Diagnose & secure your network

YATEM LogCollector®
Event Monitor™

What it does?

It provides you cost effective and robust "change tracking" of user activities on Microsoft operating systems.

Who?
When?
Where?
What happened?

System Load?

No overhead on CPU and network.

Reports & Queries

GUI and reports allows you to easily retrieve the data you seek.

Quick, Simple, Easy

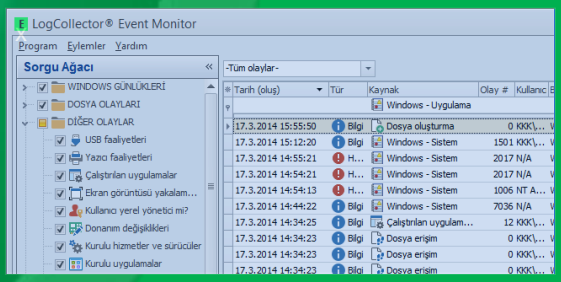
Installation takes several minutes. Settings does not bother you. Easy to learn and use.

Scalable & Robust

No matter how big and complex your network, it just works.

Legal Compliance

Supports legitimate data logging.



"LogCollector Event Monitor", is a software solution that aims to collect, keep and analyze of digital footprints of user activities on computers running Microsoft operating systems. It helps you to discover potential technical and security problems with the opportunity of real time observation. Additionally, it allows you backward investigation ability for causes of fairly new discovered problems.

Top Benefits

- **Provides awareness.** You would be the first, who notices about the activities on your network.
- **Protects your investment costs.** Supports you to protect your valuable investment and corporate data with minimum effort and cost.
- **Easy and flexible reporting.** Allows to prepare even complex reports in seconds for all your requests.
- **Supports sustainable security infrastructure.** Ensures sustainable security infrastructure on protection and development of the effectiveness of security policies by offering real-time information.
- **Built-in and scheduled reporting.** Provides built-in reports out-of-the-box for your needs. You can also create scheduled and/or alerting reports to be notified in time.
- **Scalable.** Provides enhanced features for scalability. It suits your deployment needs on your network whatever its size, architecture and complexity.
- **Saves time.** It provides the system administrator to save time during daily activities.

What can you do with LogCollector Event Monitor?

- Who did accessed, created, deleted, renamed or printed the "abc.doc"?
- Which softwares installed to which computers in past 7 days?
- Which users used USB storage devices on network?
- Are there any hardware changes on any computer on my network?
- Which applications did the user "U" execute yesterday?
- Which files did the user "U" access on his/her computer?
- Is there any user who has "Local Administrator" right on his/her computer?
- Who did changed his/her own local network card settings?
- Which network resources did the user "U" connect?
- Which events are labeled as "Critical" among my computer's event logs?

Properties

General

- **Licensing**: Per server and per user.
- **Database:** Collected logs are kept in Microsoft SQL or PostgreSQL Server database.

Event Collection

- **Architecture:** Agent based.
- **Events:** Events logs are collected rule based. Some events collected:
  - Windows events logs.
  - File system changes (file/folder create, delete, rename, move etc.).
  - USB activities.
  - Printing activities.
  - Screen capture (with captured image if needed).
  - Executed applications.
  - Local admin right check against logged in user.
  - Hardware changes.
  - Installed/uninstalled applications.
  - Network activities.
  - Network card settings changes.
  - Session (login/logout, lock-unlock) activities.
  - Folder sharing activities.
- **Event Details:** For every event the activity information of user name (who), computer Name (where), timestamp (when), object name (what) are detected and logged. The old and new value of the changed object are kept together.
- **Real Time Collection:** Events are detected recorded by the agents as soon as occurred.
- **Off Line Activity:** Agents continue to detect and collect logs of events when the computer lost the network connection. Agents protect themselves and also the data which are waiting to send. When the computer become online, the data transfer process starts automatically.
- **Agent Protection:** LogCollector prevents any user access to agents and collected event records.
- **Agent Performance:** LogCollector agents have a powerful science of art monitoring engine, it just works.
- **Agent Footprint:** LogCollector agent needs very small system resource to work. It never loads the CPU, memory and bandwidth.
- **Data Reliability :** Every event record is tagged with a MD5 hash as the event happens in order to guarantee that data is not changed. The console application marks the data which has a wrong hash.

Event querying, Analyze and Reports

- **Real Time Event Monitoring:** LogCollector has a powerful user interface in order to query, analyze and get screen and printed reports on collected data in real time.
- **Dynamic Queries:** LogCollector user interface provides simple and powerful queries to retrieve the required data.
- **Query Performance:** LogCollector provides astonishing data retrieving performance on its data store.
- **Build-in Query and Reports:** LogCollector user interface provides a large number of built-in query and reports for data investigation.
- **Interactive Graphical Analyze:** Every text data shown on GUI can easily converted to drill-down chart style.
- **Data Export:** User interface provides data exporting to well known formats like PDF, CSV/Excel, HTML and XML.
- **Scheduling Reporting:** Reports can be scheduled to save in to desired folder as various formats like pdf, excel or text files and/or sent to any email address.
- **Notifications (alarms):** Automated email notifications can be set for desired conditions.

Management

- LogCollector has a central management console tool for installing/uninstalling and tracking status of agents.

Archiving

- LogCollector includes an archiving tool to transfer old records from database to offline xml based store.
- Archiving can be achieved manually or automatically.
- Archived data can be viewed and analyzed with the archiving utility offline.

System Requirements

LogCollector Server:

- CPU: 2 GHz Pentium or above
- OS: Microsoft Windows 7 or above
- RAM: 1 GB+
- DBMS: Microsoft SQL Server 2008+ or PostgreSQL 9+ above
- Storage: 100 MB+ for initial installation and enough space for data storage.

Agents:

- OS: Windows 7 or above
- Storage: 100 MB+ including offline logging needs.

yatem yazılım teknolojileri merkezi

YATEM Information and Technology Systems Inc.
E-mail: yatem@yatem.com.tr
Phone : +90 (312) 479 4088 Fax: +90 (312) 479 4088
http://www.yatem.com.tr

AUTHORIZED DISTRIBUTOR

Document code: B-LC-EVENTMON-R6-3