BLUE LANCE
COMPUTER SECURITY SOFTWARE

LT Auditor+ 9 for Windows

Providing Clear, Concise, Actionable Intelligence

Overview

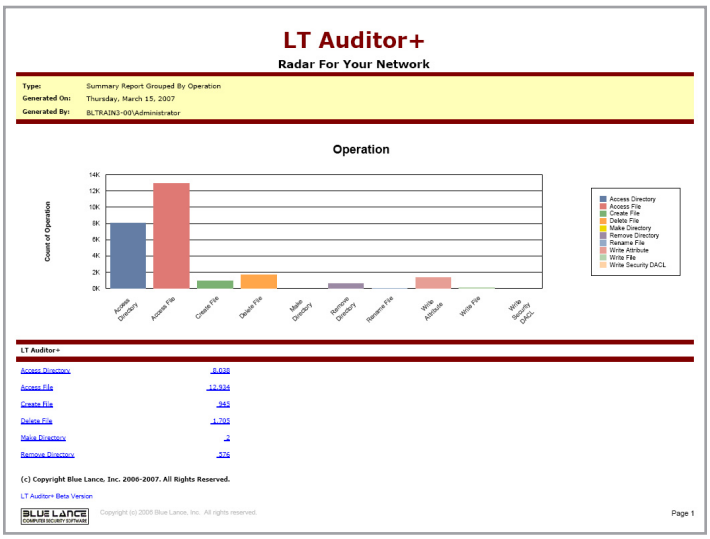
DuPont Employee Walked Away With $400 Million In Trade Secrets
Information Week - February 19, 2007

Headlines like this strike fear in the heart of every CIO, CSO and internal auditor in the nation, yet security breaches occur almost daily. How can security professionals combat this dangerous issue? With the right information and the best tools possible. Knowing exactly who is doing what, when and where on your network is critical. Blue Lance's LT Auditor+ 9 for Windows is designed to protect corporate assets by providing detailed and accurate information about insider activity and threats.

LT Auditor+ 9 is flexible and company friendly since it is simple to use and can retain audit information for extended periods of time in a MS-SQL or Oracle database, allowing an organization to store audit activity of an entire organization for several months.

This capability also allows for detailed forensic analysis when a security breach occurs and can give a clear picture of how and why it occurred.

LT Auditor+ 9 enables companies to efficiently manage and meet the rigorous guidelines for federal and international compliance regulations.


LT Auditor+
Radar For Your Network
Type: Summary Report Grouped By Operation
Generated On: Thursday, March 15, 2007
Generated By: BLTRAIN3-00\Administrator
Operation
Count of Operation
LT Auditor+
Access Directory 8,038
Access File 12,934
Create File 945
Delete File 1,705
Make Directory 3
Remove Directory 376
(c) Copyright Blue Lance, Inc. 2006-2007. All Rights Reserved.
LT Auditor+ Beta Version
Page 1

Features and Benefits

Actionable Intelligence

Don't just look at raw data. With LT Auditor+ 9, users will receive more than just volumes of raw event data – they receive actionable intelligence.

The information provided in the native event logs has a tremendous amount of irrelevant (noise) data and is typically incomplete and fragmented. LT Auditor+ 9 utilizes proprietary technology to sift through and correlate information that is relevant, thereby relieving security administrators from having to review hundreds and thousands of events to analyze one security incident.

Centralized Reporting

Reporting with LT Auditor+ 9 has never been faster and easier. Through centralized reporting, users can consolidate data or create forensic analysis reports organization wide. LT Auditor+ 9 offers hundreds of standard reports that target both security and compliance, all while adding drill down capability to individual events. Additionally, reports may be customized to display only required details.

Management Summary Reports – LT Auditor+ 9 includes several high-level graphical reports that summarize data or information with drill-down capabilities to view specific details. This alleviates the issue of parsing through hundreds of pages of data while looking for information.

Compliance Reports – LT Auditor+ 9 includes reports that help organizations stay compliant with the following regulations:

- SOX
- HIPAA
- GLBA
- FDIC/OCC/FFIEC
- FISMA
- BASEL II
- Breach notification acts
- European Privacy Directive
- PCI Data Security Standard

Early Detection/Real-Time Notification

LT Auditor+ 9 comes with an early warning detection system that alerts security administrators immediately when a breach or violation occurs. Alerts may be delivered via SMTP, SNMP, e-mail or pager.

Flexible Setup

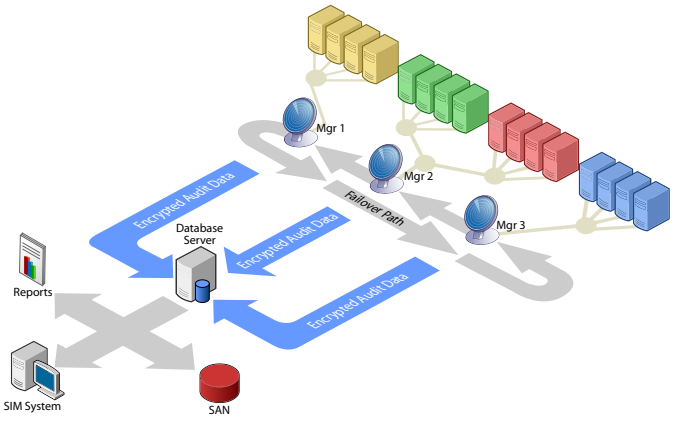
LT Auditor+ 9 is flexible and completely user friendly. It may be customized to meet any company's security or compliance needs. Utilizing four complimentary solutions, users can customize deployment to fit their company's requirements. LT Auditor+ 9 offers scalability, fault tolerance and load balancing to ensure the integrity of transmitted data.

Unique Solutions for Every Environment

Blue Lance designed LT Auditor+ 9 to include: enhanced security; exceptional auditing; multiple managers; a unique database structure; and powerful filtering capabilities.

LT Auditor+ 9 utilizes a three-tier client/server architecture to provide a flexible and reliable auditing solution with optimal performance and has four separate solutions designed to allow organizations to customize the solution to fit their specific needs.

- LT Auditor+ 9 for Windows Server
- LT Auditor+ 9 for Active Directory
- LT Auditor+ 9 for Group Policy
- LT Auditor+ 9 for Workstations



LT Auditor+ for Windows Server

LT Auditor+ 9 can produce detailed audit activity about files, folders and users on servers and workstations. The level of detail provided by LT Auditor+ 9 cannot be found on native Windows event logs. LT Auditor+ 9 clearly identifies the user and the node (IP address) used to perform the following activities on files and folders including:

- accesses, creation, deletion or renaming ; and
- changes and modifications to security permissions.

LT Auditor+ 9 for Active Directory

With LT Auditor+ 9 for Active Directory, administrators will enjoy a decreased workload and be able to constantly monitor the elevation of privileges, unauthorized and authorized changes, and the abuse of privileges. Once the system is in place, administrators can quickly run reports and set up alerts for policy violations.

The auditing capability of LT Auditor+ 9 for Active Directory extends beyond the basic native event logs to supply detailed information within Active Directory. Using LT Auditor+ 9 for Active Directory, users can track:

- Creation and deletion of users, groups, organizational units or any Active Directory object;
- Modifications to any attributes in the Active Directory schema;
- Modifications to security permissions of Active Directory objects;
- Password changes;
- Directory authentications (success and failure); and
- Kerberos and NTML authentications.

LT Auditor+ 9 for Group Policy

One unauthorized change, even an accidental change to the Domain Group Policy, can bring a company to its knees. To find the mistake or breach in the traditional manner could take weeks in down time and affect the entire enterprise. With LT Auditor+ 9 for Group Policy, Blue Lance introduced a new solution designed to provide detailed auditing and monitoring of Group Policy Objects (GPOs). Any changes within the GPO are not recorded in the event logs. LT Auditor+ 9 includes proprietary technology to clearly alert and report who changed a particular GPO as well as providing the old and new values of the modified GPO setting. GPO oversees:

- Audit policies;
- Password policies;
- Security options;
- Account lock out policies;
- Registry modifications;
- Event log settings;
- File system changes;
- User rights assignments;
- System service modifications; and
- Restricted groups modifications.

LT Auditor+ 9 for Workstations

Want to know who is moving information into and out of the organization? With LT Auditor+ 9 for Workstations, all workstations, laptops and USB drives can be audited. This provides administrators full details about a breach or violation, including who is responsible and what happened.

Specifically, administrators will learn who is logging on to each workstation. Also, if a hacker has broken into the local system to gain access to company servers, the security team will be notified. If removable devices are being used to move sensitive information out of the company or bringing questionable applications into the company, an alert can be generated.

LT Auditor+ 9 for Workstations is another essential level of defense in the fight for the protection and security of corporate information systems.

System Requirements

LT Auditor+ Manager

Processor - Intel Pentium 4 Processor or above
RAM- 1 GB RAM
Hard Disk - 200+ GB
Operating System -

- Microsoft Windows 2003 /
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP

Software - .NET v1.1

LT Auditor+ Agent

Processor – Intel Pentium 166 MGHz or above
RAM - 256 MB RAM
Hard Disk - 80+ GB
Operating System

- Microsoft Windows 2003
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP

Software - .NET v1.1

LT Auditor+ Database Server

Processor - Intel Pentium 4 Processor or above
RAM - 1 GB RAM
Hard Disk - 200+ GB
Operating System

- Microsoft Windows 2003
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP

Software

- Microsoft SQL Server 2000
- Oracle 9i or 10i

LT Auditor+ Management and Reporting Console

Processor – Intel Pentium 166 MGHz or above
RAM - 256 MB RAM
Hard Disk - 2+ GB
Operating System

- Microsoft Windows 2003 /
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP

Software - .NET v1.1

LT Auditor+ Installation Set up Minimum Requirements

1 Manager
1 Agent
Active Directory Enabled
Group Policy Settings
Windows audit policies activated for:

- Active Directory,
- Group Policies
- Selected folders on NTFS drives that require monitoring.

Administrator Privileges To Install

Contact Sales for More Information

Blue Lance, Inc.
Five Houston Center
1401 McKinney, Ste. 950
Houston, TX 77010

Toll Free: 800.856.2583
713.255.4800
Fax: 713.622.1370
www.bluelance.com

BLUE LANCE
COMPUTER SECURITY SOFTWARE