

Trend Micro™

# LeakProof™ 3.0

Protezione completa dei dati sensibili a riposo, in uso e in movimento

La perdita di informazioni proprietarie e di proprietà intellettuale può dare origine a multe, controversie, danni d'immagine e pubblicità negativa. Per proteggere i dati sensibili, le aziende hanno bisogno di una soluzione efficace di prevenzione delle fughe di dati (DLP, Data Leak Prevention), che tenga traccia delle potenziali perdite di informazioni al punto di utilizzo. Tuttavia, l'esplosione dei sistemi di messaggistica, le connessioni di rete wireless e i dispositivi di storage USB hanno reso difficile la protezione dei dati aziendali critici. Si sta pertanto registrando un incremento delle perdite e dei furto di dati ad opera di dipendenti o fornitori che, volontariamente o accidentalmente, causano fughe di dati.

Inoltre, per garantire la conformità normativa rispetto alla governance aziendale e alle norme sulla privacy (quali SB-1386, GLBA, EU DPD, Sarbanes-Oxley e HIPAA) sono necessari criteri di sicurezza completi con cui tutelare la riservatezza delle informazioni e la privacy dei clienti. Per raggiungere tali obiettivi occorrono soluzioni intelligenti di filtro dei contenuti, che applichino i criteri di sicurezza e forniscano ai dipendenti informazioni riguardo la corretta gestione dei dati.

Trend Micro™ Leak Proof™ impedisce le fughe di dati aziendali grazie a una strategia esclusiva che unisce l'applicazione dei criteri di sicurezza ai punti terminali a tecnologie avanzate per il rilevamento delle impronte e la corrispondenza dei contenuti. La soluzione LeakProof completa è costituita da un client software e da un dispositivo:

- **Client LeakProof Anti-Leak:** comprende un potente software non intrusivo di monitoraggio e applicazione dei criteri di sicurezza che rileva e previene le fughe di dati in corrispondenza dei diversi punti terminali. Il client comunica con il server DataDNA™ per ricevere gli aggiornamenti dei criteri e delle impronte e segnala al server eventuali violazioni.
- **Server LeakProof DataDNA™:** è un dispositivo che offre un punto centrale di visibilità, la configurazione dei criteri e l'estrazione delle impronte dalle origini dei contenuti. Un'interfaccia Web supporta un flusso di lavoro amministrativo per l'individuazione, la classificazione, l'impostazione dei criteri e la segnalazione.

## PROTEZIONE COMPLETA: DATI, PORTE, CANALI, RETI

LeakProof assicura la più ampia copertura possibile per il perimetro della rete e i punti terminali. La copertura comprende canali di rete quali HTTP/S, SMTP, Webmail, FTP e IM, oltre all'input/output ai punti terminali quale il trasferimento dei file su unità USB o masterizzatori CD/DVD. I moduli di filtro incorporati ispezionano il contenuto prima che venga codificato, per proteggere attività tramite browser Web e applicazioni e-mail. I responsabili informatici possono disattivare facilmente dispositivi specifici.

## RILEVAMENTO ACCURATO CON LA TECNOLOGIA DATADNA™

Una tecnologia con brevetto in via di approvazione rileva i dati sensibili con precisione e prestazioni di massimo livello. I motori che si occupano delle corrispondenze assicurano il filtro in tempo reale tramite rilevamento delle impronte, espressioni regolari, parole chiave e metadati. Potenti algoritmi estraggono le informazioni dal contenuto e creano una sequenza di DNA, o "impronta", esclusiva per ciascun documento, che consente di eseguire l'applicazione dei criteri di sicurezza basata su punti terminali online o offline.

## NOVITÀ! FORMAZIONE INTERATTIVA DEI DIPENDENTI, CRITTOGRAFIA E FLUSSO DI LAVORO

Gli "avvisi" interattivi consentono ai responsabili IT di definire finestre di dialogo che vengono visualizzate direttamente sul monitor dei dipendenti in base al contesto. Le finestre di dialogo contengono collegamenti URL personalizzati che forniscono ai dipendenti informazioni sulla corretta gestione dei dati riservati. È possibile bloccare i trasferimenti non autorizzati oppure richiedere ai dipendenti di copiare i dati su dispositivi USB mediante il modulo incorporato di codifica dei dati.

## INDIVIDUAZIONE DEI DATI E SCANSIONI DI SICUREZZA

Grazie al monitoraggio continuo, LeakProof™ fornisce ai responsabili della sicurezza aziendale e della conformità funzionalità di tipo radar per individuare dati sensibili e ridurre il rischio di violazione della riservatezza dei dati. LeakProof individua eventuali dati non autorizzati che risiedono nei punti terminali quali computer laptop o desktop e server.

## PREVENZIONE DELLE FUGHE DI DATI

- Sede centrale, filiali, dispositivi mobili
- Punti terminali online e offline
- Reti aziendali
- Reti pubbliche
- USB, Bluetooth, WiFi, e-mail
- Dati in movimento, a riposo e in uso

## PROTEZIONE DALLE MINACCE

- Fughe di dati
- Perdita di dati
- Minacce dall'interno

## VANTAGGI PRINCIPALI

- **Protezione della privacy:** monitoraggio e prevenzione dell'uso improprio dei dati di clienti e dipendenti
- **Protezione della proprietà intellettuale:** rilevamento, classificazione e protezione delle risorse aziendali critiche
- **Conformità alle normative sulla privacy:** monitoraggio dell'uso, scansione dei punti terminali e formazione dei dipendenti per ridurre i rischi
- **Formazione dei dipendenti:** personalizzazione di finestre di dialogo interattive per la formazione e i flussi di lavoro dei dipendenti
- **Individuazione di dati sensibili:** rilevamento di dati sensibili su computer laptop e desktop e su server

*"Trend Micro LeakProof™ assicura agli amministratori un maggiore controllo su ciò che i dipendenti vedono e sono autorizzati a fare grazie alle finestre di dialogo interattive, che forniscono informazioni e agevolano la risoluzione dei problemi di sicurezza."*

*Martin Hodgett, CIO  
Orchard Supply Hardware (OSH)*

## SINTESI DELLE CARATTERISTICHE DI LEAKPROOF PER LA PREVENZIONE DELLE FUGHE DI DATI

### Corrispondenza delle informazioni sensibili

- Corrispondenza di impronte, espressioni regolari, parole chiave, metadati
- Dati strutturati e non strutturati
- Corrispondenza parziale di file di testo e corrispondenza esatta di file binari
- Indipendenza dalla lingua

### Criteri di sicurezza granulari

- Registrazione, avvisi lato server, avvisi lato client, blocco, crittografia, giustificazione
- Criteri distinti per violazioni online e offline
- Criteri di sicurezza per dominio dei punti terminali e basati su gruppi
- Perimetro di protezione configurabile: LAN, PC, domini e-mail affidabili/non affidabili

### Individuazione e gestione della topologia dei punti terminali

- Individuazione informatica dei punti terminali aziendali
- Visualizzazione su mappa in tempo reale dello stato dei punti terminali
- Monitoraggio e gestione centralizzati dello stato dei client
- Visualizzazione dettagliata dello stato dei punti terminali
- Individuazione di dispositivi I/O non autorizzati ai punti terminali

### Controllo dispositivi e applicazioni

- Controllo di tutti i dispositivi I/O: USB, CD/DVD, floppy, Bluetooth, IrDA, dispositivi di riproduzione, porte COM e LPT ecc.
- Blocco della funzione di stampa schermata (tasto Stamp)

### Monitoraggio e segnalazione

- Dashboard in tempo reale e rapporti sulla violazione della sicurezza riepilogati per punto terminale, utente ecc.
- Analisi delle tendenze e interruzione del canale delle violazioni
- Rapporti pianificati e su richiesta sulle violazioni della sicurezza
- Funzione opzionale di acquisizione forense che registra la violazione effettiva dei file sul server DataDNA per successiva ispezione

### Modelli di conformità

- Classificazioni e criteri preconfigurati a supporto della conformità normativa quali PCI, GLBA, SB-1386 e SOX
- Criteri incorporati con moduli di convalida per elementi quali previdenza sociale, carta di credito, instradamento ABA, documenti identificativi nazionali canadesi e cinesi e riconoscimento dei nomi americani

### Amministrazione e scalabilità di sistema

- Interfaccia di gestione tramite browser Web
- Amministrazione basata sui ruoli e controllo di accesso ai contenuti sensibili
- Integrazione con LDAP e Active Directory
- Clustering del server di gestione per la scalabilità aziendale
- Comunicazione sicura tra punto terminale e server tramite SSL

## REQUISITI MINIMI DI SISTEMA

### Software client LeakProof Anti-Leak

- **Piattaforme supportate:** Microsoft Vista, Windows XP, Windows 2000, Windows 2003 Server

### Dispositivo server LeakProof DataDNA

- Dispositivo 1U installabile su rack
- Potenziamento della sicurezza
- NIC Gigabit
- Disponibile con CPU singola o doppia
- Memoria: 2 GB/4 GB
- Spazio di memorizzazione: 160 GB/300 GB RAID

## COPERTURA COMPLETA DI TIPI DI FILE, APPLICAZIONI E DISPOSITIVI



### Server LeakProof DataDNA

Il dispositivo server LeakProof DataDNA in abbinamento al software client LeakProof Anti-Leak protegge le informazioni sensibili dalla perdita e dal furto di dati e dalle minacce provenienti dall'interno.

### Tipi di file supportati

- Riconoscimento ed elaborazione di più di 300 tipi di file
- File Microsoft™ Office, compresi Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™, Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, file di testo ecc.
- File grafici: Visio, Postscript, PDF, TIFF ecc.
- File software/di progettazione: C/C++, JAVA, Verilog, AutoCAD ecc.
- File di archivio/compressi: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH ecc.

### Controllo di rete/applicazioni

- E-mail: Microsoft Outlook, Lotus Notes e SMTP Email
- Webmail: MSN/Hotmail, Yahoo, GMail, AOL Mail ecc.
- Messaggistica immediata: MSN, AIM, Yahoo ecc.
- Protocolli di rete: FTP, HTTP/HTTPS e SMTP

### Controllo dei dispositivi ai punti terminali

- USB, SCSI, (S)ATA, EIDE, PCMCIA, CD/DVD, floppy, Bluetooth, IrDA, WiFi, stampanti, dispositivi di riproduzione, porta COM, porta LPT ecc.



Trend Micro, il logo della pallina con il disegno di una T, DataDNA e LeakProof sono marchi o marchi registrati di Trend Micro, Incorporated. Tutti gli altri nomi di aziende o prodotti potrebbero essere marchi o marchi registrati dei rispettivi proprietari.  
[DS05\_TMLP\_071203IT]