

Innerbus

 **LogCenter™** Suite

Log Archiving System

Head Office: 137-060 6F, Woosung Bldg. #915-10, Bangbae-dong, Seocho-gu, Seoul, Korea

Global R&D Center: No.45, 2nd Floor, Koramangala Layout, Koramangala, Bengaluru, India

 [www.logcenter.net](http://www.logcenter.net)

 [www.innerbus.com](http://www.innerbus.com)

INNERBUS INNERBUS INNERBUS INNERBUS INNERBUS INNERBUS INNERBUS

# AGENDA

## Proposal Outline

1. Importance of log
2. Solution proposal background
3. Present scenario of log analysis
4. Log related regulation and example

## LogCenter Suite Overview

1. System configuration
2. LogCenter Suite Feature
3. LogCenter Suite primary function
4. LogCenter Suite composition and details function

## Result of Implementation

1. Construction example
2. Expectation effect

## Innerbus Introduction

1. General present condition
2. Innerbus Solution Map

# Proposal Outline

## Importance of Log

- ▲ Only Logs contain information about security, performance, threats and malfunction.
- ▲ When there is any infringement, only thing you can rely on is Logs.
- ▲ The cause for accident can be quickly identified and remedial measures are taken with the help of Logs.
- ▲ There is a need for at least 3 months backup of Logs as per the legal guideline.
- ▲ Important information about status and obstacle occurrence of system, network can be found in Logs.
- ▲ All the utilities of Logs are realised only if there is proper collection and storage of Logs.

# Proposal Outline

## Solution Proposal Background

### Efficient log collection integration for system security and log administration

- ▲ Log data collected in real time from different resources and saved safely
- ▲ Quick analysis of situation and confront infringements
- ▲ A good appliance to manage log data easily and conveniently

### Qualitative elevation and manpower reduction of log administration

- ▲ ROI maximization as a result of significant decrease in Log analysis and reporting
- ▲ Verification of multi-variety logs
- ▲ Ability to make policies and modify plans

### Raw Log verification and Log Forensics

- ▲ Raw Log verification without log compression (Agent use) or logarithmic transformation (DB use)
- ▲ Identification of traces of infringement to do Log Forensics

### Quick Response

- ▲ Necessity for specialized log collection and analysis for fast and accurate accident response

# Proposal Outline

## Present Scenario of Log Analysis

### Lack of information about Logs

- ▲ Large quantities of unattended logs stored locally are prone to manipulation.
- ▲ The notion that large quantity of time and manpower is required to analyse logs of Giga/Tera bytes.

### Difficulty of farsighted Log verification

- ▲ The fact that logs are stored in a large Database, Report is generated through query system, dependence on the supporting platform makes log analysis toilsome.

### Limitations of other solutions

- ▲ Large majority of log analysis tools use log parsing techniques.
- ▲ There is no guarantee of integrity of log file because of compression/conversion/DB storage.

### Difficulty of analysis and administration

- ▲ The person in charge of security/system should have special knowledge of logs, causes log administration difficulty.
- ▲ The complexity of handling multiple log files of large size to search information.

# Proposal Outline

## Log Related Regulation and Example

### Government advice

- ▲ To centralize the logs
- ▲ To follow the policy of security check for information leakage, violation
- ▲ Strict adherence to personal information protection

### Guidelines

- ▲ Guidelines for log collection, storage, backup and log backup of at least 6 months
- ▲ To analyse main system information log weekly once and logs from Firewall, IDS and VPN daily
- ▲ Secure the logs so that it is not modified by common user

### Law

- ▲ Ministry of Information and Telecommunications to allow accumulation of information for business
- ▲ Permission to track down infringement accident and person responsible for it
- ▲ Allocation to record personal information to avoid forgery that is punishable

# Proposal Outline

## Log Related Regulation and Example

### The need to tackle rapid internet infringement accidents

The Government's communication law, and Ministry of Information through revision of Telecommunications Security Protection Act, make it mandatory to record, conserve and analyse Logs.

### Urgency to ensure cyber safety

The United States of America is advising the public to preserve the logs for at least 3 months. The European government made it mandatory to retain transactional information about users' activities.

# Solution Introduction

## LogCenter Overview

- ▲ Collects Log data from different IT resources in real time and saves safely
- ▲ Collects logs regardless of target in remote (Client) with ease to rapidly audit, assay, Report

- 1 Aggregated Collection**  
Integrated collection of multi-variety logs through appliance
- 2 Easy to Manage Log File**  
Easy log inspection, analysis and reporting in remote system
- 3 Powerful Log View**  
High-capacity raw log inspection of several GBs.
- 4 Unlimited Reporting**  
Infinite variety of report creation and data verification without using template
- 5 Log Forensics & Audit**  
Any Log, Any Search, Any Filtering

# Solution Introduction

## Comparative Study

Division	LogCenter Suite	Other Log Analysis Solution
Log Collection	All types of with Syslog, FTP, Agent, SNMP, LEA Strong Appliance of maximum 15000 PPSs	Selective Log collection Maximum 500 ~ 5000 PPSs
High-capacity Log Analysis	Farsighted log analysis (world first) more than 1 TB PC analysis without FS, memory restriction Text log analysis performance more than 10 MB per second	Analysis prohibition (Editor etc.) more than 500 MB GB log passivity separation and memory restriction Processing speed (Script etc.) more than 1 MB per second
Log Forensic & Audit	Any Log, Any Search, Any Filter High-capacity, Multi-variety, Raw log integration	Analysis is limited to certain type of logs Integration log chase and analysis prohibition
No DB & Reporting Tool	Raw log analysis without the database and reporting tool Infinite number of report creation	Dependent on database, reporting tool and template Report creation is dependent on type of log
Log Administration	Capable of analysing logs from a remote source Easy registration and reusability of filter, report patterns	Capable of analysing logs from only local source No reusability of patterns

# Solution Introduction

## LogCenter Suite Network Map

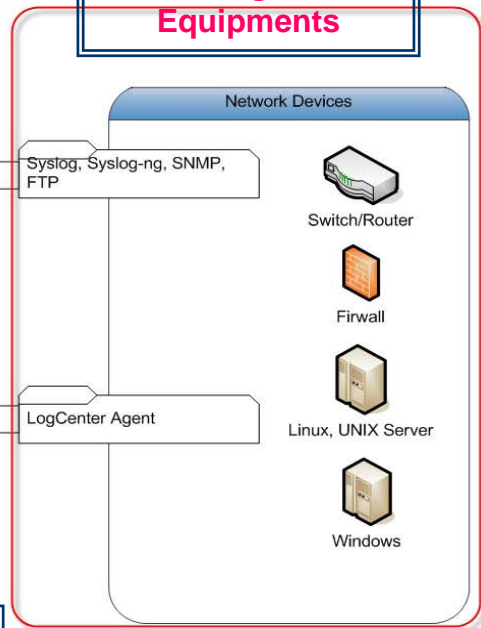
**Remote Administration Manager**



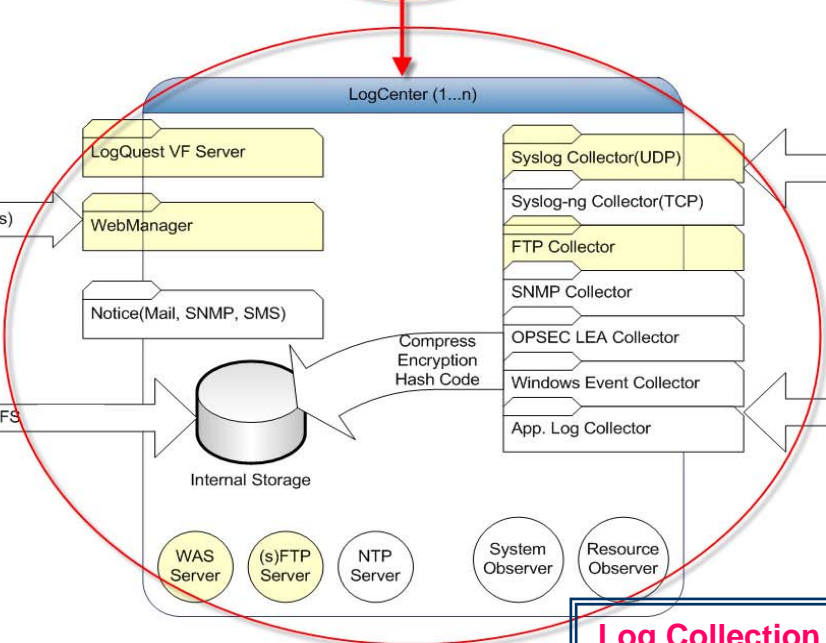
**Original Log Assay/Varification**



**Assembling & Analysis from Target Equipments**



**Log Backup**

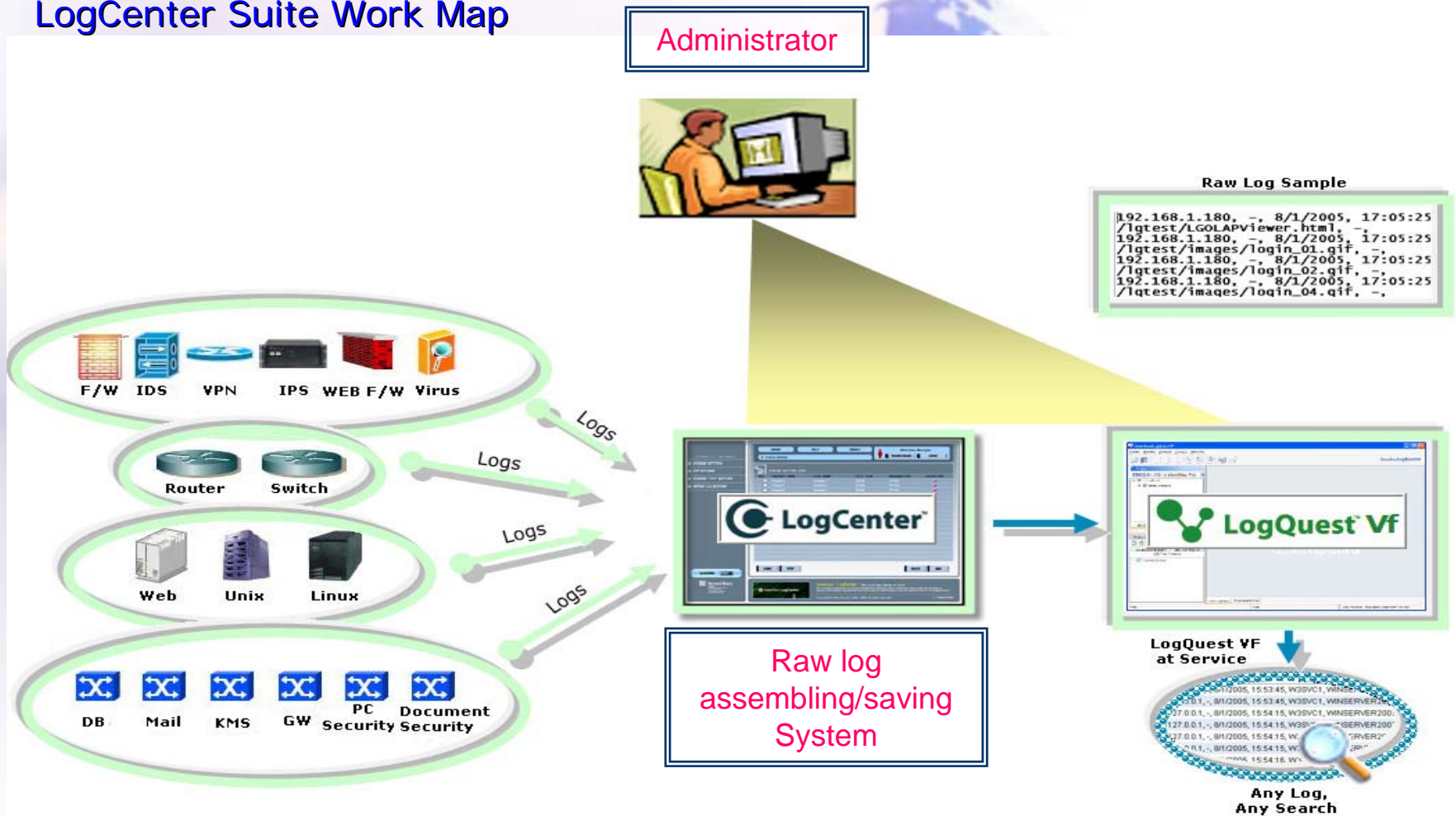


**Log Collection Appliance**



# Solution Introduction

## LogCenter Suite Work Map



# Solution Introduction

AND/OR logical function support for filtering  
Convenient filter pattern reusability

Log collection from network, security equipment, system etc.,

Log collection from various protocols such as Syslog, FTP, LEA, and SNMP

High-capacity log inspection more than several GB

Multi-variety log format support

Remote log analysis support through client system

Robust Filtering

Real Time collection

Convenient Log Administration

Powerful Reporting

Infinite number of reporting possibility

Conversion of report data for second drill-down

Log Forensics

Various Searching

Integration analysis of multi-variety logs

Log chain audit trail

Powerful search function

Real time IP chase

# Solution Introduction

## Primary Functions

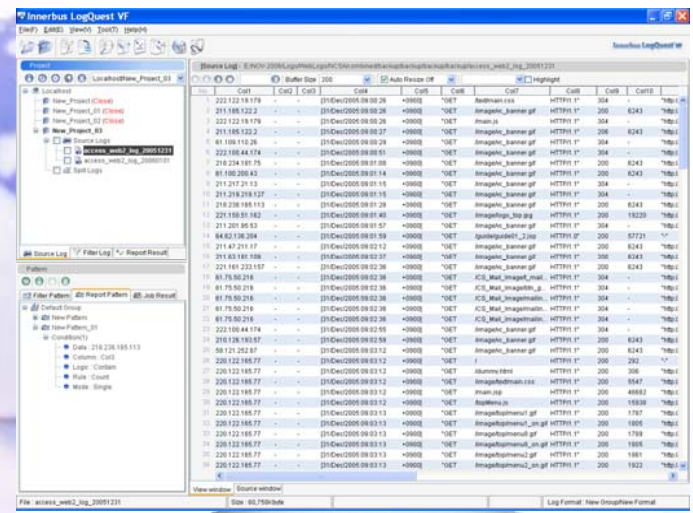
- ▲ Real Time Log File Save  
Real time file save with appending options up to 100 files
- ▲ Log collection using Syslog (TCP/UDP)  
3000 packets per second ~ maximum 15000 packets collection
- ▲ Log collection through batch job using remote FTP service  
Option to select either Binary or Ascii type
- ▲ Various conversion support for saving log file  
By time, separation save and compression (zip, gz) file save support
- ▲ High-capacity Log File save  
Log File that happen to 5 MB per second by real time save
- ▲ Exclusive Appliance with built-in software and storage  
Linux base exclusive OS with 2GByte memory, and 300GByte HDD supply
- ▲ HA (High Availability) support  
Log data save through Fail Over support and Hash function



# Overview

## Analysis and Reporting

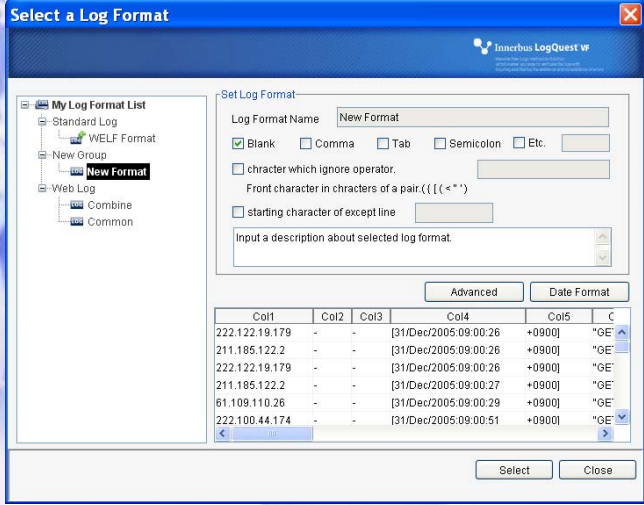
- ▲ **Filter Wizard Function**  
Powerful filtering with options to use AND/OR conditions and expressions
- ▲ **Multiple log file integration analysis**  
Efficient data analysis for multiple logs regardless of log format
- ▲ **In-depth Filtering**  
Comprehensive filtering function that can be re-run to track the required data
- ▲ **Conversion of Filter files**  
Options to convert and save Filtered file which is useful for later reference
- ▲ **Search function support**  
Various kinds of Search options such as IP Whois Search, Highlight, Condition based search
- ▲ **Report Wizard Function**  
Create up to 2000 Reports based on multiple conditions without using any template
- ▲ **Additional Reporting feature**  
Reporting function empowered with Export to Excel and saving in csv/text format for further drill down



# Overview

## Administration and other functions

- ▲ Log file split function  
Large log files can be divided into convenient sizes for easier analysis
- ▲ Raw log assessment  
High-capacity inspection of logs, of more than 10GB without the help of database and reporting tool
- ▲ Log analysis/management function  
Analysis support through LogQuest Vf(Clent) coordinated with the LogCenter Appliance
- ▲ Project Wizard function  
Supports many standard log formats, allows customization and creation of formats for display purpose
- ▲ Hash function for integrity check  
Up to 50 different Hash function support to generate the Hash code of a log file for integrity check
- ▲ Exquisite log pattern creation function  
Flexibility to merge, divide, hide and adjust the width of columns according to the requirement
- ▲ E-Mail transmission function  
Ability to send report/filter patterns and log formats through E-Mail for better support



# Overview

## LogCenter™ V2000

- ▲ 5,000 packets collection per second (Maximum : 15,000 packets)
- ▲ Device support up to 50 numbers
- ▲ Type: 2U Rackmount Network Appliance
- ▲ OS: Innerbus Embedded OS
- ▲ CPU: Dual socket LGA 771 Intel Xeon 64bit processor
- ▲ RAM: DDR II 400 512MB 4EA
- ▲ HDD: SCSI 300G 10K ppm 1EA
- ▲ 500W PFC Dual Power Supply

## LogCenter™ V1000

- ▲ 2,000 packets collection per second (Maximum: 7,000 packets)
- ▲ Device support up to 20 numbers
- ▲ Type: 1U Rackmount Network Appliance
- ▲ OS: Innerbus Embedded OS
- ▲ CPU: Intel Pentium T2300 1.66GHz 667MHz 2M L2
- ▲ RAM: DDR II 533 512M SDRAM
- ▲ HDD: SATA 80G(Seagate) 7.2K-RPM
- ▲ 200W Power Supply

# Overview

## Any Device, Any Type Log Collection

- ▲ Windows System Event Log
- ▲ Windows Security Event Log
- ▲ Microsoft Exchange Server application logs
- ▲ Microsoft SQL Server application logs
- ▲ Windows based ERP and CRM systems application logs
- ▲ Cisco and other syslog reporting routers
- ▲ Cisco and other syslog reporting switches
- ▲ Cisco PIX, Netscreen, and other syslog reporting firewalls
- ▲ Cisco, Snort and other syslog reporting IDS/IPS
- ▲ HP-UX, Solaris, and other syslog reporting Unix-based OS
- ▲ Etc.

## Using Agent Log Collection

- ▲ Apache and IIS web servers
- ▲ Linux system logs
- ▲ Windows ISA server logs
- ▲ DNS and DHCP server logs
- ▲ Host based intrusion detection/prevention systems
- ▲ Etc.

# Overview

## Project Wizard

- ▲ The Project Wizard is the first step of log analysis that includes creating convenient log formats under My Log Format List
- ▲ Supports logs of different types, logs in Binary form and compressed form
- ▲ Wide choice of data separators, column adjustments and date formats

**Project Wizard - Select a Excute Type**

Log Type

Non Finite(Text) Log  
In case of Text log has no pattern.

**Finite(Text) Log**  
In case of Text log has pattern.

---

**Select a Log Format**

My Log Format List

- Standard Log
- New Format
- New Format\_01**
- WELF Format

Set Log Format

Log Format Name: New Format\_01

Blank    Comma    Tab    Semicolon    Etc.

character which ignore operator.

Front character in characters of a pair.({ { < " ' }

starting character of except line

Input a description about selected log format.

Set/ Create Date/Time Format

Set Columns

Advanced   **Date Format**

Col1	Col2	Col4	Col5	Col6
#Software:	Micros...	Information	Services	6.0
#Version:	1.0			
#Date:	2005-1...			
#Fields:	date ti...	s-sitename	s-computername	s-ip
2005-11-29	15:00:...	SOKCHO-WE...	211.114.247.196	GET
2005-11-29	15:00:...	SOKCHO-WE...	211.114.247.196	GET

Select   Close

# Solution Introduction

## Filter Wizard

- ▲ Zeroing in on the required data from billions of log lines made easy through filter function
- ▲ Logical conditions and expressions can be used for effective filtering
- ▲ Filter result can be saved in CSV and XML format
- ▲ Filter Pattern is automatically saved for future use/modification

**Project Wizard - Select a Excute Type**

Log Type

Non Finite(Text) Log  
In case of Text log has no pattern.

Finite(Text) Log  
In case of Text log has pattern.

---

**Select a Log Format**

My Log Format List

- Standard Log
- New Format
- New Format\_01**
- WELF Format

Set Log Format

Log Format Name: New Format\_01

Blank    Comma    Tab    Semicolon    Etc.

character which ignore operator. \_\_\_\_\_

Front character in characters of a pair.({ { < " ' }

starting character of except line \_\_\_\_\_

Input a description about selected log format. \_\_\_\_\_

Set/ Create Date/ Time Format

Set Columns

Advanced   **Date Format**

Col1	Col2	Col4	Col5	Col6
#Software:	Micros...	Information	Services	6.0
#Version:	1.0			
#Date:	2005-1...			
#Fields:	date ti...	s-sitename	s-computername	s-ip
2005-11-29	15:00:...	SOKCHO-WE...	211.114.247.196	GET
2005-11-29	15:00:...	SOKCHO-WE...	211.114.247.196	GET

Select   Close

# Solution Introduction

## Log Chain Filter

Tracks down the specified piece of log data without bothering about the type, size and number of log files

Analyses and traces the cause of obstacle through chain filtering for speedy investigation



# Solution Introduction

## Report Wizard

The log data analysis can be summarized and represented graphically for better understanding of the situation/cause

Any piece of log data can be picked to quickly generate a Report

The generated Reports can be exported to Excel file and each data set can be saved in text/csv format

The screenshot shows the 'Report Wizard' interface. It includes a 'Report Information' section with 'Pattern Name: Test\_Pattern' and 'Maximum Count: 200'. Below this is a 'Report Condition' section with a table of conditions. A 'Report View' window displays a 3D bar chart and a table of data. A 'Report' window shows a summary table with 'Maximum Value: 16' and 'Minimum Value: 1'. An 'Export to Excel' button is visible at the bottom right. A 'Test-excel' window shows the exported data in an Excel spreadsheet format, including a 3D bar chart and a table of data.

No	Col3	Col2	Count
1	218.51.249.52	15:02:12	16
2	218.51.249.52	15:02:11	14
3	218.51.249.52	15:02:13	9
		15:03:23	6
		15:02:04	6
		15:02:03	4
		15:02:22	3
		15:02:21	1

No	Col3	Col2	Count
1	218.51.249.52	15:02:12	16
2	218.51.249.52	15:02:11	14
3	218.51.249.52	15:02:13	9

# Solution Introduction

## LogQuest Features

**Whois Search**

**Search**

**Job Wizard**

**Split a File**

**Split Logs**

*A glimpse of other functions*

The screenshot shows the LogQuest application interface. Several windows are highlighted with green boxes and labeled with pink text:

- Whois Search:** A window showing IP address details for 192.168.1.100, including location (USA, California) and ISP information (Verizon).
- Search:** A window displaying a list of search results with columns for IP, Date, and other metadata.
- Job Wizard:** A window for configuring a job, showing fields for Job Name, Description, and a table for filters and reports.
- Split a File:** A window for splitting a log file, with fields for file name and line count.
- Split Logs:** A window showing a list of log files to be split, with checkboxes for selection.

# Result of Implementation

## Construction Example

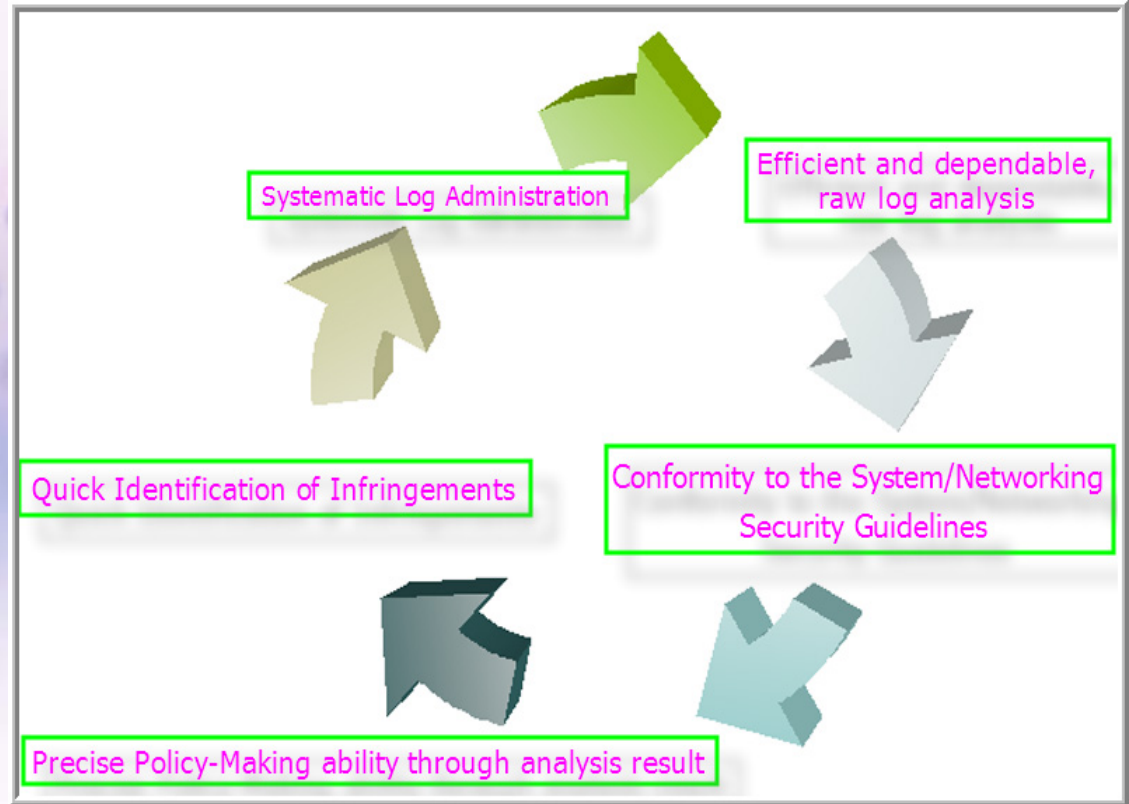
Our products are implemented in some reputed companies targeting different kinds of logs for analysis.

Company	Target log	Company	Target log	Company	Target log
Samsung Semiconductor	Firewall	Chongju University	Network, Database	Electronics and Telecommunications Research Institute	Firewall
LG Chemicals	Application	Ministry of Unification	Firewall, Mail	Korean Coast Guard	Security, Web
Naver Operation HQ	System, Security	KT	Network, Firewall	Korea Investment Co., Ltd.	Firewall
Samsung Networks	Firewall/Application	KOSCOM	Security, web	LG CNS	Application

# Result of Implementation

## Construction ROI analysis

### Expectation Effect

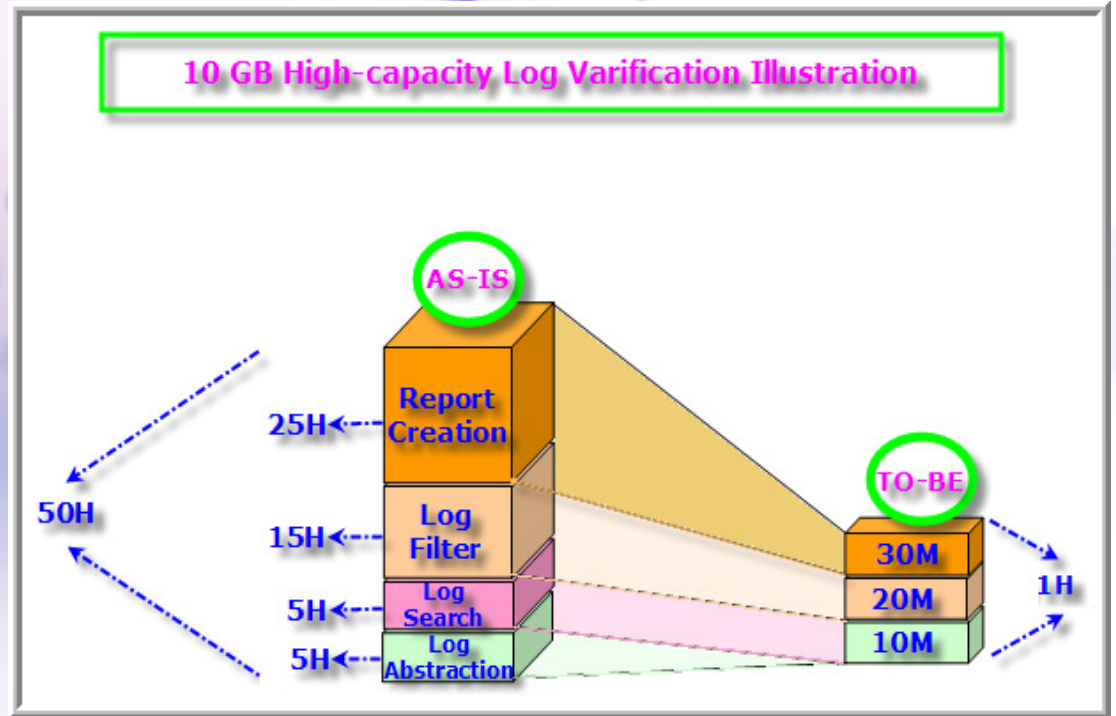


Innerbus has verified and analysed enterprise's logs to provide effective solutions in problem solving and safe computing. It has succeeded in this venture and adding on the features to make it a more viable product

# Result of Implementation

## Expectation effect (quantitative)

LogCenter Suite is a futuristic log management solution which fulfills the growing needs of an enterprise. It is designed to accommodate the increasing log sizes as the company grows. It is highly economical option for a company looking for a log verification and analysis tool.



# Innerbus Introduction

Innerbus is a software development company established in 2001 and is striving hard to be the world's best log analysis solution provider. We are providing specialized solutions in log management with the help of expertise in technology. Our products are successfully used by 200 reputed establishments like, KOSCOM, LG chemicals, LG-CNS, LG Telecom, Samsung semiconductor, Seoul National University, etc.,

## Integrated log analysis solution

- ◆ Leakage of confidential information through the employees can be analysed.
- ◆ Access instances by unauthorized person/member can be analysed.
- ◆ The misuse of time and resources by members can be analysed.



## Firewall log solution

- ◆ Network traffic security level analysis.
- ◆ Details of inbound and outbound traffic analysis.
- ◆ Analysis of details related to different IPs.

## Log Archiving solution

- ◆ Original log reporting.
- ◆ Integration of log filtering.
- ◆ Analysis of details related to different IPs.

## Web log analysis solution

- ◆ Website visitor analysis.
- ◆ Web log security/hacking analysis.
- ◆ Customer's legacy system analysis.
- ◆ Website contents, menu, page analysis.

# Innerbus Introduction

## Main Certifications and Intellectual Property Rights

The core competencies of Innerbus Company in Log Management solutions are reflected in our patented and registered ventures. The certificates and awards gained only push us further to enhance our capabilities.

Type	Description/Name	Application/Registration Number	Date of Registration	Inventor
Patent	Log file capturing and analysing method	1020040116644	2004.12.30	Innerbus@
	Device to analyse logs and report	1020040003849	2004.02	Innerbus@
	Web log analysis for Web traffic interpretation	1020030022825	2003.04.11	Innerbus@
Programme Registration	LogQuest VF	2004-01-15-483	2004.02.06	Innerbus@
	Hit Analyzer Enterprise Suite JX1.5	2002-01-15-6148	2002.10.21	Innerbus@
	LogCenter	2002-01-15-6149	2002.10.21	Innerbus@
Trademark Registration	HitAnalyzer	40-06028280000	2004.12.15	Innerbus@
	WebQuest	40-2004-0043129	2004.09.20	Innerbus@
	LogQuest	40-2004-0043128	2004.09.20	Innerbus@
	LogCenter	40-2004-0014673	2004.03.31	Innerbus@
	FireQuest	40-2004-0014674	2004.03.31	Innerbus@



**nis** 국가정보원  
적합성 검토필



Business Administration S/W

# Innerbus Introduction

## Innerbus Solution Map



# More Information

## ✓ 7 Steps For Getting The Most From Logs

1. Examine all log data
2. Plan for long term storage
3. Secure your log data
4. Remember the time source
5. Normalize in a common format
6. Prioritize all log data
7. Logs are your friend, not the enemy

### Customer

H.O Number : 02-588-9014 ~ 5  
Customer Center : 02-521-9016  
FAX : 02-588-9016  
Homepage : [www.innerbus.com](http://www.innerbus.com)  
Technical Support : [Support@innerbus.com](mailto:Support@innerbus.com)  
Head office address : 137-060 6F, Woosung Bldg. #915-10,  
Bangbae-dong, Seocho-gu, Seoul Korea.

### Business Inquiry

Contact : 02-588-9014 / [logcenter@innerbus.com](mailto:logcenter@innerbus.com)