ManageEngine
LOG360

Comparison Document

ManageEngine Log360
Vs
Splunk Enterprise Security
Comparison Document

THIS DOCUMENT IS CONFIDENTIAL AND IS FOR INTERNAL USE ONLY. THE DOCUMENT SHOULD NOT BE CITED, REPRODUCED, OR DISTRIBUTED WITHOUT EXPLICIT WRITTEN PERMISSION.

DISCLAIMER:

ManageEngine does not guarantee the accuracy of any information presented in this document, and there is no commitment, express or implied, on the part of ManageEngine to update or otherwise amend this document. The furnishing of this document does not provide any license to patents, trademarks, copyrights or other intellectual property rights owned or held by ManageEngine.

ManageEngine Log360 Vs. Splunk Enterprise Security

This document provides a feature wise comparison between ManageEngine Log360 and Splunk Enterprise Security solutions. Comparison done here is based on the information available on competitor's website and so the details may vary with the product.

Products compared

Vendor	Product
ManageEngine	Log360
Splunk	Enterprise

ManageEngine Log360 is an integrated solution that offers network security, log management, and Active Directory auditing, monitoring, & alerting capabilities in a ***single console.***

The solution simplifies the log management viz., ***log collection, analysis, correlation, and archiving process and also offers exhaustive predefined reports and real-time alerting capability*** to mitigate security attacks.

It also helps in protecting confidential data with its ***file integrity monitoring*** feature. Further, the solution also offers capabilities to perform in-depth Active Directory (AD) auditing therefore helps in monitoring the privileged user activities and thereby mitigate internal security threats.

It also offers ***out-of-the-box compliance reports*** which helps in complying with the various IT regulatory mandates' requirements at ease.

Splunk Enterprise provides the features as mentioned above, but is quite complicated to install and deploy as it consists of several components that need to be installed . For instance, compliance and Active Directory auditing are provided by separately installed components, while they are integrated into Log360.

Feature comparison

Feature description	Log360	Splunk Enterprise Security
Log collection		
Agent-less	Available	Available
Agent based	Available	Available
Cross platform log collection	Available	Available
Heterogeneous device support	Available	Available
Import logs	Available	Available
Log filter	Available	Available
Custom log parser	Available	Available
Log collection rate	20,000 Syslog/second with peak event handling capacity of 25,000 Sylogs/second. For Windows Event logs, the EPS is 2000 logs/second.	Not specified
Log formats supported		
Windows event log	Available	Available
Syslog	Available	Available
Amazon Web Services (AWS) EC2 Windows instances	Available	Available
Any format – with custom log parsing technology	Available	Available
Application logs supported	Available	Available
Proprietary applications • Microsoft IIS Web Server • FTP Server (W3C logs) • Apache Web Server • DHCP Windows • DHCP Linux	Available	Available
Database applications:	Available	Available

Oracle and MS SQL Server		
Any in-house or custom application	Available. The solution's in-build custom log parser generates required fields from the custom application log data and allows the users to perform in-depth log analysis.	Available
Other devices supported		
IBM iSeries (AS/400), And VMware	Available	Available
Custom devices • Firewalls • Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) • Anti-virus application • Mail and web application • Vulnerability Scanners • Unified threat management solutions ○ Symantec DLP Application ○ FireEye ○ Symantec Endpoint Solution	Available	Available
Log analysis		
Reports		
Predefined reports to meet security, auditing, and compliance needs	Available	Available
Ability to generate custom reports	Available	Available
Option to schedule reports	Available	Available
Option to distribute reports via email	Available	Available
Option to save reports in PDF, CSV, and HTML formats	Available	Available
Option to drill down and view raw log	Available	Available

data from the report's dashboard		
Trend reports	Available	Available
Reports for Privileged User Monitoring and Auditing (PUMA)	Available	Available
User logon/logoff auditing reports	Available	Available
Canned reports for printer server auditing	Available	Available
Premade reports for removable storage & USB auditing	Available	Available
Active Directory auditing		
Reports for user, computer, group, and OU management	Available	Requires installation of separate app – **Splunk app for Windows infrastructure**
Reports for auditing other AD object viz., • DNS • Permission • Schema • Contacts • Container configuration • Domain changes	Available	Requires installation of separate app – **Splunk app for Windows infrastructure**
Reports on attribute value changes (before and after)	Available	Requires installation of separate app – **Splunk app for Windows infrastructure**
GPO audit reports	Available	Requires installation of separate app – **Splunk app for Windows infrastructure**
Reports for member server auditing		
Summary report for member server changes	Available	Requires installation of separate app – **Splunk app for Windows infrastructure**
Out-of-the-box reports for • Policy changes • System events	Available	Requires installation of separate app – **Splunk app**

- Object management - Scheduled tasks		**for Windows infrastructure**
File integrity monitoring		
Reports on file integrity monitoring	Available	Available
Report Scheduling	Available	Available
Real-time alerts upon critical changes to files/folders being monitored	Available	Available
Audit Trail reports on files/folders changes	Available	Available
Compliance management		
Canned reports	Available	Requires installation of separate app – **Splunk app for Compliance**
Customizable report	Available	Requires installation of separate app – **Splunk app for Compliance**
Reports for new compliance	Available	Requires installation of separate app – **Splunk app for Compliance**
PCI-DSS	Available	Requires installation of separate app – **Splunk app for Compliance**
ISO 27001:2013	Available	Requires installation of separate app – **Splunk app for Compliance**
HIPAA	Available	Requires installation of separate app – **Splunk app for Compliance**
FISMA	Available	Requires installation of separate app – **Splunk app for Compliance**
SOX	Available	Requires installation of separate app – **Splunk app for Compliance**
GLBA	Available	Requires installation of

		separate app – **Splunk app for Compliance**
Log correlation		
Real-time event correlation	Available	Available
Predefined correlation rules	Available	Available
User session monitoring	Available	Available
Real-time alerting		
Predefined alert criteria for various network infrastructure	Available	Available
Capability to build custom alert profile	Available	Available
Notification – Email, SMS, Run program	Available	Available
Compliance alerts	Available	Requires installation of separate app – **Splunk app for Compliance**
Log search		
Advanced Search using Boolean, Wildcards, Grouped Search, Range search, Phrase search	Available	Available
Formatted logs	Available	Available
Raw logs	Available	Available
Save search result as report	Available	Available
Save search query as an alert profile	Available	Available
Log archiving		
Flexible log retention	Available	Available
Secured (Encrypted)	Available	Available
Tamper-proof	Available	Available
Other features		
Service Provider feature		
User based views	Available	Available
User based dashboards	Available	Available

Rebranding	Available	Not specified
User Management		
Realm & user based access	Available	Available
Active Directory based user authentication	Available	Available
RADIUS server based user authentication	Available	Not available
Implementation		
Easy to install	Yes	Quite complex to install
Web based Client	Available	Available
System Requirements		
Bundled database (PostgreSQL/MySQL)	Available	Not specified
Windows & Linux platforms support	Available	Available
64 Bit support	Available	Available
Pricing		
Based on number of servers, devices & applications	Yes	No. Based on volume of log data collected.
Annual Subscription Model	Available	Available
Perpetual Model	Available	Available
Cost	**Economical.** Licensed based on the number of devices being added for monitoring. **Starts at $495.**	Splunk Enterprise annual term licensing (per GB) model for **1 GB/day** slab is **$3,600** (including maintenance)

Product comparison document

Though every care has been taken to ensure the correctness of the information provided herein, minor variations might be found in the feature set. In case, you find any discrepancies, please write to us at: log360-support@manageengine.com