DeviceLock®

Zabezpieczy Wasze cenne informacje przed niekontrolowanym wyniesieniem na zewnętrznych nośnikach danych

Czy Twoje dane są bezpieczne?

Dane, które starasz się chronić za pomocą zapór ogniowych i haseł, prawdopodobnie wciąż przeciekają przez Twoje palce.

Na pewno zdajesz sobie sprawę, jakie konsekwencje może wywołać zgubienie lub kradzież komputera z ważnymi dla Twojej firmy danymi. Podobne zagrożenie niesie niekontrolowany wyciek informacji spowodowany w sposób świadomy lub nieświadomy przez użytkowników, którzy kopiują poufne dane z komputerów PC na pamięci przenośne, smartfony, aparaty cyfrowe, urządzenia PDA, płyty DVD/CD itp.
Innym kanałem wycieku danych może być poczta elektroniczna, komunikatory internetowe, formularze web, portale społecznościowe lub sesje telnet. Potencjalne zagrożenie dla bezpieczeństwa firmy stanowią również interfejsy bezprzewodowe stacji roboczych, takie jak: Wi-Fi, Bluetooth oraz podczerwień. W ten sam sposób komputery mogą zostać zarażone różnego rodzaju złośliwym oprogramowaniem, które jest w stanie przejąć kontrolę nad komputerem użytkownika i przesyłać przechwycone dane poprzez kanały SMTP lub FTP. **DeviceLock Endpoint Data Leak Prevention (DLP) Suite** rozwiązuje te problemy. DeviceLock wprowadza reguły ochrony danych i rozpoznaje zarówno rodzaj, jak i treść wyciekających danych.

DeviceLock®

Funkcje i zalety programu DeviceLock

DeviceLock Endpoint DLP Suite zapewnia niezbędną funkcjonalność filtrowania treści i niezawodną kontrolę przepływu danych. Dzięki temu administrator programu DeviceLock posiada pełną kontrolę nad lokalnymi portami i urządzeniami peryferyjnymi podłączanymi do firmowych komputerów.

Badania wskazują, że drukowanie dokumentów jest najczęściej wykorzystywaną metodą wynoszenia danych korporacyjnych. Mimo wszystko 75% przebadanych organizacji IT, które wykorzystują rozwiązania DLP, nie jest w stanie kontrolować treści dokumentów drukowanych na komputerach firmy!

Integracja z Active Directory. Konsola DeviceLock bezpośrednio integruje się z interfejsem konsoli MMC Zasad Grupy Active Directory (AD).

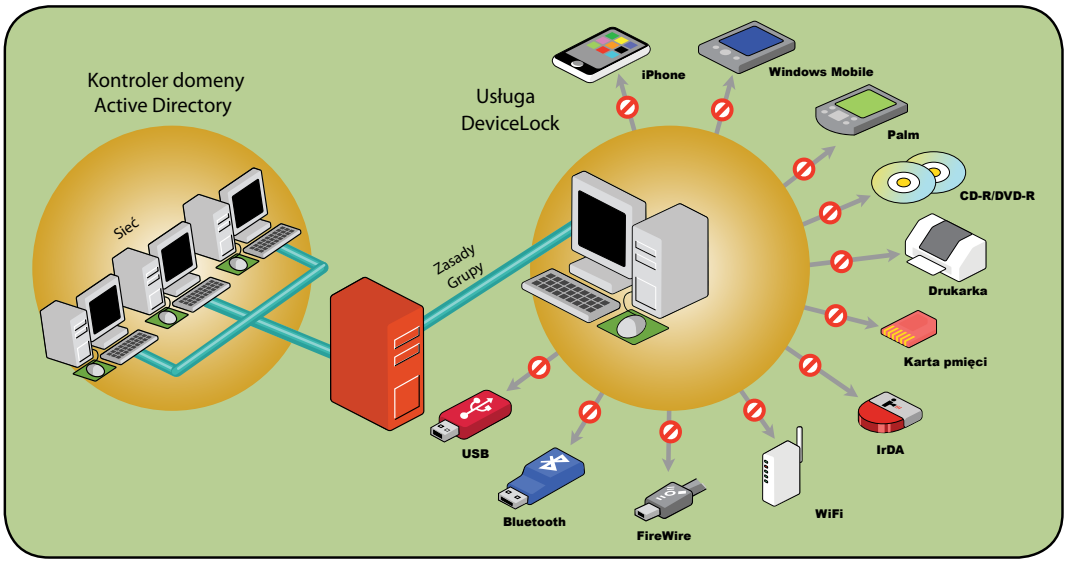
Kontrola typów plików. DeviceLock przegląda zawartość binarną pliku i określa, czy typ pliku jest prawdziwy (w porównaniu z nazwą pliku i rozszerzeniem), a następnie stosuje zdefiniowane wcześniej przez administratora reguły.

Kontrola synchronizacji urządzeń mobilnych. Dla urządzeń mobilnych z systemem Windows Mobile®, Palm® OS oraz urządzeń Apple: iPhone®, iPad®, iPod touch®, można określić rodzaje danych (pliki, zdjęcia, wiadomości email, kontakty, wpisy kalendarza, itd.), które mogą być synchronizowane z firmowymi komputerami.

Bezpieczeństwo drukowania. Drukowanie lokalne i sieciowe może podlegać ścisłej kontroli. Przechwytując, filtrując i śledząc operacje bufora drukowania, DeviceLock decyduje kto może drukować, z jakiego miejsca, kiedy i gdzie.

Kontrola schowka. DeviceLock pozwala na blokowanie wycieków w zarodku – gdy użytkownicy nieumyślnie lub celowo przesyłają poufne dane pomiędzy różnymi aplikacjami i dokumentami za pośrednictwem schowka systemu Windows.

Szyfrowanie. Dla nośników zaszyfrowanych za pomocą programów Windows 7 BitLocker, PGP® Whole Disk Encryption, TrueCrypt®, SafeDisk®, SecurStar® DriveCrypt oraz urządzeń Lexar S1100/S3000 istnieje możliwość przypisania specjalnych uprawnień.



Korzystając z programu DeviceLock Endpoint DLP Suite, firmy mogą zabezpieczyć dowolną liczbę zdalnych komputerów dzięki integracji z Active Directory i Konsolą Zarządzania Zasadami Grupy systemu Windows.

Rozpoznawanie sieci. Można określić różne polityki bezpieczeństwa pracy w trybie online oraz offline dla tego samego konta użytkownika lub komputera.

Biała lista urządzeń. Funkcja ta pozwala na tworzenie „białych list" urządzeń USB oraz nośników CD/DVD. Istnieje również możliwość zdalnego (np. telefonicznego) odblokowywania urządzeń USB przy pomocy wygenerowanego kodu.

Wyszukiwanie danych. Opcjonalny, oddzielnie licencjonowany moduł DeviceLock Search Server (DLSS) pozwala na pełnotekstowe przeszukiwanie danych raportów audytu i shadowingu DeviceLock.

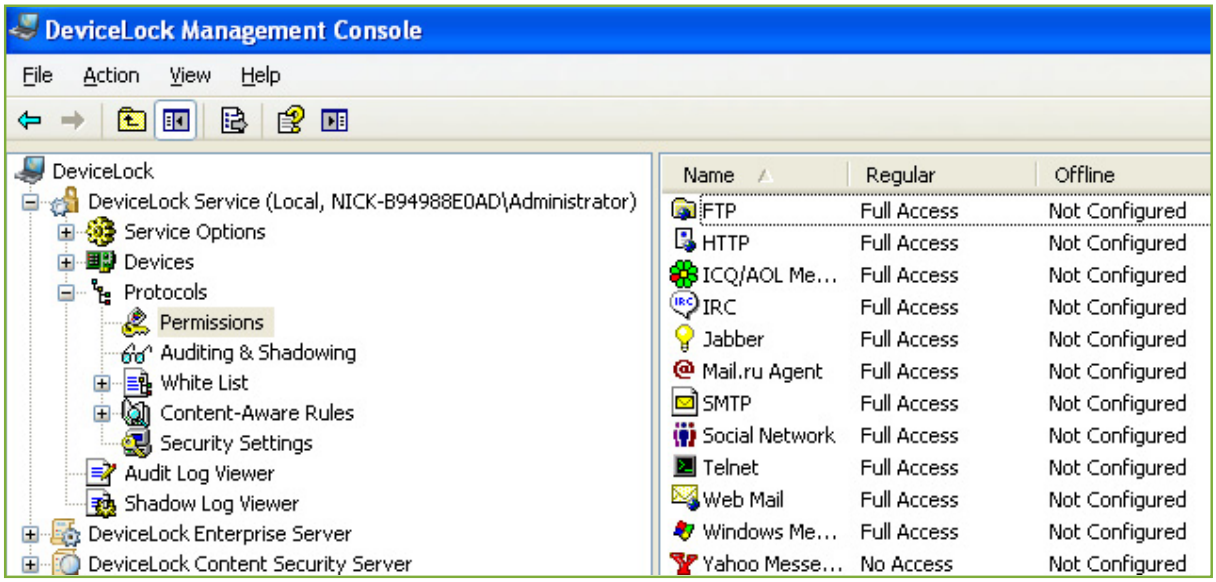
Raporty graficzne. DeviceLock może generować raporty graficzne w formacie HTML, PDF lub RTF, bazując na analizie danych raportów audytu i shadowingu zgromadzonych przez DLES.

Raporty audytu. Mechanizm audytu DeviceLock śledzi aktywność użytkownika i plików dla wybranych typów urządzeń oraz określonych portów komputera.

Shadowing danych. Funkcja ta tworzy duplikaty wszystkich danych kopiowanych na zewnętrzne urządzenia magazynujące, drukowanych, przesyłanych przez porty szeregowe, równoległe lub interfejsy sieciowe komputera.

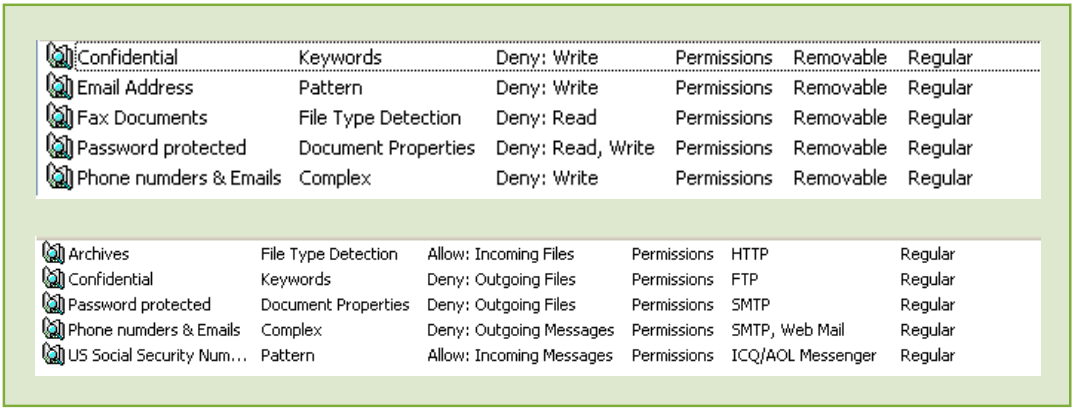
Kontrola przepływu informacji w sieci. Dodany do programu DeviceLock Endpoint DLP Suite moduł NetworkLock, pozwala na pełną kontrolę generowanego przez stacje robocze ruchu sieciowego. NetworkLock rozpoznaje protokoły sieciowe i aplikacje niezależnie od używanych przez nie portów oraz umożliwia ich selektywne blokowanie. Dzięki modułowi NetworkLock można dokonać rekonstrukcji treści i sesji z wyodrębnieniem plików lub innych danych.

Moduł ten pozwala również na zapisywanie zdarzeń oraz shadowing danych. NetworkLock może kontrolować wiadomości email, wysyłane za pomocą protokołu SMTP (wersja zwykła oraz tunelowana SSL), przetwarzając oddzielnie treść oraz załączniki. Możliwe jest również kontrolowanie dostępu do stron internetowych oraz aplikacji korzystających z protokołu HTTP, włącznie z wyodrębnieniem treści zaszyfrowanych sesji HTTPS.



Dzięki NetworkLock można zarządzać uprawnieniami użytkowników do korzystania z protokołów sieciowych wykorzystywanych przez różne aplikacje sieciowe i internetowe (portale społecznościowe, komunikatory internetowe, poczta Web mail i inne).

Filtrowanie treści. Moduł ContentLock może filtrować zarówno treść plików kopiowanych na dyski wymienne i inne urządzenia magazynujące typu Plug-n-Play, jak również dane przesyłane przez sieć za pomocą: wiadomości email, popularnych komunikatorów internetowych, stron internetowych, aplikacji HTTP (Web mail, sieci społecznościowe), protokołu FTP oraz sesji telnet. Dodatkowo można analizować i filtrować treści kopiowane za pośrednictwem schowka między aplikacjami i dokumentami. Mechanizm analizy tekstu pozwala wyodrębnić dane tekstowe z ponad 80 formatów plików i innych typów danych, a następnie zastosować efektywne i wiarygodne metody filtrowania treści bazujące na wzorcach wyrażeń regularnych. Do tworzenia reguł filtrowania treści można wykorzystać wbudowane słowniki, a także szablony wyrażeń regularnych typowych formatów danych, np.: numery kart kredytowych, numery kont bankowych, adresy, PESEL itp.



Przykładowe reguły stosowane dla wybranych urządzeń i określonych protokołów sieciowych. Przyjazny interfejs ContentLock ułatwia określenie sposobu filtrowania treści.

DeviceLock®

Czy pracownicy

Twojej firmy

korzystają z dysków

USB i innych

urządzeń wymiennych

do przechowywania

danych ?

Jeżeli tak.

Ryzykujesz wyciek

poufnych informacji

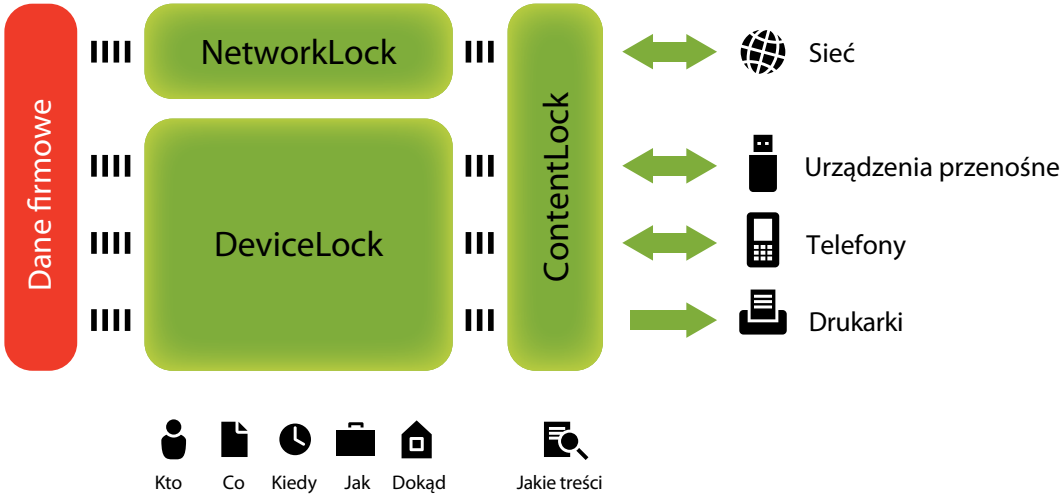
korporacyjnych !

Rodzaje modułów i sposoby licencjonowania

DeviceLock Endpoint DLP Suite składa się z modułów, które mogą być licencjonowane oddzielnie lub w dowolnej kombinacji, która odpowiada aktualnym potrzebom bezpieczeństwa firmy. Obecni klienci mogą zaktualizować podstawowy moduł DeviceLock i rozbudować ochronę punktów końcowych o wybrane nowe moduły. Podobnie nowi klienci mogą przejść na w pełni funkcjonalny system ochrony punktów końcowych DLP dodając moduły, jakich potrzebują i na jakie pozwala im budżet.

- Moduł DeviceLock® zawiera pełen zestaw mechanizmów kontroli przepływu informacji na stacjach roboczych wraz z zapisywaniem zdarzeń i shadowingiem danych podłączanych do komputera urządzeń peryferyjnych, smartfonów, urządzeń PDA oraz monitoring wydruków. DeviceLock stanowi rdzeń dla pozostałych modułów pakietu i pozwala na centralne zarządzanie nimi.
- Moduł NetworkLock™ zapewnia pełną kontrolę generowanego przez stacje robocze ruchu sieciowego. Rozpoznaje protokoły sieciowe i aplikacje niezależnie od używanych przez nie portów i umożliwia ich selektywne blokowanie. Dzięki modułowi NetworkLock można dokonać rekonstrukcji treści i sesji z wyodrębnieniem plików oraz innych danych.
- Moduł ContentLock™ wprowadza monitoring treści i filtrowanie plików przesyłanych do i z nośników wymiennych i urządzeń Plug-n-Play, jak również różnego rodzaju obiektów przesyłanych przez sieć – wiadomości email, wiadomości komunikatorów internetowych, formularzy Web, plików i sesji telnet.
- DeviceLock® Search Server (DLSS) to kolejny oddzielnie licencjonowany moduł pakietu DeviceLock Endpoint DLP Suite. Pozwala on na tekstowe przeszukiwanie centralnej bazy shadowingu i bazy zdarzeń. Zadaniem DLSS jest audyt danych, badanie incydentów oraz dokładna i szybka analiza zgromadzonych informacji.

Podstawowy moduł DeviceLock wymagany jest do instalacji pozostałych modułów. NetworkLock, ContentLock i DeviceLock Search Server są oddzielnie licencjonowanymi opcjonalnymi modułami. Modularna struktura oraz elastyczny model licencjonowania pozwala klientom na szybkie i niedrogie wdrożenie systemu DLP ochrony punktów końcowych. Proces wdrożenia można rozpocząć od instalacji modułu głównego, który dostarcza zestawu podstawowych funkcji kontroli portów i urządzeń, a w miarę wzrostu wymagań dotyczących bezpieczeństwa, dodawać nowe licencje, które aktywują dodatkowe moduły.



- **Podstawowe funkcje programu DeviceLock definiują politykę dostępu do urządzeń na poziomie portu (interfejsu), klasy, typu, modelu oraz unikalnego identyfikatora urządzenia, pory dnia, dnia tygodnia, a także według odrębnych parametrów, takich jak np. rodzaj dostępu (zapis/odczyt). Rodzaje urządzeń mogą być tak skonfigurowane, aby zezwolić na dostęp jedynie do określonych ich typów. NetworkLock daje dodatkowo możliwość kontroli generowanego przez stacje robocze ruchu sieciowego. Dodając ContentLock można być pewnym, iż tylko przefiltrowane obiekty, niezawierające treści podlegającej restrykcji, będą przesyłane dalej do miejsca przeznaczenia.**