, że w którymś momencie ich sieci zostaną spenetrowane. Z tego powodu obserwuje się ostatnio ruch w stronę bardziej nowoczesnej strategii – kompleksowego podejścia oferującego wiedzę i analizę w czasie rzeczywistym, które są niezbędne, aby móc wykryć i zrozumieć zagrożenia zaawansowane czy ataki celowane oraz zareagować na nie i zabezpieczyć przed nimi sieć.

Security Analytics

rejestruje i klasyfikuje każdy pakiet ruchu w sieci – od warstwy 2 do warstwy 7 – a jednocześnie indeksuje, klasyfikuje, wzbogaca i magazynuje dane w celu zapewnienia kompleksowej wiedzy o zagrożeniach i analizy po fakcie dla każdego zdarzenia z zakresu bezpieczeństwa. Daje specjalistom od bezpieczeństwa klarowne i zwięzłe odpowiedzi na kluczowe pytania zadawane po ataku: Kto to zrobił? W jaki sposób? Kiedy? Do jakich zasobów uzyskano dostęp?