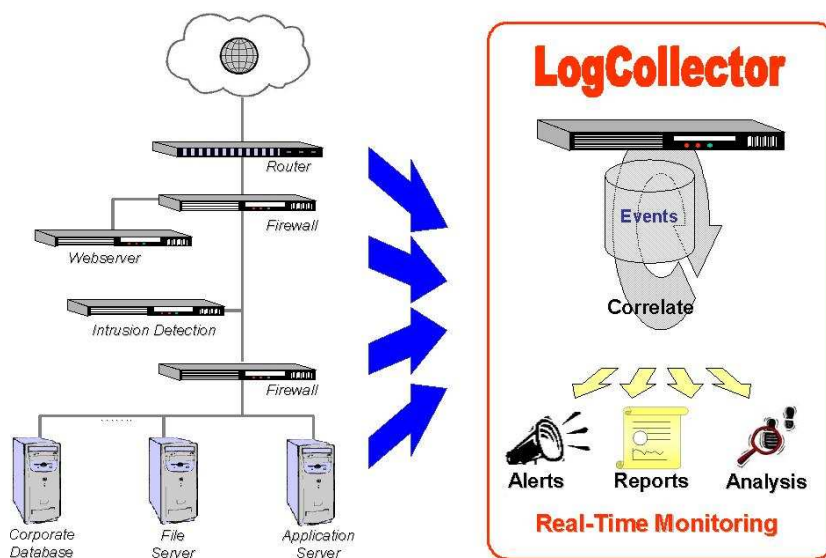


LOGCOLLECTOR

With the rising use of the Internet, companies have deployed a best-of-breed, well-maintained security infrastructure to protect their information assets against both external and internal threats. This level of security is obtained by the integration of various components coming from several vendors, running on multiple platforms. Megabytes of information about the network activity are generated and some products are even capable to generate alerts. However, the diversity of the components makes it difficult to the systems and security engineers to keep

a global view on the events taking place in this infrastructure. To analyze each suspicious event, the engineer must gather the logs on each machine individually and then, manually, analyze these logs in order to take appropriate action. Unfortunately, these alerts are not always reflecting the real dangers. An intrusion detection system might warn for the Nimda virus whereas the webserver is correctly configured and rejects the attack. The security engineers are overwhelmed with this kind of 'false positives' and might overlook the real attacks.

LogCollector centralizes and stores all event information coming from various disparate systems in a standardized and unified format enabling the correlation and analysis of all suspicious activity within the organization's IT environment.



Controls and correlates everything

LogCollector continuously monitors the infrastructure performance and security by eliminating the false alarms and showing emerging dangers. Consolidated reports based on information coming from several elements of the infrastructure show what's really going on.

Cost-effective

LogCollector centralizes the control over both open and proprietary security tools enabling the correlation of (from logs to alerts). The time spent on gathering information is reduced and more attention can be given incident resolution.

Integrates in any existing environment

Most enterprises have already deployed a multi-vendor security infrastructure. LogCollector is not linked to a limited range of products but interfaces with any type of device from any vendor whether it is a firewall, intrusion detection system, router, webserver, RAS, etc...

Easy to deploy

The all-in-one LogCollector appliance comprises the dedicated hardware, a normalized database, predefined reports, alerting functionalities and the powerful correlation engine. Through the easy-to-use configuration assistant, is up and monitoring in no time.

Scalable

From one device up to a worldwide-distributed environment, LogCollector is able to keep the complete overview. When enhancing the infrastructure, one should not be limited for choosing the product that fits the best an organization's business needs.

Secure & Robust

LogCollector makes only use of proven and standard protocols. There is no need for implementing exotic workarounds or unusual configuration changes to have the centralized monitoring system operational.

LogCollector LC-150	LogCollector LC-360
<ul style="list-style-type: none"> - Compact 1U rack-optimized - Intel Pentium III 1GHz/133MHz processor with 256K cache - 512 Mb SDRAM 133 Mhz - 2 x 10/100BT network adapters - 2 x 73 GB HDD SCSI Ultra160 - 24X IDE CD-ROM - Floppy drive SVGA, Serial RS232C port, PS/2 keyboard/mouse connectors 	<ul style="list-style-type: none"> - Compact 2U rack-optimized - Redundant Power Supply - Intel Pentium III 1GHz/133MHz processor with 256K cache - 2 Gb SDRAM 133 Mhz - 10/100BT network adapter - 5 x 73 GB HDD SCSI Ultra160 - 24X IDE CD-ROM - Floppy drive, SVGA, Serial RS232C port, PS/2 keyboard/mouse connectors