

LT AUDITOR+ 2013

NETWORK DEVICES

Real Time Auditing for Network Devices

BLUE LANCE

THE CHALLENGE

IT organizations are growing, and if they are following today's business trend, so are their share of Network Devices such as Cisco routers, firewalls, and scan guns. New projects in development include network devices in an increasing share, and these organizations are challenged with incorporating these devices seamlessly into their operations and business processes. These Network devices must also now be included as part of the organization's IT audit and will encounter difficulties meeting the more stringent audit requirements. Although demand for these systems continues to grow, the development in the native security for these network devices has not been able to keep up with new threats and from emerging regulator standards such as HIPAA and Sarbanes-Oxley.

THE SOLUTION

Blue Lance's LT Auditor+ 2013 for Network Devices alerts on user defined activity and tracks, audits, and reports on all essential activity for all network devices within an organization including routers, firewalls and scan guns, that impacts your organization. LT Auditor+ 2013 provides the intelligence required to audit network device activity in accordance with organizational policies to demonstrate compliance with regulations and guidelines such as Sarbanes-Oxley (SOX); HIPAA, PCI DSS and many more.

Transform your cryptic & chaotic logs to clear, actionable reports

```

2012-10-16 2:20:09PM 59.160.69.126 70.42.2.144:500:WAN udp/500 FW_Connection Closed
2012-10-16 2:20:09PM 59.160.69.126 70.42.2.144:500:WAN udp/500 FW_Connection Opened
2012-10-16 2:20:21PM 59.160.69.126 141.212.121.10:52289:WAN tcp/https FW_Connection Closed
2012-10-16 2:20:23PM 59.160.69.126 10.6.2.229:65535:LAN udp/netbios-ns FW_Broadcast packet dropped
  
```

```

NetworkDevices.txt - Notepad
Edit Format View Help
#Firewall sn=000681354D20 time="2012-10-16 14:
t=10.6.3.255:45740 proto=udp/netbios-dgm
#Firewall sn=000681354D20 time="2012-10-16 14:
t=59.160.69.126:3:WAN type=3 code=1
#Firewall sn=000681354D20 time="2012-10-16 14:
t=192.168.184.1:137:WAN proto=udp/netbios-ns
#Firewall sn=000681354D20 time="2012-10-16 14:
t=59.160.69.126:500:WAN proto=udp/500 sent=112
#Firewall sn=000681354D20 time="2012-10-16 14:
t=10.6.0.2:1040:LAN proto=udp/1040
#Firewall sn=000681354D20 time="2012-10-16 14:
t=74.125.223.21:90:WAN dstname=mail.google.com
#Firewall sn=000681354D20 time="2012-10-16 14:
537 src=10.6.0.2:1512:LAN dst=202.86.6.175:80
  
```

BLUE LANCE					
Network Devices Activity Report					
LT Auditor+ Oversight Report					
Generated On:	Tuesday, October 16, 2012				
Generated By:	LTAMGR\Administrator				
Date & Time	Firewall	Action	Protocol	Source IP Address	Destination IP Address
10/16/2012 2:20:09PM	59.160.69.126	FW_Connection Closed	udp/500	70.42.2.144:500:WAN	59.160.69.126:500:WAN
10/16/2012 2:20:09PM	59.160.69.126	FW_Connection Opened	udp/500	70.42.2.144:500:WAN	59.160.69.126:500:WAN
10/16/2012 2:20:21PM	59.160.69.126	FW_Connection Closed	tcp/https	141.212.121.10:52289:WAN	59.160.69.126:443:WAN
10/16/2012 2:20:23PM	59.160.69.126	FW_Broadcast packet dropped	udp/netbios-ns	10.6.2.229:65535:LAN	10.6.3.255:45740
End of Report					

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
- Automatic report scheduling and delivery
- Audit access to files, folders
- 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



LT AUDITOR+ 2013

NETWORK DEVICES

Real Time Auditing for Network Devices

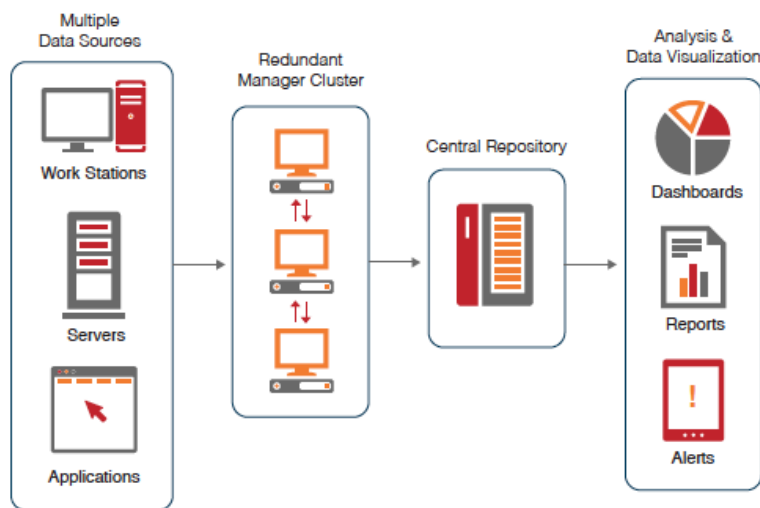
BLUE LANCE

BENEFITS

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

FIREWALL / ROUTER

- Connection Opened
- Connection Closed
- Broadcast Packet Dropped
- DNS Packet Allowed
- ICMP Packet Dropped
- Website Access Denied
- TCP Connection Dropped
- Website Accessed

