DATA SHEET

LT AUDITOR+ 2013

WINDOWS ASSESSMENT

Real Time Auditing for Windows Assessment

BLUE LANCE

THE CHALLENGE

Users with excessive permissions can significantly increase risks of data loss maliciously, accidentally or unknowingly (trojanized). IT Security administrators today have the challenging tasks of:

- Finding out who has access to critical data in the organization;
- Identifying excessive permissions to comply with principles of least privleged and "need to know"
- Identifying data owners so that data can be classified appropriately to ensure that accurate permissions are granted for access.
- Provide meaningful and concise reports to meet audit, compliance and regulatory requirements

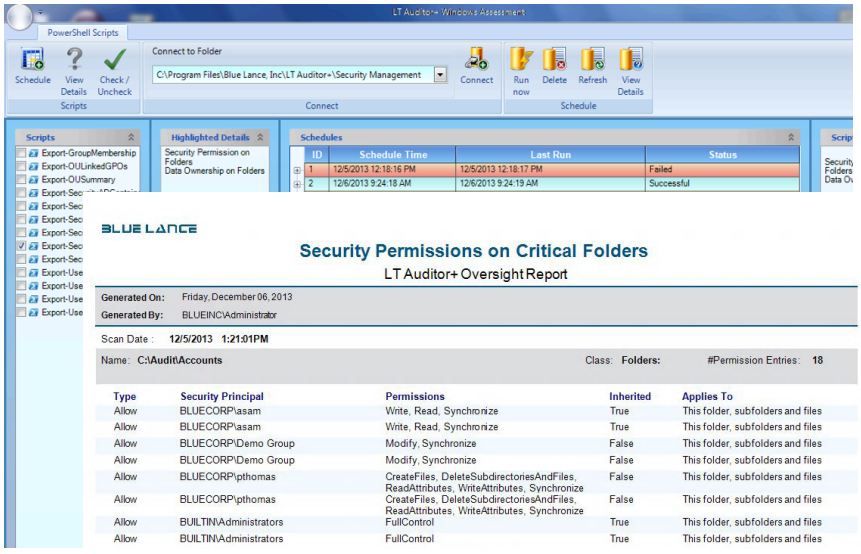
THE SOLUTION

LT Auditor+ Windows Assessment scans Active Directory Users, Groups, Organizational Units and other objects to identify security vulnerabilities. Excessive or unauthorized permissions can be detected by scanning specified files and f olders. Some of the vulnerabilities that can be reported are:

- User accounts that do not require a password
- User accounts that have no login activity for a specified period
- User accounts with membership to privileged groups like Domain Admins and Enterprise Admins
- Users with unnecessary permissions on sensitive files and folders

Plus many more….

LT Auditor+ Windows Assessment Report



REPORTS

PASSWORD SETTINGS REPORTS

User passwords expiring in 30 days
Users who cannot change their password
Users with expired passwords
Users with passwords that never expire
Users who do not require passwords

ACCOUNT EXPIRATION REPORTS

User accounts expiring in 90 days
Expired user accounts
Accounts that never expire
Locked out accounts

LAST LOGON REPORTS

Users not logged in the past 90 days
Users never logged in

GROUP MEMBERSHIP REPORTS

Membership to Domain/Enterprise Admins Groups
All Groups and Group Members
Groups with no members
Nested Groups

SECURITY PERMISSIONS REPORTS

Security Permissions on OUs
Security Permissions on Groups
Security Permission on Users
Security Permission on Folders
Security Permission on Files
Security Permissions on Containers

THINK: Ahead.

DATA SHEET

LT AUDITOR+ 2013

WINDOWS ASSESSMENT

Real Time Auditing for Windows Assessment

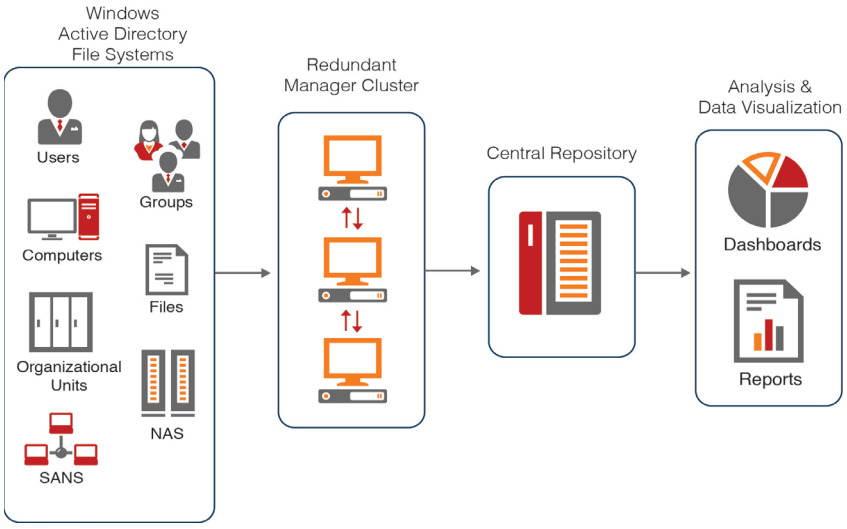
BLUE LANCE

BENEFITS & FEATURES

LT Auditor+ Windows Assessment integrates seamlessly into the LT Auditor+ framework which allows leverage of core capabilities such as:

- Audit Trails – Bridging the collection of assessment data on permissions and configurations on entities within Active Directory with who and how these changes were made provides enhanced security visibility for auditors and IT security administrators.
- Extensibility – Designed to address any IT audit and assurance requirements by allowing customizations to fit any business.
- Automation - Scans and reports can be scheduled to directly deliver reports to the people that need them.
- Noise Reduction - Powerful querying can deliver easy to read reports that are clear and concise.

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.

REPORTS

ORGANIZATIONAL UNIT (OU) REPORTS

OU Summary
OUs with linked GPOs
Empty OUs
OUs not protected from deletion

USER SETTING REPORTS

Disabled Users
Groups belonged to
User Settings
Users with no email addresses
Users with no managers
Users with managers

THINK: Ahead.