

Synopsis	InfoWatch is making Malaysia it's first target market in Asia Pacific. "We see great potential in Malaysia as a platform to expand the product market for the DLP solution," says Business Development Director Andrey Sokurenko. According to research carried out by InfoWatch in 2013, 44% of data leakage in companies is a result of malicious intent while another 46% is accidental. Sokurenko shared that if an employee tries to upload information to an email or a USB drive, DLP 10 would automatically trigger InfoWatch's software to prevent the spread of information.
Date	Wednesday, April 9, 2014

Sengaja sabotaj

@ BERITAIT

Oleh Afiq Hanif
afiq_hanif@media-
prima.com.my

44% kebocoran data berniat jahat

Infowatch, syarikat perkeraja teknologi perkhidmatan pencegahan kebocoran data atau Data Loss Prevention (DLP) berasaskan teknologi analisis semantik dan linguistik menjadikan Malaysia pasaran pertama di Asia Pasifik selepas menerajui Russia.

Pengarah Pembangunan Perniagaannya, Andrey Sokurenko berkata, pihaknya melihat Malaysia mempunyai potensi besar sebagai platform memperluaskan pasaran produk penyelesaian DLP itu.

"Kami fokus kepada pembangunan penyelesaian berasaskan perisian yang memantau, menganalisis dan melindungi data korporat,

"Ini kerana kebanyakan syarikat hari ini berhadapan cabaran besar melindungi data sensitif mereka dari-

pada diceroboh, selain mengurus data yang tidak berstruktur dan sukar dicapai," katanya.

Berdasarkan kajian Infowatch, 44 peratus kebocoran data dalam sesebuah syarikat berpunca daripada niat jahat individu di samping 46 peratus lagi disebabkan masalah tidak disengajakan yang dikesan syarikatnya pada 2013.

Sokurenko memberitahu, penyelesaian DLP tradisional yang menggunakan teknologi pengesanan cap jari tidak lagi relevan untuk perlindungan data penting kerana ia lebih mudah terdedah kepada masalah kebocoran.

Katanya, sesebuah syarikat perlu memahami DNA sesebuah data terlebih dahulu dan itu yang dilakukan teknologi DLP Infowatch yang mana ia mengawal pergerakan data secara menyeluruh termasuk menerusi aplikasi web.

Teknologi terbabit juga sangat unik kerana dilengkapkan polisi sekuriti yang dapat



SOKURENKO

menentukan sama ada sesuatu dokumen itu boleh dibuka atau tidak pada satu-satu masa mengikut konteks hak pengguna yang telah ditetapkan.

"Untuk peringkat awal memastikan masalah DLP ini dapat dicegah, pihak kami dalam usaha meningkatkan kesedaran dan pengetahuan pengguna mengenai teknologi ini terutama dalam kalangan individu dalam pengurusan perniagaan," jelasnya.

Masalah kehilangan data bukan perkara biasa yang kita ketahui kerana ia berlaku setiap masa dan tanpa kita sedari.

Tahun 2012 hingga 2013 berlaku peningkatan 18 peratus kehilangan data dan dijangka meningkat selepas budaya bawa peranti sendiri (BYOD) mula diperkenalkan secara meluas.

Platform keselamatan DLP ini mengamalkan tiga konsep iaitu mencari, memantau dan mengawal keluar masuk maklumat.

"Perisian ini adalah platform pertama dalam industri yang memberi banyak pilihan kepada pengguna untuk mencari dan memperbaiki masalah kehilangan data.

"Maklumat seperti data kad kredit, peribadi pelanggan serta data pelanggan korporat adalah sulit dan tidak harus mengalir keluar dari simpanan syarikat," katanya.

Menurut Sokurenko, sekiranya pekerja cuba muat naik maklumat ke e-mel atau USB, DLP 10 secara automatik menggerakkan perisian Infowatch untuk menghalang berlakunya penyebaran maklumat.