



## InfoWatch Traffic Monitor Enterprise

Control corporate information flow and protect your intellectual property

### Information Control is a Business Priority

Modern business' sustainability and efficiency to a great extent depends on how well their sensitive information is protected. The loss of confidential data, such as customer database, intellectual property, financial or legal documentation, market research or personal data can significantly affect businesses of any size. Even a single data leak can result in spoiled reputation, regulatory fines, customer churn or loss of competitiveness.

The ever growing data volumes, typical for modern enterprises, severely complicate the challenging task of safeguarding corporate information. Huge amounts of data generated by business processes and personnel make it hard to precisely identify what information is confidential and requires protection: usually only about 20 per cent of data is structured, about 10 per cent of sensitive data is modified each day, and newly created (so called "zero-day") confidential documents account for about 10% of sensitive data volume in an enterprise.

Rapid proliferation of mobile computing devices, sensitive data sharing across geographically distributed offices, widespread outsourcing projects, etc. create additional difficulties in securing information confidentiality, making the traditional infrastructure security approach insufficient.

It means that nowadays efficient data management and protection can be only achieved while focusing on the data itself.

**Total amount of leaks in 2010 increased, as compared with 2009 by around 12%**

*InfoWatch Global Data Leakage Report 2010*

**The average total per-incident costs in 2010 were \$7.2 million**

*Ponemon Institute, Cost of a Data Breach Study 2010*

*"We decided to choose InfoWatch Traffic Monitor Enterprise, as it combines the most effective data analysis technologies. The solution helped us to prevent 369 information security violations during about half a year after implementation."*



### Solution: InfoWatch Traffic Monitor Enterprise to Safeguard Corporate Information

To address the issue of safeguarding sensitive information InfoWatch has developed a comprehensive data monitoring, analysis and archiving solution [InfoWatch Traffic Monitor Enterprise](#).

The solution gives businesses full control over their information flow and provides them with visibility into what types of data travel across the infrastructure, where and how they are transmitted, and who uses them.

The solution monitors the major data transmission channels, intercepts the sent data and analyses it using several technologies to detect sensitive information leaving corporate network unauthorized in emails, web-posts, instant messages, copied to removable mass-storage devices or printed.

Based on analysis results and corporate information security rules the solution meets automatic decision on how the intercepted information piece should be treated further: transmitted to the intended recipient, blocked or sent for additional processing, for example presented to the corporate security officer for consideration. InfoWatch Traffic Monitor provides extensive information about the nature of the intercepted data without direct access to its contents to comply with existing personal privacy regulations.

The intercepted information packed with analysis results is stored in a centralized unchangeable protected archive – Forensic Storage for further retrospective analysis and investigation. The solution is managed by solution administrator via user-friendly management console.



## Product Functionality

### Monitoring and Protection

The solution includes two modules for information monitoring – InfoWatch Gateway Protection and InfoWatch Endpoint Protection Modules.

The **Gateway Protection Module** intercepts email (SMTP), Web (HTTP), secure Web (HTTPS)<sup>1</sup> and instant messaging traffic (OSCAR-based IMs – 40+ client types, XMPP-based – including Google Talk and Facebook Chat, Mail.ru agent and Windows Live Messenger are currently supported). The solution supports both inline traffic filtering and interception in the monitoring mode (for example, Cisco SPAN), as well as features proxy-server integration via ICAP<sup>2</sup>. The traffic is intercepted at the gateway level, so no installation of additional software at employee workstations is required.

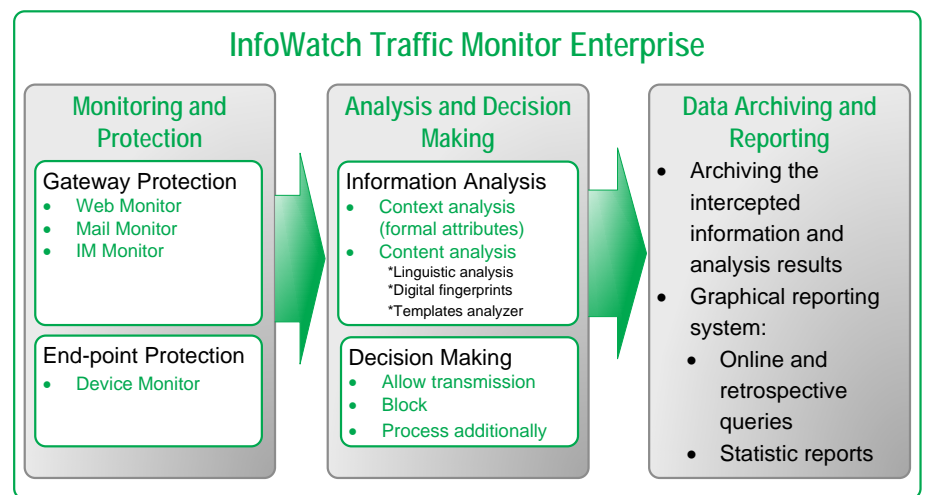
The **Endpoint Protection Module** (InfoWatch Device Monitor) includes a local security agent – Device Monitor – that is installed at user workstations and InfoWatch Device Monitor Server to centrally manage security policies at controlled PCs. Due to Microsoft Active Directory integration, the security agent can be centrally installed at all employee workstations and security policies can be applied to users or user groups from the corporate directory.

When the data is copied to removable mass-storage devices (26 device types are currently supported) or sent to a printer, the local agent Device Monitor makes shadow copies of all the files (including text extraction from graphic formats – optical character recognition, OCR).

These shadow copy files are collected at the InfoWatch Device Monitor Server, where they are packed with formal attribute information, for example workstation ID, date and time of copying or printing, file size, name, etc.

For additional protection InfoWatch CryptoStorage Enterprise can be used to encrypt information stored at user workstations or copied to removable mass storage devices.

*Beeline (OJSC VimpelCom) is a leading Russian and CIS mobile carrier with 25+ million subscribers. The implementation of InfoWatch Traffic Monitor Enterprise helped Beeline to achieve sensitive information security and comply with FSFR code requirements, which proved extremely beneficial in Beeline investor and counteragents relations.*



*InfoWatch Traffic Monitor Enterprise: logic diagram*

### Analysis and Decision Making

The information intercepted in communication channels and shadow copies of data printed or copied to mass-storage devices are sent to the high-performance (up to 100Mb) Linux-based InfoWatch Traffic Monitor server for analysis and decision making.

Here the data is first analyzed according its formal attributes (such as monitor type, sender/recipient, sent date and time, file name/type/size, etc.).

Then the contents of data packets are extracted and analyzed using several content analysis technologies: digital fingerprints, templates analyzer and **linguistic analysis** (with morphologic support for English, German, French,

<sup>1</sup> In integration with partner solutions. Please contact InfoWatch representatives for details.

<sup>2</sup> Internet Content Adaptation Protocol. Integration with proxy-servers supporting ICAP (for example, BlueCoat Proxy SG, Cisco IronPort, Aladdin eSafe) is required to enable traffic blocking. Please contact InfoWatch representative for details



# INFOWATCH

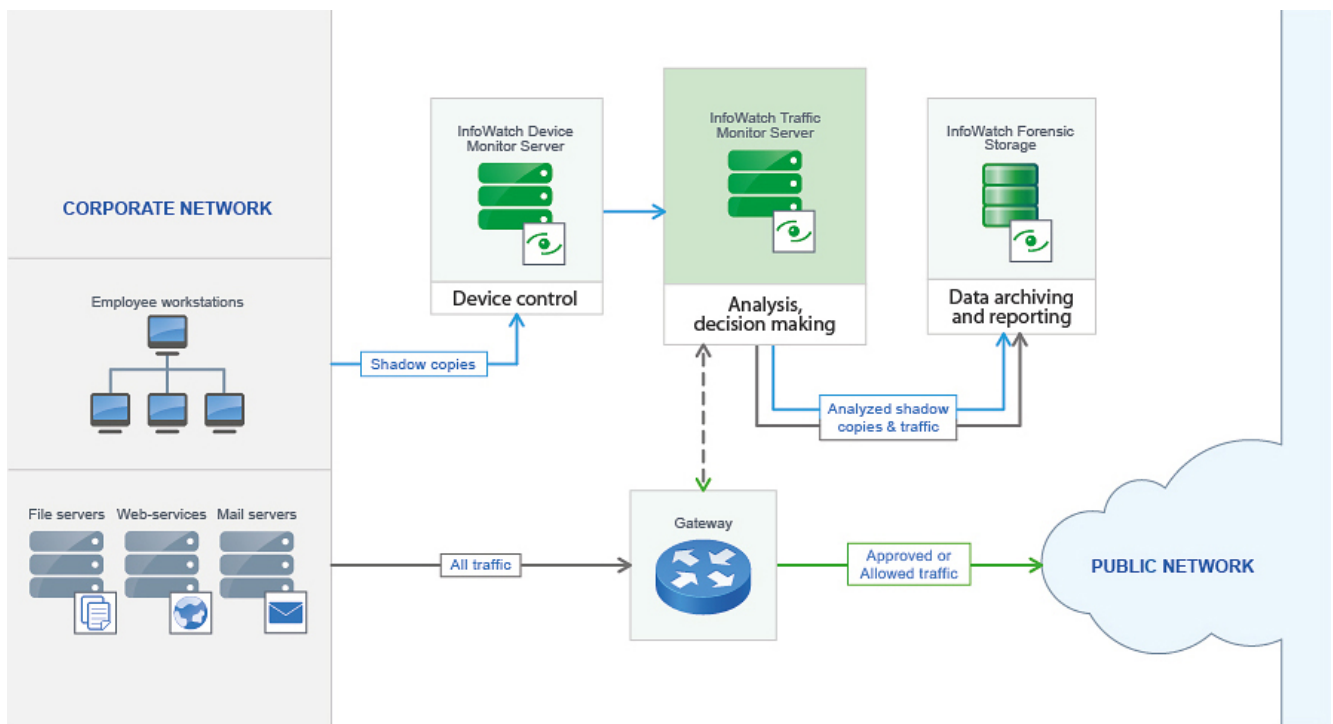
Italian, Spanish, Russian, etc.). Combined application of these technologies helps resolving the most challenging information protection task – reliable confidential data identification.

InfoWatch competitive advantage is its carefully-optimized linguistic analysis technology that proves efficient in analyzing unstructured data. This data type is intended for human consumption and usually comprises up to 80 per cent of all enterprise data. Another advantage of InfoWatch linguistic analysis is arbitrary custom-defined category hierarchy to consider company business field and information flow specifics and thus protect exactly the information important for a specific company.

The solution precisely identifies even so called “zero-day” data – documents that have just been created and are not categorized yet, to which no confidentiality level has been assigned and for which no related documents exist. **InfoWatch Traffic Monitor** efficiently categorizes such data on the fly, making sure it doesn't leak.

The analysis results trigger the automatic decision on how to handle the intercepted information further: either allow transmission, or forward for additional processing to the person in charge or block. **InfoWatch Traffic Monitor** provides detailed information about the nature of the intercepted object without direct access to its contents to comply with existing personal privacy regulations. Access to the contents of the intercepted information is possible, but requires special legal permission.

Integration with Microsoft Active Directory enables unified user identification for all monitored data transfer channels.



*InfoWatch Traffic Monitor Enterprise: data flow*



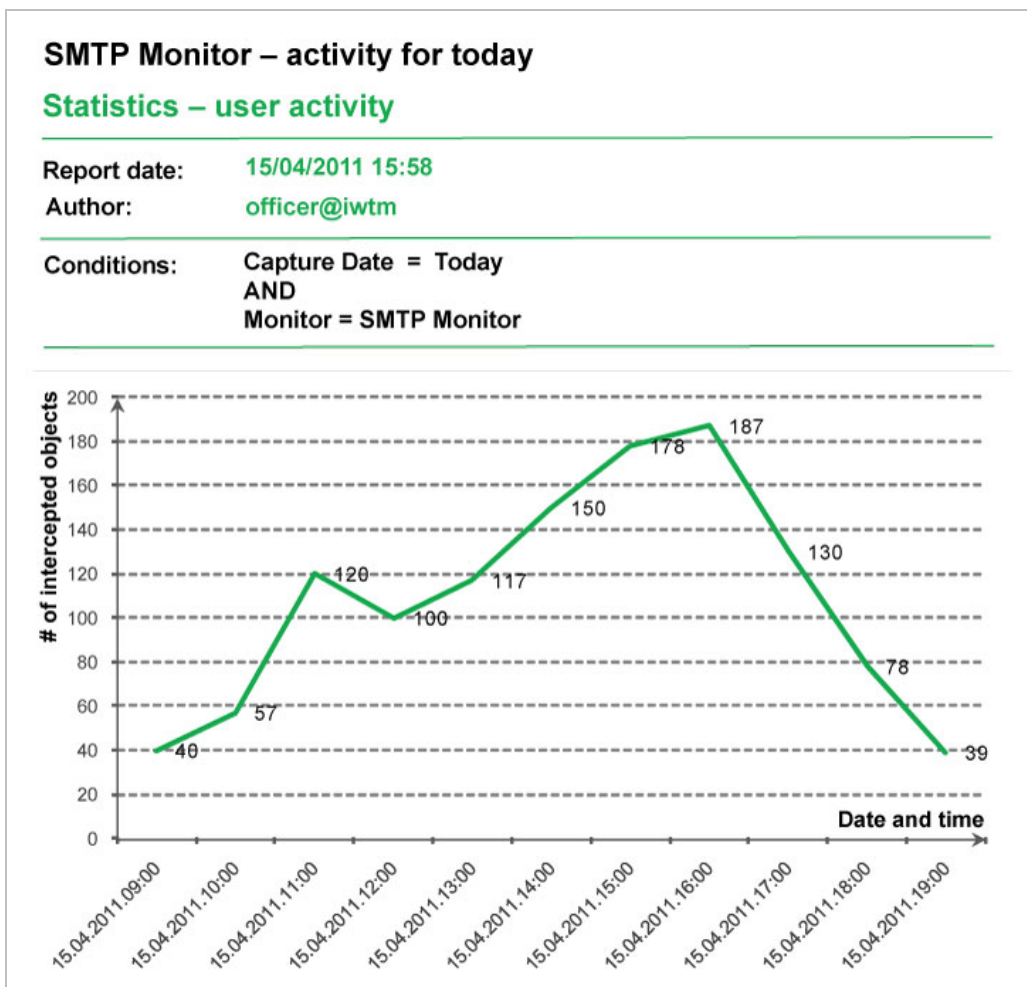
## Data Archiving and Reporting

The intercepted data along with the analysis results is stored in a centralized protected archive – Forensic Storage. Due to the responsibility zones feature hierarchical access of several information security officers to reporting and analysis results can be easily introduced. **InfoWatch Traffic Monitor** allows viewing the data transmission history and features monitoring of current actions with sensitive data (online queries) as well as retrospective analysis and investigation (analytic queries).

The required data can be searched by:

- formal attributes of the intercepted objects (monitor type, sender/recipient, sent date/time, etc.)
- attributes added during the object's content analysis
- contents of the intercepted objects (full-text search)<sup>3</sup>.

The integrated graphical reporting system clearly shows the specifics of sensitive information flow. For example, graphic Web-usage reports can be applied to track uploading confidential information to various web sites, etc.



*InfoWatch Traffic Monitor Enterprise: report example.*

*This report shows the dynamics of emails generated by company employees throughout a day.*

The solution includes 60 pre-installed reports, developed by InfoWatch after careful study of various industries needs and our customers' feedback. Custom reports can be easily created.

<sup>3</sup> In accordance with existing privacy regulations special legal or workers' council permission is required to enable full-text search.



## Vertical Markets Served

To speed up the implementation and let enterprises immediately benefit from an information protection solution, **InfoWatch Traffic Monitor** is supplied with a set of preinstalled data processing rules, the content filtering database, text objects templates and decision-making rules, customized for several vertical market segments. Currently **InfoWatch Traffic Monitor** supports the following segments: banking and finance, oil and gas, telecommunications, insurance, software development and government.

*Lukoil Inform LLC is IT services provider for LUKOIL, the 2<sup>nd</sup> largest non-state publicly traded oil company worldwide with annual turnover of over \$80 billion. InfoWatch Traffic Monitor Enterprise, implemented by Lukoil Inform provides real-time information control, rapid data processing and easy maintenance.*



## Who needs InfoWatch Traffic Monitor Enterprise?

- **Banks and financial institutions** to prevent leaks of their customer personal data and to ensure compliance with regulative requirements
- **Telecom operators** to protect customer data, to comply with personal data protection regulations and to safeguard their intellectual property
- **Oil&gas companies** to protect intellectual property and to mitigate risks that may arise from loss or disclosure of their valuable information
- **Government institutions** to protect citizens' information against leakage and unauthorized disclosure and to comply with personal data processing requirements

## With InfoWatch Traffic Monitor Enterprise the Customer Gains

- Full control over sensitive data turnover
- Compliance with internal policies & standards, external rules and regulations, industry standards (for example PCI DSS, SOX, GLBA, HIPAA) and customer security requirements
- Minimization of financial, legal and reputational risks, associated with data loss
- Corporate culture improvements by employee education regarding security policies implementation
- Cost transparency and flexibility thanks to modular solution architecture

## InfoWatch Traffic Monitor Enterprise Benefits

- **Accurate identification of sensitive data** with combined application of several analysis technologies
- **Reliable protection of enterprise security perimeter** thanks to the control over the most common data transfer channels, data copying and printing
- **Support for multiple file formats**, including Microsoft Office and Open Office
- **Pre-installed security rules and content filtering base** to let enterprises immediately benefit from a data protection solution
- **Forensic Storage** for monitoring of current actions with sensitive information (online queries) and retrospective analysis and investigation (analytic queries)
- **Flexible deployment options:** inline, ICAP and interception in the copy mode (SPAN, port mirroring, etc.)
- Support for **standard RHEL-core** for low-level traffic interception to avoid possible hardware incompatibility issues
- **High performance and reliability**
- Integration with **InfoWatch CryptoStorage Enterprise** to protect information stored on removable mass-storage devices, laptops, PCs, network resources, in virtual or cloud architectures by using encryption technologies



## Solution Modules

- **End-point protection module:**
  - InfoWatch Device Monitor featuring control over local and network printers, portable devices and removable media (CDs, DVDs; LTP-, COM-, USB-connected devices - 26 device types are currently supported) and shadow copying of the printed or written to a device data.
- **Gateway protection module:**
  - Web Monitor to control data sent via web-mail, blogs, Internet-forums, etc.
  - Mail Monitor to control information turnover via corporate email-systems.
  - IM Monitor to control information transmitted via OSCAR-based instant messengers (40+ IM client types). Monitoring of message texts, file transfers and SMS-over-IM.
- **Analysis Engine:**
  - Linguistic analysis to analyze unstructured data – define its subject (category), sensitivity level, etc.
  - Digital fingerprinting technology to detect in information flow quotes from information, previously labeled as confidential.
  - Templates Analyzer to control template-based data, for example, social security or tax file numbers.
  - InfoWatch Autolinguist – the module for automatic creation of a content filtering database required for linguistic analysis.
- **Forensic Storage** – a centralized protected archive that stores the intercepted data for analytic purposes.

## System Requirements

Gateway protection module:	End-point protection module:	Management Console
<b>InfoWatch Traffic Monitor Server</b> <b>Hardware</b> <ul style="list-style-type: none"><li>• Server: HP DL360 G7</li><li>• CPU: Intel Xeon x86 3GHz, Dual Quad-Core CPU</li><li>• RAM 2 GB</li><li>• HD 160GB</li></ul> <b>Software</b> <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux Server release 5 x64</li></ul> <b>Forensic Storage</b> <b>Hardware</b> <ul style="list-style-type: none"><li>• Server: HP DL360 G7</li><li>• CPU: Intel Xeon x86 2.4GHz or higher</li><li>• RAM 4 GB</li><li>• RAID level 1 or higher (200GB)</li></ul> <b>Software</b> <ul style="list-style-type: none"><li>• Oracle RDBMS 11gR2 (11.2.0.1)</li></ul>	<b>InfoWatch Device Monitor Server</b> <b>Hardware</b> <ul style="list-style-type: none"><li>• CPU: Intel Pentium 4 2GHz or higher</li><li>• RAM 1 GB</li><li>• HD 100GB</li></ul> <b>Software</b> <ul style="list-style-type: none"><li>• Windows 2003 Server Service Pack 1, Windows 2008 R2</li><li>• RDBMS: Oracle / MS SQL Server / PostgreSQL / MS SQL Express</li><li>• .NET Framework 3.0</li></ul> <b>InfoWatch Device Monitor Client</b> <b>Hardware</b> <ul style="list-style-type: none"><li>• CPU: Intel Pentium 4 2GHz or higher</li><li>• RAM 512 MB</li></ul> <b>Software</b> <ul style="list-style-type: none"><li>• Windows 2000 Professional SP 4 (limited support)</li><li>• Windows XP SP3, Windows Vista, Windows 7</li></ul>	<b>Hardware</b> <ul style="list-style-type: none"><li>• CPU: Pentium 4, 3GHz</li><li>• RAM: 1 GB</li></ul> <b>Software</b> <ul style="list-style-type: none"><li>• Microsoft Windows XP SP2, Windows 7</li></ul>