
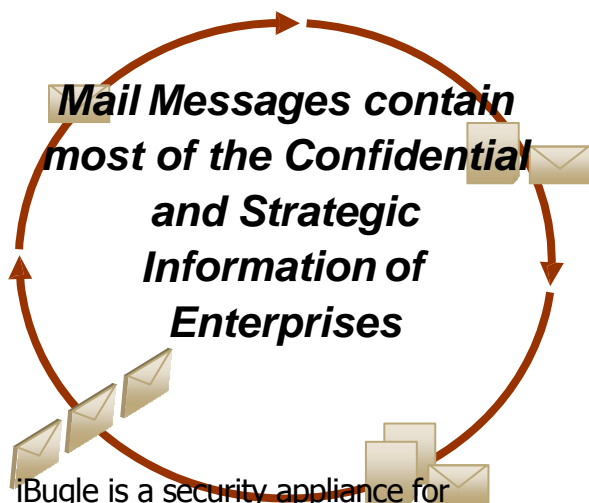


iBugle

Information Security Appliance

In Collaboration with 



iBugle is a security appliance for monitoring information leakages on mail backbones of enterprises. iBugle can be configured to detect regulatory policy violations, strategic information transmittals and IP thefts.

Regulatory Compliance puts new demands on mail message monitoring. Competitive market pressures demand stringent content analysis for detecting valuable information hidden deep inside the attachments of mails.

Insider Information Leakage Detective Service



iBugle : Next Generation Information Security Appliance

Real Time Protocol
Decoding Mail
Reconstruction
Policy Based Pattern
Search

Non Intrusive Message Monitoring

iBugle does not affect the network characteristics or the performance of the existing enterprise mail backbone.

iBugle comes with one set of policy templates. iBugle library of patterns is continuously being updated for ever changing vocabularies and profiles of user communities.

Archival

It is possible to archive the captured mails for easy retrievals based on time, theme, department, policy, incident, people etc.

Policy

Policies can be defined to include or exclude specific groups of people. Policies can be configured to run at specific timings on week days or weekends or at a particular interval after the office hours begin for example.

Keywords, phrases and regular expressions are used to describe the theme of the message of interest.

Lexicons & Mail Profiling

Lexicons are part and parcel of a policy. Lexicons are built with



iBugle can search deep within 120 + types of formats of attachments.

A basic library of policy templates and customizable common search parameter based industry patterns are provided with the appliance.

weighted categories of expressions and phrases.

Sensitivity

Mail messages are given a score based on the sensitivity with respect to policy.

Offline Forensics

It is possible to do offline digital forensics on message repositories.

Alerts & Case Worker Support

Alerts are generated by iBugle for relevant case workers

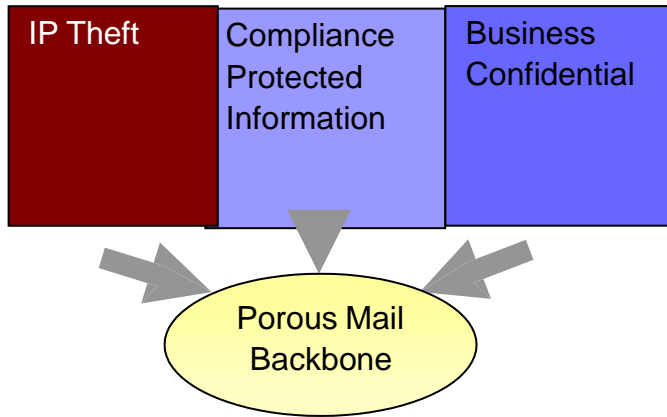
Fail Safe Redundancy

iBugle is available in dual box configuration mode to provide fail safe redundancy for near line speed message capture and fast policy processing.

Basic iBugle can process up to 50,000 outbound mail messages and 4 Giga bytes of data per day with 4 normal real time policies

iBugle

Information Security Appliance



Insider Information Leakage Detective Service

End to End Solutions & Services

Offers policy design consultation to select clients.

Offers mail analytics and security incident processing services to select clientele for a mutually agreed duration.

Offers the services, in transition, for mail archival, indexing, retrieval and theme based historical repository analytics

- It is possible to specify watch lists and white lists for selective screening of people and departments within the organization.
- It is possible to specify time and date durations for chosen policies
- Credit cards, Personal Identification information, zip codes etc can be identified in mail messages.
- Case Worker Module is provided for digital forensics on security incidents reported
- Newer pattern identification libraries and unique mail attachment scanners are provided on demand

Impact

can a company compute the cost of the loss of product launch plans to competition?

What are the consequences of a Regulatory penalty on the brand of an organization?

Stolen personal consumer information from company's databases: Definite decrease in market share.

Leakage of source code or trade secrets relating to product designs: Competitive advantage is reduced

Leakage of client list or client information in banks and financial institutions: Serious damage to business and Brand

Search Every Mail Message with researched contextual analysis templates