sealpath™
Document Security Everywhere

Kontrola dokumentów niezależnie od miejsca, gdzie się znajdują

Nadzór nad dokumentami, gdziekolwiek się znajdują. Zdalne blokowanie lub modyfikacja uprawnień dostępu w czasie rzeczywistym



Sealpath Information Rights Management

© 2018 SealPath Technologies S.L. – Proprietary

Informacje zawarte w tym dokumencie są poufne i stanowią własność SealPath Technologies S.L. Żadna część tego dokumentu nie może być rozpowszechniana, wykorzystywana ani reprodukowana bez uprzedniej pisemnej zgody przedstawiciela SealPath Technologies S.L.

1 Opis rozwiązania Sealpath IRM

Zarządzanie bezpieczeństwem informacji

Ochrona kluczowych zasobów firmy dotyczy przede wszystkim metod zabezpieczania jej najsłabszego ogniwa, którym jest zwykle indywidualny użytkownik. Często najlepsze i najbardziej zaawansowane narzędzia do ochrony przed wyciekami poufnych informacji (DLP) są skuteczne tylko pod warunkiem ich właściwego wdrożenia i dalszego zarządzania. Kluczowym elementem takiego wdrożenia jest klasyfikowanie informacji, zapewnienie właściwej metody zabezpieczenia (szyfrowanie) oraz precyzyjnej kontroli obiegu informacji zarówno w obrębie firmy jak też na zewnątrz.

SealPath to rozwiązanie klasy Information Rights Management (IRM) przeznaczone do automatyzacji procesów klasyfikacji, zabezpieczania oraz kontroli dokumentów w obiegu elektronicznym zarówno w obrębie organizacji jak i poza nią.

1.1. SealPath - korzyści dla organizacji:

- Wspiera organizację w:
  - procesie zabezpieczenia dostępu do treści dokumentów,
  - automatyzacji procesów ochrony i monitorowania dokumentów,
  - kwestii zapewnienia zgodności z wymaganiami **audytów** i wymogami **RODO.**
- Chroni przed ujawnieniem treści osobom nieuprawnionych (nieuczciwa konkurencja, wyniesienie treści, wysłanie plików przez pomyłkę, kradzież plików)
- Dostęp do treści mają tylko osoby upoważnione – rozwiązanie typu Information Right Management.
- Dla dostępu do dokumentów MSOffice **nie jest wymagane instalowanie na komputerze dodatkowego oprogramowania**.
- Bez względu na to, gdzie pliki się znajdują, wewnątrz organizacji, czy też gdziekolwiek indziej na świecie:
  - Umożliwia określenie kto i co może zrobić z treścią w dokumencie
  - Jednym kliknięciem można wycofać prawa dostępu,
- Integracja w środowisku Microsoft
  - synergia z pozostałymi elementami infrastruktury oraz aplikacjami,
  - ograniczenie kosztów wdrożenia,
  - proste wdrożenie rozwiązania,
  - minimalizacja problemów adaptacyjnych,
  - nie wymaga specjalistycznej wiedzy od użytkowników końcowych.
- Dostępne wersje językowe klienta: angielska, hiszpańska, niemiecka, **polska**

1.2. SealPath - wsparcie bezpieczeństwa w organizacji

- Wspiera organizację w:
  - kwestii zachowania **Tajemnicy Przedsiębiorstwa** i wymogów **RODO (GDPR)**
  - zarządzaniu prawami dostępu do informacji w postaci elektronicznej
  - ochronie przed utratą/wyciekiem wrażliwych informacji

© 2018 SealPath Technologies S.L. - Confidential

- zachowaniu bezpieczeństwa przechowywania, współdzielenia i przekazywania dokumentów
- zapewnieniu integralności i poufności dokumentów niezależnie od miejsca, gdzie się znajdują - wewnątrz oraz na zewnątrz organizacji
- w automatycznym zabezpieczaniu dokumentów przed nieupoważnionym dostępem

1.3. Funkcjonalności

- Określenie **co można zrobić z treścią w dokumentach** zgodnie z centralnie zarządzanymi lub indywidualnymi politykami zabezpieczeń w całym cyklu elektronicznego obiegu oraz przechowywania
- Nadawanie uprawnień do odczytu, edycji, kopiowania i wstawiania treści, drukowania oraz dodania nowych odbiorców
- Automatyczne szyfrowanie i zabezpieczanie dokumentów elektronicznych według predefiniowanych kryteriów polityk zabezpieczeń (katalogi współdzielone oraz lokalne)
- Zarządzanie rolami i uprawnieniami użytkowników oraz administratorów
- Ograniczanie czasu dostępu do chronionych dokumentów
- Automatyczne oznaczanie dokumentów sygnaturami (znak wodny – pliki graficzne i pliki pdf)
- Automatyzacja zabezpieczania wysyłanych treści e-maili oraz załączników przesyłek pocztowych

1.4. Cechy

- **Zabezpieczenia przypisane do pliku** – taki sam poziom ochrony dla plików wewnątrz organizacji, jak i dla przeniesionych na zewnętrzne nośniki danych, wysłanych na zewnątrz organizacji czy też umieszczonych w zasobach/aplikacjach chmurowych
- **Żadne zabezpieczane pliki nie są przechowywane po stronie rozwiązania SealPath – są one u nadawcy i odbiorcy**
- Bezpieczna współpraca pomiędzy użytkownikami i grupami użytkowników
- Informacje na temat dostępu do chronionych dokumentów (logi – **kto i kiedy miał dostęp**)
- Możliwość przekazywania uprawnień do chronionych informacji w przypadku zmian organizacyjnych lub utraty dostępu przez pracownika
- Integracja ze środowiskiem Microsoft, w tym z Active Directory - użytkownicy wewnątrz firmy nawet nie muszą wiedzieć, że korzystają z zabezpieczeń
- Użytkownicy na zewnątrz mogą korzystać z zabezpieczonych dokumentów – w przypadku dokumentów **MSOffice nie jest wymagane instalowanie na komputerze dodatkowego oprogramowania**, w przypadku innych dokumentów **konieczne jest zainstalowanie oprogramowania SealPath Lite na koncie użytkownika – nie są wymagane uprawnienia administracyjne**.
- Konta użytkowników i przypisane uprawnienia można modyfikować
- Odzyskiwanie dostępu do zabezpieczonych treści jest możliwe z poziomu platformy administracyjnej
- **Odebranie uprawnień dostępu odcina niepożądane osoby od jakichkolwiek zabezpieczonych wrażliwych zasobów**

© 2018 SealPath Technologies S.L. - Confidential

2 Zestawienie głównych funkcji systemu Sealpath IRM

	Funkcja
FUNKCJE ZABEZPIECZANIA	Ochrona obrazów za pomocą zarządzania prawami cyfrowymi (DRM)
	Ochrona plików CAD za pomocą zarządzania prawami cyfrowymi (DRM)
	Szyfrowanie innych plików bez DRM
	Ochrona w Dropbox, SkyDrive, Google Drive itp.
	Automatyczna ochrona folderów na komputerach
	Automatyczna ochrona folderów na serwerach plików (dowolny typ, nawet sprzętowy NAS) bez używania skryptów
	Automatyczna ochrona folderów w Dropbox itp.
	Grupowe zabezpieczanie dokumentów
	Zabezpieczanie poczty email
	Ochrona użytkowników i grup użytkowników
	Ochrona bez przesyłania plików do chmury
	Dynamiczny znak wodny
	Dostęp offline z synchronizacją w tle licencji offline (bez konieczności otwierania pliku wcześniej w trybie online).
	Uprawnienia do przeglądania, edycji, drukowania, kopiowania i wklejania oraz pełna kontrola
	Funkcja “Dodawania użytkowników”
	Możliwość ustawienia dat wygaśnięcia

© 2017 SealPath Technologies S.L. - Confidential

FUNKCJE DOSTĘPU	Przeglądaj i edytuj dokumenty Office bez wtyczek
	Obsługa formatów Adobe, Foxit, Nitro, Nuance bez przeglądarki i wymagających dodatkowych płatnych dodatków.
	Odbiorca e-mail nie potrzebuje programu Outlook ani wtyczki do otwierania treści
	Zachowaj plik formatu Office bez dodawania rozszerzeń

ODWOŁYWANIE DOSTĘPU I ODBEZPIECZANIE	Możliwość odwoływania uprawnień dostępu z poziomu użytkownika końcowego
	Grupowe odwoływanie dostępu dla użytkowników końcowych (bez potrzeby wykonywania jednego po drugim)
	Cofnięcie dostępu jest dozwolone dla administratora
	Automatyczne przenoszenie uprawnień właściciela dokumentu
	“Czarna lista” użytkowników
	Odbezpieczenie przez administratora w przypadku nagłej potrzeby (z kontrolą w logach)
	Grupowe odbezpieczanie dokumentów

POLITYKI / ADMINISTRATORZY	Tworzenie polityk przez administratora
	Tworzenie polityk przez użytkowników końcowych
	Użytkownicy mogą udostępniać polityki innym użytkownikom i grupom
	Przypisywanie polityk do określonych grup użytkowników wewnętrznych i zewnętrznych
	Użytkownik może zostać "odpowiedzialnym za dane"
	Użytkownicy widzą tylko przypisane do nich polityki
	Możliwość ustanawiania delegowanych administratorów
	Tryb superadministratora do usuwania ochrony dokumentów za pomocą dziennika audytu administratora

© 2018 SealPath Technologies S.L. - Confidential

UWIERZYTELNIANIE	Uwierzytelnianie za pomocą rozwiązań innych niż AD
	Użytkownicy mogą mieć konta osobiste (np. Gmail)
	Integracja z Active Directory
	Integracja z różnymi „lasami” i złożonymi topologiami
	Integracja z LDAP od innych dostawców
	Administrator nie musi tworzyć polityk do współpracy z użytkownikami zewnętrznymi
	Oprogramowanie do otwierania dokumentów nie wymaga uprawnień administratora
	Możliwość posiadania relacji zaufania w chmurze
	Możliwość pracy z grupami AD / LDAP
	Grupy w szablonach mogą zawierać zewnętrzne wiadomości e-mail
	Użytkownicy zewnętrzni mogą znajdować się w lokalnej bazie danych lub AD / LDAP
	W wersji On-Premise wszystko, w tym użytkownicy zewnętrzni, jest przechowywane w wewnętrznej bazie danych

MONITOROWANIE	Śledzenie dokumentu przez administratora
	Śledzenie dokumentu przez użytkownika końcowego
	Monitorowanie działań typu zablokowanie dostępu, zdjęcie ochrony itp.
	Raporty typu alarmy, najczęściej używane zabezpieczenia itp.
	Raporty dla użytkownika końcowego: dostęp do dokumentów, alerty itp..
	Drukowanie do PDF ze znakiem wodnym
	Uzyskaj informacje z pliku "niedostępnego"
	Dziennik kontroli administratora: śledzenie działań administracyjnych
	Wyszukiwanie “pełnotekstowe” zdarzeń dostępu do dokumentów

© 2018 SealPath Technologies S.L. - Confidential

MODELE WDROŻENIA INTEGRACJA	Wdrożenie w wersji On-Premise
	Wdrożenie w wersji Cloud / SaaS
	Wdrożenie na platformach zwirtualizowanych VMWare, Hyper-V
	Możliwość wdrożenia na fizycznym sprzęcie
	Możliwość indywidualizacji wyglądu komponentów aplikacji (tzw. white labeling)
	Integracja z CRM, ERP, DMS za pomocą SDK
	Integracja z zewnętrznymi systemami klasyfikacji
	Integracja z systemami DLP

UŁATWIENIA	Zabezpieczanie za pomocą “prawego klawisza”
	Zabezpieczanie w pasku zadań Office
	Zabezpieczanie w dedykowanym pulpicie metodą drag&drop

WSPIERANE PLATFORMY	Windows XP, Windows Vista
	Windows 7 (bez instalacji rozszerzeń z uprawnieniami admina)
	Windows 8, 8.1, 10
	WS 2003, 2008, 2008 R2, 2012, 2016 (zabezpieczanie folderów)
	Mac OSX
	iOS (iPhone, iPad) z możliwością otwierania plików Office oraz PDF
	Android z możliwością otwierania plików Office oraz PDF

© 2018 SealPath Technologies S.L. - Confidential

3 SealPath Enterprise - podsumowanie

- Użytkownicy mogą tworzyć własne zasady ochrony, aby udostępniać je innym, bez kontaktu z działem IT. Możliwe jest tworzenie przez użytkowników końcowych (nie tylko administratora systemu) szczegółowych zasad dla konkretnych przypadków użycia a nie tylko bardzo ogólne zasady klasyfikacji typu Poufne, Wewnętrzne itp.
- Polityki bezpieczeństwa mogą zawierać dane użytkowników zewnętrznych, których nie ma w domenie. Zasady nie są ograniczone tylko dla użytkowników wewnętrznych. Użytkownicy mogą zabezpieczać dokumenty nie tylko na pojedynczych użytkowników lub grupy z AD, ale też na całe domeny firm zewnętrznych (*@firma.pl), co daje dużą elastyczność dostosowania do współpracy z kooperantami.
- Proste udostępnianie użytkownikom zewnętrznym: wysyłanie zaproszeń indywidualnych, automatyczna rejestracja itp.
- Odbiorcy nie muszą instalować oprogramowania agenta wymagającego uprawnień administratora.
- Można chronić dokumenty również użytkowników, których nie ma w AD (np. Gmail, Hotmail itp.).
- Obsługa plików PDF za pomocą różnych przeglądarek (Adobe, Foxit, Nitro, Nuance itp.).
- Foldery na serwerze plików (również firm trzecich takich jak np. Alfresco itp.) mogą być automatycznie zabezpieczane.
- Foldery w usłudze SharePoint chronione przez polityki zabezpieczeń. Kopię pobraną przez użytkownika można odwołać i udostępnić innym użytkownikom mającym dostęp do tej samej polityki.
- Użytkownicy końcowi sami mogą zarządzać zabezpieczaniem plików w folderach (FileServer) bez zaangażowania działu IT.
- Chronieni adresaci poczty e-mail nie wymagają programu Microsoft Outlook do otwierania wiadomości e-mail.
- Wsparcie dla XP/Office 2003. Win7/Office 2010 bez poprawek. Odbiorcy też nie muszą używać nowszych wersji.
- Uprawnienia "Dodaj użytkowników" pozwalają swobodnie zarządzać gronem uprawnionych użytkowników chronionych dokumentów.
- Obsługa dynamicznych znaków wodnych w dokumentach pozwala uniknąć niekontrolowanych zrzutów ekranu.
- Użytkownik może samodzielnie śledzić chronione przez siebie dokumenty i sprawdzać alerty dostępu do nich zarówno wewnątrz jak i na zewnątrz organizacji.
- Zaawansowane śledzenie: np. menedżer może śledzić dokumenty chronione przez swojego podwładnego.
- Użytkownik może samodzielnie śledzić chronione przez siebie dokumenty i sprawdzać alerty dostępu do nich zarówno wewnątrz jak i na zewnątrz organizacji.

© 2018 SealPath Technologies S.L. - Confidential

- Zaawansowane śledzenie: np. menedżer może śledzić dokumenty chronione przez swojego podwładnego.
- Użytkownicy mogą unieważnić dostęp do dokumentów indywidualnie lub według narzuconych zasad.
- Użytkownicy mogą odwołać wysłane wiadomości e-mail.
- Pamięć masowa jest oddzielona od szyfrowania: wszystkie dokumenty mogą znajdować się w usłudze Office 365, ale klucz szyfrowania jest oddzielony od platformy. Szyfrujący nie ma dostępu do pliku.
- Platformy mogą być wdrażane zarówno w modelu On-Premise jak i Cloud oferują te same funkcje.
- Super-administrator może wyłączyć ochronę dowolnego dokumentu. Włączanie tego super-użytkownika i usuwanie zabezpieczeń z plików jest w pełni kontrolowane.
- Możliwe jest skonfigurowanie różnych departamentów organizacji z różnymi administratorami / politykami / informacjami śledzenia dla tej samej firmy.
- Obsługa wielu aktywnych katalogów w różnych lasach AD z lub bez relacji zaufania.

© 2018 SealPath Technologies S.L. - Confidential