HYPROVISION **DLP**

www.hyprovision.com

Data Loss Prevention

Kompleksowa ochrona przed wyciekiem danych

Kontrola urządzeń

Klasyfikacja i ochrona treści

Znakowanie dokumentów

Szyfrowanie

Budowanie świadomości

Hyprovision DLP – skuteczny system klasy DLP

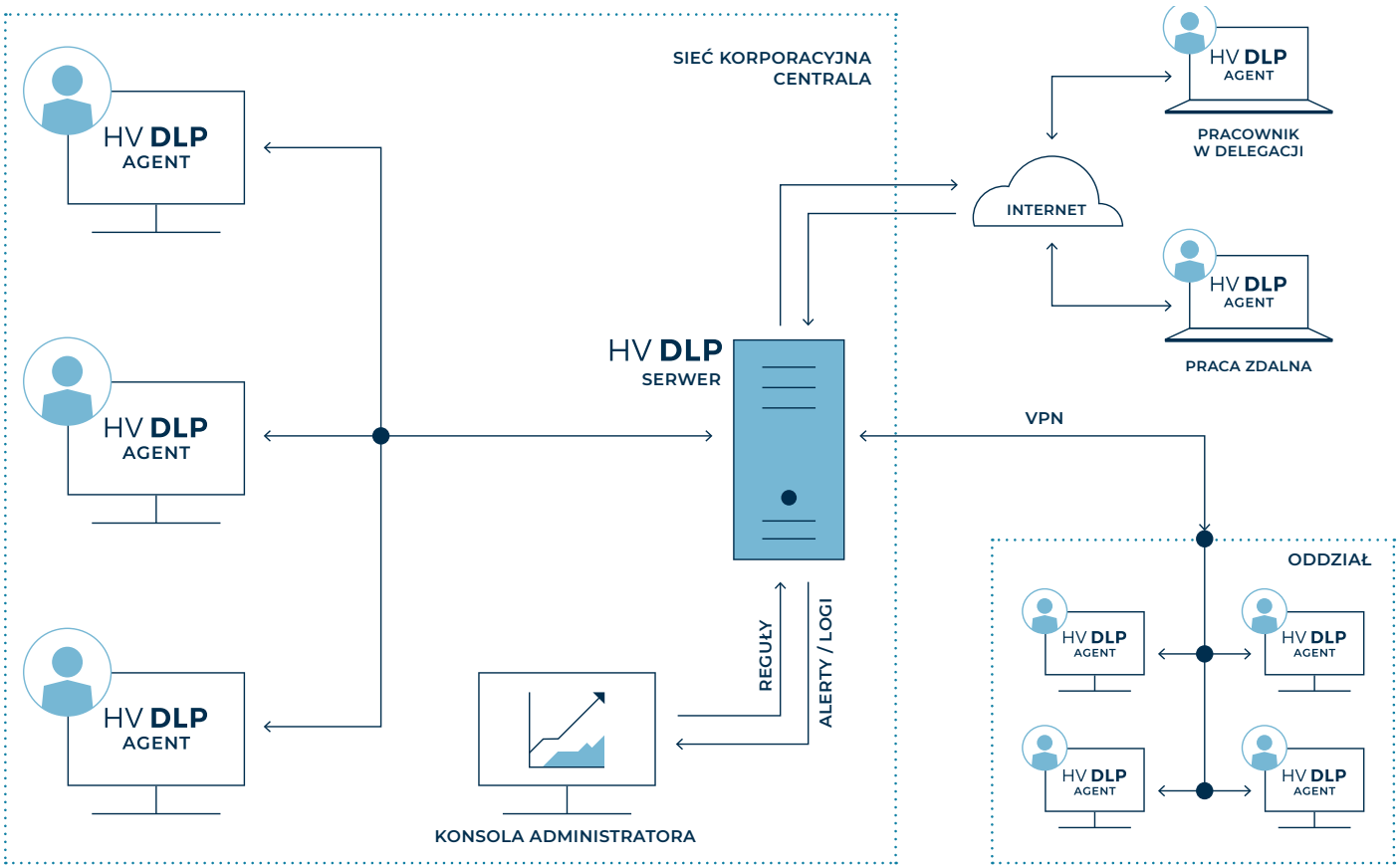
Hyprovision DLP to profesjonalne rozwiązanie DLP (Data Loss Prevention), które oferuje szerokie możliwości ochrony przed przypadkowym lub celowym wyciekiem danych, które mogą trafić w niepowołane ręce poprzez użycie przenośnych pamięci USB (pendrive), dysków twardych, wydruku, transferu za pośrednictwem poczty e-mail, komunikatorów internetowych, formularzy na stronach internetowych, korzystania z aplikacji oraz usług w chmurze.

Hyprovision DLP umożliwia zdefiniowanie polityk bezpieczeństwa (metod ochrony), które wpięte w reguły (gdzie, kto oraz kiedy) monitorują, wykrywają oraz blokują nieautoryzowany przepływ informacji.

KLUCZOWE CECHY

Ochrona treści	Monitorowanie i kontrola danych chronionych, podejmowanie decyzji czy dane mogą opuścić organizację wybranymi kanałami, urządzeniami oraz w wyniku działania poszczególnych użytkowników.
Klasyfikacja treści	Automatyczne wyszukiwanie i identyfikacja treści wymagających ochrony na komputerach lokalnych, serwerach, macierzach dyskowych. Identyfikacja może odbywać się w locie (dla danych w użyciu) oraz zgodnie z zaplanowanym harmonogramem.
Znakowanie dokumentów (fingerprint)	Automatycznie nadawanie niewidocznych znaczników na dokumenty w oparciu o zdefiniowane reguły.
Kontrola urządzeń	Monitorowanie i kontrola USB oraz portów peryferyjnych. Ustanawianie praw dla urządzeń i użytkowników.
Wymuszanie szyfrowania	Automatyczne wymuszanie szyfrowania danych kopiowanych na napędy USB oraz napędy udostępnione, z zastosowaniem szyfrowania AES 256 bit.

Jak działa Hyprovision DLP?



KONTROLOWANE TYPY URZĄDZEŃ

- Napędy dyskietek
- Napędy CD/DVD/BD
- Dyski wymienne: nośniki flash, karty pamięci, pendrive itd.
- Dyski twarde wewnętrzne i zewnętrzne
- Dyski sieciowe
- Napędy udostępnione
- Napędy taśmowe
- Napędy ZIP
- Adaptery Wi-Fi
- Urządzenia Bluetooth
- Urządzenia pamięci masowej PCMCIA
- Aparaty cyfrowe / kamery internetowe / thunderbolt
- Urządzenia z systemem Apple iPhone / iPod touch / iPad, BlackBerry, Windows Mobile i Palm OS
- Urządzenia biometryczne
- Odtwarzacze mp3
- Drukarki (USB, lokalne, sieciowe i wirtualne)
- Inne

INTEGRACJA Z SZYFROWANIEM*

- Windows BitLocker To Go
- PGP® Whole Disk Encryption
- TrueCrypt®
- Lexar® Media SAFE S1100 & S3000 Series
- SafeDisk®
- SecurStar® DriveCrypt® (DCPPE)
- Sophos SafeGuard Easy (DCPPE)
- SafeToGo
- inne

OCHRONA PORTÓW

- USB
- FireWire
- Podczerwień
- Szeregowe i równoległe

IDENTYFIKOWANE FORMATY PLIKÓW

- MS Office, OpenOffice, Lotus 1-2-3, CSV, TXT, DBF, XML, Unicode
- pliki MIME
- archiwa: GZIP, RAR, ZIP, inne

KONTROLA KOMUNIKACJI SIECIOWEJ

- Poczta Web Mail: MAPI (Microsoft Exchange), SMTP/SMTPS, IBM Notes (Lotus Notes), Gmail, Yahoo! Mail, Hotmail (Outlook.com), AOL Mail, Microsoft Outlook Web App (OWA, formerly Outlook Web Access), GMX.de, Web.de, Mail.ru, Rambler Mail, Yandex Mail
- Portale społecznościowe: Facebook, Twitter, Google+, LinkedIn, Tumblr, Myspace, VKontakte, XING.com, LiveJournal, MeinVZ.de, StudiVZ.de, Disqus, LiveInternet.ru, Odnoklassniki.ru
- Komunikatory internetowe: Skype, ICQ/AOL, Windows Live Messenger, Yahoo! Messenger, IRC, Jabber, WhatsApp Web, Mail.ru Agent
- Protokoły internetowe: HTTP/HTTPS, FTP/FTPS, Telnet, Torrent
- Serwisy chmurowe: Amazon S3, BitTorrent Sync, Box, Copy, Cloud Mail.ru, Cubby, Dropbox, GMX.de, Google Drive, iCloud, Knowhow Cloud, Mediafire, Mega, Microsoft OneDrive (SkyDrive), Mozy, Spideroak, Strato HiDrive, Tresorit, Own Cloud, Web.de, Yandex Disk i inne definiowane

FILTROWANIE TREŚCI

- Słowa kluczowe
- Lokalizacja i kanał transferu danych
- Zaawansowane wzorce wyrażeń regularnych
- Predefiniowane szablony wyrażeń regularnych (PESEL, NIP, numer dowodu osobistego, numer paszportu, numer karty kredytowej, numer konta bankowego, adres, numer prawa jazdy, data, adres e-mail, kod pocztowy, numer telefonu itd.)
- Słownik: Międzynarodowa Klasyfikacja Chorób i Procedur Medycznych ICD-9, ICD-10
- Słowniki słów kluczowych
- Atrybuty plików (nazwa, rozmiar, data/czas, szyfrowanie itd.)

IDENTYFIKOWANE TYPY DANYCH

- dowolnie definiowane pliki
- pliki pakietu MS OFFICE
- pliki PDF, TXT, XML
- predefiniowane pliki multimedialne
- predefiniowane pliki MIME

KONTROLA SCHOWKA

- Operacje kopiowania/wklejania treści między aplikacjami
- Identyfikowanie typu danych: pliki, dane tekstowe, multimedia oraz inne
- Zrzuty ekranu (Print Screen i aplikacje innych firm)

* na zapytanie

Kontrola urządzeń

Blokada, kontrola oraz monitoring urządzeń, a także peryferii w celu uniemożliwienia kradzieży danych. Sprawdź, w jaki sposób możesz sprawować kontrolę nad tym, co i kiedy może być podłączane do komputerów, które znajdują się w Twojej infrastrukturze informatycznej.

USTAWIENIA GLOBALNE

Domyślnie wszystkie prawa do urządzeń są ustalone globalnie. Jednak w praktyce definiuje się dodatkowe reguły dotyczące wybranych grup urządzeń.

USTALENIE PRAW DLA UŻYTKOWNIKA

Prawa dostępu mogą być ustalone dla użytkownika niezależnie od urządzeń, z jakich korzysta czy też będzie korzystał w przyszłości.

USTALENIE PRAW DLA KOMPUTERÓW

Prawa można indywidualnie definiować dla każdego komputera. Funkcja jest szczególnie przydatna dla komputerów, które pełnią specjalną rolę w organizacji (np. serwerów czy też komputerów administratorów).

USTALENIE PRAW DLA URZĄDZENIA

Prawa mogą być ustalone dla konkretnego urządzenia w oparciu o numer seryjny, identyfikator dostawcy oraz identyfikator produktu. System identyfikuje nośniki szyfrowane.

USTALENIE PRAW DLA GRUPY URZĄDZEŃ

Urządzenia mogą być dowolnie grupowane, dzięki czemu mamy możliwość zdefiniowania różnych praw dostępu dla wybranych obszarów działalności lub elementów struktury organizacyjnej.

MONITOROWANIE PLIKÓW

Wszystkie transfery lub próby transferów plików (dokumentów) na urządzenia pamięci USB są rejestrowane, dzięki czemu system daje możliwość podjęcia odpowiedniego działania (np. blokowanie).

URZĄDZENIA ZAUFANE

W przypadku urządzeń zaszyfrowanych prawa dostępu są konfigurowane w oparciu o poziom / metodę szyfrowania.

KOPIE PLIKÓW (DOKUMENTÓW)

Pliki kopiowane na nośniki zewnętrzne mogą być zapisywane w repozytorium, tak aby później podczas audytu mogły zostać zweryfikowane.

POWIADOMIENIA ADMINISTRACYJNE

Powiadomienia administracyjne w formie e-mail są wstępnie zdefiniowane we wszystkich politykach bezpieczeństwa. Są w pełni definiowalne.

DASHBOARD

W celu odpowiedniej prezentacji graficznej stworzyliśmy zaawansowany dashboard, na którym znajduje się kilkaset widżetów, które można dowolnie konfigurować.

NIESTANDARDOWE METODY GRUPOWANIA

Prawa można nadać dla urządzeń w grupach tworzonych dynamicznie – np. w oparciu o fragment nazwy, wersji, struktury organizacyjnej, identyfikator, producenta, dostawcę, oraz metodami statycznymi – poprzez bezpośrednie wskazanie.

HASŁO TYMCZASOWE

Hasło tymczasowe pozwala na czasową (np. 30 min) zmianę praw dostępu do urządzeń dla wybranego użytkownika – co ważne – bez wprowadzenia trwałej zmiany reguł bezpieczeństwa.

MONITORING I ANALIZA

Aktywność użytkowników oraz urządzeń zapisuje się w wysokowydajnej bazie danych SQL. System jest wyposażony w zaawansowane mechanizmy eksportu danych do wybranych formatów, a dodatkowo – w dwa wysokowydajne systemy raportujące: SAP Crystal Reports oraz Stimulsoft.

POWIADOMIENIA UŻYTKOWNIKA

Powiadomienia użytkownika mają na celu budowanie świadomości w zakresie bezpieczeństwa IT oraz mają służyć ostrzeganiu o działaniach, które w konsekwencji mogą prowadzić do naruszeń bezpieczeństwa. Powiadomienia mają charakter wyskakujących okien (pop-up). Są w pełni definiowalne.

Ochrona danych w spoczynku

Kluczowym aspektem ochrony danych w spoczynku jest identyfikacja miejsc składowania danych oraz klasyfikacja znalezionych danych. Hyprovision DLP skanuje zawartości plików danych pod kątem znalezienia treści odpowiadającej danej klasyfikacji. Dokument może być oznaczony odpowiednim znacznikiem (fingerprint).

WYRAŻENIA WYKLUCZONE

Wykorzystaj zdefiniowane mechanizmy analizy treści lub zdefiniuj algorytmy samodzielnie do zbudowania statycznych czarnych list (black list).

ATRYBUTY PLIKÓW SKANOWANYCH

Możesz ograniczyć zakres skanowanych plików poprzez ustalenie przedziału rozmiaru pliku czy zdefiniowanie okresu utworzenia pliku.

BIAŁA LISTA PLIKÓW

Zdefiniuj białą listę plików w oparciu o szablon nazwy, rozszerzenie, rozmiar, datę utworzenia. Pliki te nie podlegają skanowaniu i nie będą brane pod uwagę w analizach.

CZARNA LISTA PLIKÓW

Zidentyfikuj pliki na podstawie ich nazwy i monitoruj zmianę lokalizacji. W oparciu o wyniki sporządź listę plików niedozwolonych. Skorzystaj z funkcji usuwania, szyfrowania, archiwizowania.

CZARNA LISTA TYPÓW PLIKÓW

Wykorzystaj czarną, modyfikowalną listę typów plików do wykrywania tylko określonych dokumentów, np. dokumentów pakietu MS Office, archiwów, plików wykonywalnych, plików graficznych, plików erotycznych itp.

BIAŁA LISTA PLIKÓW MIME

Możesz wykluczyć ze skanowania pliki typu MIME umieszczając je na białej liście. Otrzymasz mniejszą ilość wyników lepszej jakości, będziesz skuteczniej zarządzał bezpieczeństwem.

ZASZYFRUJ DANE

Wybrane dane możesz zaszyfrować za pomocą silnego szyfrowania AES 256. Wykorzystaj do tego celu posiadane narzędzia do szyfrowania.

USUŃ ZBĘDNE DANE

Zidentyfikuj i usuń (zarchiwizuj) nadmiarowe lub zbędne dane. Weź pod uwagę rozporządzenie RODO dotyczące danych osobowych.

KLASYFIKACJA I OZNACZANIE PLIKÓW

Wybrane pliki możesz w procesie skanowania oznaczyć niewidzialnym znacznikiem.

PRECYZYJNE SKANOWANIE WG SZABLONÓW

Za pomocą zdefiniowanych szablonów przeszukiwań, takich jak ICD-9, ICD-10 zidentyfikuj dane medyczne i podejmij odpowiednie kroki zabezpieczające.

MONITORING I ANALIZA

Wynik działania procesów skanowania jest dostępny w konsoli administracyjnej w postaci danych tabelarycznych oraz widżetów. Możesz zawęzić agregację danych za pomocą dowolnie definiowanych filtrów statycznych i dynamicznych.

CZARNA LISTA TREŚCI

Zdefiniuj czarną listę treści takich jak numery PESEL, dowodów osobistych, kart kredytowych, kont bankowych i innych umożliwiających identyfikację osób celem znalezienia plików, miejsc ich występowania i ilości duplikatów. Podejmij odpowiednie działania zabezpieczające.

EKSPORT DANYCH

Każdą tabelę z danymi w aplikacji możesz wyeksportować do wielu formatów lub wysłać e-mailem do dowolnej osoby. Możesz skorzystać również z gotowych raportów w standardach Stimulsoft lub SAP Crystal Reports.

SKANOWANIE PLIKÓW I ZAWARTOŚCI

Twórz dowolne reguły identyfikacji treści chronionej w zależności od atrybutów pliku – nazwa, typ, szablonów treści, zawartość. Wykonaj skanowanie zasobów sieciowych i lokalnych pod kątem występowania wybranych danych.

NIESTANDARDOWA CZARNA LISTA TREŚCI

Wykorzystaj czarną listę treści w celu zdefiniowania słów kluczowych. Lista będzie wykorzystana do znajdowania słów i wyrażeń z nich złożonych w dokumentach.

Ochrona danych w użyciu

Ochrona danych w użyciu bazuje na monitorowaniu prób dostępu do plików z wykorzystaniem certyfikowanych przez Microsoft sterowników.

MONITOROWANIE OPERACJI NA PLIKACH

Twórz dowolne reguły dostępu do plików (edycji, usuwania, modyfikacji, tworzenia). Nadaj użytkownikom odpowiednie prawa do plików, niezależnie od ich lokalizacji oraz domeny.

ATRYBUTY PLIKÓW MONITOROWANYCH

Możesz ograniczyć zakres monitorowanych plików poprzez ustalenie przedziału rozmiaru pliku czy zdefiniowanie okresu utworzenia pliku.

BIAŁA LISTA PLIKÓW MIME

Możesz wykluczyć z monitorowania wybrane typy plików MIME, umieszczając je na białej liście. Ogranicza to ilość zapisów z operacji na plikach.

ZASZYFRUJ DANE*

Wybrane pliki po edycji możesz zaszyfrować za pomocą silnego szyfrowania AES 256. Wykorzystaj do tego celu posiadane narzędzia do szyfrowania.

MONITORUJ DRUKOWANIE

Zablokuj możliwość wydruku wybranym plikom i użytkownikom. Zbuduj zaawansowane reguły bezpieczeństwa wydruków.

MONITORUJ KOPIOWANIE ZAWARTOŚCI

Monitoruj i blokuj kopiowanie zawartości dokumentu wybranym użytkownikom. Zbuduj zaawansowane reguły bezpieczeństwa kopiowania w oparciu o konkretną treść.

CZARNA LISTA PLIKÓW

Monitoruj pliki na podstawie ich atrybutów (nazwa, rozszerzenie, wielkość, data utworzenia) i monitoruj dostęp do nich. Lista logów pozwoli na analizę kto i kiedy uzyskał dostęp do pliku, zmodyfikował plik lub usunął plik.

MONITORUJ PRINT SCREEN

Monitoruj i blokuj użycie klawisza Print Screen. Analizuj kopiowaną treść pod względem występowania grafiki i tekstu.

CZARNA LISTA TYPÓW PLIKÓW

Wykorzystaj czarną, modyfikowalną listę typów plików do monitorowania tworzenia, edycji, usuwania, kopiowania zawartości. Wybierz główne typy chronionych plików, np. dokumenty pakietu MS Office, archiwa, pliki tekstowe, pliki graficzne itp.

EKSPORT DANYCH

Każdą tabelę z monitorowanymi plikami możesz wyeksportować do wielu formatów lub wysłać e-mailem do dowolnej osoby. Możesz skorzystać również z gotowych raportów w standardach Stimulsoft lub SAP Crystal Reports.

BIAŁA LISTA PLIKÓW

Zdefiniuj białą listę plików w oparciu o szablon nazwy, rozszerzenie, rozmiar, datę utworzenia. Pliki te są wyłączone z monitorowania, a działania użytkowników na tych plikach nie podlegają analizie.

MONITORING I ANALIZA

Dokonuj zaawansowanej analizy działań użytkowników na poszczególnych plikach. Dzięki wydajnej webowej konsoli administracyjnej uzyskanie interesujących zestawień będzie bardzo szybkie i proste.

MONITOROWANIE PLIKÓW OZNACZONYCH

Wykorzystaj znaczniki plików (fingerprint) do identyfikacji plików podlegających odrębnym regułom monitorowania. Nie zezwalaj na dokonywanie zmian w tego typu plikach, monitoruj kopiowanie i usuwanie tych plików, monitoruj kopiowanie treści z tych plików.

* na zapytanie

Ochrona danych w ruchu

Ochrona danych w ruchu bazuje na monitorowaniu prób transferu danych w postaci plików, treści w dokumentach, tekstu w komunikatorach.

CZARNA LISTA PLIKÓW

Blokuj transfer plików posiadających odpowiednie atrybuty (nazwa, rozszerzenie, wielkość, data utworzenia).

BIAŁA LISTA PLIKÓW

Zezwól na transfer plików z tzw. białej listy plików. Lista jest tworzona w oparciu o szablon nazwy, rozszerzenie, rozmiar, datę utworzenia.

CZARNA LISTA TYPÓW PLIKÓW

Zbuduj czarną listę plików bezwzględnie chronionych i zapobiegaj transferowi tych plików wybranymi kanałami.

BIAŁA LISTA PLIKÓW MIME

Pozwól na transfer wybranych typów plików MIME, umieszczając je na białej liście.

TRANSFER PLIKÓW ZASZYFROWANYCH

Zezwól lub zabroń transferu plików szyfrowanych. Wymuś zaszyfrowanie plików przed transferem.

TRANSFER PLIKÓW E-MAILEM

Monitoruj i blokuj transfer plików za pośrednictwem poczty elektronicznej.

TRANSFER TREŚCI KOMUNIKATORAMI

Monitoruj i blokuj transfer treści z wykorzystaniem komunikatorów.

MONITOROWANIE KOPIOWANIA PLIKÓW

Twórz dowolne reguły monitorujące kopiowanie plików z dysku na dysk (np. lokalny), na dyski zewnętrzne.

EKSPORT DANYCH

Każdą tabelę z monitorowanymi plikami możesz wyeksportować do wielu formatów lub wysłać e-mailem do dowolnej osoby. Możesz skorzystać również z gotowych raportów w standardach Stimulsoft lub SAP Crystal Reports.

MONITOROWANIE TREŚCI

Monitorowanie treści odbywa się w oparciu o analizę danych w spoczynku (okresowe skanowanie), bądź w oparciu o analizę danych w użyciu (np. edytowalny plik Word z treścią chronioną) i nadanie plikom niewidzialnych znaczników (fingerprint). Tak oznaczone pliki podlegają specjalnej ochronie.

MONITORING I ANALIZA

Dokonuj zaawansowanej analizy działań użytkowników na poszczególnych plikach. Dzięki wydajnej webowej konsoli administracyjnej uzyskanie interesujących zestawień będzie bardzo szybkie i proste.

TRANSFER PLIKÓW DO CHMUR

Monitoruj i blokuj transfer plików do chmur: BitTorrent Sync, Box, Copy, Cubby, Dropbox, Google Drive, Knowhow Cloud, Mediafire, Mega, Microsoft OneDrive, Mozy, Spideroak, Strato HiDrive, Tresorit, Own Cloud.

TRANSFER PLIKÓW FTP

Monitoruj i blokuj transfer plików do/z serwera FTP.

WYMAGANIA TECHNICZNE

e-Agent	Microsoft Windows 7/8.x/10, Microsoft Windows Server 2008 R2/2012/2016/2019, RAM: min. 4 GB, HDD min. 200 MB
e-Serwer	Windows 64-bit (Windows Server 2012 / Windows 7 lub nowsze), 8 GB RAM, 40 GB HDD, processor 64-bit
Serwer aplikacji	Windows 64-bit (Windows Server 2012 / Windows 7 lub nowsze), Java 8 (JRE lub JDK), Apache Tomcat 8.5, 8 GB RAM
Konsola administracyjna	przeglądarka stron WWW zgodna z HTML5 (np. Firefox, Chrome, Opera, Internet Explorer 11)
Baza danych	Microsoft SQL Server od 2012 (wszystkie wersje), RAM: min. 8 GB RAM / zalecane 16 GB, HDD: min. 4 GB / na każde 100 komputerów, procesor 64-bit

LICZBA KOMPUTERÓW	0 – 500	501 – 2000	2001 – 5000	5001 – 10001+
RAM	8 GB	16 GB	32 GB	64 GB
PROCESOR	64-bit	64-bit	64-bit	dual, 64-bit

BTC Sp. z o.o. oferuje nowoczesne i innowacyjne rozwiązania
w obszarze zarządzania oraz bezpieczeństwa infrastruktury IT.
Stawiamy na rozwiązania, które z powodzeniem znajdują zastosowanie
u Klientów z sektora administracji publicznej oraz firm prywatnych.
Chcesz dowiedzieć się więcej o naszych produktach? Zachęcamy do kontaktu!

Sprawdź naszą ofertę na **www.btc.com.pl**