Grupa internet.pl

cryptzone

AppGate Network Security

Bezpieczeństwo zasobów IT

Przejmij pełną kontrolę nad dostępem do zasobów i usług IT chroń je przed nieautoryzowanym dostępem.

Data Leak Prevention

Bezpieczeństwo danych

Zabezpieczaj, szyfruj i blokuj dostęp do wrażliwych danych.

Policy Management

Zarządzanie polityką bezpieczeństwa

Prawdziwa kontrola i edukacja pracowników w zakresie procedur bezpieczeństwa.

cryptzone

Cryptzone Group jest wywodzącym się ze Szwecji producentem systemów bezpieczeństwa IT, działającym na rynku od 2003 roku (pierwsze wdrożenie systemu AppGate – 1997 rok). Grupa została stworzona przez spółkę Cryptzone poprzez przejęcia i połączenia z firmami takimi jak: AppGate Network Security, ControlGuard, NETconsent oraz SE46. Cryptzone dostarcza kompleksowe rozwiązania w pięciu kluczowych obszarach bezpieczeństwa:

- Kontrola dostępu oparta na rolach użytkowników (RBAC),
- Zabezpieczanie i kontrola portów i urządzeń oraz zarządzanie uprawnieniami użytkowników,
- Szyfrowanie i kontrola treści oraz bezpieczeństwo informacji,
- Policy Management oraz eLearning,
- Application Control – White Listing.

Celem Cryptzone Group jest dostarczanie rozwiązań przyjaznych zarówno dla użytkownika jak i administratora przy zachowaniu najwyższego stopnia bezpieczeństwa i maksymalnym zminimalizowaniu ryzyka wycieku informacji. Siedziba główna znajduje się w Goeteborgu w Szwecji, ponadto firma posiada oddziały w: Austrii, Holandii, Izraelu, Polsce, Stanach Zjednoczonych oraz Wielkiej Brytanii. Działalność handlową prowadzi poprzez sieć ponad 150 firm partnerskich i dystrybutorów. Akcje Cryptzone notowane są na Giełdzie First North w Sztokholmie.

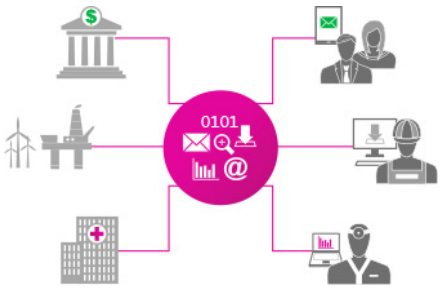
AppGate Network Security

Bezpieczeństwo zasobów IT

AppGate Security Server jest rozwiązaniem zapewniającym kontrolę dostępu do zasobów i usług IT chroniąc je przed nieautoryzowanym dostępem. Kontrola ta opiera się na uprawnieniach użytkownika i przypisanej mu roli w organizacji (RBAC).
System AppGate charakteryzuje się zintegrowaniem wszystkich niezbędnych elementów bezpieczeństwa, takich jak: uwierzytelnienie, autoryzacja, szyfrowanie transmisji (VPN), kontrolę dostępu, kontrolę użytkowników i ich urządzeń, firewall, monitoring, raportowanie oraz alerty bezpieczeństwa.

Działanie: Rozwiązanie AppGate dostarczane jest, jako appliance lub jako system działający na środowisku VMware. AppGate Security Server umieszczany jest pomiędzy urządzeniami użytkowników a serwerami firmy działając, jako certyfikowany firewall.

Komunikacja między użytkownikami i systemem AppGate jest w całości szyfrowana (VPN). Szyfrowanie to odbywa się zarówno przy połączeniach z zewnątrz jak i wewnątrz firmy. Zależnie od typu aplikacji i wrażliwości danych może być stosowany inny algorytm szyfrowania. Każdy użytkownik musi mieć przyznane uprawnienia, aby mógł korzystać z zasobów niezbędnych do wykonania swojej pracy (RBAC). Uprawnienia te mogą być przyznawane indywidualnie lub jako role dla grup użytkowników. W momencie zalogowania użytkownik widzi jedynie te aplikacje, do których ma przyznany dostęp.
Zarządzanie AppGate Security Server jest łatwe i wykonywane z jednego centralnego punktu, daje przy tym możliwość ścisłej kontroli nad użytkownikami i zasobami firmy i nie wymaga zaangażowania dużego zespołu administratorów i służb IT.



Podstawowa funkcjonalność

Zarządzanie rolami i uprawnieniami – dostęp do zasobów jest precyzyjnie granulowany i oparty na przydzielonych rolach. Uprawnienia są przydzielane w oparciu o rolę użytkownika, metodę uwierzytelnienia, rodzaj wykorzystywanego urządzenia, miejsca, z którego użytkownik się loguje (łącznie z podziałem geograficznym), pory dnia jak i innych parametrów zdefiniowanych w polityce bezpieczeństwa firmy. Zarządzanie uprawnieniami, rolami oraz politykami dostępu wykonywane jest centralnie.

Mechanizmy kryptograficzne - cała komunikacja pomiędzy serwerem AppGate a użytkownikami jest szyfrowana, zarówno w połączeniach wewnątrz firmy jak i spoza niej. Appgate wykorzystuje następujące metody szyfrowania: AES (128, 192, 256 bit), Arcfour/ RC4 (128 bit), Blowfish (128 bit), 3-DES-CBC (168 bit). System ma możliwość pracy w tzw. FIPS mode (FIPS 140-2 poziom 1).

Network Admission Control - weryfikacja urządzenia klienta – w momencie uwierzytelniania użytkownika, system AppGate wysyła do PC zestawy reguł dla weryfikacji, że urządzenie umożliwi bezpieczne szyfrowane połączenie podczas sesji i uruchamia moduł kontroli, który przydziela lub blokuje dostęp do zasobów.

Firewall – rozwiązanie posiada dwa typy firewall:
• Osobisty Firewall - gwarantujący, iż urządzenie użytkownika podczas połączenia z zasobami firmy jest w pełni zabezpieczone i nie może zostać wykorzystany, jako back-door dla osób i programów nieuprawnionych,
• Firewall – serwery Appgate występują, jako firewall przed serwerami aplikacyjnymi (certyfikat: Common Criteria Level 2+).

Uwierzytelnianie – AppGate daje możliwość zastosowania dwupoziomowego uwierzytelnienia, np. używając wbudowanej technologii haseł jednorazowych - OTP (One Time Password) lub rozwiązań firm trzecich. Pozostałe metody uwierzytelniania użytkowników: hasła, LDAP, Radius, Token cards, RSA SecurID, Certificates/PKI od VeriSign, Entrust, itd.

Analiza działań użytkowników – wykonywana jest w formie tekstowej i graficznej w czasie rzeczywistym. Informacja ta może być eksportowana w dowolnym formacie jak np. CSV. Elastyczność raportowania w systemie AppGate pozwala również na generowanie własnych zdefiniowanych raportów.

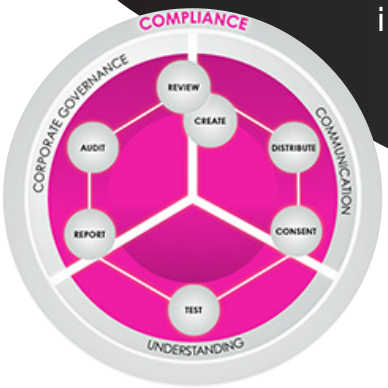
Segmentacja – umożliwiająca oddzielenie sieci i podsieci oraz szczególnie krytycznych systemów i serwerów. Serwer posiada od 4 do 12 interfejsów sieciowych.

Data Leak Prevention

Bezpieczeństwo danych

Kluczowym i nieodzownym modułem DLP jest SEP Server – jest to centralna konsola do zarządzania poszczególnymi modułami. Daje ona możliwość przypisywania uprawnień i ról dla poszczególnych grup lub indywidualnych użytkowników. Umożliwia również synchronizowanie tych danych, np. z AD lub innym LDAP.

System DLP firmy Cryptzone, czyli Simple Encryption Platform może zostać zbudowany z następujących modułów:



Secured eFile – system do szyfrowania plików i folderów zarówno na dyskach lokalnych jak i sieciowych. Wykorzystuje algorytm AES256.

Secured eCollaboration – system do zabezpieczania i szyfrowania zasobów udostępnianych poprzez Microsoft SharePoint. Poza szyfrowaniem z użyciem algorytmu AES256, daje on możliwość właścicielowi pliku przypisywania uprawnień i praw dostępów dla wybranych użytkowników i odbierania tych praw i blokowania dokumentu nawet po jego wgraniu na lokalny dysk użytkownika.

Secured eMail – szyfrowanie poczty elektronicznej. Odbiorca zaszyfrowanej wiadomości ma możliwość odszyfrowania jej i odczytania na dowolnym urządzeniu mobilnym i komputerze dzięki technologii Global Communication.

Secured eDevice – kontroluje i blokuje zdefiniowane porty (np. USB, FireWire) i urządzenia (np. CD/DVD lub WiFi) zabezpieczając przed podłączaniem nieautoryzowanych urządzeń i kopiowaniem danych. Dodatkowo kontroluje i blokuje np. typy plików, pliki o określonej zawartości lub rozmiarze. Przydziela limity kopiowania danych itp.

Secured eUSB – szyfrowanie pamięci/dysków typu USB. System posiada wbudowaną opcję Kill Pil umożliwiającą zdalne wyczyszczenie całej zawartości dysku, zablokowanie lub zmianę hasła. DCR – Data Content Reporting daje możliwość zdalnej inwentaryzacji oraz szczegółowej weryfikacji zawartości dysków USB.

Secured eDisk – pełne szyfrowanie dysków HDD z wykorzystaniem: DES, 3DES, IDEA, AES-128,AES-192, AES-256. Daje możliwość dwustopniowego uwierzytelniania oraz Single Sign On z Windows. Posiada certyfikat Common Cartiera EAL-4 oraz FIPS 140-2 Level 2.

Secured eUSB

Jest to profesjonalne narzędzie, którego głównym celem jest zabezpieczenie danych przechowywanych i przenoszonych na dyskach flash USB, zewnętrznych dyskach HDD oraz płytach CD/DVD. System jest w pełni „customizowany" i może być przystosowany do szczególnych wymagań klienta łącznie z umieszczeniem logo, własnych tekstów itp.

Secured eUSB daje możliwość wymuszania szyfrowania wszelkich dysków USB podłączanych do komputerów firmowych, dzięki czemu mamy możliwość zabezpieczenia danych firmowych. Możemy również umożliwić użytkownikom odczyt danych z dowolnych urządzeń wraz z restrykcją, iż zapis danych odbywa się tylko na zaufane i zaszyfrowane pamięci.

System dedykowany jest szczególnie dla przedsiębiorstw i z myślą o nich posiada dodatkowe funkcjonalności podwyższające poziom bezpieczeństwa oraz nadzór nad danymi firmowymi, urządzeniami i użytkownikami.

Najważniejszymi cechami są:

Kill Pill – w przypadku kradzieży lub zagubienia dysku istnieje możliwość wydania zdalnej komendy: zablokowania, wykasowania zawartości dysku lub zmiany hasła dostępu. Jest to również przydatne w sytuacji, gdy przedsiębiorstwo planuje zwolnienie pracownika i chce zabezpieczyć swoje dane zawarte na dyskach udostępnionych pracownikowi.

Centralna inwentaryzacja – system daje możliwość dokonania kompletnej inwentaryzacji wszystkich dysków USB z przypisaniem ich do nazwanych użytkowników

Centralne raportowanie i audyt – system daje następujące możliwości administratorowi:
- Device report – podstawowe dane o dyskach USB
- Content report – kontrola zawartości dysku USB a w tym: nazwy plików, ostatnie zmiany, rozmiar, przez kogo zmieniony
- Content analysis – kontrola zawartości i działania na każdym pliku
- Origin report – możliwość śledzenia i kontroli, z jakiego źródła pochodzi plik (wraz z podaniem pełnej ścieżki dostępu) i gdzie został przekazany – co w sytuacjach krytycznych może stanowić materiał dowodowy dokumentujący wypływ wrażliwych danych.

Możliwość przypisywania grup użytkowników – daje to możliwść ograniczenia przekazywania danych i rozszyfrowywania dysku jedynie na komputerach upoważnionych pracowników.

Możliwość nadawania ról uprawnionym użytkownikom – Manager – wszelkie prawa do dysku USB, Contributor – jedynie możliwość odczytywania i zapisywania plików, reader – jedynie możliwość odczytywania danych.

Odzyskiwanie haseł – narzędzie umożliwa bezpieczne odzyskanie hasła i odblokowanie dysku przez administratorów lub HelpDesk.

Blokowanie portów – centralna konsola SEP daje możliwość blokowania portów USB. W tym wypadku użytkownik będzie w stanie kopiować i przenosić dane firmowe wyłącznie na, zaszyfrowanych firmowych dyskach USB (za pomocą Secured eUSB). W momencie podłączenia dowolnego dysku/urządzenia – będzie on miał możliwość odczytania danych jednak nie będzie posiadał możliwość zapisania jakichkolwiek danych z komputera firmowego.

Policy Management

Zarządzanie polityką bezpieczeństwa

NETconsent Compliance Suite – narzędzie do proaktywnego i zrównoważonego wdrażania oraz zarządzania cyklem życia polityk, procedur oraz dokumentów towarzyszących. Pomaga on w podniesieniu świadomości oraz zrozumieniu obowiązujących procedur przez pracowników, ułatwia menadżerom nadzorowanie przestrzegania obowiązujących procedur, minimalizuje odpowiedzialność pracodawcy, umożliwia audytorom pomiar zgodności procedur i ich przestrzegania. System składa się z modułów:

NETconsent Policy Manager – umożliwia: zarzadzanie dokumentami (np. Polityka, procedury, wytyczne, standardy, treści e-learningowe), ustalanie grup dystrybucyjnych, zasad postępowania, kontroli i weryfikacji wersji itp.

NETconsent Examiner – umożliwia przeprowadzenie testów i zbadanie poziomu zrozumienia obowiązujących procedur, standardów, wytycznych oraz treści e-learningowych.

NETconsent Assessor – służy do tworzenia i dystrybuowania ankiet, do okresowych ocen i analiz pracowników, ich postaw oraz opinii.

NETconsent Informer – Pozwala na dystrybucję ważnych i kluczowych informacji, przekazywanych dotąd poczta elektroniczną. Wiadomości mogą być przedstawione wybranej grupie użytkowników w wybranym okresie czasu. Mogą być wykorzystywane do tworzenia kampanii informacyjnej, powiadamiania o aktualizacji procedur i polityk.

NETconsent Reporter – daje możliwość kompleksowego raportowania działań we wszystkich modułachNETconsent poprzez analizowanie, śledzenie, prezentowanie oraz zarządzanie ryzkiem i polityką informacji.

Internet.pl Sp. z o.o.
ul. Achera 9a
02-495 Warszawa
+48 22 867-80-00
www.internet.pl/cryptzone