

Trend Micro™

LeakProof™ 5.0

Umfassender Schutz vor Datenverlust senkt Kosten und Verwaltungsaufwand

Schutz vor Datenverlust (DLP) ist unerlässlich, um unbeabsichtigte oder mutwillige Datenlecks zu schließen - unabhängig davon, ob es sich um Kundendaten, Finanzdaten, geistiges Eigentum oder Geschäftsgeheimnisse handelt. Schon ein einziger Vorfall reicht aus, um Kosten in Millionenhöhe durch Imageschäden, Geldbußen und Haftungsansprüche zu verursachen.

Der Schutz vor Datenverlust muss in der Lage sein, alle vertraulichen Daten im Speicher, bei der Bearbeitung und bei der Übertragung zu erkennen, nachzuverfolgen und zu schützen. Diese Aufgabe gestaltet sich wegen der zunehmenden Risikofaktoren, wie Mitarbeiter, die um ihren Arbeitsplatz fürchten, mobiles Personal und andere undichte Stellen, wie USB-Laufwerke, Webmail, Instant Messaging und CDs/DVDs, immer schwieriger.

Trend Micro™ LeakProof™ ist eine Lösung zum Schutz vor Datenverlust (DLP), die Aufwand und Kosten senkt - mit umfassendstem Schutz, höchster Leistung und größtmöglicher Flexibilität bei der Verteilung. Die Lösung ist in zwei Versionen verfügbar. Durch den Schutz von Mitarbeiter- und Kundendaten hilft **LeakProof Standard** bei der Einhaltung behördlicher Auflagen. **LeakProof Advanced** bietet zusätzlich zu den Standard-Funktionen erweiterte DataDNA™ Authentizitätsprüfung zum Schutz geistigen Eigentums. Beide Versionen bestehen aus Client und Server:

- **LeakProof Client:** Eine im Hintergrund ausgeführte Software zur Überwachung und Durchsetzung von Richtlinien, die an allen Endpunkten Datenverluste entdeckt und verhindert. Der Schutz erstreckt sich auf eine Vielzahl unterschiedlicher Infektionswege, egal ob online oder offline. Der Client kommuniziert mit dem Server, von dem er Richtlinien- und Authentizitätsdaten-Updates erhält; im Gegenzug meldet der Client dem Server Verstöße gegen die Sicherheitsrichtlinien.
- **LeakProof Server:** Die Appliance bietet einen zentralen Übersichts- und Steuerungspunkt für Erkennung, Extraktion von Authentizitätsdaten, Richtliniendurchsetzung und Berichterstellung. Der Server ist als Hardware-Appliance oder virtuelle Software-Appliance erhältlich und ermöglicht dadurch größere Flexibilität bei geringeren Kosten.

FUNKTIONEN ZUM SCHUTZ VOR DATENVERLUST

Senkt Kosten und Verwaltungsaufwand

- Liefert schnelleren Schutz mit neuen Vorlagen zur Regeleinhaltung auf Knopfdruck
- Spart Zeit mit neuer Benutzeroberfläche, ActiveDirectory-Integration und Benutzer-/Gruppenrichtlinien
- Verringert den IT-Aufwand durch delegierte Administration sowie Geräte- und Zugriffskontrolle von Endbenutzern
- Bietet verschiedene Preisgestaltungsoptionen und Flexibilität mit zwei Versionen und unterschiedlichen Formfaktoren

Erweiterter Kundendatenschutz

- Erweiterte Kontrollstellen unterstützen die Einhaltung von Auflagen und Richtlinien und bieten größtmöglichen Schutz
- Enthält neue Filter für Skype, P2P, Windows Dateifreigaben, ActiveSync, Zwischenablage und Netzwerkdrucker
- Schützt andere Netzwerkkanäle, wie E-Mail, Webmail, HTTP/S, FTP und Instant Messaging
- Sichert Ein- und Ausgang von Daten an den Endpunkten (zum Beispiel Dateitransfer auf USB-Laufwerke und CD-/DVD-Brenner)

Datenerkennung und Suchläufe

- Findet vertrauliche Daten auf Laptops, Desktops und Servern mit der Präzision eines Radargerätes
- Verwendet Richtliniendurchsetzung und unterschiedliche Abgleich-Engines zum Schutz in Echtzeit
- Verhindert Datenverluste durch dauerhafte Überwachung von Daten im Speicher, bei der Bearbeitung und Übertragung
- Sperrt unerlaubten Datentransfer

Erweiterter Schutz geistigen Eigentums (nur LeakProof Advanced)

- Schützt geistiges Eigentum mit hochpräziser DataDNA™ Technologie zur Authentizitätsprüfung
- Reduziert die Größe des Fingerabdrucks um über 90 % und erhöht damit die Skalierbarkeit ohne Verzicht auf Präzision
- Verbessert die Leistung mit neuem Fingerabdruck-Crawler am Endpunkt und ermöglicht dadurch Identifizierung in Echtzeit

Interaktive Mitarbeiterschulungen und Korrekturmaßnahmen

- Macht Mitarbeiter auf vertrauliche Inhalte und gefährliches Verhalten aufmerksam und verfügt über Optionen zum Sperren oder Zulassen bei ausreichendem Grund
- Verwendet Dialogfelder, um Mitarbeiter im angemessenen Umgang mit vertraulichen Daten zu schulen
- Beeinträchtigt keine Unternehmensabläufe

SCHUTZ VOR DATENVERLUST

- Mobile Mitarbeiter, Zweigstelle, Hauptsitz
- Endpunkte – online oder offline
- Unternehmensnetzwerke
- Öffentliche Netzwerke
- P2P, Skype, Bluetooth, WiFi und mehr
- Daten im Speicher, bei der Bearbeitung oder Übertragung

SCHUTZUMFANG

Externe Bedrohungen

- Malware, die Daten entwendet
- Hacker

Interne Bedrohungen

- Unbeabsichtigter Datenverlust
- Mutwilliger Datenverlust

ENTSCHEIDENDE VORTEILE

- **Schutz der Privatsphäre:** Den Verlust vertraulicher Daten erkennen, überwachen und verhindern – innerhalb und außerhalb des Netzwerks
- **Schutz geistigen Eigentums:** Geschäftsgeheimnisse erkennen, überwachen und schützen
- **Einhaltung behördlicher Bestimmungen:** Kontrollmöglichkeiten für Schutz, Sichtbarkeit und Durchsetzung implementieren
- **Erziehen und korrigieren:** Interaktive Dialoge anpassen, um riskantes Mitarbeiterverhalten und Datenverluste zu unterbinden
- **Vertrauliche Daten entdecken:** Vertrauliche Daten auf Laptops, Desktops und Servern finden

Von Kunden empfohlen

- „Trotz bereits bestehender Verfahren zur Überprüfung von Daten erhielten wir erst durch Trend Micro LeakProof die erforderliche Transparenz, um gewünschte Datenschutzzvorgaben zu gewährleisten und auch zu belegen.“

Lucia Johnson

Information Systems Manager
Associated Fuel Pump Systems Corporation

LeakProof 5.0		
Wichtige Funktionen zum Schutz vor Datenverlust	Standard	Advanced
Erkennen, Überwachen, Sperren und Verschlüsseln vertraulicher Daten mit Anzeige des Endpunktstatus in Echtzeit	✓	✓
Leistungsstarke Filter, basierend auf Schlüsselwörtern, Meta-Daten und regulären Ausdrücken, mit geringer Auswirkung auf die Systemleistung	✓	✓
Gezielte Richtliniendurchsetzung nach ActiveDirectory-Benutzer oder -Gruppe, Windows Domäne und Endpunktgruppen	✓	✓
Überwachung von Ein-/Ausgabegeräten: USB, CD/DVD, IrDA, Bluetooth, COM- und LPT-Ports und vieles mehr	✓	✓
Umfassender Schutz von Kommunikationssystemen: E-Mail, Webmail, IM, P2P, FTP, Skype, Windows Dateifreigaben, ActiveSync und vieles mehr	✓	✓
Flexible und skalierbare Verteilung wahlweise mit Hardware-Appliance oder virtueller Software-Appliance	✓	✓
Geringer Administrationsaufwand und niedrige Gesamtbetriebskosten (TCO) durch neue Benutzeroberfläche, Warnmeldungen, zehnfach schnellere Verteilung, Vorlagen für die Regeleinhaltung, Verschlüsselung und vieles mehr.	✓	✓
Schutz geistigen Eigentums durch DataDNA™ Technologie mit um 90 % kleinerem Fingerabdruck ermöglicht höhere Leistung, Skalierbarkeit und Präzision		✓

SYSTEMVORAUSSETZUNGEN

LeakProof Client Software

Unterstützte Microsoft Plattformen:

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

LeakProof Server Hardware-Appliance

- Zweckmäßige 1U-Rack-montierbare Appliance
- Sicherheitsoptimiert
- **CPU:** Quad Core Xeon E5410 Prozessor
2 x 6 MB Zwischenspeicher, 2,33 GHz,
1333 MHz FSB, PE1950, OEM (223-5027)
- **Arbeitsspeicher:** 4 GB 667 MHz
(4 X 1 GB), Single Ranked Fully Buffered DIMMs
- **Speicher:** 250 GB 7,2 K RPM Serial ATA
3 GB/sek 3,5 Zoll HotPlug Festplatte
- **NIC:** Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet Netzwerkkarte

LeakProof Server: Virtuelle Appliance – VMWare

- **CPU:** Intel XEON oder AMD Opteron
Dual-Core-Prozessor
- **Arbeitsspeicher:** 512 MB
- **Speicher:** 30 GB
- VMWare ESX Server 3i 3.5.0
- VMWare Workstation 6.0, 6.5

UMFASSENDE SCHUTZ VON DATEITYPEN, ANWENDUNGEN UND GERÄTEN

Unterstützte Dateitypen

- Erkennt und verarbeitet mehr als 300 Dateitypen
- Microsoft™ Office Dateien inkl. Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™ für E-Mails; Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, Text usw.
- Grafikdateien: Visio, Postscript, PDF, TIFF usw.
- Software-/Entwicklerdateien: C/C++, JAVA, Verilog, AutoCAD usw.
- Archivierte/komprimierte Dateien: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH usw.

Unterstützte Netzwerkanwendungen

- E-Mail: Microsoft Outlook, Lotus Notes und SMTP-E-Mail
- Web-Mail: MSN/Hotmail, Yahoo, GMail, AOL Mail und andere
- Instant Messaging: MSN, AIM, Yahoo und andere
- Netzwerkprotokolle: FTP, HTTP/HTTPS und SMTP

Unterstützte Endpunktgeräte

- USB, SCSI, (S)ATA, EIDE, PCMCIA, CD/DVD, Disketten, IrDA, WiFi, Drucker, bildnerzeugende Geräte, COM- und LPT-Ports



©2009 by Trend Micro Incorporated. Alle Rechte vorbehalten.
Trend Micro; das Trend Micro T-Ball-Logo, DataDNA und LeakProof sind
Marken oder eingetragene Marken von Trend Micro Incorporated. Alle
anderen Firmen- oder Produktnamen sind Marken oder eingetragene
Marken ihrer jeweiligen Eigentümer. [DS05_LeakProof5_090420DE]

www.trendmicro.com