

Trend Micro

Data Loss Prevention

Umfassender Schutz vor Datenverlust verringert Risiken und erhöht die Transparenz

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. Unternehmen müssen heutzutage in der Lage sein, Daten im Speicher, bei der Bearbeitung und Übertragung zu erkennen, nachzuverfolgen und zu schützen. Diese Aufgabe gestaltet sich wegen der zunehmenden Risikofaktoren, wie z. B. mobile Mitarbeiter, die weit verbreitete Nutzung von USB-Laufwerken, Webmail, Instant Messaging und CDs/DVDs, immer schwieriger.

Trend Micro™ Data Loss Prevention ist eine Produktfamilie, die entwickelt wurde, um das Risiko von Datenverlust zu minimieren und die Transparenz von Datenverwendungsmustern und risikoreichen Unternehmensabläufen zu erhöhen – so bleiben Ihre vertraulichen Informationen geschützt. Sie profitieren von umfassendem Schutz, hoher Leistung und flexiblen Verteilungsmöglichkeiten, die Sie brauchen, um behördliche Auflagen einzuhalten. Die DLP-Lösungen von Trend Micro bieten außerdem erweiterte DataDNA™ Authentizitätsprüfungen zum Schutz unstrukturierter Daten und geistigen Eigentums sowohl innerhalb als auch außerhalb des Netzwerks.

TREND MICRO™ DLP ENDPOINT

- Unterstützt die Einhaltung branchenspezifischer Richtlinien
- Schult Benutzer im richtliniengemäßen Umgang mit Unternehmensdaten
- Schützt unstrukturierte Daten und geistiges Eigentum
- Unterstützt mehrere Funktionen wie Echtzeitüberwachung, Sperren und Erkennen von Daten – mit nur einem einzelnen, leichten Agent

TREND MICRO™ DLP NETWORK MONITOR

- Überwacht Ihr Netzwerk rund um die Uhr in Echtzeit
- Unterstützt vom Trend Micro™ Smart Protection Network™
- Protokolliert und dokumentiert vertrauliche Daten, die durch die Ausgangsports des Netzwerks fließen
- Unterstützt die Regeleinhaltung, erkennt risikoreiche Unternehmensabläufe und verbessert den richtliniengemäßen Umgang mit Unternehmensdaten

TREND MICRO™ DLP MANAGEMENT SERVER

- Bietet einen zentralen Übersichts- und Steuerungspunkt für Erkennung, Extraktion von Authentizitätsdaten, Richtliniendurchsetzung und Berichterstellung von Sicherheitsverstößen
- Erhältlich als Hardware-Appliance oder virtuelle Software-Appliance und ermöglicht dadurch größere Flexibilität bei geringeren Kosten

Die wichtigsten Funktionen	Trend Micro DLP Endpoint	Trend Micro DLP Network Monitor
Erkennen, Überwachen, Sperren und Verschlüsseln vertraulicher Daten mit Anzeige des Endpunktstatus in Echtzeit	✓	Unterstützt nur Überwachung
Leistungsstarke Filter, basierend auf Schlüsselwörtern, Metadaten 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	✓	✓
Geringer Administrationsaufwand und niedrige Gesamtbetriebskosten (TCO) durch neue Benutzeroberfläche, Warnmeldungen, zehnmals schnellere Verteilung, Vorlagen für die Regeleinhaltung, Verschlüsselung und vieles mehr	✓	✓
Schutz geistigen Eigentums durch DataDNA™ Technologie mit 90 % kleinerem Fingerabdruck ermöglicht höhere Leistung, Skalierbarkeit und Präzision	✓	Unterstützt nur Überwachung

SOFTWARE- UND NETZWERK-APPLIANCE

Schutz vor Datenverlust

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

Bedrohungsschutz

- Mobile Mitarbeiter
- Interne autorisierte Benutzer
- Versehentlicher Datenverlust
- Mutwilliger Datenverlust
- Externe Bedrohungen
- Datenstehlende Malware
- Hacker
- Partner/Zulieferer

ENTSCHEIDENDE VORTEILE

- **Schutz der Privatsphäre:** Den Verlust vertraulicher Daten erkennen, überwachen und verhindern – innerhalb und außerhalb des Netzwerks
- **Schutz geistigen Eigentums:** Kritische Unternehmensdaten erkennen, überwachen und schützen – innerhalb und außerhalb des Netzwerks
- **Einhaltung von Richtlinien:** Möglichkeiten zur Steuerung von Schutz, Transparenz und Durchsetzung implementieren
- **Schulung der Mitarbeiter:** Interaktive Dialoge individuell anpassen, um Mitarbeiter über risikoreiches Verhalten zu informieren und bei Bedarf Benutzerberechtigungen anzufordern
- **Entdecken von Daten:** Vertrauliche Daten auf Laptops, Desktops und Servern finden
- **Datenstehlende Malware erkennen:** Bot-Netze, verborgene FTP-Prozesse, Keylogger, Spyware und Trojaner erkennen, die versuchen Daten zu sammeln und zu versenden

DIE WICHTIGSTEN FUNKTIONEN

Weniger Kosten und Verwaltungsaufwand

- Liefert schnelleren Schutz mit neuen Vorlagen zur Regeleinhaltung auf Knopfdruck
- Spart Zeit mit Workflow-Navigation-Engine, Active-Directory-Integration und Benutzer-/Gruppenrichtlinien
- Verringert den IT-Aufwand durch delegierte Administration sowie Geräte- und Zugriffskontrolle von Endbenutzern
- Bietet verschiedene Preisgestaltungsoptionen und Flexibilität mit zwei Modulen und unterschiedlichen Formfaktoren

Erweiterter Datenschutz

- 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)

Erkennung datenstehlender Malware mit Unterstützung durch das Smart Protection Network

- Erkennt Keylogger, Spyware, Trojaner und Bot-Netze, die versuchen Daten zu stehlen

Datenerkennung und Suchläufe

- Findet vertrauliche Daten auf Laptops, Desktops und Servern mit der Präzision eines Radargeräts
- 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

- Schützt unstrukturierte Daten mit hochpräziser DataDNA™ Authentizitätsprüfung
- Reduziert die Größe des Fingerabdrucks um über 90 % und erhöht damit die Skalierbarkeit ohne Präzisionsverlust
- 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
- Verwendet Dialogfelder, um Mitarbeiter im angemessenen Umgang mit vertraulichen Daten zu schulen
- Beeinträchtigt keine Unternehmensabläufe

UMFASSENDE SCHUTZ VON DATEITYPEN, ANWENDUNGEN UND GERÄTEN

Unterstützte Dateitypen

- Erkennt und verarbeitet über 300 Dateitypen
- Microsoft® Office Dateien, inklusive 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.

Kontrollpunkte für Daten bei der Übertragung

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

Kontrollpunkte für Daten während der Bearbeitung

- USB, CD/DVD, COM- und LPT-Ports, Kopieren/Einfügen, Wechselspeichermedien, Disketten, Infrarot- und bildgebende Geräte, Geräte mit Bildschirm-Druckfunktion, Modems, PCMCIA

„ Mit Trend Micro Data Loss Prevention haben wir eine Sicherheitsgrundlage geschaffen, und wir wissen jetzt sehr genau, wie unsere Benutzer Patientendaten verwenden. Wir erhalten sehr viele nützliche und auswertbare Informationen, die es uns ermöglichen, unsere Sicherheitsrichtlinien und deren Einhaltung zu verbessern. “

Yvan Fournier

Chief Security Officer, Centre Hospitalier Universitaire de Québec und Centre de Recherche de l'Université LAVAL



© 2010 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro T-Ball-Logo und DataDNA sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. [DS02_DLP_101013DE]

www.trendmicro.com

MINDESTSYSTEMVORAUSSETZUNGEN

Unterstützte Microsoft Plattformen für Trend Micro DLP Endpoint

- Windows 2008, 2003, Vista, 7 (32 Bit) und XP

Trend Micro DLP Endpoint

- Prozessor: 300 MHz Intel® Pentium® oder vergleichbarer Prozessor
- Arbeitsspeicher: 512 MB
- Speicherplatz: 300 MB

Trend Micro DLP Network Monitor Software-Appliance

- Prozessor: 2 x Intel® Quad Core X5550 Xeon® CPU, 2,66 GHz, 8 MB Cache, 6,40 GT/s QPI, Turbo
- Arbeitsspeicher: 8 GB Arbeitsspeicher (4 x 2 GB), 1066 MHz, Dual Ranked RDIMMs für 1 Prozessor
- Festplatte: 300 GB 15.000 RPM SAS 3,5-Zoll-Hot-Plug-Festplatte
- NIC: Intel PRO 1000 PT 1 GbE Dual Port NIC, PCIe-4
- Zertifiziert für Ausführung auf Dell R710

Trend Micro DLP Management Server Hardware-Appliance

- Zweckmäßige 1U-Rack-montierbare Appliance
- Sicherheitsoptimiert
- Prozessor: Quad Core Xeon E5506 2,13 GHz, PE R610
- Arbeitsspeicher: 6 GB, 1.333 MHz (6 x 1 GB)
- Speicherplatz: 250 GB 7.200 RPM Serial ATA 3 Gbit/s 2,5-Zoll-Hot-Plug-Festplatte
- NIC: Quad Embedded Broadcom NetXtreme II 5709 Gigabit Ethernet NIC

Virtuelle Trend Micro DLP Management Server Software-Appliance

- Prozessor: Intel XEON oder AMD Opteron Dual-Core- oder vergleichbarer Prozessor
- Arbeitsspeicher: 2 GB
- Speicherplatz: 30 GB
- VMware ESX und ESXi 3.5