accelops

# Integrated Data Center and Cloud Monitoring

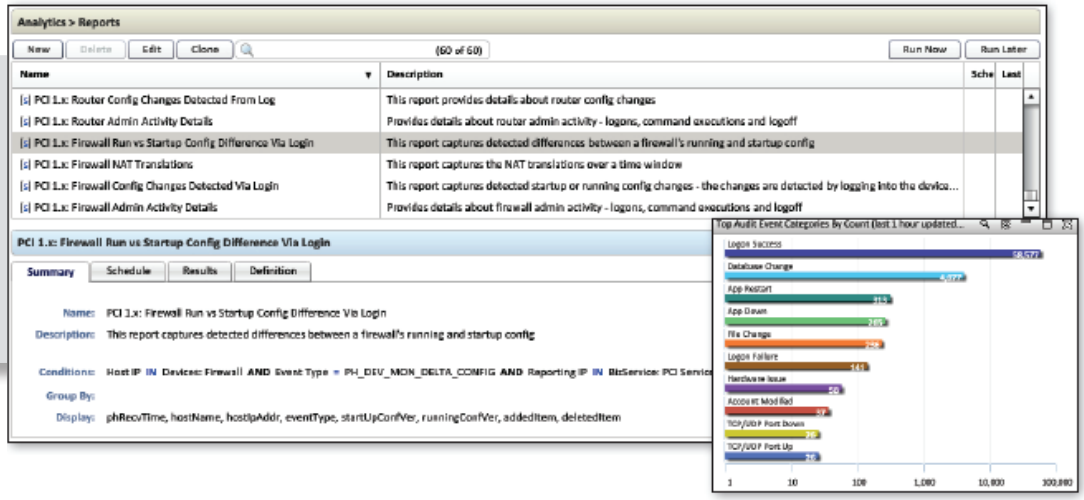
*Intelligent. Proactive. Secure.*

## Automate Compliance Processes

Gain situational awareness, actionable intelligence and compliance oversight. AccelOps' Security Information Event Management platform cuts through operational silos and disparate infrastructure technologies to yield unparalleled visibility, expedited incident response, efficient forensics and audit assurance.

- Complete event log data management, broad and flexible device support, dynamic web GUI and integrated analytics across security, network, application, configuration, virtualization, identity, location and compliance.
- Log consolidation and agent-less, direct device communication to improve detection, investigation and remediation for all types of policy infractions and breaches.
- Robust knowledgebase and powerful cross-correlation engine leverage a clustered, virtual appliance architecture for deployment agility, high performance, online data retention, multi-tenancy and scalability.
- Empowers proactive alerting, expansive threat and violation insight, streamlined investigations, reduced audit expenditure, and automated compliance reporting.

Quickly tag assets and applications as logical compliance-relevant groups to track policy violations, identify access, file integrity and configuration issues, manage cases, and auto - generate pre-defined and custom reports; such as ISO, PCI, SOX, HIPAA, GLBA and Cobit.




## Manage Business Risk and Optimize Audit Capabilities

Standards and compliance are all about implementing procedures and technologies that reduce business risk and efficiently validate that controls are working according to stated policy expectations and mandated requisites. The question then becomes finding the right technologies that best automate control verification and documentation, as well as those that streamline audit and investigation processes. Solutions must:

- Be able to monitor broad compliance-relevant controls
- Quickly pinpoint and detail attacks, insider threats, incidents and violations
- Facilitate conducting timely investigations and forensics
- Record incident handling
- Address multiple specifications, and
- Reduce overall audit expenditure

Delivered as a scalable virtual appliance or SaaS, AccelOps offers a better SIEM and beyond SIEM. AccelOps' SIEM provides real time correlation, long-term analysis and compliance management. The platform is easy to implement with rich multi-vendor device support that can be extended without waiting for an upgrade. Advanced event log management, cross-correlation and interactive dashboards present in-depth security, object, configuration, identity, location and operational details. This solution provides the necessary context to detect and assess blended threats, investigate policy violations, as well as root out non-security events. Enterprise search capabilities allow for an effective means to quickly analyze volumes of online raw logs, parsed events and incident data, as well as to easily generate new and custom reports. Built-in ticketing functionality facilitates case management and investigation documentation.

AccelOps provides organizations a highly automated, integrated and comprehensive security monitoring platform to advance security operations, fortify compliance processes and meet timely audit objectives.


2905 Stender Way, Suite 48
Santa Clara, CA 95054, USA
PHONE +1.408.490.0903
FAX +1.408.970.9666
www.accelops.net

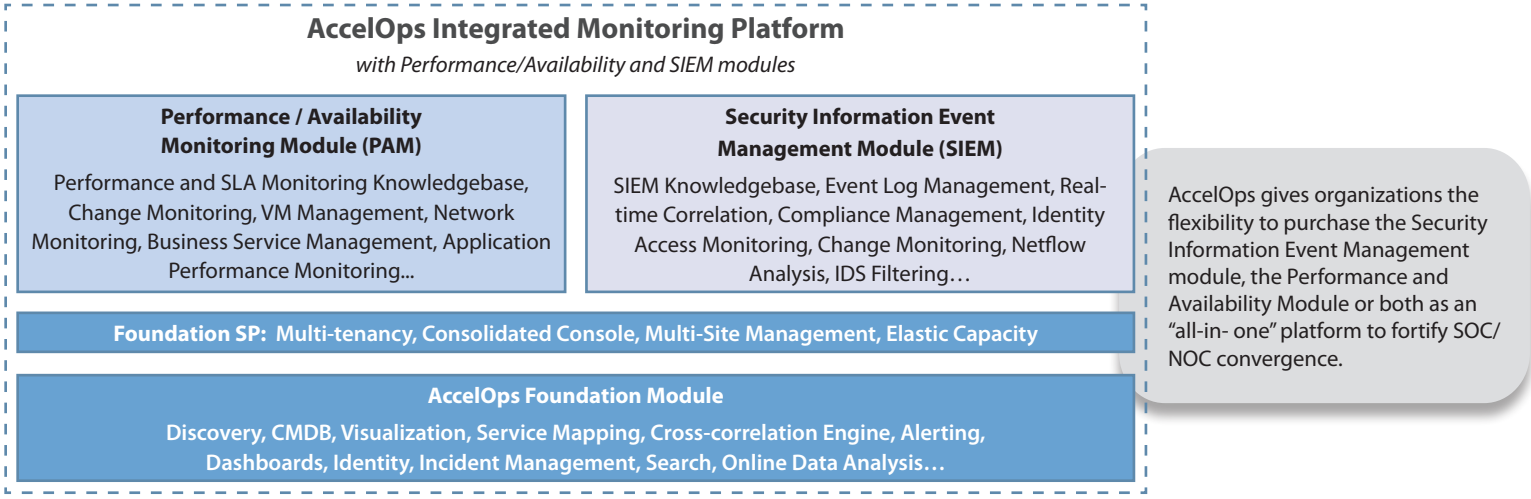
accelops

# Extensive Compliance Automation Through an Integrated Security Information Event Management Platform

### AccelOps SIEM: Compliance Monitoring, Investigation and Reporting

Beyond comprehensive security information event management (SIEM) and log management functionality, AccelOps provides broad verification of controls and compliance documentation. The solution ships with extensible compliance-relevant dashboards, rules and reports leveraging advanced discovery, event log normalization and consolidation, cross-correlation, file integrity and configuration change monitoring, pattern profiling, identity access monitoring, and object-based compliance grouping. One single platform addresses multiple mandates including ISO, PCI DSS, SOX, GLBA, HIPAA and privacy.

+ Fully extensible **compliance management dashboard** with built-in rules, reports and widgets mapped to compliance standards
+ **Auto-populating CMDB** (Configuration Management Database) with versioning and alerting to identify config. change violations
+ Interactive Layer-2/3 topology mapping to **instantly document compliance segregated environment** and visually assess incidents
+ Auto-discovery and in-depth config. monitoring of **DMZ, NAT, Wireless AP**, as well as hardware, VM, server, and application
+ Track and report successful and failed logins, authentication, and location with **network behavior and user behavior profiling**
+ Identity Access Management binding IP address to machine, login, user association and event — **capturing TRUE identity behind shared credentials, resource access and activity.**
+ **Monitor suspicious activity** ie. terminated or service account use
+ **Monitor and document compliance-critical event:** vulnerability scanner, application firewall, DLP and MTA encryption activity
+ **Filter IDS false positives** with automated patch exception mgmt.
+ **Track physical and logical access** and monitor/alert on violations to PII/financial data: **user, location & rogue user network access**
+ Monitor the performance, availability and security of compliance-relevant systems to **quickly negate non-security issues**
+ Smart network/system behavior rules **pinpoint botnet attacks**
+ **Advanced rule engine** and GUI to track & alert **for any scenario**
+ **IT business service mapping** for issue prioritization, impact analysis and collaboration as analytics are applied to logical group
+ **Expedite incident response** with **alert drill-through** for complete incident details, object status, configuration and file integrity changes, identity and **trouble-ticketing**
+ **Enterprise search** of all real-time and historic raw, normalized and incident details supporting fast keyword and structured search
+ **Satisfies secure, long-term data retention requirements**
+ **Centralize all event / log management with scale-out architecture for virtually unlimited performance and online data management capacity** — all operation data is readily available with means to expand processing and storage on demand




### Intelligent. Proactive. Secure.

Whether you are investigating log management systems, upgrading your present SIEM, assessing compliance requisites, or have to meet an audit deadline — contact sales@accelops.net or visit www.accelops.net to explore our depth, breadth and value.