

Trend Micro™

# LeakProof™ 5.0

Kompletna ochrona przed utratą danych, niższe koszty i prostota obsługi

Ochrona przed utratą danych (DLP) jest konieczna dla zapobiegania przypadkowym i złośliwym wyciekom istotnych danych, takich jak informacje o klientach, dane finansowe, własność intelektualna lub tajemnice handlowe. Każdy taki incydent może kosztować miliony, doprowadzając do utraty reputacji i klientów, kar finansowych, a nawet spraw sądowych.

Identyfikowanie, śledzenie i zabezpieczanie wszystkich poufnych informacji: przechowywanych, używanych, a także przesyłanych, to prawdziwe wyzwanie. Jest to coraz trudniejsze z uwagi na wzrastające czynniki ryzyka, do których można zaliczyć zestresowanych pracowników obawiających się zwolnień, pracowników mobilnych, a także punkty wycieku danych, takie jak dyski USB, webmail, komunikatory i dyski CD/DVD.

**Trend Micro™ LeakProof™** to rozwiązanie służące do zapobiegania utracie danych. Redukuje koszty, jest proste w obsłudze i oferuje najszerszy dostępny zakres ochrony, najwyższą wydajność i elastyczne metody instalacji. Rozwiązanie to jest dostępne w dwóch wersjach: **LeakProof Standard**, która umożliwia organizacjom zachowanie zgodności z przepisami poprzez ochronę danych pracowników i klientów, oraz **LeakProof Advanced**, oferującej identyczną ochronę, a ponadto zaawansowaną technologię fingerprintingu DataDNA™, chroniącą własność intelektualną za pomocą sygnatur, będących cyfrowymi odpowiednikami „odcisków palców”. Obie wersje oparto na architekturze klient-serwer:

- **Klient LeakProof** to nieinwazyjne oprogramowanie do monitorowania i egzekwowania reguł, wykrywające utratę danych i zapobiegające jej w każdym punkcie końcowym. Komponent ten uwzględnia w swoim działaniu szerokie spektrum zagrożeń, występujących zarówno w trybie online, jak i offline. Komunikuje się z serwerem, z którego pobiera aktualizacje fingerprintów oraz do którego przesyła raporty o naruszeniach.
- **Serwer LeakProof** stanowi centralny punkt analizy i kontroli. Wykrywa i odczytuje fingerprinty, egzekwuje reguły i zawiera narzędzia do raportowania. Komponent serwerowy jest dostępny jako urządzenie sprzętowe lub wirtualne (wówczas jego rolę pełni oprogramowanie), co zapewnia wysoką elastyczność i mniejsze koszty.

## ZALETY ROZWIĄZANIA DO OCHRONY PRZED UTRATĄ DANYCH

### Niskie koszty i prostota obsługi

- Szybsza ochrona dzięki nowym szablonom zgodności, uruchamianym jednym przyciskiem.
- Oszczędność czasu za sprawą nowego interfejsu użytkownika, integracji z usługą Active Directory oraz zasadom na poziomie grup i pojedynczych użytkowników.
- Mniejsze obciążenie działu IT dzięki administracji delegowanej oraz kontroli nad dostępem i urządzeniami użytkownika końcowego.
- Zróżnicowane opcje cenowe oraz elastyczność wyboru spośród dwóch wersji i wielu postaci rozwiązań.

### Rozszerzona ochrona prywatności

- Pomoc w zapewnieniu zgodności poprzez zwiększenie liczby punktów kontroli i rozszerzenie zakresu ochrony.
- Nowe filtry dla programów Skype, P2P, udziałów plikowych systemu Windows, programu ActiveSync, schowka i drukarek sieciowych.
- Zabezpieczenie innych kanałów sieciowych, takich jak poczta elektroniczna, webmail, protokoły HTTP/S, FTP oraz komunikatory.
- Zabezpieczenie wejść i wyjść punktów końcowych, takich jak transfer plików na dyski USB i dyski CD/DVD.

### Wykrywanie danych i skanowanie

- Niezwykle precyzyjne wyszukiwanie danych wrażliwych na komputerach przenośnych, stacjonarnych i serwerach.
- Ochrona w czasie rzeczywistym, zapewniona

dzięki bieżącemu egzekwowaniu zasad i zastosowaniu wielu silników dopasowywania reguł.

- Stałe monitorowanie danych przesyłanych, przechowywanych i używanych, zapobiegające ich utracie.
- Blokowanie nieautoryzowanych prób przesyłania danych.

### Zaawansowana ochrona własności intelektualnej (tylko w wersji LeakProof Advanced)

- Zabezpieczanie danych chronionych prawem autorskim przy użyciu niesłychanie skutecznej technologii fingerprintingu DataDNA™ fingerprinting.
- Zmniejszenie rozmiaru fingerprintów aż o 90%, a w rezultacie wzrost skalowalności bez ustępstw na polu skuteczności działania algorytmów fingerprintingu.
- Zwiększenie wydajności, wynikające z zastosowania nowej funkcji wyszukiwania fingerprintów na poziomie punktów końcowych, co umożliwia ich identyfikację w czasie rzeczywistym.

### Interaktywna edukacja pracowników i środki zapobiegawcze

- Ostrzeżenie pracowników o specjalnym charakterze danych i o ryzykownych zachowaniach, z możliwością blokowania tych zachowań lub zezwolenia na nie przy odpowiednim ich uzasadnieniu.
- Użycie okien dialogowych w celu edukowania pracowników na temat odpowiedniego obchodzenia się z poufnymi informacjami.
- Brak negatywnego wpływu na przebieg procesów biznesowych.

## OCHRONA PRZED UTRATĄ DANYCH

- Urządzenia przenośne, działy, całe korporacje
- Punkty końcowe, działające w trybie online i offline
- Sieci korporacyjne
- Sieci publiczne
- Komunikacja Peer-to-Peer, Skype, Bluetooth, WiFi itp.
- Dane przesyłane, przechowywane, używane

## OCHRONA PRZED ZAGROŻENIAMI

### Zagrożenia zewnętrzne

- Złośliwe oprogramowanie do kradzieży danych
- Hakerzy

### Zagrożenia wewnętrzne

- Ochrona przed przypadkową utratą danych
- Ochrona przed celowo spowodowaną utratą danych

## GŁÓWNE KORZYŚCI

- **Ochrona prywatności** — wykrywanie, monitorowanie i ochrona przed utratą poufnych danych zarówno w sieci, jak i poza nią.
- **Ochrona własności intelektualnej** — identyfikowanie, monitorowanie i ochrona tajemnic handlowych.
- **Zgodność z przepisami** — wdrożenie kontroli w zakresie ochrony, widoczności i egzekwowania reguł.
- **Edukowanie i zapobieganie** — używanie dostosowanych przez użytkownika, interaktywnych okien dialogowych w celu zapobiegania ryzykownym działaniom pracowników oraz utracie danych.
- **Wykrywanie danych wrażliwych** — wyszukiwanie danych o szczególnym znaczeniu na komputerach przenośnych, stacjonarnych i serwerach.

## Polecane przez klientów

“ Choć mieliśmy już ustalone procedury sprawdzania danych, dopiero przejrzystość, jaką zaferowało nam rozwiązanie Trend Micro LeakProof, pozwoliła nam poczuć się pewnie i zyskać dowody, że dane zostały dostatecznie zabezpieczone. ”

Lucia Johnson  
Menedżer ds. systemów informacyjnych  
Associated Fuel Pump Systems Corporation

LeakProof 5.0		
Najważniejsze funkcje ochrony przed utratą danych:	Standard	Advanced
Wykrywanie, monitorowanie, blokowanie i szyfrowanie danych prywatnych oraz przegląd stanu punktów końcowych w czasie rzeczywistym.	✓	✓
Wysokowydajne filtrowanie z wykorzystaniem słów kluczowych, metadanych i wyrażeń regularnych przy minimalnym obciążeniu dla komputerów.	✓	✓
Zaawansowane egzekwowanie zasad na poziomie użytkownika lub grupy Active Directory, domen systemu Windows i grup punktów końcowych.	✓	✓
Kontrola urządzeń wejścia/wyjścia: porty USB, napędy CD/DVD, komunikacja Bluetooth, IrDA, porty COM, LPT i inne.	✓	✓
Obsługa szerokiej gamy systemów komunikacyjnych: poczta elektroniczna, webmail, komunikatory, protokoły P2P, FTP, Skype, udziały plikowe systemu Windows, program ActiveSync i nie tylko.	✓	✓
Elastyczność i skalowalność wdrażania, z możliwością wyboru urządzenia w wersji sprzętowej lub wirtualnej, opartej na oprogramowaniu.	✓	✓
Ograniczenie zakresu administracji i łącznego kosztu posiadania dzięki nowemu interfejsowi użytkownika, dziesięciokrotnie szybszej instalacji, szablonom zgodności, szyfrowaniu itp.	✓	✓
Zabezpieczenie własności intelektualnej przy użyciu technologii fingerprintingu DataDNA™ zmniejszającej o 90% rozmiar fingerprintów i zwiększającej wydajność, skalowalność i skuteczność identyfikacji.		✓

## MINIMALNE WYMAGANIA SYSTEMOWE

### Oprogramowanie LeakProof Client Obsługiwane platformy Microsoft:

- Windows 2008
- Windows 2003
- Windows Vista
- Windows XP

### Urządzenie sprzętowe LeakProof Server

- Dedykowane, montowane w szafie urządzenie o wielkości 1U
- Podwyższony stopień bezpieczeństwa
- **Procesor:** Quad Core Xeon E5410, pamięć podręczna 2 x 6 MB, 2,33 GHz, magistrala FSB 1333 MHz, PE1950, OEM (223-5027)
- **Pamięć:** 4 GB 667 MHz (4 x 1 GB), moduły pamięci DIMM typu Single Rank z pełnym buforowaniem
- **Pamięć masowa:** 250 GB, 7200 obr./min, interfejs Serial ATA 3 Gb/s, 3,5-calowy dysk twardy typu HotPlug
- **Karta sieciowa:** Dual Embedded Broadcom NetXtreme II 5708, standard Gigabit Ethernet

### Urządzenie wirtualne LeakProof Server — wersja VMWare

- **Procesor:** Intel XEON lub dwurdzeniowy AMD Opteron
- **Pamięć:** 512 MB
- **Pamięć masowa:** 30 GB
- VMWare ESX Server 3i 3.5.0
- VMWare Workstation 6.0, 6.5

## SZEROKI ZAKRES OCHRONY TYPÓW PLIKÓW, APLIKACJI I URZĄDZEŃ

### Obsługiwane typy plików

- Rozpoznawanie i przetwarzanie ponad 300 typów plików
- Pliki pakietu Microsoft™ Office, łącznie z formatami wersji Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™; Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, format tekstowy itp.
- Pliki graficzne: Visio, Postscript, PDF, TIFF itd.
- Pliki zawierające kod źródłowy oraz biblioteki: C/C++, JAVA, Verilog, AutoCAD itp.
- Pliki zarchiwizowane i skompresowane: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH itp.

### Kontrola sieci i aplikacji

- Poczta elektroniczna: Microsoft Outlook, Lotus Notes oraz poczta SMTP
- Webmail: MSN/Hotmail, Yahoo, GMail, AOL Mail i inne
- Komunikatory internetowe: MSN, AIM, Yahoo i inne
- Protokoły sieciowe: FTP, HTTP/HTTPS i SMTP

### Kontrola punktów końcowych

- Porty USB, SCSI, (S)ATA, EIDE, PCMCIA, napędy CD/DVD, stacje dyskietek, komunikacja IrDA, WiFi, drukarki, urządzenia do przetwarzania obrazów, porty COM oraz LPT



©2009 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo t-ball firmy Trend Micro, DataDNA i LeakProof są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Trend Micro Incorporated. Pozostałe nazwy firm i produktów mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. [DS05\_LeakProof5\_090420PL]

[www.trendmicro.com](http://www.trendmicro.com)