

Kontrolle über sensible Daten in Unternehmen hat höchste Priorität

Die Zukunftsfähigkeit und Effizienz eines Unternehmens hängt im großen Maße davon ab, wie gut vertrauliche Informationen geschützt werden. Der Verlust vertraulicher Daten wie Kundendatenbanken, geistiges Eigentum, Finanz- oder Rechtsdokumente, Marktforschungen oder persönliche Daten kann Unternehmen jeder Größe treffen. Ein einziger Datenverlust kann bereits dazu führen, dass die Unternehmensreputation leidet, Vertragsstrafen fällig werden, Kunden verloren gehen oder die Wettbewerbsfähigkeit in Frage gestellt wird.

Die rasche Ausbreitung von mobilen Computer-Devices, die gemeinsame Nutzung von Daten in mehreren Niederlassungen oder die verbreitete Auslagerung von Projekten und vielem mehr verursachen zusätzliche Probleme, vertrauliche Informationen sicher zu halten. Sie sind durch die traditionelle Vorgehensweise, wie Netzwerke gesichert werden, unzureichend geschützt.

Ein anderes Problem besteht darin, dass auf Grund der großen Menge an Daten Unternehmen nicht genau überblicken können, welche Daten im Einzelfall als vertraulich einzustufen sind. Normalerweise sind nur etwa 20 Prozent der Daten strukturiert. Dabei werden über 10 Prozent sensibler Daten pro Tag geändert. Neu erstellte, sogenannte Zero-Day-Dokumente, machen einen Anteil von etwa 10 Prozent am gesamten Volumen vertraulicher Daten in einem Unternehmen aus.

Das bedeutet, dass heutzutage ein umfassender Schutz sensibler Daten nur dann erreicht werden kann, wenn man den Fokus auf die Daten selbst legt.

Um den Anforderungen essentiellen Informationsschutzes gerecht zu werden, hat InfoWatch mit **InfoWatch Traffic Monitor Enterprise** eine umfangreiche Lösung zum Schutz Ihrer Daten entwickelt.

Die Software-Lösung bietet Unternehmen die Möglichkeit, die Flut an Informationen vollständig zu beherrschen und macht sichtbar, welche Daten vertraulich sind, wo und wie sie übermittelt oder gelagert werden und wer sie benutzt.



Die durchschnittlichen
Kosten für einen
Datenverlust betragen
2009 etwa 6,75
Millionen Dollar.

*Ponemon Institute,
Cost of a Data Breach Study 2009*

"Wir haben uns entschieden, InfoWatch zu wählen, weil die Produkte die effektivsten Technologien in der Datenanalyse kombinieren. Die Lösung hat uns innerhalb eines halben Jahres nach der Implementierung geholfen, 369 Verletzungen der Informationssicherheit zu verhindern."

*Svetlana Belyalova
Information Security Director
Raiffeisen Bank Russia*

Mit InfoWatch Traffic Monitor Enterprise Unternehmensdaten schützen

InfoWatch Traffic Monitor ist eine umfangreiche, aus mehreren Modulen bestehende Datenschutz-Lösung, die verschiedene Wege absichert, über die Daten nach außen gelangen können. Die Module der Lösung:

- **End-Point-Sicherheits-Modul** mit
 - Print Monitor zur Kontrolle von Druckern an Arbeitsplätzen
 - Device Monitor kontrolliert den Zugriff auf portable Geräte und entfernbare Medien und überwacht die Daten, die auf diese kopiert werden
- **Gateway-Sicherheitsmodul** mit
 - Web Monitor zur Kontrolle von Daten, die per Web-Mail, Blogs, Internet-Foren etc. gesendet werden
 - Mail Monitor zur Kontrolle von Informationen, die über das firmeninterne Mailsystem versendet werden
 - Instant Messenger Monitor zur Kontrolle von Informationen, die per Instant Messenger wie ICQ, Jabber oder andere übermittelt werden
 - Network Print Monitor zur Kontrolle von Drucker-Servern im Netzwerk
- **Forensic Storage** – ein zentrales Archiv, in dem Daten zu analytischen Zwecken aufbewahrt werden.

Zielgruppe

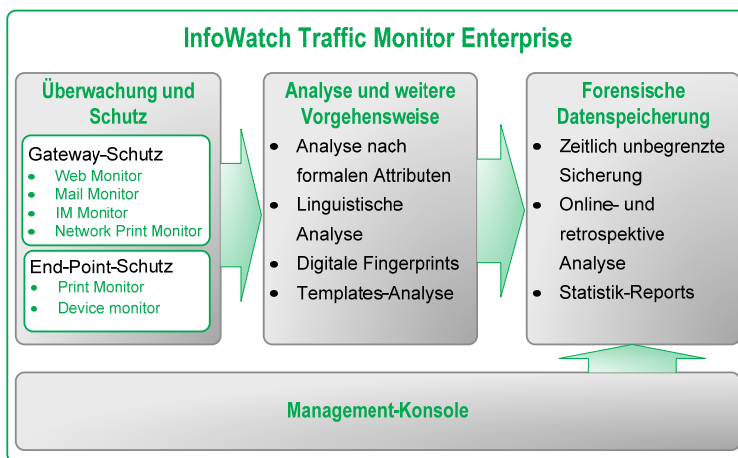
Die Lösung richtet sich an **Unternehmen**

- zur **Sicherstellung der Einhaltung von Datenschutzbestimmungen** bei Verarbeitung persönlicher Daten (Gesundheitsbereich, Banken, Hotels und weitere)
- die wertvolle Informationen (IT, pharma-zeutischer Bereich etc.) besitzen und diese vor **Verlusten schützen** müssen, die sich aus der öffentlichen Verbreitung dieser Informationen ergeben würden

Features von InfoWatch Traffic Monitor:

- Überwachung und Analyse von Daten die aus dem Unternehmensnetzwerk nach außen gesendet werden. Dies betrifft Unternehmens-E-Mail oder Web-Mail, Webseiten, Instant Messengers oder Daten, die gedruckt oder auf tragbare Laufwerke und entfernbare Speichermedien kopiert werden.
- Sensitive Data Leakage Prevention durch Blockieren von Übertragungen, wenn Verletzungen von Security-Policies festgestellt werden (beispielsweise, wenn an einen unbefugten Mitarbeiter vertrauliche Daten gesendet werden).
- Sicherung und Analyse von Daten zur forensischen Analyse.

Die Lösung lässt sich über eine benutzerfreundliche Management-Konsole administrieren.



Die Software-Architektur

Die Gesamtzahl an Datenverlusten ist 2009 gegenüber 2008 um 39 Prozent angestiegen.

InfoWatch Global Data Leakage Report 2009

Mit InfoWatch bekommen Kunden

- Volle Kontrolle über den Datenfluss vertraulicher Informationen
- Einhaltung der Datenschutzbestimmungen
- Minimierung von finanziellen, rechtlichen oder imageschädigenden Risiken, die im Zusammenhang mit Datenverlusten einhergehen
- Verbesserung der Unternehmenskultur durch die Ausbildung von Mitarbeitern bezüglich der Durchführung von Security-Policies

Produkt-Funktionalität

Überwachung und Filterung des Datenverkehrs

Gateway Schutz-Modul

Das InfoWatch Gateway Schutz-Modul kann E-Mail-Systeme (SMTP), das Web (HTTP), gesicherte Webverbindungen (HTTPS¹), Instant Messenger und den Datenverkehr von Netzwerk-Druckern überwachen. Dadurch wird die Kontrolle des Unternehmens über Informationen optimiert, die über firmeninterne Mail-Systeme, Web-Mail, Internet-Foren, Chats oder über Instant Messenger übermittelt oder an Netzwerk-Drucker gesendet werden. Die Lösung unterstützt sowohl das Filtern und Blockieren von Traffic als auch die Überwachung im Schattenkopie-Modus (zum Beispiel Cisco SPAN). Der Gateway-Schutz ist mit Proxy-Server-Integration per ICAP ausgestattet.

Endpoint-Schutz

Das InfoWatch Endpoint-Schutz-Modul beinhaltet zwei lokale Sicherheits-Agenten - Device Monitor und Print Monitor. Diese Module werden an den Arbeitsplätzen der Benutzer installiert und helfen, unabsichtliche oder auch bewusste Datenlecks zu verhindern, die durch lokales Drucken, portable Laufwerke sowie entfernbare Speichermedien oder Kommunikations-Ports auftreten könnten. Werden Daten auf portable Datenträger oder entfernbare Medien kopiert oder an einen Drucker gesendet, fertigt das Endpoint-Schutz-Modul Schattenkopien aller Dateien (inklusive Text-Extrahierung aus Grafikformaten per OCR) an. Diese Daten werden zur Analyse an den InfoWatch Traffic Monitor Server gesendet. Dank der Integration mit Microsofts Active Directory können die Sicherheits-Agenten zentral an allen Arbeitsplätzen entweder per Microsoft Active Directory oder mit Hilfe eines remote-bedienbaren Installationstools installiert werden. Das InfoWatch Endpoint Schutz-Modul stellt die Anwendung von Sicherheits-Policies durch Benutzer und Benutzergruppen aus dem Corporate Directory sicher.

Beeline (OJSC VypelCom) ist einer der führenden russischen CIS Mobilfunkunternehmen mit über 25 Millionen Kunden. Die Implementierung von InfoWatch Traffic Monitor Enterprise hat Beeline geholfen, sensible Informationen zu sichern und den Ansprüchen des FSFR-Kodes zu entsprechen, der sich bei Beelines Investor Relations als erwiesenermaßen nutzbringend gezeigt hat.



Beeline™

¹ In Integration mit Partnerlösungen. Weitere Informationen können von InfoWatch Repräsentanten bekommen.

Analyse und weitere Vorgehensweise

InfoWatch Traffic Monitor analysiert zunächst die überwachten Daten nach formalen Eigenschaften (wie Monitor-Typ, Sender/Empfänger, Zeitpunkt der Übermittlung und Dateinamen, Dateityp und Dateigröße, etc.). Danach werden die Inhalte dieser Daten extrahiert und mit verschiedenen Technologien der Inhaltsanalyse ausgewertet.

Nach der Analyse trifft die Lösung automatisch eine Entscheidung darüber, ob das untersuchte Objekt gesendet oder geblockt wird. Die Entscheidung kommt auf der Basis von vordefinierten Security-Policies und Regeln zustande. Die Softwarelösung erlaubt dabei eine flexible Anpassung der Regularien.

Im Falle eines Übertritts der Security-Policies, wird der Sicherheitsbeauftragte alarmiert. InfoWatch Traffic Monitor gibt dem Sicherheitsbeauftragten detaillierte Information über das untersuchte Objekt, ohne diesem direkten Zugang einzuräumen, damit Persönlichkeitsrechte bei der Korrespondenz gewahrt bleiben. Der Sicherheitsbeauftragte kann der Vorgehensweise des Systems zustimmen oder diese abändern.

Datensicherung und nachträgliche Analyse

Die überwachten Daten werden in einem zentralen Archiv - Forensic Storage - für einen unbegrenzten Zeitraum gesichert. InfoWatch Traffic Monitor erlaubt es, die Historie der übermittelten Daten nachzuverfolgen, die momentanen Aktivitäten der User zu kontrollieren (z.B. Online-Status), nachträgliche Analysen zu erstellen und Untersuchungen anzustellen (analytische Abfragen).

Die erforderlichen Daten können nach folgenden Merkmalen gesucht werden:

- Nach formalen Attributen der untersuchten Objekte (Monitor-Typ, Sender/Empfänger, Zeitpunkt des Versands etc.)
- Nach Attributen, die während der Inhaltsanalyse hinzugefügt werden
- Nach den Inhalten der überwachten Objekte (Volltextsuche)

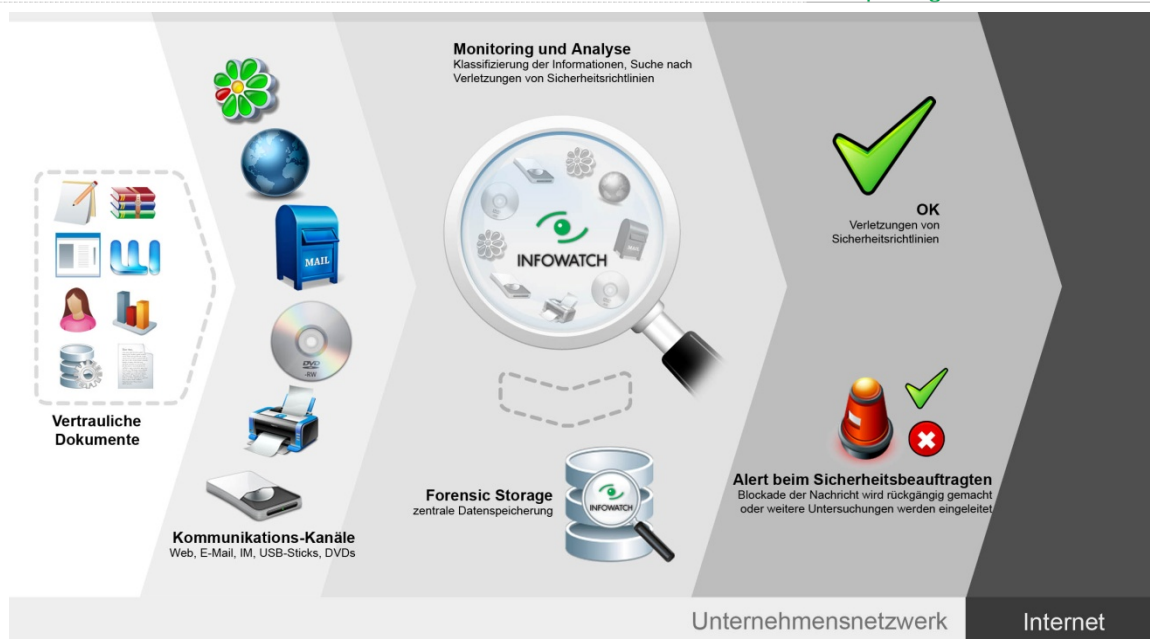
Die Lösung kann Statistik-Reports über alle überwachten Daten, auch grafischer Art, erstellen.

Verschiedene Technologien zur Identifikation vertraulicher Daten

Die schwierigste Aufgabe beim Datenschutz ist die Identifikation vertraulicher Daten. InfoWatch Traffic Monitor beinhaltet einen Engine zur intelligenten Inhaltsanalyse, der verschiedene Technologien zum noch genaueren Erkennen und Identifizieren vertraulicher Daten nutzt. Es kommt eine kombinierte Anwendung verschiedener Technologien zum Einsatz: Stoppworte, reguläre Ausdrücke, komplexe Analyse von Textobjekten (Templates Analyzer), digitale Fingerprints und linguistische Analysen (mit morphologischer Unterstützung von Deutsch, Englisch, Französisch, Italienisch, Spanisch, Russisch u.a.). Diese erhöhen die Zuverlässigkeit der Ermittlung immens und sichern vertrauliche Informationen während ihres gesamten Fortbestehens.

Die Lösung schützt sogar 'Zero Day'-Daten, Dokumente, die gerade erst erstellt wurden und noch nicht kategorisiert sind, Daten, deren Vertraulichkeitsstufe noch nicht ermittelt worden ist und für die keine entsprechenden Vergleichsdokumente existieren. InfoWatch Traffic Monitor kategorisiert solche Daten effizient on-the-fly und stellt sicher, dass diese nicht nach außen dringen.

InfoWatches linguistische Analyse-Technologie unterstützt die deutsche Sprache mit deren semantischen und morphologischen Feinheiten.



InfoWatch Traffic Monitor Enterprise: Flussdiagramm

Bedienung vertikaler Märkte

Um die Implementierung zu beschleunigen und Unternehmen sofort von einem Informationsschutz-System profitieren zu lassen, wird InfoWatch Traffic Monitor mit einem Set vorinstallierter Regeln zur Verarbeitung von Daten ausgeliefert, die für verschiedene vertikale Marktsegmente individualisiert worden sind. Dies sind Datenbanken, die Inhalte filtern sowie Templates für Textobjekte und Regeln zu automatisierten Vorgehensweisen. Momentan findet InfoWatch Traffic Monitor in folgenden Bereichen Einsatz: Im Bereich Banken und Finanzdienstleister, Öl und Gas, Telekommunikation und anderen.

Lukoil Inform LLC ist ein IT-Service-Provider für LUKOIL, den zweigrößten öffentlichen, nicht-staatlichen Öl-Konzern weltweit mit einem jährlichen Umsatz von über 80 Milliarden Dollar. InfoWatch Traffic Monitor Enterprise, das von Lukoil Inform eingesetzt wird, bietet eine Echtzeit-Kontrolle über Informationen mit verschiedenen Response Modes, schneller Datenübertragung und einfacher Wartung.



Leistungsüberblick

- **Korrekte Identifizierung vertraulicher Daten** mit Hilfe kombinierter Anwendung verschiedener Technologien
- **Verlässlicher Schutz des Unternehmens-Sicherheitsbereichs** dank Kontrolle der gängigsten Wege, über die Daten transferiert werden, sowie über das Kopieren und Drucken von Daten
- **Support vieler Dateiformate**
- **Vorinstallierte Sicherheitsregeln und Datenbanken, die Inhalte filtern**, um Unternehmen sofort von der Datenschutz-Lösung profitieren zu lassen
- **Forensic Storage** überwacht die momentanen Aktivitäten der Benutzer und ist die Basis um Analysen und Untersuchungen auch in der Retrospektive durchzuführen
- **Flexible Einsatzoptionen:** Inline, ICAP und Untersuchung im Copy Mode (SPAN, Port Mirroring, etc.)

Systemvoraussetzungen

Gateway Sicherheits-Modul:	End-Point Sicherheits-Modul:
InfoWatch Traffic Monitor Server Hardware <ul style="list-style-type: none">• Server: HP DL360 G6• CPU: Intel Xeon x86 3 GHz, 2 CPU mit 4 Kernen• RAM 2 GB• HD 160 GB Software <ul style="list-style-type: none">• Red Hat Enterprise Linux Server Release 5 upd 4, x86-32 Forensic Storage Hardware <ul style="list-style-type: none">• Server: HP DL360 G6• CPU: Intel Xeon x86 2.4 GHz oder höher• RAM 4 GB• RAID Level 1 oder höher (200 GB) Software <ul style="list-style-type: none">• Oracle RDBMS 11gR1 (11.1.0.7)	InfoWatch Device Monitor Server Hardware <ul style="list-style-type: none">• CPU: Intel Pentium 4 2GHz oder höher• RAM 1 GB• HD 100 GB Software <ul style="list-style-type: none">• Windows 2003 Server Service Pack 1• RDBMS: Oracle / MS SQL Server / PostgreSQL / MS SQL Express• .NET Framework 3.0 InfoWatch Device Monitor Client Hardware <ul style="list-style-type: none">• CPU: Intel Pentium 4 mit 2 GHz oder höher• RAM 512 MB Software <ul style="list-style-type: none">• Windows 2000 Professional SP 4, Windows XP SP2 oder Windows Vista
	Management-Konsole Hardware <ul style="list-style-type: none">• CPU: Pentium 4 mit 3 GHz• RAM: 1 GB Software <ul style="list-style-type: none">• Microsoft Windows XP Service Pack 2

Kontakt:

www.infowatch.de
Tel.: +7 (495) 22 900 22
sales@infowatch.com
sales-oem@infowatch.com

Partner-Kontakte:

Österreich und Schweiz: sales-ach@infowatch.com, +49 (8152) 969340
Deutschland: sales-de@infowatch.com, +49 (4207) 689933
Benelux und Mittelmeerstaaten: sales-be@infowatch.com, +32 47792090