Intellitactics

SAFE LP

Logging Just Got Smarter

There are many choices for collecting, storing and exposing logs. More useful than exposing logs is finding the important information hidden in the logs. Continuous, efficient, high-speed parsing uncovers the hidden information in the logs and presents them as events. Logging plus event management is value-added security information management (SIM). Logging plus event management gives you a head start on eliminating false positives, isolating threats and doing something about them. Events make reporting and notification more effective and your security team more efficient. Make the smart choice for logging plus event management with SAFE LP.

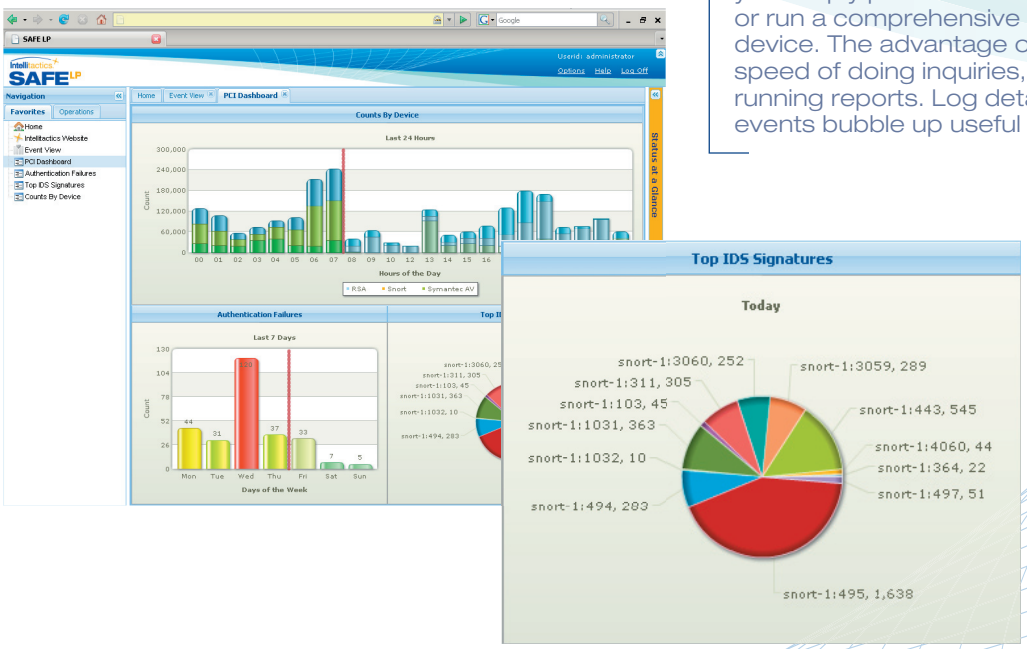
Intellitactics SAFE LP

Intellitactics SAFE LP (SAFE LP) is the logging plus event management appliance in the family of security management appliances called Intellitactics SAFE (SAFE). SAFE appliances work together or stand alone to collect, store, search and report on logs and events. SAFE appliances enable every organization to actively manage more logs from more devices. Each appliance is architected for consistent performance and optimal capacity. Intellitactics simplified and packaged what best-in-class companies have been doing to comply with policies and regulatory standards and to secure the enterprise, and then put all of that know how in the appliances.

Effective Compliance and Security

Indicators of compliance and policy violations, network health issues and security threats are hidden in terabytes of log data. Whether your compliance initiatives are PCI, SOX, HIPAA, GLBA, BASEL II, NERC or FISMA, SAFE LP satisfies the log management mandate of any regulatory standard or internal security policies. Using embedded real-world know-how SAFE LP identifies important audit and security events in real time. SAFE LP automates many steps of audit preparation and response and at the same time provides information to actively defend information assets. SAFE LP 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.

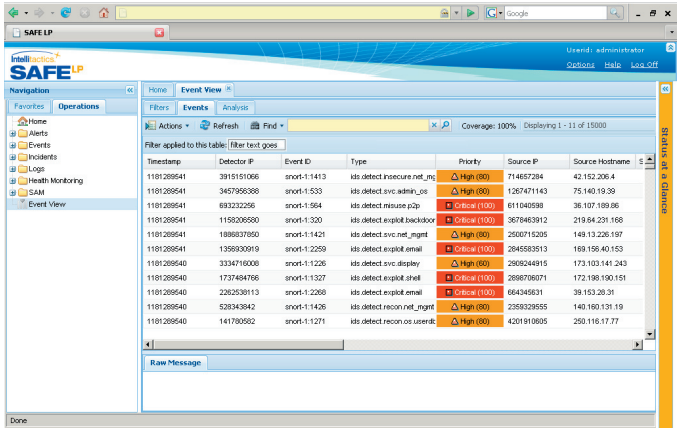
From the Configurable SAFE LP dashboard, you simply point and click to begin an investigation or run a comprehensive report on any monitored device. The advantage of events over logs is the speed of doing inquiries, and investigations and running reports. Log detail remains available while events bubble up useful information faster.



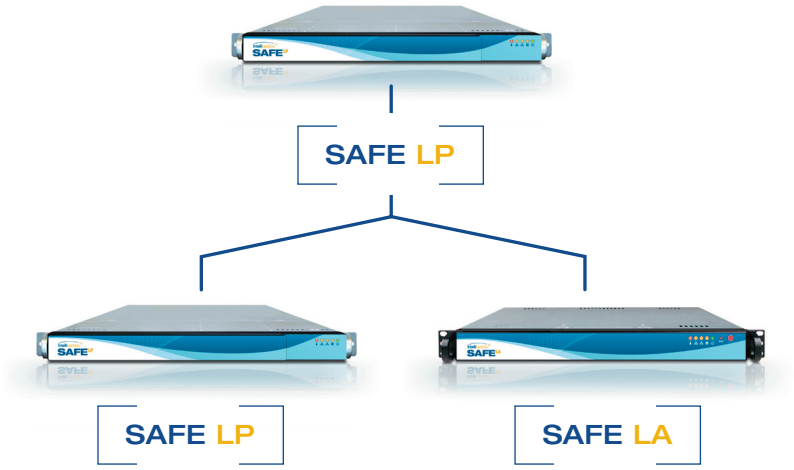
Efficient Log Collection and Processing

SAFE LP collects and processes all log data from all sources at consistently high speeds. Raw and parsed data is available for you to view or for SAFE LP to analyze. Intellitactics' parsing technology makes a big difference in the quality of reports and enables visual analysis of events. Parsed events make correlation and dashboard summarization possible. SAFE LP links from parsed events to associated raw logs at any time.

All logs, raw and parsed, are stored in the Intellitactics Security Data Warehouse™ (SDW). The SDW is a multi-dimension data warehouse that stores millions of logs in compressed flat files and stores parsed, selected logs (events) in a relational database. The SDW plays a key role in most SAFE appliances. Because the appliances can be deployed hierarchically, the SDW enables one appliance to provide centralized data management. Adhering to forensic quality standards, the SDW will file, secure, monitor and retain all log data to satisfy any regulatory standard using highly optimized data compression and indexing techniques.



Use SAFE LP Event Explorer to conduct pre-incident research by searching parsed events stored in compressed form in the Security Data Warehouse™ (SDW). Event Explorer can also be used for troubleshooting, tracking user activity and forensic investigation.



Implementations Range from one SAFE LP to a hierarchical deployment of multiple appliances to align with remote geographic sites or to meet separation of data requirements. In this diagram, one SAFE LP is receiving logs and events from another SAFE LP and SAFE LA. SAFE LA simply collects and forwards logs to another appliance with an SDW like SAFE LP. SAFE LP accepts logs directly from any source or from another SAFE appliance. SAFE LP, with its own SDW, centralizes logging plus event management when more than one appliance is in play. The SDW enables fast, iterative searching and retrieval of data using reports or notifications.

Sensibly Sized: Choose one of the five hardware configurations available for SAFE LP and get all the capacity and functionality you need on one appliance. SAFE LP is built on a hardened Linux OS, optimized and certified for use in appliances, and is completely locked down from user access. Software updates and configuration changes are made through a web-based graphical user interface.

Committed to Your Success

Intellitactics features a low total cost of ownership. Primarily agentless data collection reduces the burden on the infrastructure. The unique Security Data Warehouse, which combines an embedded, self-managing relational database requiring no DBA and compressed stores of raw logs, is easy on the storage budget. The product architecture grows with you as you add more data sources or evolve your risk policies. Intellitactics features 'security know-how' in packaged reports, metrics and correlations. The Customer Center, located at www.intellitactics.com, features instant access to new reports and metrics, and automates support functions for faster response to all inquiries.

Intellitactics
Enterprise Security Management
intellitactics.com
1800 Alexander Bell Drive
Reston, Virginia 20191
703 620 3800 | 877 746 7658