DeviceLock®

Główne funkcje programu DeviceLock®

Kontrola dostępu. Można decydować, którzy z użytkowników mają dostęp do portów USB, FireWire, IrDA, COM oraz LPT, urządzeń WiFi oraz Bluetooth ; dowolnego typu drukarki, włącznie z drukarkami lokalnymi, sieciowymi i wirtualnymi; komputerów PDA i smartfonów wykorzystujących system Windows Mobile, BlackBerry i iPhoneOs; a także napędów DVD/BD/CD-ROM, stacji dyskietek i innych urządzeń wymiennych oraz Plug and Play. Można również ustawiać urządzenia w trybie tylko-do-odczytu i kontrolować dostęp do nich w zależności od czasu lub dnia tygodnia.

Kontrola przepływu informacji w sieci NetworkLock rozpoznaje rodzaj i protokół aplikacji sieciowej bez względu na wykorzystywane porty. Można kontrolować pocztę Web mail, komunikację za pośrednictwem portali społecznościowych, komunikatorów internetowych, operacje transferu plików i sesje telnet. NetworkLock może przechwytywać, badać i kontrolować szyfrowane i zwykłe połączenia SMTP, analizując osobno wiadomości i załączniki, a także aplikacje bazujące na protokole HTTP i szyfrowane sesje HTTPS. Pliki, dane i informacje parametrów są rekonstruowane z wiadomości i sesji, a następnie są przesyłane do modułu ContentLock w celu przefiltrowania względem zawartości.

Filtrowanie treści. ContentLock obsługuje filtrowanie zawartości danych kopiowanych na dyski wymienne, inne urządzenia pamięci masowej Plug-n-Play i poprzez sieć chronioną przez moduł NetworkLock. ContentLock rozpoznaje ponad 80 formatów plików i rodzajów danych. Moduł ten wyodrębnia i filtruje zawartość plików i innych typów danych włącznie z wiadomościami email, komunikatorami internetowymi, formularzami web, aplikacjami portali społecznościowych, itd. ContentLock filtruje strumienie danych bazując na wzorcach wyrażeń regularnych oraz warunkach numerycznych i logicznych. Można wykorzystać ponad 50 parametrów. Są to min. użytkownicy, komputery, grupy, porty, interfejsy, urządzenia, kanały przepływu danych, kireunki przepływu danych, przedziały czasu, itd.

Integracja z AD. Najpopularniejsza konsola DeviceLock integruje się bezpośrednio z Konsolą zarządzania Microsoft (MMC - ang. Microsoft Management Console) platformy Zasad Grupy Active Directory (AD). Ponieważ interfejsy w stylu MMC i Zasad Grupy są dobrze znane administratorom Microsoft, nie jest wymagane poznawanie żadnego nowego interfejsu programu ani kupowanie dodatkowego narzędzia do efektywnego centralnego zarządzania punktami końcowymi. Obecność konsoli MMC DeviceLock na komputerze administratora zasad grupy pozwala na bezpośrednią integrację z Konsolą zarządzania Zasad Grupy (GPMC) lub konsolą Użytkownicy i Komputery Active Directory (ADUC) bez potrzeby stosowania żadnych skryptów, szablonów ADO czy zmian schematów. Administratorzy bezpieczeństwa mogą dynamicznie zarządzać mechanizmami zabezpieczającymi przed wyciekami danych na punktach końcowych i ustawieniami audytu wraz z innymi zadaniami Zasad Grupy. Poza konsolą MMC Zasad Grupy, DeviceLock udostępnia również tradycyjne konsole administracyjne, dzięki którym można centralnie zarządzać agentami każdej sieci (AD, LDAP, Grupy robocze) komputerów Windows. Szablony polis, oparte na XML, mogą być współdzielone w obrębie wszystkich konsol DeviceLock.

Dokładna kontrola typów plików. Administratorzy mogą ograniczyć dostęp do ponad 4000 typów plików dla nośników wymiennych. Po skonfigurowaniu polisy dla typów plików, DeviceLock będzie przeglądał zawartość binarną pliku, określał czy typ pliku jest prawdziwy (w porównaniu z nazwą pliku i rozszerzeniem) oraz stosował mechanizmy kontroli i shadowingu zgodnie ze stosowaną polityką. Reguły Content-Aware dla typów plików mogą być zdefiniowane dla użytkowników lub grup na poziomie typu urządzenia. Reguły typów plików mogą być również stosowane do przefiltrowania plików shadowingu w celu ograniczenia objętości przechwyconych danych.

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 w systemach Windows. Operacje kopiowania i wklejania mogą być filtrowane, czy nie występuje w nich wymiana danych między aplikacjami (np. z programu Word do programu Excel). DeviceLock posiada zdolność selektywnej kontroli dostępu użytkownika do obiektów danych różnych typów kopiowanych do schowka, m.in. plików, danych tekstowych, obrazów i dźwięków (np. nagrań przechwyconych przez Windows Sound Recorder), oraz innych danych nieokreślonego typu. Operacje tworzenia zrzutów ekranu funkcją PrintScreen i oprogramowaniem innych firm mogą być blokowane dla określonych użytkowników na określonych komputerach.

Biała lista USB. Pozwala na autoryzowanie określonego modelu urządzenia USB, przy jednoczesnym blokowaniu wszelkiego innego sprzętu. Można nawet dodać do białej listy jedno unikatowe urządzenie blokując wszystkie pozostałe urządzenia tej samej marki. Wszystko to wymaga jedynie znajomości numeru identyfikującego urządzenie (na przykład, numeru seryjnego).

Biała lista nośników. Pozwala na autoryzację dostępu do określonych płyt DVD/CD-ROM identyfikowanych na podstawie specjalnej sygnatury. Dostęp będzie możliwy nawet wtedy, gdy DeviceLock® w inny sposób blokuje napęd DVD/CD-ROM. Biała lista nośników pozwala także na zdefiniowanie użytkowników i grup użytkowników, którzy będą posiadali autoryzację na uzyskiwanie dostępu do płyt DVD lub CD-ROM.

Tymczasowa biała lista. Pozwala na nadanie tymczasowych uprawnień dostępu do urządzenia USB poprzez przekazanie specjalnego kodu dostępu - bez potrzeby modyfikowania ustawień programu DeviceLock®. Funkcja ta jest bardzo przydatna, gdy konieczne jest nadanie uprawnień a administrator nie dysponuje połączeniem sieciowym. Przykładem może być sytuacja, w której menedżer pracujący poza firmą potrzebuje uzyskać dostęp do pendrive'a na swoim firmowym laptopie.

Biała lista protokołów. Pozwala na określenie polityki białych list według adresu IP, zakresu adresów, masek podsieci, portów sieciowych i ich zakresów.

Audyt. Funkcje audytu DeviceLock śledzą aktywność użytkowników oraz plików dla konkretnych rodzajów urządzeń, portów i zasobów sieciowych na lokalnym komputerze. Można filtrować zdarzenia audytu według użytkowników/grup, daty/czasu, rodzaju portu/urządzenia/protokołu, operacji odczytu/zapisu i operacji zakończonych sukcesem/błędem. DeviceLock wykorzystuje standardowy system rejestrowania zdarzeń i zapisuje raporty audytu w dzienniku Podglądu Zdarzeń systemu Windows. Dane można wyeksportować do wielu formatów plików a następnie zaimportować w wybranym programie służącym do zarządzania raportami. Dodatkowo, wpisy audytu mogą być automatycznie zbierane ze zdalnych komputerów i składowane centralnie na serwerze SQL. Nawet użytkownicy z prawami lokalnego administratora nie mogą modyfikować, usuwać lub w inny sposub manipulować wpisami audytu wysyłanymi do DeviceLock Enterprise Server.

Tworzenie cienia danych. Opcjonalna funkcja tworzenia cienia danych pozwala na jeszcze lepsze zapewnienie, że poufne dane korporacyjne nie opuszczają firmowej sieci za pośrednictwem nośników wymiennych. Funkcja ta przechwytuje kompletne kopie plików, które są kopiowane na autoryzowane urządzenia oraz PDA/smartfony (działające pod kontrolą systemu Windows Mobile), nagrywane na płyty CD/DVD a nawet drukowane przez autoryzowanych użytkowników. Cienie danych są przechowywane centralnie na istniejącym serwerze lub przy użyciu infrastruktury SQL zgodnej z ODBC.

Kontrola DLP urządzeń mobilnych. Dla urządzeń mobilnych wykorzystujących systemy Windows Mobile, iPhone OS lub Palm OS, można stosować reguły granularnej kontroli dostępu, audytu i shadowingu. Można określić typy danych, jakie wybrani użytkownicy lub grupy mogą synchronizować między firmowymi komputerami a ich urządzeniami mobilnymi. Mogą to być m.in. pliki, zdjęcia, kalendarze, wiadomości email, zadania i notatki. DeviceLock wykrywa obecność urządzeń mobilnych próbujących nawiązać połączenie poprzez interfejsy USB, COM, IrDA lub Bluetooth.

Rozpoznawanie sieci. Administratorzy mogą zdefiniować różne polityki bezpieczeństwa dla tego samego konta użytkownika w zależności od tego czy komputer jest online czy offline. Często stosowaną polityką jest wyłączenie interfejsu WiFi gdy laptop użytkownika jest podłączony do sieci firmowej i włączenie WiFi gdy komputer jest poza firmą.

Integracja z szyfrowanymi nośnikami wymiennymi. Klienci mogą wybrać rozwiązanie szyfrowania, które najbardziej im odpowiada. Dostępne rozwiązania to: Windows BitLocker To Go™, PGP® Whole Disk Encryption dla standardowego szyfrowania certyfikowanego FIPS; TrueCrypt® dla bezpłatnego szyfrowania Open Source; SafeDisk®, SecurStar® DriveCrypt Plus Pack Enterprise (DCPPE); i urządzenia flash USB Lexar Media's S1100/S3000 series. Ponadto, każde szyfrowane urządzenie USB może być wpisane na białą listę. DeviceLock pozwala na stosowanie dyskretnych reguł dostępu zarówno dla szyfrowanych i nieszyfrowanych partycji tego typu urządzeń.

Search Server. DeviceLock Search Server daje możliwość przeszukiwania danych zgromadzonych na DeviceLock Enterprise Server. W ten sposób można uzyskać dane, których nie da się znaleźć poprzez filtrowanie informacji w przeglądarkach raportów. Możliwość pełno-tekstowego wyszukiwania jest szczególnie przydatna w sytuacjach gdy trzeba odnaleźć cienie dokumentów bazując na ich treści. DeviceLock Search Server może automatycznie rozpoznawać, indeksować, wyszukiwać i wyświetlać dokumenty wielu formatów, takich jak: Adobe Acrobat (PDF), Ami Pro, Archiwa (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (dokumenty, arkusze kalkulacyjne i prezentacje), Quattro Pro, WordPerfect, WordStar i wiele innych.

Dodatkowe funkcje programu DeviceLock®

Ochrona przed keyloggerami. DeviceLock® wykrywa keyloggery podłączane do portów USB i blokuje podłączane do nich klawiatury. Ponadto, DeviceLock® zamazuje dane wprowadzane z klawiatur PS/2 i zmusza keyloggery podłączane do tych portów do rejestrowania śmieci zamiast faktycznych danych wprowadzanych z klawiatury.

Monitoring. DeviceLock® Enterprise Server może w czasie rzeczywistym monitorować zdalne komputery w celu kontrolowania stanu usługi DeviceLock. (czy jest ona uruchomiona czy też nie) oraz integralności polityki. Szczegółowe informacje są zapisywane w specjalnym dzienniku. Możliwe jest także definiowanie polityki nadrzędnej, która będzie automatycznie stosowana na wszystkich wybranych komputerach, w przypadku gdy ich bieżące polityki są przeterminowane lub nieprawidłowe.

Obsługa RSoP. Można korzystać ze standardowej wtyczki Resultant Set of Policy systemu Windows w celu przeglądania stosowanej w danym momencie polityki DeviceLock®, jak również do przewidywania, jaka polityka byłaby najodpowiedniejsza w danej sytuacji.

Przetwarzanie wsadowe. Pozwala na definiowanie ustawień dla całej grupy podobnych komputerów wyposażonych w podobne urządzenia (na przykład, komputery wyposażone w porty USB i napędy CD-ROM) w obrębie rozległych sieci korporacyjnych. Przy użyciu narzędzia DeviceLock® Enterprise Manager usługa DeviceLock® Service może być automatycznie instalowana lub uaktualniana na wszystkich komputerach w sieci.

Raporty graficzne. DeviceLock może automatycznie generować raporty graficzne bazując na wpisach audytu i shadowingu.

Raporty o uprawnieniach. Można generować raporty zawierające informacje o uprawnieniach oraz regułach audytu, które zostały zdefiniowane na wszystkich komputerach w sieci.

Raporty o urządzeniach Plug-n-Play. Można generować raporty dotyczące urządzeń USB, FireWire oraz PCMCIA podłączonych w danym momencie do komputerów w sieci oraz urządzeń, które były do nich podłączone w przeszłości.

Kształtowanie ruchu. DeviceLock® pozwala na definiowanie limitów związanych z wysyłaniem raportów z audytów oraz cieni danych przez usługi DeviceLock® Service do serwera DeviceLock® Enterprise Server. Pomaga to w zmniejszeniu obciążenia sieci.

Kompresowanie strumieni. Można skonfigurować program DeviceLock® tak, aby kompresował raporty z audytów oraz cienie danych przesyłane przez usługi DeviceLock® Services do serwera DeviceLock® Enterprise Server. Dzięki temu można zmniejszyć objętość przesyłanych danych, a tym samym zredukować obciążenie sieci.

Optymalny wybór serwera. W celu zapewnienia optymalnego transferu raportów z audytów oraz cieni danych usługi DeviceLock® Service mogą automatycznie wybierać najszybszy dostępny serwer DeviceLock® Enterprise Server.

Informacja o wymaganiach systemowych:

- OS: Windows NT4/2000/XP/2003/Vista/2008/7/8/8.1/2012, Apple OS X 10.6.8/10.7/10.8/10.9
- 64-bit: Tak
- RAM: 64 MB
- HDD: 100 MB

Rodzaje kontrolowanych urządzeń:

- Stacje dyskietek
- CD-ROM/DVD/BD
- Dowolne urządzenia wymiany danych(urządzenia flash, karty pamięci, itp.)
- Dyski twarde
- Napędy taśmowe
- Karty WiFi
- Bluetooth
- Urządzenia Apple iPhone/iPod touch/iPad, BlackBerry, Windows Mobile oraz Palm OS
- Drukarki (lokalne, sieciowe oraz wirtualne)

Chronione porty:

- USB
- FireWire
- Podczerwień
- Szeregowy oraz równoległy

Kontrola komunikacji sieciowej:

- Web Mail: Gmail, Yahoo!Mail, Windows Live Mail, AOL Mail, Mail.ru, Yandex Mail, Rambler-Mail, GMX.de, Web.de
- Social Networking: Google+, Facebook, Twitter, LiveJournal, LinkedIn, MySpace, Odnoklassniki, Vkontakte, XING.com, Studivz.de, Meinvz.de, Schuelervz.net

- Komunikatory: ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent
- Protokoły internetowe: FTP, FTP przez SSL, HTTP/HTTPS, SMTP oraz SMTP przez SSL
- Sesje Telnet

Kontrola schowka:

- Operacje kopiuj/wklej w aplikacjach
- Oddzielna kontrola rodzajów danych: typy plików, dane tekstowe, obrazki, audio, niezdefiniowane
- Zrzuty ekranów(PrintScreen oraz inne aplikacje)

Kontrola danych:

- Ponad 4000 rodzajów plików
- Dane i obiekty synchronizowane za pomocą: Microsoft ActiveSync®, Palm® HotSync, iTunes®
- Zdjęcia zwierające tekst jako obrazek (osadzone w MS Office, dokumentach PDF oraz jako samodzielne pliki graficzne)
- Analizowane formaty plików:
- Ponad 80 formatów plików między innymi Microsoft Office, Adobe PDF, OpenOffice, Lotus 1-2-3, WordPerfect, WordStar, Quattro Pro, repozytoria Email oraz archiwa, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP.

Kontrola treści - Content Filtering Technologies:

- Słowa kluczowe
- Zaawansowane wzorce wyrażeń regularnych z warunkami numerycznymi oraz wyrażenia Booleanowskie
- Zdefiniowane gotowe szablony RegExp (PESEL, numer karty kredytowej, konto bankowe, adres, paszport)
- Branżowe słowniki słów kluczowych
- Plik/Dane właściwości obiektu (nazwa, rozmiar, chronione hasłem, zawiera tekst, data/czas, itp.)

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