

LT AUDITOR+ 2013

## GROUP POLICY

Real Time Auditing for Group Policy

BLUE LANCE

## THE CHALLENGE

When it comes to Group Policy configurations, a small change to a security policy, desktop configuration, software deployment or other setting can severely impact performance and productivity, threaten an enterprise's security, and cause non-compliance with critical government regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA). Furthermore, failure to properly monitor and control Group Policy changes can produce devastating internal results including service disruptions, replication challenges, over privileged administrators and even malicious GPO modifications.

## THE SOLUTION

LT Auditor+ 2013 for Group Policy is designed to provide detailed auditing and monitoring of Windows Group Policy activity — delivering clear, concise, actionable intelligence. LT Auditor+ 2013 for Group Policy goes beyond native Windows event logs and interacts seamlessly and unobtrusively with the Windows operating system to capture such events as machine policy changes including changes to security settings, user rights assignments, password policy, restricted groups, registry, and User policy changes including changes to administrative templates. LT Auditor+ 2013 for Group Policy delivers the user defined captured events in a bullet-proof audit trail, through easy-to-read forensic reports to precisely identify and show Who did What, from Where and When.

## Transform your cryptic &amp; chaotic logs to clear, actionable reports

BLUE LANCE			
Group Policy Activity Report			
LT Auditor+ Oversight Report			
Generated On: Monday, September 24, 2012			
Generated By: LTAMGRAdministrator			
Date & Time	User	Node	Remarks
9/24/2012 12:38:28PM	BLUECORP.COM\administrator	BLCORPDC	On [Sep 24 2012 12:38PM], user [administrator] changed password policy, set [Minimum Password Length] from [5 characters] to [8 characters] for the group policy object [Default Domain Controllers Policy] from node [BLCORPDC] on server [blcorpdc.bluecorp.com]
9/24/2012 12:38:28PM	BLUECORP.COM\administrator	BLCORPDC	On [Sep 24 2012 12:38PM], user [administrator] changed password policy, set [Maximum Password Age] from [Not Defined] to [30 days] for the group policy object

## 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 Group Policy machine and user policy changes including before and after values

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

Built-in agent status and health monitoring



LT AUDITOR+ 2013

# GROUP POLICY

Real Time Auditing for Group Policy

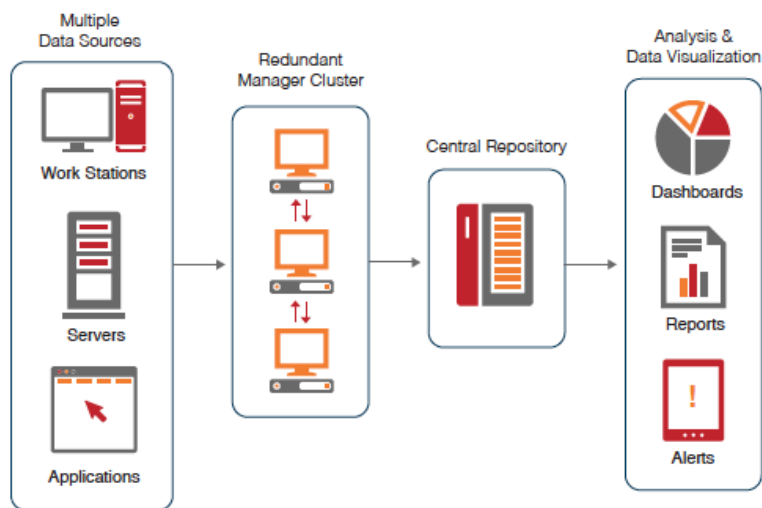
**BLUE LANCE**

## BENEFITS

LT Auditor+ 2013 for Group Policy is configurable to fit seamlessly into any organization, large or small. LT Auditor+ 2013 allows your organization to immediately reap the benefits of continuous security and compliance monitoring by enabling your organization to improve incident response time, provide comprehensive audit reports, meet compliance control transformation requirements, ensure privacy, confidentiality and integrity, all while saving time and money.

Reporting with LT Auditor+ 2013 for Group Policy has never been faster and easier. Through centralized reporting, users can consolidate data or create forensic analysis reports organization-wide. LT Auditor+ 2013 for Group Policy 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.

## Information Flow



## ABOUT BLUE LANCE

Blue Lance is a global provider of cybersecurity governance solutions helping organizations protect their digitally managed assets for over 25 years. Blue Lance solutions allow organizations to minimize risk from sophisticated Cyber thieves, complex industry and government regulations. Blue Lance stands with customers as a trusted partner offering cybersecurity governance solutions that enable expanded oversight and validation of audit readiness for internal policies, industry or government regulations; and the safe keeping of confidential information, trade secrets, intellectual property, critical infrastructure, and other digitally managed assets. Blue Lance is headquartered in Houston, Texas.

## AUDITED OPERATIONS

### MACHINE POLICY AUDITING ACTIVITY

- Change Password Policy
- Change Account Lockout Policy
- Change Audit Policy
- Change Security Settings
- Change Event Log Settings
- Define user rights
- Undefine user rights
- Add/Remove user rights member
- Change security option
- Change event log settings
- Create/Delete restricted group
- Add/Remove member to restricted group
- Make/Remove restricted group member of
- Add/Remove/Change file system security policy
- Change file system security descriptor
- Change Administrative template
- Add/Remove/Change Extra registry settings
- Change system service policy
- Change system service security descriptor
- Add/Remove/Change registry security policy
- Change registry security descriptor
- Change Administrative Templates
- Add/Remove/Change Extra registry settings

### USER POLICY AUDITING ACTIVITY

- Change Administrative Templates
- Add/Remove/Change Extra registry settings

