Publication : The Integrator
Date: July issue
Headline : **TechKnow – InfoWatch Group**

Andrey Sokurenko
Business Development Director
InfoWatch Group

Battle lines drawn

Beyond firewalling and endpoint security is perhaps the biggest future security battleground, Data Protection. Andrey Sokurenko, Business Development Director at InfoWatch Group discusses the set of technologies the company has in its arsenal in this crucial fight.

Discuss briefly a typical process of securing client information from leakage/theft

In brief the process of data leakage prevention consists of three main stages which we call Pre-DLP, DLP and Post-DLP. Pre DLP stage includes deep data analysis and categorization (with help of InfoWatch Auto-linguist engine and consultancy of InfoWatch linguists), since 80% of data in modern companies are unstructured and spread over different documents, files and storages; companies simply do not know which of their data are confidential and therefore can't protect them effectively. After all data classification into several categories of confidentiality (strictly confidential, confidential, non-confidential, etc.) a DLP system can be installed. The set of monitors is installed on all data transfer channels and starts monitoring all data circulating inside the company and transferring outside the company perimeter. If there is any attempt of confidential data transfer outside the corporate network the system will either block the process or alert information security officer. Post-DLP stage includes investigation of data leak incidents with help of InfoWatch Forensic Storage. It's a specialized storage containing an archive of all information flows in the organization, including incidents of security policy breach and leakage of confidential information; this storage is a legally relevant evidence base for internal incident investigation and court proceedings.

Who's at risk of data leakage in the Middle East and why?

Of course, the companies with most valuable information are most at risk. First of all they are companies which have big volumes of personal data (mobile operators, big online retailers, authorities working with citizens, etc.) Then there are companies which possess different trade secrets (manufacturing, oil and gas, etc.) Banks, big insurance companies, governmental structures also operate highly sensitive data. We can add to the list any other company which considers its information valuable.

Discuss InfoWatch'ssolutions for protecting data, networks or endpoint clients

InfoWatch has a set of information security solutions among which are InfoWatchEndPoint Protection (protection of enterprise endpoints from a variety of threats),InfoWatchAppControl for securing company's applications from backdoors and vulnerabilities, InfoWatch Targeted Attack Detector aimed at detection and prevention of attacks the target of which is frequently large corporations, government agencies and defense

companies. But of course the key InfoWatch expertise lies in field of Data Loss Prevention since we are already for more than 10 years in the market and have accumulated a huge experience of DLP systems successful integrations in hundreds of companies in different industries worldwide.

> ***"The companies with most valuable information are most at risk. First of all they are companies which have big volumes of personal data. Then there are companies which possess different trade secrets"***

Are regional firms taking the concept of information protection seriously and investing in the same?

Since the number of data leaks worldwide grows increasingly and ME being no exception, we see the growing demand for data protection solutions in the region. InfoWatch is working in the Gulf region for several years already and from our clients and partners experience we can say the companies understand the severity of data leakage problem and the necessity for reliable protection and so are ready to invest.

Discuss briefly your partner strategy/ channel programme in the Middle East

InfoWatch Group actively invests into good channel partners in Gulf region to build a reliable partner chain. Our strategy for Middle East includes three key elements – efficient regional representative, several successful partners in the region and active marketing promotion. We have a strong desire to support and invest into good partners and are open for winning cooperation with the channel.

We have an extended program for partner technical education. InfoWatch technical experts regularly come to ME countries to educate partner technical teams providing them with the deepest knowledge and expertise in data leakage prevention and other information security areas and thus with extra competitive advantage in terms of selling IT security solutions. All our partners undergo InfoWatch certification and so get the status of InfoWatch Group certified partners.

InfoWatch Group organizes special channel events in the region and actively takes part in events held by our partners. We stand for active cooperation with the channel and contribute our budget, resources and expertise into establishing reliable partner chain in Middle East.

Discuss the challenges of information protection brought on by increased mobility and BYOD

The main challenge BYOD brings to the network is a security risk, where the more convenient and mobile the technologies are, the less they are secure. There are three main challenges BYOD brings in the network.

The first, among other challenges, is the loss of mobile devices. The major vulnerability in this case is the human factor where people fail to use the necessary security tools, such as encryption, on their mobile devices. At the same time they constantly forget or misplace their gadgets in public places.

The second challenge is the vague limit between personal and corporate data on private mobile devices of employees. This data should be used and stored separately on a private device, thus companies require special policies for BYOD regarding personal and corporate data processing.

The last difficulty is intellectual property protection. Employees often regard the results of their intellectual work as their private property, where as a matter of fact, it is usually the company's property.

Discuss the future of information protection in the age of Big Data, Cloud, Internet of Things and other emerging trends

I believe several trends will dominate in field of information security in future. First of all they are different privacy protection technologies. For example when a mobile device user wants to stay private he will just need to press some button and immediately switch to the "private mode". Newsecuritytools will follow new communication trends as especially in the matter of private space protection.

Another promising trend is further development of content and behavior analysis technologies including for the purposes of detecting malicious insiders in corporate environment at an early stage. Today's security systems normally work in "catch after the incident" mode. But crime prevention is much more important than cure of effects. Until an employee illegitimately copies client database we never know he is malicious insider. But every man has his personal characteristics and if it suddenly changes dramatically it may be alarming for his chief. With help of content and behavior analysis systems it will be possible to detect such offences at a preparation stage, thus proactive systems for protection against insiders are a promising field.

Besides, development of security systems against targeted attacks will be in demand. Current antivirus solutions are good in protection against mass attacks (mass viruses and phishing, etc.) but they are unable to combat sophisticated targeted attacks aimed at specific organizations (often strategic sites and big corporations). Obviously one should invent specific protection tools providing higher level of security.