BLUE LANCE
COMPUTER SECURITY SOFTWARE

DATA PROTECTION
OUT OF BOX
COMPLIANCE REPORTING

LTAuditor+ 9 for Active Directory

360° View of Active Directory Changes

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 Active Directory is designed to provide detailed auditing and monitoring of Windows Active Directory activity—delivering clear, concise, actionable intelligence.

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

- Active Directory Object Creations/Deletions;
- Account modifications, including enabling and disabling of accounts; and
- Group membership changes.

LT Auditor+ 9 for Active Directory 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**.

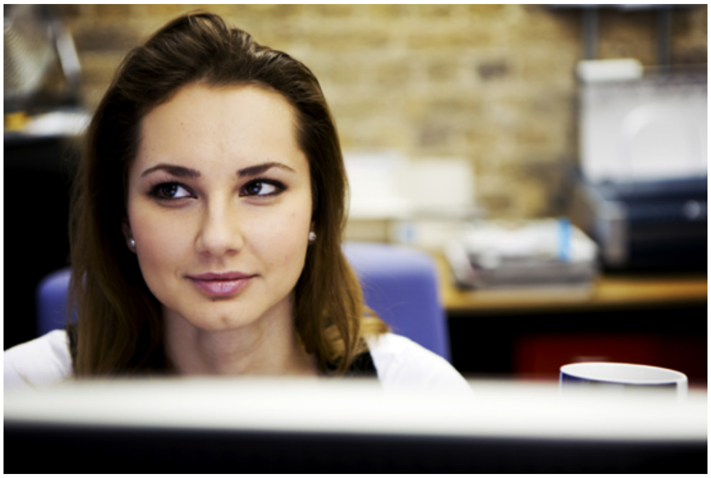
One look and you will see why thousands of organizations have chosen LT Auditor+ for more than 20 years to maximize the return on their security and compliance investment.

Compliance in a Click

LT Auditor+ 9 for Active Directory, 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 Active Directory 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 Active Directory object creations, deletions and modifications; access control changes made by privileged users and administrators; group membership changes and Active Directory administrative changes including audit policy changes. LT Auditor+ 9 for Active Directory 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 documenting changes to controls and privileges that create material weaknesses. Compliance control transformation requirements are met by monitoring all Active Directory changes, and providing the ability to verify authorized changes against established organizational security policies.

Ensure privacy, confidentiality and integrity of sensitive information by monitoring critical security changes to high profile Active Directory groups that define user and group access permissions to critical servers, files and folders. LT Auditor+ 9 for Active Directory comprehensively audits account modifications such as enabling and disabling of accounts, modification of security DACL to other sensitive objects within Active Directory.

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 Active Directory Object and Account Modifications, Group Membership and administrative activity
- 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

Improve incident response through immediate alerts of monitored high profile Active Directory changes such as adding members to security sensitive groups (Enterprise Admins, Domain Admins, etc.). LT Auditor+ 9 for Active Directory accurately documents configuration changes to the directory, thereby, determining deviations from established security baselines and pinpointing vulnerabilities created. Real-time alerts on unauthorized changes help security personnel quickly respond to vulnerabilities, mitigating the risk of a possible exposure. If an incident does occur, comprehensive reports document the activity leading up to the event, thus reducing the time required to investigate the scope and magnitude of the exposure.

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

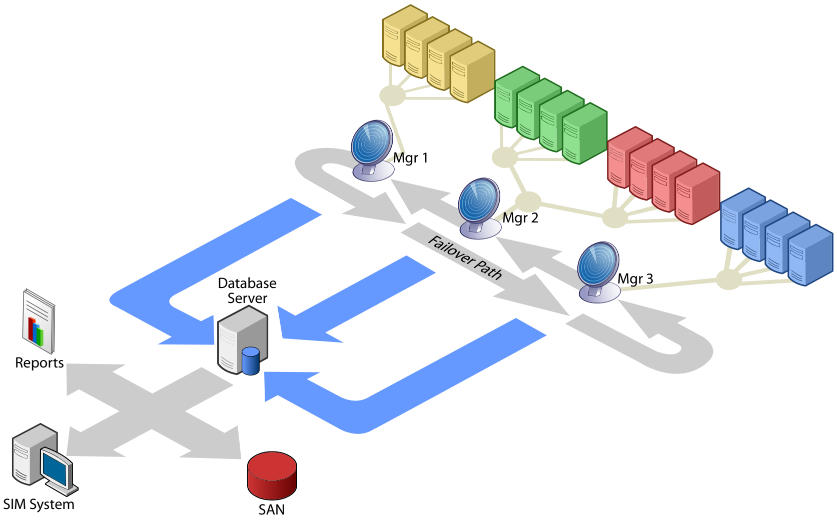
Engineered for Flexible, Reliable Auditing

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 Active Directory 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.



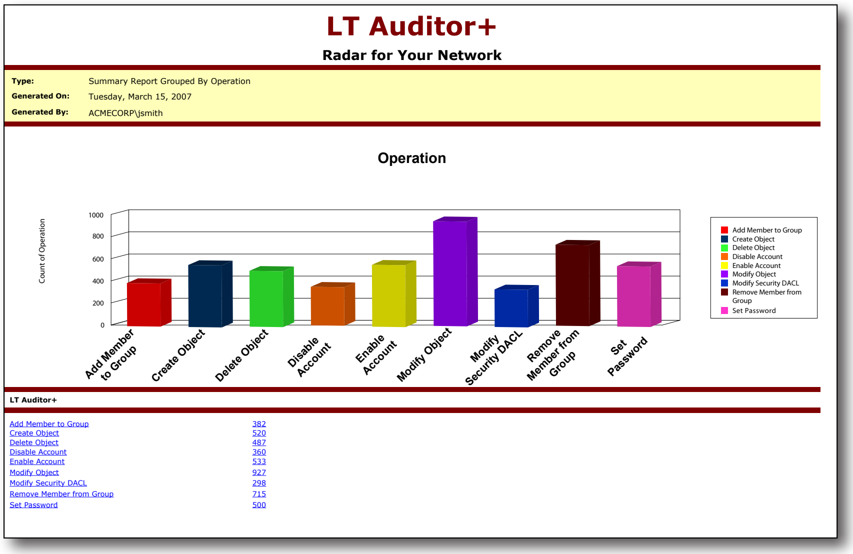
Comprehensive Reporting and Alerting

LT Auditor+ 9 for Active Directory 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 Active Directory has never been faster and easier. Through centralized reporting, users can consolidate data or create forensic analysis reports organization-wide. LT Auditor+ 9 for Active Directory 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 Active Directory 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.



LT Auditor+

Radar for Your Network

Type: Summary Report Grouped By Operation
Generated On: Tuesday, March 15, 2007
Generated By: ACMECORP\jsmith

LT Auditor+

Add Member to Group	382
Create Object	520
Delete Object	487
Disable Account	360
Enable Account	533
Modify Object	927
Modify Security DACL	298
Remove Member from Group	715
Set Password	500

Audited Operations

Active Directory Object Auditing Activity

- Create Object
- Delete Object
- Modified Object
- Modify Security DACL

Account Modification Auditing Activity

- Enable Account
- Disable Account
- Set Password
- Change Password

Group Membership Auditing Activity

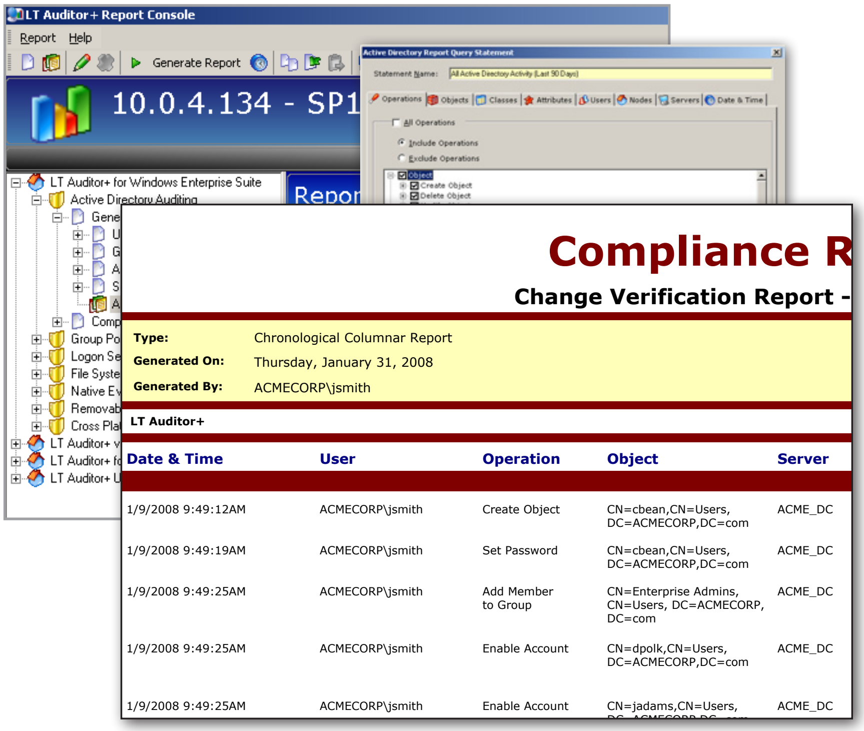
- Add Member to Group
- Remove Member from Group

Active Directory Administration Activity

- Trusted Domain Added
- Audit Policy Change

Compliance Reports

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



Statement Name: All Active Directory Activity (Last 90 Days)

☐ All Operations

● Include Operations

○ Exclude Operations

☑ Object
☑ Create Object
☑ Delete Object

Compliance R

Change Verification Report -

Type:	Chronological Columnar Report
Generated On:	Thursday, January 31, 2008
Generated By:	ACMECORP\jsmith

LT Auditor+

Date & Time	User	Operation	Object	Server
1/9/2008 9:49:12AM	ACMECORP\jsmith	Create Object	CN=cbean,CN=Users, DC=ACMECORP,DC=com	ACME_DC
1/9/2008 9:49:19AM	ACMECORP\jsmith	Set Password	CN=cbean,CN=Users, DC=ACMECORP,DC=com	ACME_DC
1/9/2008 9:49:25AM	ACMECORP\jsmith	Add Member to Group	CN=Enterprise Admins, CN=Users, DC=ACMECORP, DC=com	ACME_DC
1/9/2008 9:49:25AM	ACMECORP\jsmith	Enable Account	CN=dpolk,CN=Users, DC=ACMECORP,DC=com	ACME_DC
1/9/2008 9:49:25AM	ACMECORP\jsmith	Enable Account	CN=jadams,CN=Users,	ACME_DC

Get Started Now

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

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

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