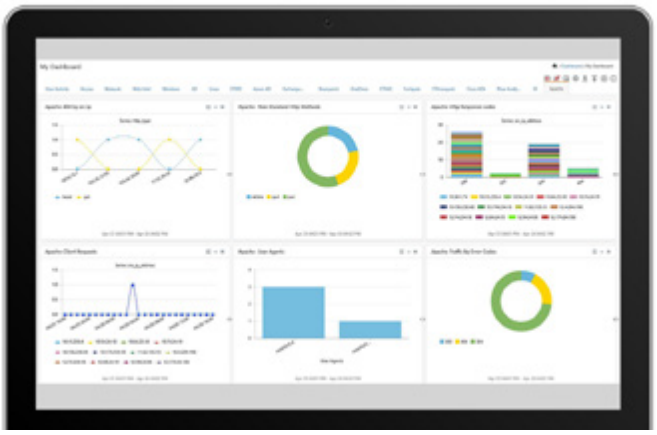
Netsurion
EventTracker
Actionable Security Intelligence

EventTracker Log Manager: Any Log. Any Format.

- Over 1,500 pre-defined security and compliance reports
- Comprehensive support for PCI-DSS, HIPAA, ISO 27001, NIST 800-171, DoD RMF, GDPR, and more
- Support for thousands of devices and applications
- Access to over 20,000 log definitions for Windows, Linux, Firewalls, Applications
- Out-of-the-box alerts, reports, dashlets, and search queries
- Deterministic pricing based on number of log sources (not log volume)



Overview

EventTracker Log Manager is a proven, scalable log management solution that provides network and system administrators with early threat detection, operational awareness, and the ability to demonstrate compliance with industry regulations and internal security policies. The foundation of EventTracker technology, EventTracker Log Manager, allows administrators to monitor the systems and components that they are responsible for and provide them with real-time alerting and in-memory correlation.

Discovering the critical intelligence hidden in your log data helps you identify potential threats and risks to your network.

EventTracker Log Manager constantly collects disparate log data and provides actionable intelligence reports to help you secure your network while meeting compliance requirements. With over 1,500 pre-defined reports and high-speed indexed search for all logs, we help you quickly simplify log management.

Key Benefits

- Reduces cost by automating the collection and compression of event log data across environments
- Addresses regulatory and policy compliance by compressing and storing critical event log data for audits
- Improves internal security proactively, altering in real time
- Sends real-time notifications to enable immediate response to the most critical events
- Provides on-the-spot forensic analysis of security incidents

Features

Real-Time Alerting

- Rule-based alerts with dashboard updates and email notifications
- Incident Response Management: acknowledge, annotate, forward
- Pre-configured alerts for hundreds of security and operational conditions

Fast Log Search

- Logs are indexed to Elastic Search using an extensible Common Indexing Model, flexible UI allows drill down, pivot, and include/exclude, export
- Time slicing, trending and hundreds of pre-built common search queries using Lucene

Dashboards

- Drillable dashboards to visualize important data

Secure Log Storage

- Optimized, high performance Event Vault with no DBMS license required
- Archives are tamper evident with SHA-I checksum
- Over 90% compression for efficient long-term log archiving

Specifications

Hardware recommendations: Quad Core, 8GB RAM, 250 GB SSD, or better.