LOG MANAGEMENT ENTERPRISE

SCALABLE COMPLIANCE & SECURITY INFORMATION MANAGEMENT

Trustwave Log Management Enterprise provides scalable compliance and security information management capabilities in an easy to deploy, use, and maintain appliance offering.

ADVANCED LOG MANAGEMENT

System logs are front and center in every organization's plan to comply with regulatory and industry requirements. Log information from assets is used for audit requirements, forensic investigation, support of IT operations functions, as well as holistic security analysis to manage overall business risk.

However, collecting and processing logs and making sense of all the available data can be challenging. As an easy to deploy, operate and manage appliance-based solution, Trustwave's Log Management Enterprise (LME) helps simplify these challenges.

Trustwave LME includes support for hundreds of auditing devices from a myriad of vendors and offers a primarily agent-less approach which simplifies ongoing operational maintenance requirements and reduces total cost of ownership.

Using embedded real-world expertise, LME identifies important audit and security events in real-time. LME automates many steps of audit preparation and response, at the same time providing information to actively defend information assets. LME is a cost-effective way for any organization to implement the security operations functions that reduce compliance or security-related incidents—with or without a dedicated security operations staff.

LME can work independently, hierarchically, or as part of a larger SIEM strategy that includes other solutions in the Trustwave SIEM portfolio and LME also supports high availability.

LOG MANAGEMENT FOR ALL

Choose one of six available LME models and get the needed capacity and functionality in a single appliance. Each appliance is architected for consistent performance and optimal capacity to assist organizations with their log management needs. Software updates and configuration changes are made through an intuitive and easy to use Web-based graphical user interface.

KEY FEATURES AND BENEFITS

Analytics and Intelligence

Analytics

- Powerful visual filtering capabilities help conduct pre-incident analysis through optimized search of the self-contained Security Data Warehouse™ (SDW) log repository.
- LME's Event Explorer can be used for troubleshooting, tracking user activity and forensic investigation, as well as, Visual Analysis.

Anywhere Log Management

- Deployments range from a single appliance to a hierarchical implementation of multiple appliances, aligned with remote geographic sites or to meet separation of data requirements
- Logs accepted directly from almost any source or from other Trustwave Log Management appliances
- Centralized logging plus event management with SDW when more than one appliance is deployed

Threat Intelligence

- Trustwave's optional Threat Correlation Services help you clearly identify emerging threats
- Intelligence feeds are securely synchronized from the cloud, enhancing detection and notification capabilities for threats which might otherwise fly under the radar

Compliance Support

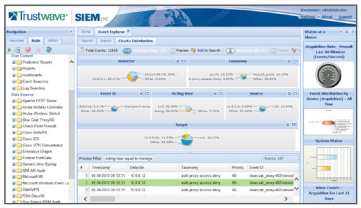
- Indicators of compliance and policy violations, network health issues and security threats are hidden in terabytes of log data. LME empowers your discovery, remediation and compliance.
- Satisfies the log management mandate of industry regulatory standard and internal security policy including:
  - COBIT
  - FISMA (NIST 800-53)
  - GLBA
  - GPG 13
  - HIPAA
  - ISO 27002
  - NERC CIP
  - PCI DSS

APPLIANCE MODELS

	TRUSTWAVE LOG MANAGEMENT APPLIANCE MODELS					
	LME 2-10	**LME 2-20**	**LME 2**	**LME 3**	**LME 4**	**LME 5**
EPS*	115	230	460	925	1,735	3,400
EPD*	10 million	20 million	40 million	80 million	150 million	300 million
RAM	12 GB	12 GB	12 GB	16 GB	24 GB	48 GB
Effective Storage**	9 TB	9 TB	9 TB	18 TB	29 TB	44 TB
Online Retention***	5 years	4 years	3 years	3 years	2 years	1 year
Redundant Power	Yes	Yes	Yes	Yes	Yes	Yes
Interfaces	4 GIG Eth	4 GIG Eth	4 GIG Eth	4 GIG Eth	4 GIG Eth	4 GIG Eth

* Events Per Second and Events Per Day rates are calculated based on full functionality and normalization of average data types and sizes. Rates will vary by location based on the data types and sizes being processed. Rates for acquisition go up to 100,000 EPS or 8.6 billion EPD.
** Effective storage rates are local storage online all the time. Storage is included with the appliances and is configured with redundancy (RAID) to protect data in the case of drive failure.
*** Online retention is based on average data types and sizes. Retention times will vary depending on the data types and sizes processed. Purchasing a larger appliance and processing less data will increase data retention.

CORRELATION AND NOTIFICATIONS

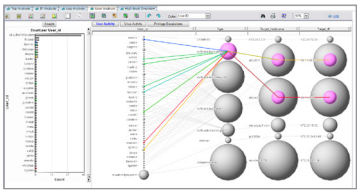


LME includes over 70 correlation templates; templates that can be configured to meet a wide variety of near real-time notifications about important security and compliance exceptions. LME correlations, filters, and reports can also leverage contextual intelligence about your environment, providing targeted results with higher accuracy and fewer false positives.

REPORTING FOR SECURITY AND COMPLIANCE

Audit preparation can be a daunting task. LME is here to help. Over 1,200 configurable reporting templates are included at no additional cost to help you meet your security and compliance reporting, monitoring, and review requirements. Reports can be scheduled, published, and you can dynamically filter and investigate ad-hoc reports within the appliance user interface.

INVESTIGATION AND VISUALIZATION



The advanced filtering and intuitive workflow of LME empower users to quickly find relevant events to answer the questions you need answered. Use the Event Explorer, Event Data Exporter, or Log Explorer functions or choose to visually investigate data through the Chart Distribution features. Whether you need to drill into a chart and automatically update filter criteria, export log data, or save and share filters with other colleagues, LME's workflow enables you to quickly navigate the huge volumes of logs collected from across your heterogeneous environment. The visual analysis component further compliments investigations and troubleshooting by highlighting relationships in large volumes of data that would otherwise be very difficult to find; bringing that proverbial needle in the haystack into direct focus.

For more information on the full SIEM Product Portfolio visit:
www.trustwave.com/downloads/siem-portfolio-overview.pdf

Trustwave®
Smart security on demand

For more information: https://www.trustwave.com