

LT Auditor+ 9

for Windows Server

360° View of Server Authentication, File, USB Drive Activity

Clear, Concise, Actionable Intelligence

Ensuring the privacy, integrity and availability of sensitive and confidential files is key to meeting compliance and security initiatives.

LT Auditor+ 9 for Windows Server is designed to provide detailed auditing and monitoring of Windows server activity—delivering clear, concise, actionable intelligence.

LT Auditor+ 9 for Windows Server goes beyond native Windows event logs and interacts seamlessly and unobtrusively with the operating system to capture:

- Successful/Failed Authentications;
- Successful/Failed File and Folder Operations; and
- Removable Storage Activities including USB and flash drives.

LT Auditor+ 9 for Windows Server delivers a bullet-proof audit trail, through easy-to-read forensic reports and real-time alerts, to precisely identify **who** did **what**, from **where** and **when**.

One look and you will see why thousands of organizations have chosen LT Auditor+ for more than 20 years to maximize the return on their security and compliance investment.

Compliance in a Click

LT Auditor+ 9 for Windows Server, part of the LT Auditor+ 9 for Windows family, provides the intelligence required to audit user and administrative activity in accordance with organizational policies to demonstrate compliance with regulations and guidelines such as FFIEC, GLBA, Sarbanes-Oxley, HIPAA and FISMA.

LT Auditor+ 9 for Windows Server provides executive summary reports, with drill-down capability detailing administrative and user activity about files, folders and users on servers. Reports may be scheduled for automatic distribution to administrative personnel at desired intervals.

The built-in scalability and fault tolerance prevents audit data loss and ensures the consolidation of audit data from servers within the organization. Without fear of loss, encrypted data collected through all LT Auditor+ agents is deposited into a single, secure repository, which provides accurate compliance reports on-demand.



Product Benefits

LT Auditor+ 9 allows organizations to immediately reap the benefits of continuous security and compliance monitoring including:

Prepare for the IT security audit process with comprehensive reports delivering clear, concise, and complete information on unsuccessful login and authentication attempts; access control changes made by privileged users and administrators; and access to sensitive files and resources. LT Auditor+ 9 for Windows Server simplifies the IT security audit process by providing automated report delivery using a robust scheduler and valuable report templates.

Meet compliance control transformation requirements pertaining to accountability, transparency and integrity by monitoring changes to controls and privileges that create material weaknesses. Compliance control transformation requirements are met by monitoring system login activity, application access, and modifications/deletions of sensitive files, including system configuration files. LT Auditor+ 9 for Windows Server ensures the availability and integrity of mission critical servers hosting databases containing sensitive information, such as financial data, health records and other confidential information.

Ensure privacy, confidentiality and integrity of sensitive information by monitoring changes to the Discretionary Access Control Lists (DACL) that define user and group access permissions to critical servers, files and folders. LT Auditor+ 9 for Windows Server comprehensively audits creations, deletions, modifications and access (successful

Product Features

- ❖ 24x7 Monitoring with real-time alerts
- ❖ Management Summary reports with drill-down capability
- ❖ Over 100 security and compliance report templates
- ❖ Translation and correlation of raw event log data into plain English reports and alerts
- ❖ Multiple report formats including Excel, Word, HTML and PDF
- ❖ Automatic report scheduling and delivery
- ❖ Audit files, folders, user authentications and USB storage devices
- ❖ Automatic archiving of Windows native event logs
- ❖ Enterprise-wide data consolidation
- ❖ Comprehensive Auditing with Granular filtering
- ❖ Audit the Auditor
- ❖ Robust, fault tolerant and load balanced architecture
- ❖ Multi-Manager-Agent architecture
- ❖ Automatic audit policy deployment
- ❖ Remote installation and deployment
- ❖ Built-in agent status and health monitoring
- ❖ Secure communication using PKI and AES encryption

and unsuccessful) to sensitive files and folders, including files copied to removable drives (USB and Flash Drives).

Improve incident response through immediate alerts of monitored authorized and unauthorized server authentications, after hours logins, account lockouts, failed logins and access to files and folders. LT Auditor+ 9 for Windows Server accurately tracks the execution, modifications and deletions of critical files and helps determine the scope of damage due to unauthorized user activity or the execution of malware (virus, trojans, and spyware). Comprehensive reports detail the activity leading up to an event, thus; reducing the time required to investigate the magnitude of a security incident.

Save Time and Money with clear, concise, easy-to-read LT Auditor+ reports and alerts in plain English, thus eliminating the complex task of sifting through large volumes of fragmented, incomplete data provided by native event logs, dispersed throughout the organization. LT Auditor+ 9 for Windows Server's scalable, fault tolerant design, coupled with superior audit data filtering and enterprise-wide data consolidation provides a powerful auditing solution with optimal performance.

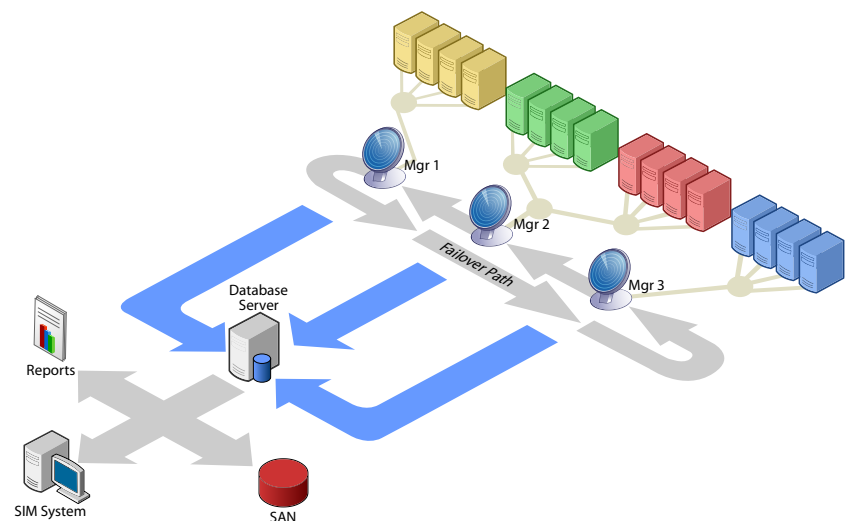
Engineered for Flexible, Reliable Auditing

Secure and Scalable

LT Auditor+ 9 for Windows Server employs a secure and scalable architecture which allows consolidation of audit data from thousands of servers within an enterprise into a centralized repository. The flexible manager-agent architecture allows for logical grouping of servers, each of which can be handled by separate managers, to easily oversee the deployment of audit policies and schedule the encrypted transfer and consolidation of audit data.

Built-in Fault Tolerance

With built-in fault tolerance, LT Auditor+ 9 for Windows Server ensures the availability of audit data. If the link between an audited server and its manager is severed, the communication is automatically rerouted to the first available manager. The audit agent will continue to monitor the availability of its primary manager, shifting back once communications are restored.





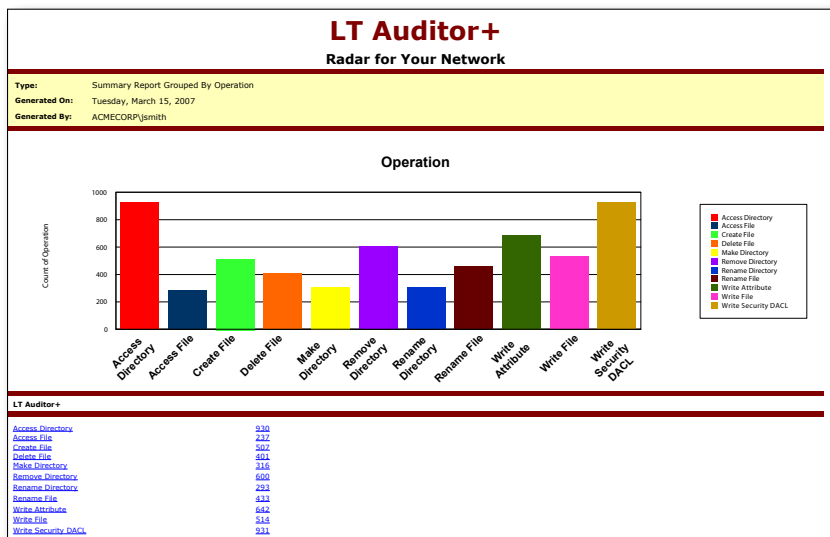
Comprehensive Reporting and Alerting

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

Reporting with LT Auditor+ 9 for Windows Server has never been faster and easier. Through centralized reporting, users can consolidate data or create forensic analysis reports organization-wide. LT Auditor+ 9 for Windows Server offers over 100 standard reports that target both security and compliance, all while adding drill-down capability to individual events. Additionally, new reports may be created and customized to display only required details and scheduled for automated delivery.

Management Summary Reports

LT Auditor+ 9 for Windows Server 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.



Audited Operations

Files/Directory Auditing Activity

- ❖ Create File
- ❖ Delete File
- ❖ Modified File
- ❖ Change Rights/Assign Rights
- ❖ Rename File
- ❖ Make Directory
- ❖ Remove Directory
- ❖ Rename Directory
- ❖ Open/Access File
- ❖ File Attribute Change
- ❖ Take Ownership

Authentication Auditing Activity

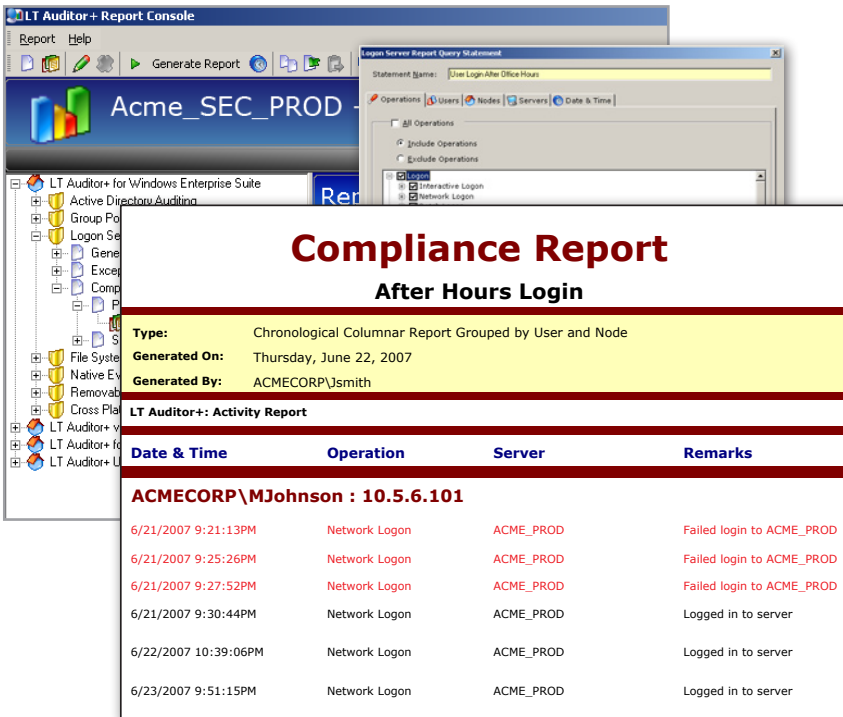
- ❖ Interactive Logon/Logout
- ❖ Network Logon/Logout
- ❖ Batch Logon/Logout
- ❖ Service Logon/Logout
- ❖ Unlock Logon
- ❖ Kerberos Authentication Ticket Granted
- ❖ Kerberos Authentication Ticket Renewed
- ❖ Kerberos Service Ticket Granted
- ❖ NTLM Authentication

System Activity

- ❖ Date/Time Changes
- ❖ Event Log Clear
- ❖ Application Load
- ❖ Application Unload

Compliance Reports

LT Auditor+ 9 for Windows Server includes reports that help organizations stay compliant with regulations such as FFIEC, GLBA, Sarbanes-Oxley, HIPAA, and FISMA.



The screenshot shows the LT Auditor+ Report Console interface. A report titled "Compliance Report After Hours Login" is displayed. The report details include:

- Type:** Chronological Columnar Report Grouped by User and Node
- Generated On:** Thursday, June 22, 2007
- Generated By:** ACMECORP\Jsmith

The report is categorized as "LT Auditor+: Activity Report". Below this, a table lists login events for user ACMECORP\MJohnson on server 10.5.6.101.

Date & Time	Operation	Server	Remarks
6/21/2007 9:21:13PM	Network Logon	ACME_PROD	Failed login to ACME_PROD
6/21/2007 9:25:26PM	Network Logon	ACME_PROD	Failed login to ACME_PROD
6/21/2007 9:27:52PM	Network Logon	ACME_PROD	Failed login to ACME_PROD
6/21/2007 9:30:44PM	Network Logon	ACME_PROD	Logged in to server
6/22/2007 10:39:06PM	Network Logon	ACME_PROD	Logged in to server
6/23/2007 9:51:15PM	Network Logon	ACME_PROD	Logged in to server

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
- Database - Microsoft SQL Server 2000/2005, Oracle 9i/10g

LT Auditor+ Agent

Processor – Intel Pentium 166 Mhz 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

Get Started Now

LT Auditor+ 9 for Windows Server is configurable to fit seamlessly into any organization—from the largest to the smallest. In addition to LT Auditor+ 9 for Windows Server, Blue Lance also offers comprehensive, flexible and reliable auditing solutions for Active Directory, Group Policy, and workstations.



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