BLUE LANCE
COMPUTER SECURITY SOFTWARE

DATA PROTECTION
OUT OF BOX
COMPLIANCE REPORTING

LTAuditor+ 9
for Workstations

360° View of User Desktops and Laptops: USB Drive, File and Local Account 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 Workstations is designed to provide detailed auditing and monitoring of Windows workstation activity—delivering clear, concise, actionable intelligence.

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

- Successful/Failed Interactive and Network Logins;
- File and Folder Operations on Removable Storage Activities including USB and flash drives connected to Windows workstations
- Successful/Failed File and Folder Operations on local drives; and
- Operations performed on critical local user and group (SAM) accounts.

LT Auditor+ 9 for Workstations 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 Workstations, 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 provides executive summary reports, with drill-down capability detailing critical workstation activity about files, folders and local users. 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 workstations 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:

Ensure privacy, confidentiality and integrity of sensitive information by monitoring authentication and connection attempts to workstations; access control changes to local (SAM) accounts; and access to sensitive files and resources including unauthorized duplication of files to local drives and removable USB storage devices.

Improve incident response through immediate alerts of monitored authorized and unauthorized authentications, after hours logins and failed login attempts. LT Auditor+ 9 for Workstations accurately tracks the execution, modification and deletion 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 and respond to the security incident .

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 local system login activity,

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, local SAM accounts 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

application access, and modifications/deletions of sensitive and confidential files and resources residing on workstations.

Prepare for the IT security audit process with comprehensive reports delivering clear, concise, and complete information on activities performed on all workstations within the organization. LT Auditor+ 9 for Workstations simplifies the IT security audit process is simplified by automating the delivery of plain English reports using a robust scheduler and valuable report templates.

Save Time and Money with clear, concise, easy-to-read LT Auditor+ reports and alerts in plain English by 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 Workstations' scalable, fault tolerant design, coupled with superior audit data filtering and enterprise-wide data consolidation provides a flexible, reliable auditing solution with optimal performance.

Engineered for Flexible, Reliable Auditing

Secure and Scalable

LT Auditor+ 9 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 Workstations 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.
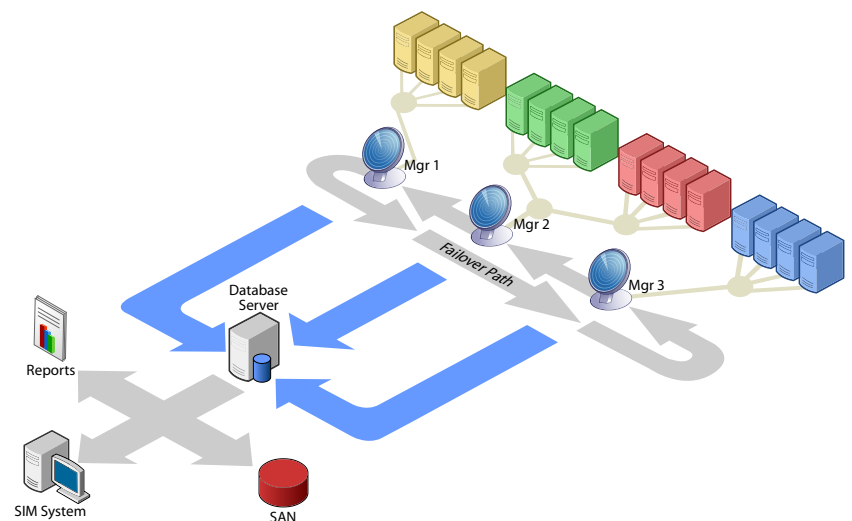
Comprehensive Reporting and Alerting

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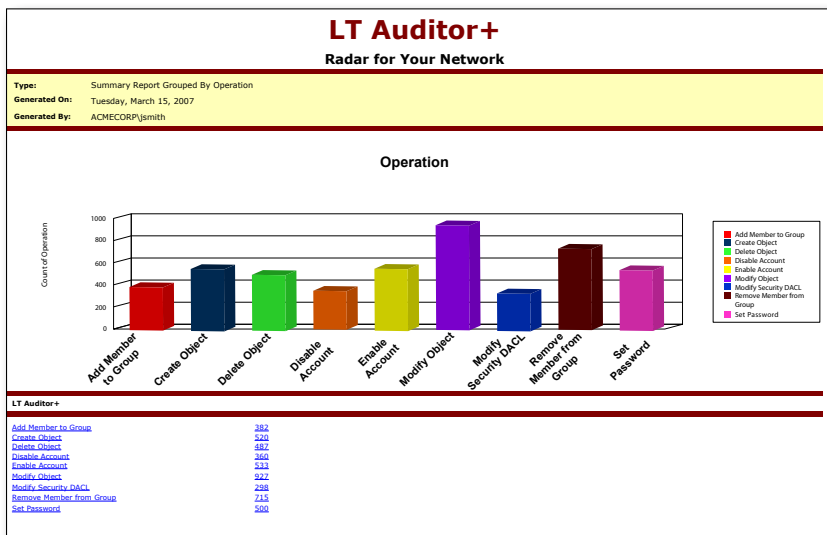
Audited Operations

USB Device Activity
- ❖ Create File
- ❖ Delete File
- ❖ Modified File
- ❖ Rename File
- ❖ Make Directory
- ❖ Remove Directory
- ❖ Rename Directory
- ❖ Open/Access File

Authentication Auditing Activity
- ❖ Interactive Logon/Logout
- ❖ Network Logon/Logout
- ❖ Batch Logon/Logout
- ❖ Service Logon/Logout
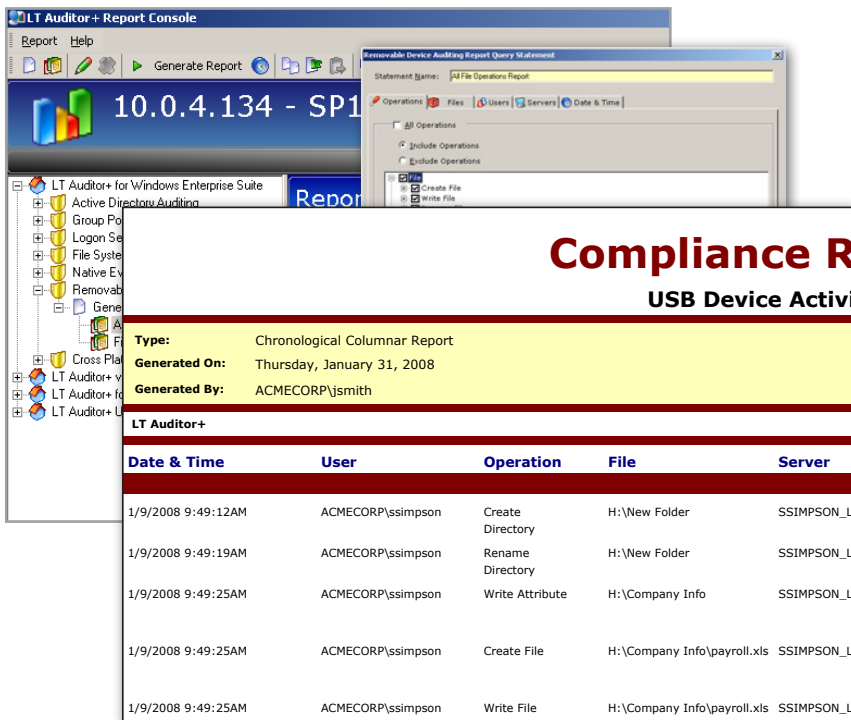- ❖ Unlock Logon

System Activity
- ❖ Event Log Clear
- ❖ Application Load
- ❖ Application Unload

Local (SAM) Account Activity
- ❖ Create User/Group
- ❖ Delete User/Group
- ❖ Add Member
- ❖ Remove Member

Compliance Reports

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

Get Started Now

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

BLUE LANCE
COMPUTER SECURITY SOFTWARE