

Business Standard

Demand for data leakage prevention software is on the rise: Vadim Kuznetsov, InfoWatch

In this interview, Vadim Kuznetsov, International Sales Director, InfoWatch, elaborates on importance of data protection and analysis for manufacturing companies

Rakesh Rao | Mumbai July 28, 2014 Last Updated at 19:45 IST

1



Vadim Kuznetsov, International Sales Director, InfoWatch

Information flow for many big conglomerates transcends across continents with a threat of espionage looming large on their big data repository. Data leaks can cost a company financially as well as its reputation. While banking and financial institutions have already realised it, manufacturing industry is slow to react to this reality.

However, **Vadim Kuznetsov**, International Sales Director, InfoWatch, believes things are changing with number of manufacturing companies requesting its [data leakage prevention](#) (DLP) solutions increasing. In this interview with Rakesh Rao, Kuznetsov elaborates on importance of data protection and analysis for companies and the market for [DLP](#) software.

Why data protection and analysis is gaining importance among the corporates across the world?

The main driver of data protection and analysis market is a stable growth in a number of data leaks worldwide. So, according to [InfoWatch](#) Global Data Leakage Report 2013, more than 561 million records were compromised worldwide, including financial and personal data, which is 22% higher than the number of leaks registered in 2012. And that is only what became publicly known (was published in press, internet, etc) which is at most 4-8% of the estimated total number of leaks.

Companies across the world incur significant financial and reputational losses as a result of data leaks. According to Ponemon Institute research, 'Cost of data breach study: Global analysis', the average total cost of a data breach for the companies participating in this research increased 15% to \$3.5 million in 2013.

These factors spur development of the global data protection and analysis market.

Is the demand for software for data security and analysis from manufacturing industries (ie, companies not involved in financial and telecom sectors) increasing? And what is driving this demand?

Yes, it is increasing. InfoWatch experience shows manufacturing companies most often run the risk of confidential data misuse by their employees for their own profit. This happens because manufacturing industries possess expensive manufacturing secrets, tender documentation, etc. It is common for manufacturing companies to have no data protection rules implemented at all or to have few inexplicit.

Besides, manufacturers often face the difficulty of confidential data detection in a huge volume of data and documentation.

Their employees are often unaware of basic information security rules and data protection measures. Keeping in mind these factors and the mentioned above situation with data leakage InfoWatch registers the increasing number of requests for data leakage prevention (DLP) solutions from manufacturing companies.

How is market for data security and analysis software in India?

As India is the country where many sectors in the economy are in active transition from paperwork to digital documents workflow – potential for internal information security is very notable. Especially we should note BFSI segment, where all public banks are obliged to implement in 2014-2015 Core Banking systems, which obviously raise quite a bit a demand for full-fledged internal information security solution to protect information assets. Thus, for BFSI we see very high time for DLP projects in this FY2014 as well as in 2015.

What are the possible consequences of data leakage in an oil & gas company and how can they be prevented?

According to InfoWatch multi-year experience of working with the companies of oil & gas sector, the main consequences of data leak for these companies are significant financial losses. Thus, an average oil and gas company for instance with over 6000 employees on board faces more than 90 incidents of confidential information theft at purchasing stage and around 7 incidents of industrial espionage. Its financial losses during purchasing tenders amount to at an average \$3,26,000, and 20% of budget go into theft and corruption.

Companies in oil & gas sector should implement both specialised data protection solutions and a set of specific data security rules and measures to create secure environment for confidential data usage, storage and flow in corporate perimeter. InfoWatch provides a number of reliable data protection solutions customised for oil & gas industry and together with partners deep consultancy in implementing data protection policies in companies of the industry.

Given InfoWatch's experience in providing DLP solutions to the Russian energy sector, what are the best practices it plans to introduce in the Indian energy sector?

Taking specific nature of oil & gas companies into account, InfoWatch is ready to offer its Indian clients the DLP system customised to specific industry requirements, namely specialised industry Content Filtering Database (CFD). A CFD not only describes the categories of information that are circulated within a company, it also takes into account various attributes to determine its confidentiality, including the specific nature of the company's business and its requirements for security. As a result, a text or a document is automatically assigned to the appropriate category of confidentiality based on its topic and content. This provides high efficiency of confidential data detection.

Besides, companies of oil & gas sector mainly have very distributed multi-level structure with numerous branches across the country. To meet this challenge InfoWatch implements a DLP management system with multi-level and multi-layered structure and high information capacity based on wide range of equipment and software used in different company branches.

How does InfoWatch plan to compete with other DLP solution providers who are present in the Indian energy sector?

For over 8 years of DLP market existence (in 2005 [IDC](#) first introduced the term and named it a separate segment of information security market) DLP solutions made a long way from a technology of content filtration to a complex solution including broad set of data analysis technologies, data categorisation and consulting. Most InfoWatch competitors still sell DLP as a software ('install and forget' principle) and say DLP is a technology solution but sure enough it is not.

DLP is a process and the first essential stage is understanding what information is confidential in the company and, thus, must be controlled and protected. If we do not know what we are looking for we simply cannot find it. That is why InfoWatch implements DLP as a process by understanding the confidentiality of the information; we analyse and categorise information before we actually serve to [data leakages](#) and internal security threats. This is the only way how DLP systems can efficiently prevent data leaks and this approach radically differentiates InfoWatch from its competitors.

What are your growth plans for InfoWatch in India?

We already have two strong partnership networks in West India (Mumbai) and in North (Delhi). These networks are in active business development and very open for new cooperations in terms of more partners and opportunities development. Same time InfoWatch plans to establish strong technology office in India which will add very good technical back-up for the market, which is very important for proper support of DLP projects during whole project life-cycle and IW offers here the best possible support.

[Source](#)