Lepide

Website: www.lepide.com

Price: Full Auditor Suite, 1000 AD users - £15.12 per user

|	
Performance	★★★★★
Features	★★★★★
Value for Money	★★★★★
Ease of Use	★★★★☆
Support	★★★★☆
Overall	★★★★★

Verdict: The price of compliance doesn't get much lower than this. Lepide's affordable Auditor Suite is a powerful auditing solution that delivers a wealth of information about business-critical systems and apps.

Faced with ever stricter data protection regulations, businesses of all sizes must implement IT change management and security auditing to demonstrate compliance and avoid hefty fines. There's no shortage of solutions on the market today and Lepide's Auditor Suite stands out for a number of sound reasons.

Auditor Suite has every angle covered as along with essential support for Active Directory (AD) and Group Policy, it can audit Exchange, SQL Server plus SharePoint and report on Windows File Servers and NetApp filers. The latter provides detailed analysis of file and folder activity and this latest version adds threshold alerting for real time notifications of critical file server changes.

There's much more as Lepide provides valuable snapshot, rollback and restore services for AD and Group Policy. All restoration processes are wizard driven and it includes options to restore tombstoned objects as well.

Lepide
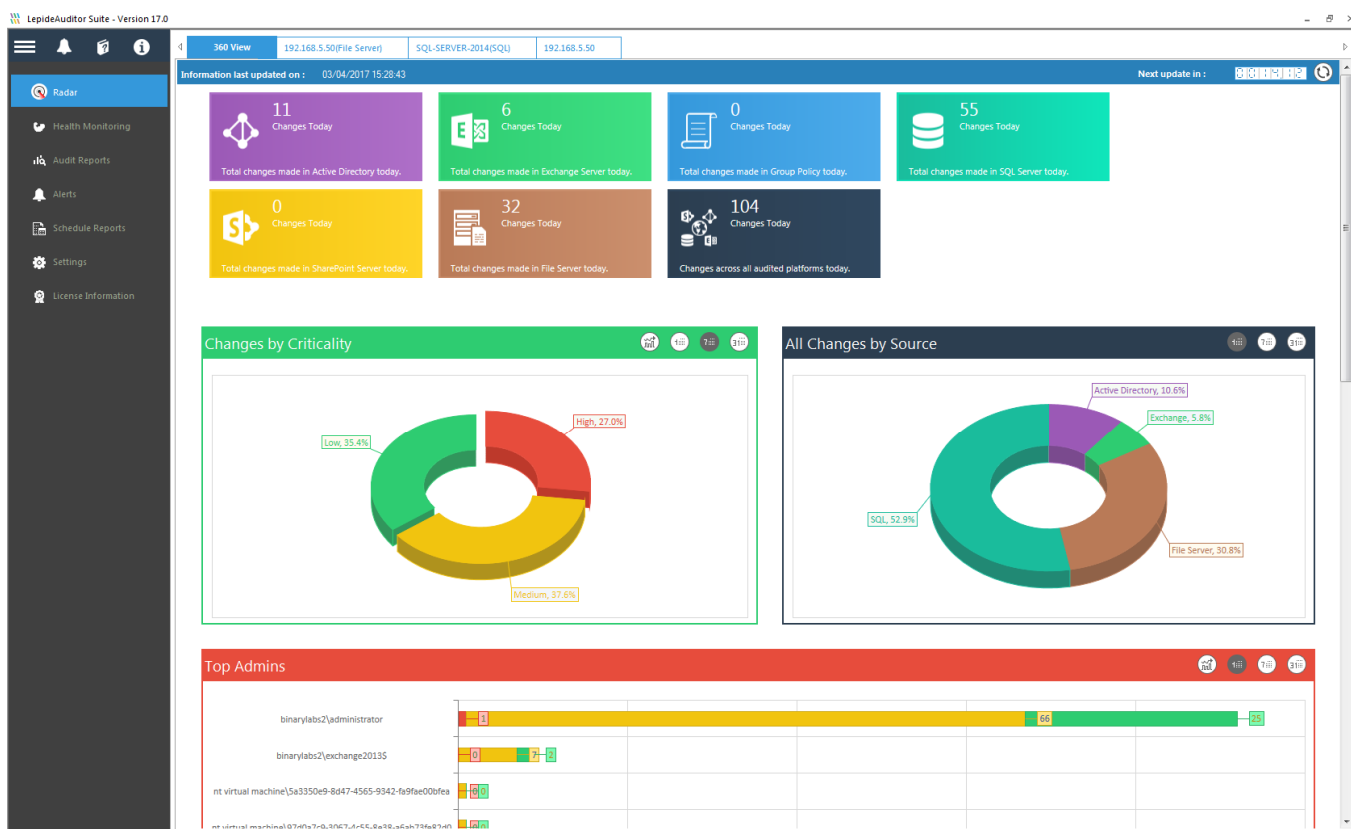
The Radar's 360 dashboard delivers an impressive all-round view of detected changes

Deployment and documentation

For testing, we used a Windows Server 2012 R2 AD domain controller along with Hyper-V VMs providing Exchange 2013 and SQL Server 2014 services. Before installing Auditor Suite, some preparatory work is required which is clearly explained in the thorough documentation.

Host system requirements are undemanding and it took ten minutes to install Auditor Suite on a modestly specified Windows 7 desktop and point it at a local SQL Express database for storing audit data. We had no problems adding our AD, Exchange, SQL and File servers and the install routine automatically made all the necessary changes to our domain controller for auditing requirements.

An agent is provided but, in most cases, there's no need to install it on audited systems. It may be needed in large environments where its log compression can reduce bandwidth requirements.
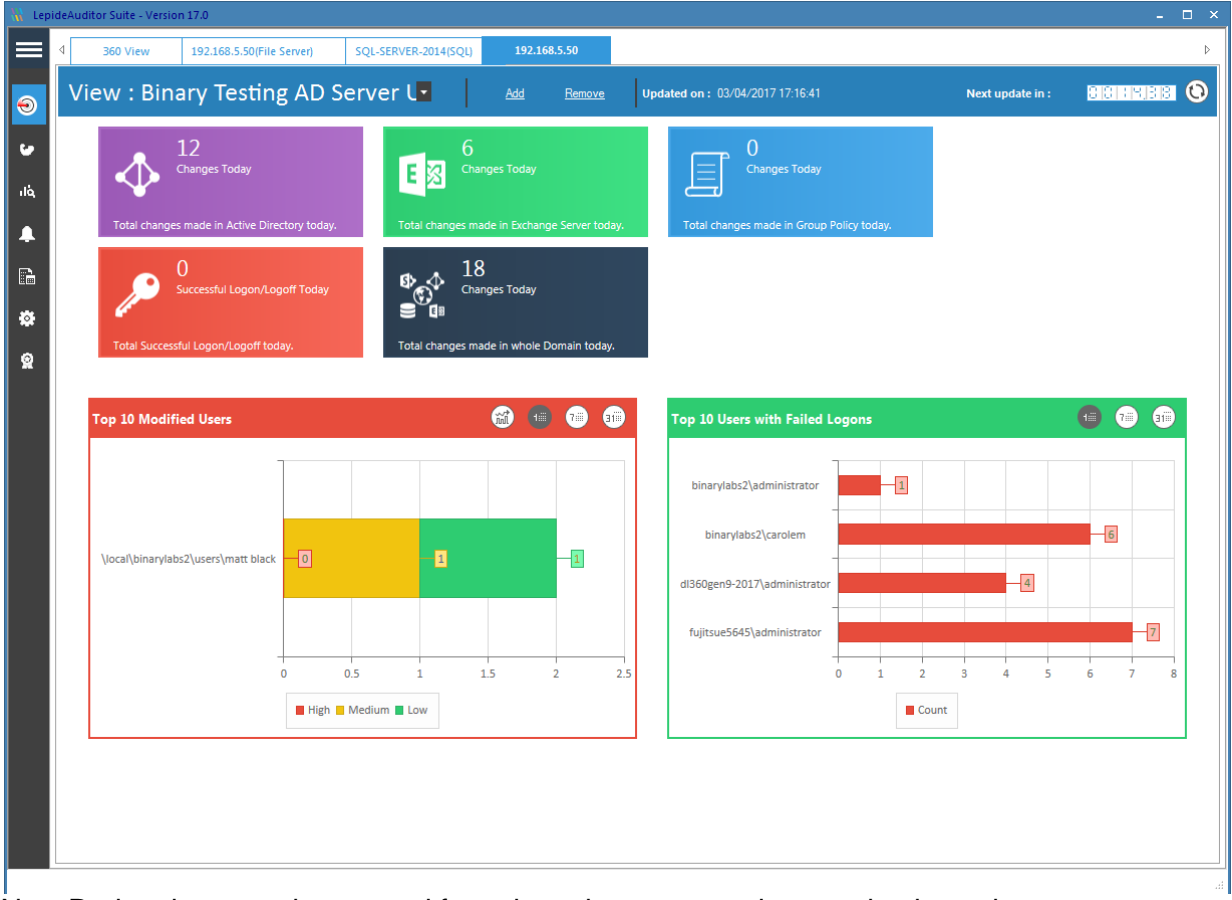
New Radar views can be created for selected systems and customised to suit

The Auditor Suite Console

The main console is simple to work with and capable of presenting a wealth of easily accessible information. Its smart Radar screen and 360 dashboard showed everything occurring for all apps plus a complete overview of our audited AD, Exchange, SQL and File servers.

Chunky colour blocks corresponding to installed suite components provide a highly visible count of daily changes along with sets of graphs showing top administrators, changes graded by criticality and trends. We recommend using a big monitor for the 360 dashboard as although you can change the graph view time periods, you can't resize any of them or move them around.

Extra Radar tabs are provided for monitored systems which allowed us to design our own dashboards. We created new Radar views, decided which systems they applied to and picked from a selection of graphs and trend views.

With health monitoring enabled, we found extra graphs further down the Radar screens showing CPU and memory utilisation. The Health Monitoring pane also revealed speedo-style utilisation dials along with details such as system availability, AD activity, Exchange mail flows and SQL database performance.
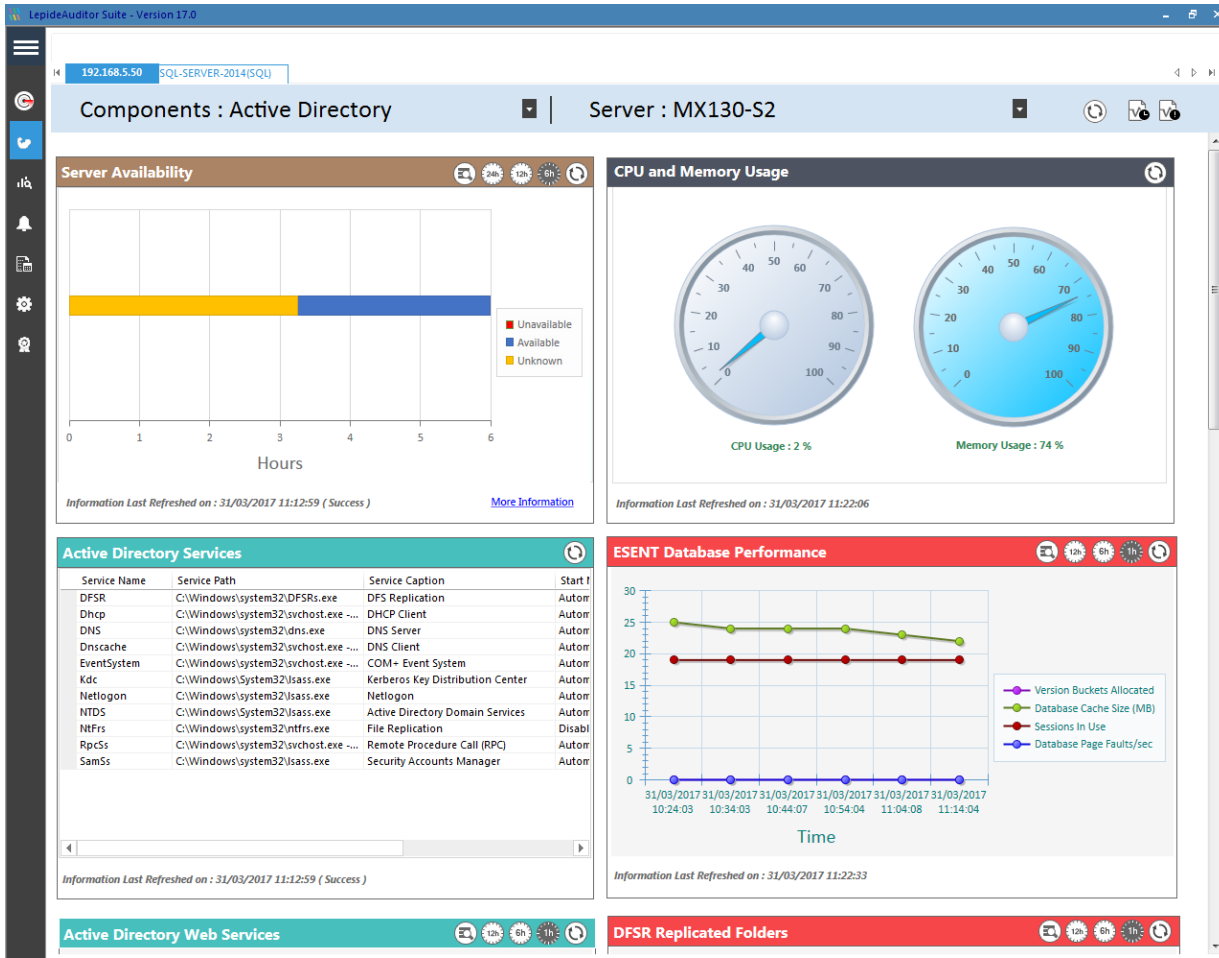
Health monitoring keeps you posted on areas such as system availability plus memory and CPU utilisation

Alerts and LiveFeeds

It؈s important to know immediately about AD or Group Policy modifications and we found the alerting facilities to be very effective. Lepide provides plenty of predefined alerts including all key modifications to AD, Group Policy, Exchange mailbox, SQL Server and File Server plus options for health monitoring thresholds.

We created multiple alerts by selecting the relevant systems, choosing what we wanted to be notified on and deciding on the delivery method. Alerts can be emailed to multiple recipients, shown in the console؈s LiveFeed or sent directly to registered app users.

The Android and iOS apps require a small footprint App Server installed on a Windows system and pointed at the main console host. After creating an account, we used the iOS app to scan the QR code presented by the console straight from our monitor after which our iPad started to receive LiveFeeds immediately.
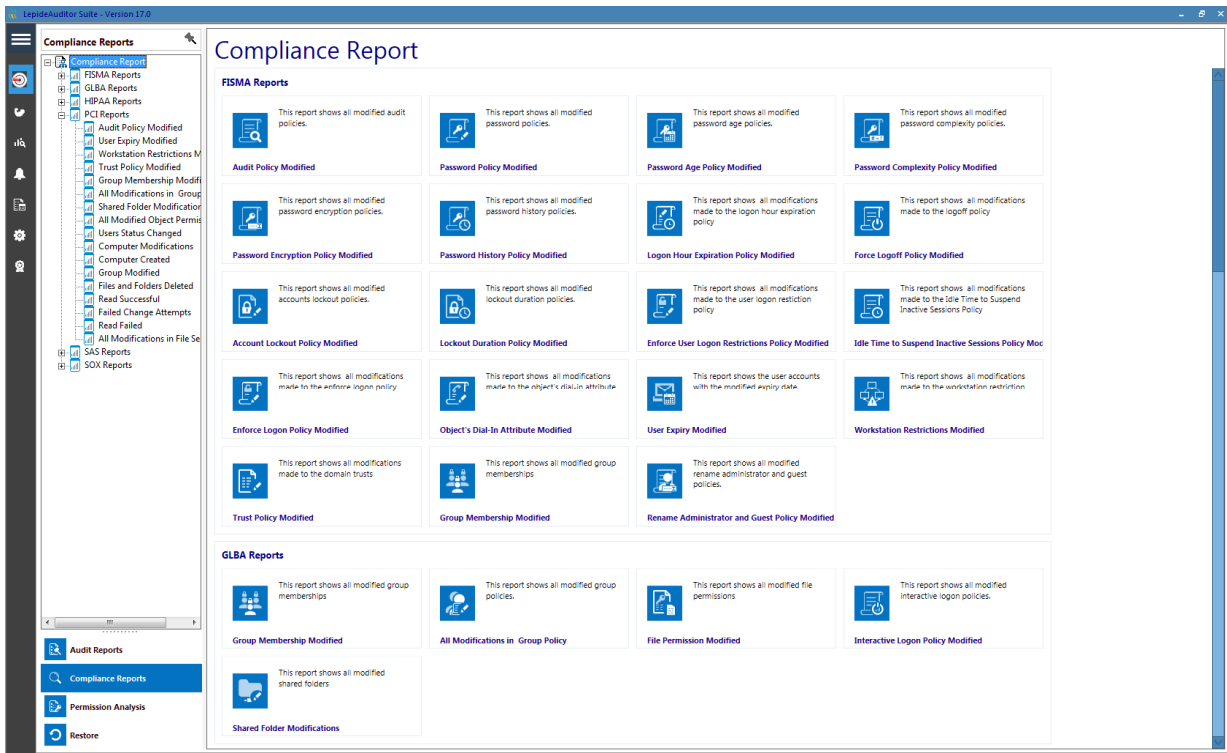
Auditor Suite is endowed with a comprehensive range of predefined compliance reports

Reports and actions

Auditor Suite wonʼt be beaten for its reporting capabilities. It provides hundreds of predefined reports which can be run on-demand or at scheduled intervals and sent as emails or saved to disk in CSV, MHT or PDF formats.

These allowed us to see precisely what had been changed or added, when and where they happened and who made them. We also applied filters to refine the information presented and used comparison reports to see changes over specific periods.

Lepide makes light work of proving compliance as it includes reports for FISMA, PCI, HIPAA, SOX, SAS and GLBA. We could run these on demand, apply filters and view their output in the console or schedule them and email or save them to disk.

Active Directory Cleaner transparently handles inactive accounts by emailing daily reports and run actions at specific intervals to set random passwords, disable accounts, move them to another OU and, if still unused, delete them. Password purgatory is also avoided as countdown reminders can be set to warn admins and users when account passwords are due to expire.

•SQL Modification Feed•

03/04/2017 11:39:22

Database : Unknown
was Altered by BINARYLABS2\Administrator From SQL-SERVER-2014

•SQL Modification Feed•

03/04/2017 11:39:22

Database : BinaryTestingDB6
was Created by BINARYLABS2\Administrator From SQL-SERVER-2014

•File Server Modification Feed (192.168.5.50)•

03/04/2017 11:33:13

Folder Renamed:- From: F:\New folderTo: F:\Test 2 by: BINARYLABS2\Administrator from: MX130-S2

•File Server Modification Feed (192.168.5.50)•

03/04/2017 11:33:11

Folder Created:- F:\New folder by: BINARYLABS2\Administrator from: MX130-S2

•File Server Modification Feed (192.168.5.50)•

03/04/2017 11:33:08

File Read:- F:\$RECYCLE.BIN\S-1-5-21-1188990186-3116171392-3182962886-500\desktop.ini by:
BINARYLABS2\Administrator from: MX130-S2

•File Server Modification Feed (192.168.5.50)•

03/04/2017 10:17:59

File Modified:- F:\Hyper-V\Virtual Hard Disks\Exchange2013_3A2E7A80-B96F-4D2B-AAAC-37E19A489650.avhdx
by: NT VIRTUAL MACHINE\97D0A7C9-3067-4C55-8E38-A6AB73FE82D0 from: MX130-S2

•File Server Modification Feed (192.168.5.50)•

31/03/2017 17:38:50

File Modified:- F:\Hyper-V\Virtual Hard Disks\Exchange2013_3A2E7A80-B96F-4D2B-AAAC-37E19A489650.avhdx
by: NT VIRTUAL MACHINE\97D0A7C9-3067-4C55-8E38-A6AB73FE82D0 from: MX130-S2

•File Server Modification Feed (192.168.5.50)•

03/04/2017 10:17:59

Alert Name: App Test; There are 180 more events. Please see the 192.168.5.50(File Server)\File Server Modification
Reports\All Modifications in File Server\ Report for all events.

We used Lepide's iOS app on our iPad to receive LiveFeed modification alerts

Conclusion

Lepide's Auditor Suite takes the strain out of change auditing and regulatory compliance with one of the most comprehensive solutions on the market. We found the entire suite reasonably easy to deploy and capable of presenting a wealth of audit information about business critical systems.

The well-designed console puts all this information at your fingertips while the alert and reporting facilities will make compliance with data protection regulations a breeze. Lepide's perpetual licensing model also makes it an affordable choice for enterprises and SMEs alike.

Lepide