GFI EndPointSecurity™

Control of USB sticks, iPods and other endpoint devices

Kompleksowa kontrola wykorzystania pamięci USB oraz innych urządzeń przenośnych

Dyski i serwery komputerowe przechowują wszystkie dane firmy, od tych mało znaczące po ważne i poufne informacje. Często można przeczytać o przypadkach kradzieży lub wypłynięcia danych firmowych wyniesionych wprost z dysków twardych przy wykorzystaniu przenośnych urządzeń magazynujących dane, takich jak pamięci USB, smartfony i inne urządzenia mobilne posiadające wbudowaną pamięć. GFI EndPointSecurity™ pozwala skutecznie wykrywać nieautoryzowane kopiowanie ważnych dokumentów. Dzięki temu uzyskamy większe poczucie bezpieczeństwa i kontroli nad przepływem ważnych danych przechowywanymi na urządzeniach firmowych.

- **Świadomość przepływu informacji**
- **Ocena ryzyka wycieku danych**
- **Kontrola dostępu faksów zgodnej z wymogami prawa**

Dowiedz się więcej i rozpocznij

DARMOWY OKRES PRÓBNY

www.gfi.com/endpointsecurity

Sun Capital Sp. z o.o.

ul. Ołtaszyńska 92C/6
53-034 Wrocław
tel.: +48 071 360-81-00
sprzedaz@suncapital.pl

www.suncapital.pl

Wydajny i opłacalny serwer faksów

GFI EndPointSecurity™ pozwala centralnie zablokować dostęp do urządzeń przenośnych skutecznie chroniąc sprzęt firmowy przed wypływem danych oraz przed szkodliwymi aplikacjami, które mogą rozprzestrzeniać się za pośrednictwem urządzeń przenośnych.

Oczywiście istnieje możliwość zablokowania dostępu do urządzeń takich jak CD, dyskietek w BIOSie maszyny. W praktyce jest to jednak wysoce niewygodne rozwiązanie ze względu na konieczność każdorazowego wyłączenia komputera w sytuacji, kiedy potrzeba wgrać nowe oprogramowanie lub dokonać innej operacji wymagającej wykorzystania urządzenia zewnętrznego. GFI EndPointSecurity™ zapewnia prostą kontrolę urządzeń takich jak:

- dyskietki
- CD/DVD-ROM
- iPod/iPhone
- pamięci przenośne
- drukarki
- palmtopy
- adaptery sieciowe
- aparaty/kamery

Przegląd korzyści

- Zapobieganie wyciekom/kradzieżom danych poprzez kontrolę dostępu do pamięci przenośnych przy niewielkim nakładzie pracy administracyjnej
- Szyfrowanie zapobiega przypadkowej utracie danych wskutek zgubienia lub kradzieży urządzenia
- Ocena ryzyka wycieku danych na poziomie przenośnych urządzeń końcowych i przedstawienie sposobów jego ograniczenia
- Ochrona danych poza biurem dzięki szyfrowaniu urządzeń przenośnych
- Możliwość blokowania urządzeń ze względu na ich rodzaj, rozszerzenia plików, złącze lub identyfikator urządzenia
- Pozwala administratorom ustanawiać tymczasowy dostęp do urządzeń lub złącz w określonym terminie

Pełna lista korzyści na stronie:
www.gfi.com/endpointsecurity

Wymagania systemowe:
Windows 2000 (SP4), X P, Vista, 7, and 8, Windows Servers 8 i 2012 (w wersji x86 lub x64)
Internet Explorer 5.5 lub nowszy
.NET Framework w wersji 4.0
Port: port TCP 1116 (domyślnie)
Silnik bazy danych: SQL Server 2000/2005/2008; jeśli jest niedostępny, GFI EndPointSecurity może automatycznie pograć, zainstalować i skonfigurować silnik SQL Server Express.

GFI®

Ze względu na rosnącą popularność takich urządzeń jak smartfony, odtwarzacze multimedialne, pamięci przenośne, urządzenia sieciowe i łatwe w ukryciu pendrive'y USB obserwujemy zwiększone ryzyko wycieku danych, zainfekowania wirusami, instalacji nielicencjonowanych programów i gier oraz innych złośliwych działań prowadzonych za pośrednictwem sieci.

Co prawda większość firm stosuje oprogramowanie antywirusowe, zapory ogniowe oraz ochronę ruchu www i poczty e-mail w celu zabezpiezenia się przed zagrożeniami z zewnątrz, jednak niewiele z nich zdaje sobie sprawę, jak łatwo pracownik może skopiować ogromne ilości poufnych i wrażliwych handlowo informacji na pamięć przenośną bez niczyjej wiedzy.

Fizyczna blokada wszystkich złącz USB jest niepraktyczna i właściwie niewykonalna. Dlatego zarządzanie wykorzystaniem urządzeń przenośnych wymaga instalacji rozwiązania, które pozwoli administratorom sprawdzać, jakie urządzenia końcowe są aktualnie używane, kto ich używa oraz jakie dane zostały na nie skopiowane.

Zasada działania

W celu kontroli dostępu GFI EndPointSecurity automatycznie instaluje na urządzeniach w sieci ukryty program-agenta, który jest odporny na próby obejścia zabezpieczeń. Do jego zainstalowania w całej sieci wystarczy kilka kliknięć. Program jest wysoce odporny nawet na ingerencje ze strony użytkowników posiadających prawa administratora.

Zarządzanie dostępem i ochrona sieci przed zagrożeniami z pamięci przenośnych

GFI EndPointSecurity pozwala całkowicie zablokować użytkownikom dostęp do pamięci przenośnych, co uniemożliwia im kradzież danych oraz wprowadzanie danych, które mogłyby stanowić zagrożenie dla sieci. Co prawda niektóre złącza można blokować na poziomie BIOS, lecz w praktyce takie rozwiązanie okazuje się niewygodne, a poza tym obejście takiego zabezpieczenia dla zaawansowanego użytkownika nie stanowi większego problemu. GFI EndPointSecurity zapewnia kontrolę nad szeroką gamą urządzeń.

Logowanie aktywności urządzeń przenośnych w sieci

Oprócz blokowania dostępu do przenośnych urządzeń magazynujących dane GFI EndPointSecurity zapisuje aktywność użytkowników związaną z urządzeniami w dzienniku zdarzeń oraz na centralnym serwerze SQL. Każdorazowo przy podłączeniu autoryzowanego urządzenia zapisywana jest lista wszystkich plików na danym urządzeniu, do których nastąpił dostęp.

Szyfrowanie urządzeń przenośnych

Użytkownikom można zezwolić na przechowywanie danych na urządzeniach USB pod warunkiem ich zaszyfrowania. Dostęp do nich poza siecią firmy można ściśle kontrolować za pomocą specjalnej aplikacji przenośnej, która stanowi cześć GFI EndPointSecurity.

Pozostałe funkcje:

Kreator polityki kontroli, umożliwiający szczegółową kontrolę dostępu
Podsumowanie dzienne/tygodniowe
Monitoring i alarmy w czasie rzeczywistym
Kompleksowe raporty na temat wykorzystania urządzeń generowane za pomocą dodatku GFI ReportPack
Obsługa funkcji Bitlocker To Go w systemie Windows 7
Definiowanie wiadomości wyświetlanych w przypadku, gdy użytkownik nie ma prawa skorzystać z urządzenia
Możliwość przeglądania przechowywanych w bazie danych dzienników aktywności użytkowników i wykorzystania urządzeń
Możliwość grupowania komputerów ze względu na dział, domenę itp.
Współpraca z systemami operacyjnymi w każdej wersji językowej zgodnej z Unicode
...i wiele innych!

SUNCAPITAL
ul. Ołtaszyńska 92C/6
Wrocław, 53-034
Tel.: +48 (0) 71 360-81-00
Fax: +48 (0) 71 794-93-76
sprzedaz@suncapital.pl