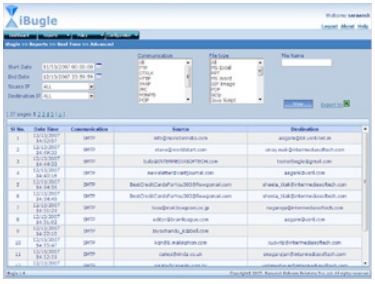
iBugle

Protect Enterprises from Insider Information Leakage

The Daunting Challenge of Information Leakage

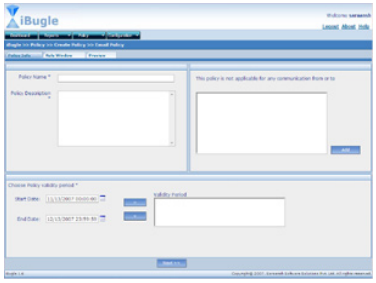
To-date organizations have invested huge resources into protecting their internal environment from external attacks. However, as organizations rely more on information technology to increase competitiveness and efficiency, they also increase their vulnerability to information leakage from insiders. This information leakage could be perpetrated with malicious intent or caused inadvertently by human error and the result is potentially devastating. There are several reports that bear this out.

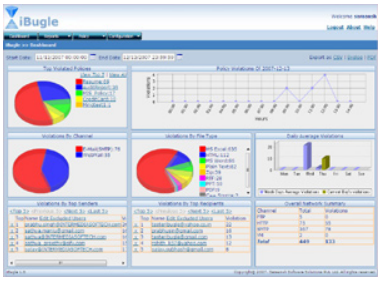
- Gartner studies indicate that a majority of real data losses have been caused by insiders.
- A CSI/FBI Computer Crime Survey indicated that 80% of the respondents' reported security incidents involved insiders.



The Problem of Information Leakage

- Organizations are required to ensure integrity and accuracy of reporting as legislated in the Sarbanes Oxley Act of 2002 (SOX). The financial industry is required to protect confidential customer information, as legislated by the Gramm-Leach-Bliley Act (GLBA).





- Organizations are increasingly threatened by the ease with which intellectual property can be made available to competitors or impostors. Organizations want to ensure that intellectual assets and their crown jewels, such as, patents, trademarks, brands, trade secrets, software code, designs, architectures, algorithms are not leaked and abused.
- Organizations want protection against leakage of internal confidential information, which can be very damaging to customer trust to the company brand and finances.
- Privileged information, such as customer data, patient information, financial information, business plans etc., can be surreptitiously hidden in common applications, such as those of common spread sheets, word processors, presentation packages etc., and may be to outsiders.

The above problems can be catastrophic and behoves organizations to invest in a solution that prevents information leakage. Such a solution would need to provide high performance, real-time vigilance against all information that leaves the organization.

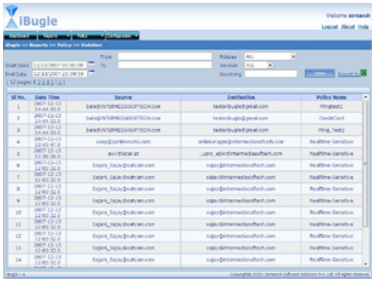
iBugle Solution

Saraansh's iBugle is a security appliance that provides complete visibility to information leaving the enterprise in near real-time and protects against information leakage.

Real Time Information Capture & Analysis

• Packet Capture & Protocol Decoding Engine

iBugle employs a Packet Capture Engine that captures every outgoing packet on the network at line speed, in passive mode. Many of the commonly used protocols are supported by the system and include HTTP, SMTP, IP, FTP, Telnet, POP, IMAP, Web Mail, Chat etc.



• Content Analysis Engine

This engine can analyze various file formats including .Doc, .PPT, HTML Files, .PDF etc. It can also monitor for structured data items, such as social security numbers, credit card numbers, URL's and personnel ID's.

• Forensic Analysis Engine

The Audit and Forensic Engine allows an administrator to analyze the trail of alert events and to extract patterns of information. These alerts can be the basis of a periodic report, or can trigger appropriate notification via email, an instant message or other preferred communications medium.

Easy to Administer

• Policy Definition User Interface

An administrator can define the desired security policy through the Policy Definition GUI. The security policies that can be set through the Policy Definition module include, the type of document or content to track, the protocols to decode, the keywords or key phrases that need to be searched, the threshold for alerts to be generated and the preferred notification vehicle.

• Security Alerts

iBugle provides real-time alerts, based on the policies set up through the Policy Definition Engine.

• Browser Based Graphical Management Dashboard

iBugle has a centralized, easy to use browser-based graphical user interface, for policy administration. The dashboard is customizable and can display the alerts generated, when a specified policy is breached, using either tabular data or charts.

Easy to Deploy

• Appliance Form Factor

iBugle is available as a 2 U appliance that plugs into an existing enterprise network and is hence very easy to deploy.

• Zero Impact Integration

iBugle is easy to integrate because it is a passive device and does not disrupt the performance or stability of the enterprise network.

Conclusion

Saraansh's iBugle appliance is a comprehensive scaleable solution to the information leakage problem faced by organizations.

For further information please contact:

Saraansh Software Solutions Pvt Ltd,
#3, 1st Main Road, 3rd Block,
4th Stage, Basaveshvarnagar,
Bangalore - 560079,
INDIA
Ph: + 91-80-23145432 / 2314 5433
marketing@saraansh.com
Website: www.saraansh.com