accelops

Datasheet

AccelOps Security Information and Event Management (AccelOps SIEM)

Key Benefits :

- Software solution, cloud and virtualization ready
- Scale on-demand
- 360° views for rapid triage
- Comprehensive SIEM solution
- Native multi-tenancy

"AccelOps is not only much better in architecture and in analytic intelligence but the beautiful GUI and the ease of use makes it the obvious choice"

Byron Walker
Data Center Director
Raytheon (Applied Signal Technology)

Raytheon
Applied Signal Technology

The Legacy Way

Legacy security tools assume the enterprise knows what needs to be monitored and this assumption is the cause for monitoring blind spots. Virtualization and cloud create new blind spots as these fast changing environments create multiple new vulnerability points within and outside enterprise firewalls. Scaling today's hardware-based systems to accommodate virtual machine growth involves repeated and expensive data migration and fork lift upgrades. Compounding these difficulties is lack of comprehensive information needed to resolve incidents. Simple questions such as "what changed, what business services are affected, are these patterns observed elsewhere," require a large team viewing multiple product screens and correlating data from disparate systems. Thereby frequently exposing the enterprise to clear and present vulnerability. Finally, lack of context such as user identity, user location, user role, and affected application make prioritization of scarce resources even more challenging. What you are left with is high TCO for security tools and a lot of unaddressed risks.

The AccelOps Way

AccelOps' virtual appliance based software-only solution is easy to deploy and scale. Our discovery driven approach automatically detects what is in the environment and monitors those elements with the right policies. AccelOps' patent-pending distributed cross-correlation technology is extremely efficient at detecting sophisticated patterns in streaming mode. Distributed correlation enables you to scale your SIEM solution by scaling horizontally or adding virtual machines. No more expensive data migration or hardware upgrades. We combine security, performance, configuration, and change information in a unified platform to ensure that critical information necessary to solve problems is just two-clicks away - we automatically connect the dots for you. AccelOps also provides an industry-first technology that enables you to extend monitoring to new or custom environments while maintaining speeds of natively compiled code. AccelOps provides you unparalleled richness and flexibility at vastly improved performance, scale and total cost of ownership.

How It Works?

Once the virtual appliance based product is deployed, simply provide the range of IP addresses and appropriate access credentials. The software automatically discovers devices and categorizes them into servers, storage, networks, applications etc. and even maps their inter-relationships. The information is gathered in an agentless manner.

With auto-discovered knowledge, the product immediately captures the right information such as log files, configuration metrics, network flow data etc. from the right source and stores them in standard enterprise storage systems — i.e. no specialized vendor supplied hardware or storage is needed. The product builds on the knowledge of the environment to automatically apply appropriate rules, policies and event notifications. As a result you see outcomes within hours of product installation.

Distributed Correlation

AccelOps' industry-first patent pending technology distributes correlations across a cluster of virtual machines. This allows you to speedily do temporal pattern based rules including nested and chained rules based on keyword combinations or expressions involving ANY captured attribute with time of day operators etc. Moreover you can easily scale your system to handle additional load by adding virtual machines — no expensive data loads, transfers and hardware upgrades.

Other Key Features :

- Log Management
- Normalize and categorize events
- Search and Analytics
- Integrated Network Flow Analytics
- Configuration Change Detection
- Compliance Reports
- Performance and Availability

"As a provider of e-Discovery solutions, assuring the integrity and protection our company and clients' information assets are paramount.. We have a complex, dynamic infrastructure and an extensive security management program. AccelOps provides our security team with the comprehensive situational awareness and extensive audit capacity necessary to support our ISO compliance requirements."

Ed McCraken
COO at RenewData

"AccelOps provides greater SIEM functionality, versatility and efficiency compared to using multiple tools. Migrating from Cisco was easy as AccelOps is very automated and robust."

Eric Hoy
Manager of IT
Global Network
Services, Dionex

Learn More

Web: www.accelops.com/siem
Email: info@accelops.com
Tel: +1 (408) 970-9668
Fax: +1 (408) 970-9666

FREE TRIAL DOWNLOAD
www.accelops.com/download

accelops

Enterprise Search and Analytics

All data obtained by AccelOps is fully indexed and stored in a flat-file database. Search and ad-hoc analytics capability is built into the product. AccelOps also allows users to write rules, patterns and computations using any indexed data through an easy to use graphical user interface.

Business Service Prioritized

With AccelOps you can easily compose Business Services with a drag and drop interface by leveraging auto-discovered data. Security incidents are prioritized based on importance and criticality of business services; thus focusing your key resources on the most important problems.

Comprehensive Context

The most common questions when security incidents occur are — what changed to cause this incident, what applications are affected, what is the user's identity and location, and how to remediate the situation. AccelOps provides answers to these questions by presenting all security, performance, configuration, change, user identity, and dynamic user location data on a common platform. Key information is clicks away.

Extensibility Without Performance Penalty

With AccelOps' patent-pending industry-first innovation you can field-extend the product to support new devices yet maintain native speeds. Monitor any number of new attributes 'on the fly' simply by adding or editing XML scripts. You are no longer dependent on vendor product schedules to secure your environment in the most comprehensive manner.

Built-In Incident Management

AccelOps allows you to natively manage security incidents. Incident reports are presented in Fishbone view, Topological view, Calendar view and Location View. Mean time to repair reporting using ticketing system and SLA reporting enable process improvements.

Network Flow Analysis

With AccelOps you can profile network traffic flow and firewall logs to detect network services and baseline communication patterns by days-of-month, days-of-week, and by business and off-business hours.

Threat Mitigation

AccelOps' ability to detect fine-grained patterns and track user identity, even under mobility, allows you to automatically mitigate threats with precision, immediacy and with confidence.

© Copyright 2011 AccelOps, Inc. All rights reserved. AccelOps and the AccelOps logo are trademarks of AccelOps, Inc. All other product names references are used for identification purposes only and belong to their respective companies. The information contained herein is subject to change without notice.