

Trend Micro™

Schutz vor Datenverlust

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.

Die Produktfamilie Trend Micro™ Data Loss Prevention (DLP) schützt Ihre privaten Daten und Ihr geistiges Eigentum und senkt gleichzeitig Kosten und Verwaltungsaufwand. Sie profitieren von umfassendem Schutz, hoher Leistung und flexiblen Verteilungsmöglichkeiten, die Sie brauchen, um behördliche Auflagen einzuhalten und Mitarbeiter- und Kundendaten zu schützen. Die DLP-Lösungen von Trend Micro bieten außerdem erweiterte DataDNA™ Authentizitätsprüfung. Damit schützen Sie unstrukturierte Daten, geistiges Eigentum und Daten in allen Bearbeitungszuständen: gespeichert, verwendet oder in Bewegung.

- **Trend Micro™ DLP for Endpoint:** eine im Hintergrund ausgeführte Software zur Überwachung und Durchsetzung von Richtlinien, die Datenverluste an allen Endpunkten entdeckt und verhindert. Der Schutz erstreckt sich auf eine Vielzahl unterschiedlicher Infektionswege – online wie offline.
- **Trend Micro™ DLP for Network*:** Unterstützt durch das Trend Micro Smart Protection Network™, überwacht diese Lösung Ihr Netzwerk rund um die Uhr, um den Verlust vertraulicher Daten und geistigen Eigentums über verschiedenste Übertragungswege zu erkennen und zu dokumentieren. *Erwartet für 2. Quartal 2010
- **Trend Micro™ DLP Management Server:** Bietet einen zentralen Übersichts- und Steuerungspunkt zur Erkennung, Extraktion von Authentizitätsdaten, Richtliniendurchsetzung und zur Erstellung von Berichten über Sicherheitsverstöße. Der Server ist als Hardware-Appliance oder virtuelle Software-Appliance erhältlich und ermöglicht dadurch größere Flexibilität bei geringeren Kosten.

FUNKTIONEN ZUM SCHUTZ VOR DATENVERLUST

Weniger 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 permanente Überwachung von Daten im Speicher, in Gebrauch oder in Bewegung
- Sperrt unerlaubten Datentransfer

Erweiterter Schutz geistigen Eigentums

- Schützt geistiges Eigentum mit hochpräziser DataDNA™ Technologie zur 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 bei ausreichendem Grund
- Verwendet Dialogfelder, um Mitarbeiter in angemessenem Umgang mit vertraulichen Daten zu schulen
- Beeinträchtigt keine Unternehmensabläufe

SCHUTZ VOR DATENVERLUST

- Daten in Bewegung, im Speicher oder in Gebrauch
- Mobile Mitarbeiter, Zweigstelle, Hauptsitz
- Endpunkte – online und offline
- Unternehmensnetzwerke
- Öffentliche Netzwerke
- P2P, Skype, Active Sync und mehr

SCHUTZUMFANG

Interne Bedrohungen

- Versehentlicher Datenverlust
- Mutwilliger Datenverlust

Externe Bedrohungen

- Datenstehlende Malware
- Hacker

ENTSCHEIDENDE VORTEILE

- **Privatsphäre schützen:** Den Verlust vertraulicher Daten erkennen, überwachen und verhindern – innerhalb und außerhalb des Netzwerks
- **Geistiges Eigentum absichern:** Geschäftsgeheimnisse erkennen, überwachen und schützen
- **Behördliche Richtlinien einhalten:** Möglichkeiten zur Kontrolle von Schutz, Transparenz und Durchsetzung schaffen
- **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 [DLP] die erforderliche Transparenz, um gewünschte Datenschutzvorgaben zu gewährleisten und auch zu belegen.“

Lucia Johnson

Information Systems Manager
Associated Fuel Pump Systems Corporation

Trend Micro DLP		
Wichtige Funktionen zum Schutz vor Datenverlust	für Endpunkt	für Netzwerk
Erkennen, Überwachen, Sperren und Verschlüsseln vertraulicher Daten mit Anzeige des Endpunktstatus in Echtzeit	✓	Nur Erkennen und Überwachen
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 Regeleinholung, Verschlüsselung und vieles mehr	✓	✓
Schutz geistigen Eigentums durch DataDNA™ Technologie mit um 90 % kleinerem Fingerabdruck ermöglicht höhere Leistung, Skalierbarkeit und Präzision	✓	Nur Überwachen

SYSTEMVORAUSSETZUNGEN

Unterstützte Microsoft Plattformen

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

Trend Micro DLP für Endpoint Software

- **CPU:** 300 MHz Intel™ Pentium™ oder vergleichbarer Prozessor
- **RAM:** 512 MB
- **Speicher:** 300 MB

Virtuelle Trend Micro DLP Management Server Appliance

- **CPU:** Intel XEON oder AMD Opteron Dual-Core- oder vergleichbarer Prozessor
- **Arbeitsspeicher:** 2 GB
- **Speicher:** 30 GB
- VMWare ESX und ESXi 3.5

Virtuelle Trend Micro DLP Management 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/s 3,5 Zoll HotPlug Festplatte
- **NIC:** Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet NIC

UMFASSENDE SCHUTZ VON DATEITYPEN, ANWENDUNGEN UND GERÄTEN

Unterstützte Dateitypen

- Erkennt und verarbeitet über 300 Dateitypen
- Microsoft™ Office Dateien inkl. Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™ E-Mail; 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-Mails
- 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, CD/DVD, COM- und LPT-Ports, Wechselspeichermedien, Disketten, Infrarot- und bildgebende Geräte, Geräte mit Bildschirm-Druckfunktion, Modems, PCMCIA

