BLUE LANCE
COMPUTER SECURITY SOFTWARE

LT Auditor+ 9 for SUSE® Linux eDirectory

360° View of SUSE Linux eDirectory™ Changes

Clear, Concise, Actionable Intelligence

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

LT Auditor+ 9 for SUSE Linux eDirectory™ is designed to provide detailed auditing and monitoring of SUSE Linux eDirectory™ activity—delivering clear, concise, actionable intelligence.

LT Auditor+ 9 for SUSE Linux eDirectory™ interacts seamlessly and unobtrusively with the operating system to capture:

- eDirectory™ Object Creations/Deletions
- Account modifications, including enabling and disabling of accounts
- Password changes
- Group membership changes ; and
- Changes to the directory schema

LT Auditor+ 9 for SUSE Linux eDirectory™ 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 SUSE Linux eDirectory™, part of the LT Auditor+ 9 for SUSE Linux 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 Sarbanes-Oxley (SOX); GLBA; FDIC/OCC; FFIEC; PCI DSS; HIPAA; and FISMA; and IT security frameworks such as COBIT 4.1 and NIST SP800-53.

LT Auditor+ 9 for SUSE Linux eDirectory's built-in scalability and fault tolerance prevents audit data loss and ensures the consolidation of data from SUSE Linux servers within the organization. Audit data in a single, secure repository provides accurate compliance reports on-demand.

LT Auditor+ 9 for SUSE Linux eDirectory™ provides executive summary reports, with drill-down capability detailing administrative and user activity about files, folders and users on servers. Reports can be scheduled for automatic distribution to administrative personnel at designated intervals.

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 eDirectory™ object creations, deletions and modifications; access control changes made by privileged users and administrators; group membership changes and eDirectory™ administrative changes including trustee changes. LT Auditor+ 9 for SUSE Linux eDirectory™ 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 eDirectory™ 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 eDirectory™ groups that define user and group access permissions to critical resources. LT Auditor+ 9 for SUSE Linux eDirectory™ comprehensively audits account modifications such as enabling and disabling of accounts, and modification of security settings to other sensitive objects within eDirectory™.

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 user activity into plain English reports and alerts
- Multiple report formats including Excel, Word, HTML and PDF
- Automatic report scheduling and delivery
- Audit eDirectory Object and Account Modifications, Group Membership and administrative activity
- 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

Improve incident response through immediate alerts of monitored high profile eDirectory™ changes such as adding trustees with supervisor rights to organization objects or granting security equivalences to the admin user. LT Auditor+ 9 for SUSE Linux eDirectory™ 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 reports and alerts in plain English, LT Auditor+ eliminates the complex task of sifting through large volumes of fragmented, incomplete data provided by the system logs, dispersed throughout the organization. LT Auditor's scalable, fault tolerant design, coupled with superior audit data filtering and enterprise-wide data consolidation provides a powerful auditing solution with optimal performance.

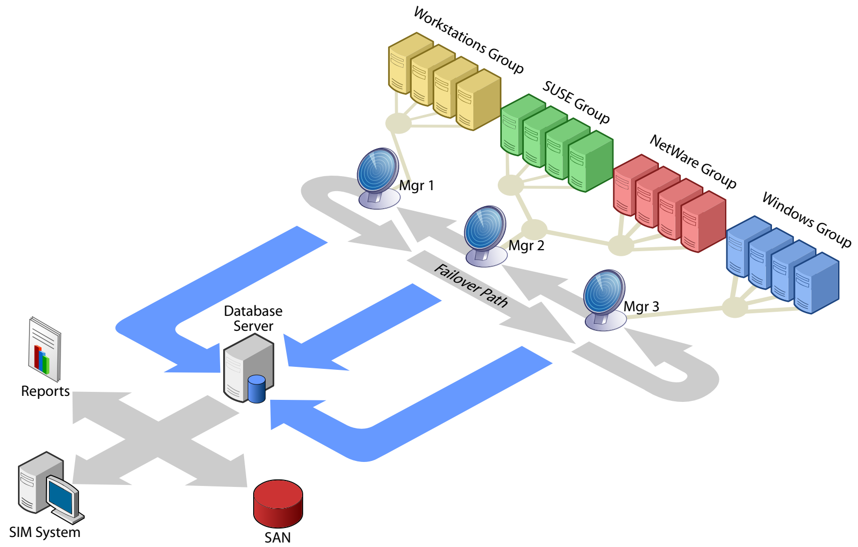
Engineered for Flexible, Reliable Auditing

Secure and Scalable

LT Auditor+ 9 for SUSE Linux eDirectory 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 transfer and consolidation of audit data.

Built-in Fault Tolerance

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



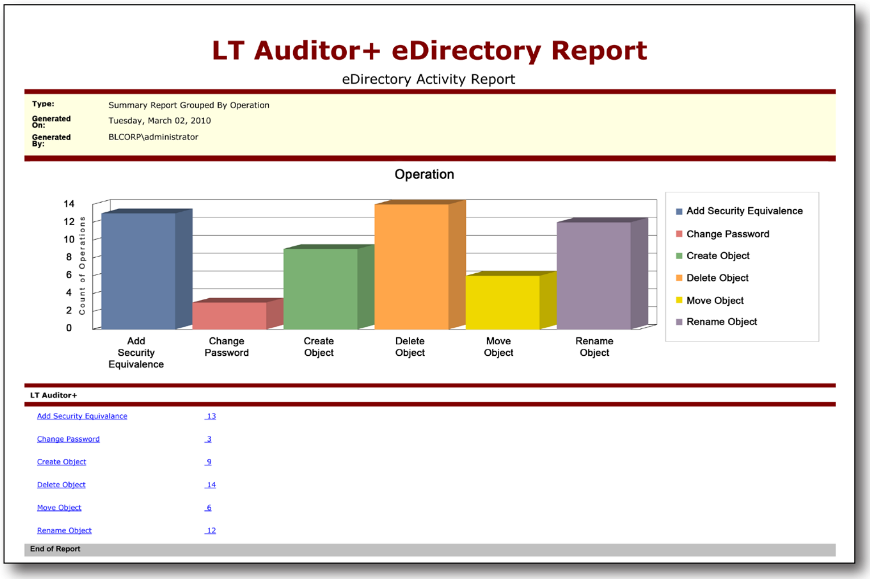
Comprehensive Reporting and Alerting

LT Auditor+ 9 for SUSE Linux eDirectory™ 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 Syslog messages.

Reporting with LT Auditor+ 9 has never been faster or easier. Centralized reporting allows users to consolidate data and create forensic analysis reports organization-wide. LT Auditor+ 9 offers over 100 standard reports that target both security and compliance, all while adding drill-down capability to individual events. Consolidation offers reporting across multiple platforms including Windows, NetWare and SUSE Linux; providing true enterprise wide reporting of user activity. 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 SUSE Linux eDirectory™ includes several high-level graphical reports that summarize data and information with drill-down



LT Auditor+ eDirectory Report

eDirectory Activity Report

Type:	Summary Report Grouped By Operation
Generated On:	Tuesday, March 02, 2010
Generated By:	BLCORP\administrator

LT Auditor+

Add Security Equivalance	13
Change Password	3
Create Object	9
Delete Object	14
Move Object	6
Rename Object	12

End of Report

Audited Operations

eDirectory Object Auditing Activity

- Create Object
- Delete Object
- Rename Object
- Move Object
- Modified Object
- Add NDS Value
- Delete NDS Value
- Add Security Equivalence
- Remove Security Equivalence

Directory Auditing

- Schema Class Added
- Schema Class Removed
- Schema Attribute Added
- Schema Attribute Removed

Account Modification Auditing Activity

- Enable Account
- Disable Account
- Set Password
- Change Password
- Account Locked Out
- Account Unlocked

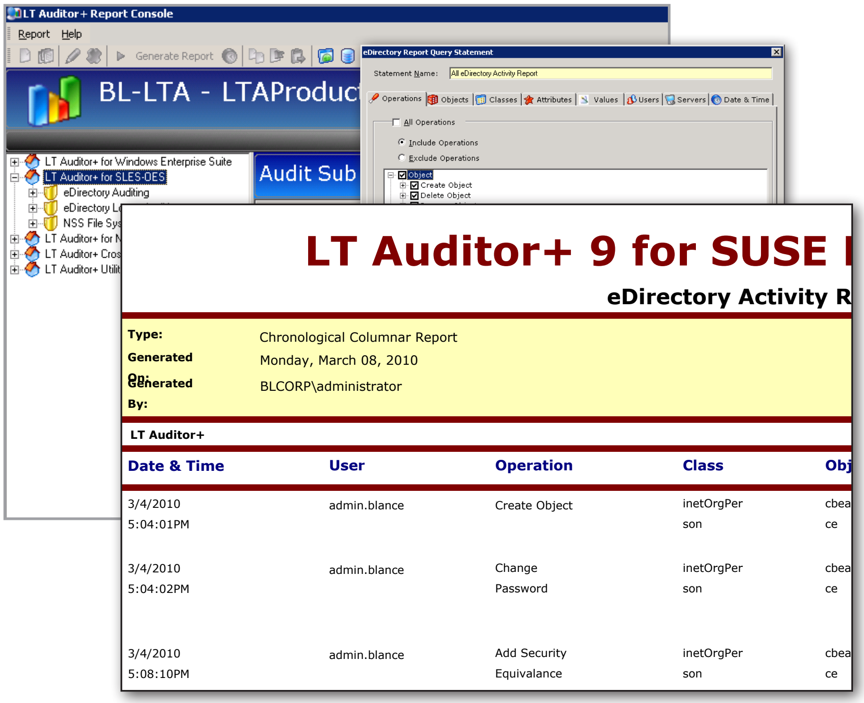
Group Membership Auditing Activity

- Add Member to Group
- Remove Member from Group

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 for SUSE Linux eDirectory™ includes reports that help organizations stay compliant with regulations such as Sarbanes-Oxley (SOX); GLBA; FDIC/OCC; FFIEC; PCI DSS; HIPAA; and FISMA; and IT security frameworks such as COBIT 4.1 and NIST SP800-53.



Statement Name: All eDirectory Activity Report

☐ All Operations

● Include Operations

○ Exclude Operations

☑ Object
- ☑ Create Object
- ☑ Delete Object

LT Auditor+ 9 for SUSE L

eDirectory Activity R

Type:	Chronological Columnar Report
Generated On:	Monday, March 08, 2010
Generated By:	BLCORP\administrator

LT Auditor+

Date & Time	User	Operation	Class	Obj
3/4/2010 5:04:01PM	admin.blance	Create Object	inetOrgPer son	cbea ce
3/4/2010 5:04:02PM	admin.blance	Change Password	inetOrgPer son	cbea ce
3/4/2010 5:08:10PM	admin.blance	Add Security Equivalance	inetOrgPer son	cbea ce

Get Started Now

LT Auditor+ 9 for SUSE Linux eDirectory™ is configurable to fit seamlessly into any organization—from the largest to the smallest. In addition to LT Auditor+ 9 for SUSE Linux eDirectory™, Blue Lance also offers comprehensive, flexible and reliable auditing solutions for NSS file systems and a full complement of products for Windows 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 Server 2003/2008
- Microsoft Windows 2000 SP4+ / MDAC v. 2.7
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Software - .NET v1.1
- Database - Microsoft SQL Server 2005/2008, Oracle 9i/10g/11g

LT Auditor+ Agent

- RAM - 512 MB RAM
- Hard Disk - 10+ GB
- Operating System
- SUSE Linux Enterprise Server 10 with Service Pack 2
- Open Enterprise Server (OES2) with Service Pack 1

Blue Lance, Inc.
410 Pierce Street, Ste. 303
Houston, TX 77002

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

BLUE LANCE
COMPUTER SECURITY SOFTWARE