accelops

Solution Brief

AccelOps for Managed Security Service Providers

MSSP Benefits:

- One platform to monitor Security (SIEM), Compliance and Performance
- One click customer on boarding
- Reduce upfront and recurring IT costs to maximize profits
- Offer differentiated services without additional costs
- Virtual solution scales on customer demand
- Real-time and historical log analysis in one solution
- White label solution for MSSP branding

"The AccelOps solution has allowed us to quickly become a managed security services provider. Not only do we have a new revenue stream, but the operational and security visibility of the AccelOps solution enables us to establish more strategic relationships with our customers."

Dave Nelson
President of Integrity Technology Systems, an Iowa-based information security, risk management, and compliance consulting firm

The Challenge

Managed Security Service Providers (MSSPs) must expand their market reach, service offerings and increase their customer base while improving internal efficiencies to maximize customer satisfaction and their own profitability. At the same time, today's complexity and scale of IT environments creates multiple points of vulnerability - internal and external as well as regulatory and compliance management headaches. MSSPs today face multiple challenges that include:

Evolving security complexity and customer needs

- Specialized, complex and highly dynamic nature of IT security
- Multiple customers, divisions and business needs at varying levels

Need: A true multi-tenant solution that continuously learns and adapts to new challenges

Round-the-clock security concerns

- Customer security concerns around outsourced IT and associated data
- Manage multiple different escalation paths for many customers

Need: Fine-grained business policy based event escalations

Compliance automation

- Compliance liabilities and time-consuming lengthy audit cycles
- Staying on top of patch management and upgrades
- Need for both real time and historical analysis

Need: Reduce business risk by automating policy controls and compliance efforts

Reporting

- Provide daily, weekly, monthly or on-demand customized reporting based on client requirements
- Security compliance and regulatory reports such as Sarbanes-Oxley, HIPPA

Need: Easy and quick customization without writing code

Offer differentiated services

- Provide integrated availability, performance and security
- Business services based security monitoring

Need: Single platform to manage performance, availability and security (SIEM)

Budget constraints

- Large upfront and recurring hardware investments
- Over capacity boxes with specialized and finite storage
- Duplicated hardware due to high availability demands

Need: Fully virtual software based solution that scales on customer requirements

The AccelOps Solution

The AccelOps virtual appliance based software-only solution offers MSSPs an intelligent and cost-effective way to meet service levels, and offer new lines of service delivery opportunities. The AccelOps virtualized architecture allows MSSPs to remotely monitor customer environments across their data centers, private or cloud environments. All data obtained by AccelOps is fully indexed and stored in a flat-file database with search and ad-hoc analytics capabilities built into the product. AccelOps also allows users to write rules and patterns using any indexed data through an easy to use graphical user interface.

AccelOps enables user to create Business Services through a drag and drop interface to leverage auto-discovered data. Security incidents can be prioritized based on importance and criticality of business services; thus focusing your key resources on the most important problems. The most common questions when security incidents occur are — what changed to cause this incident, what applications are affected, who is the user, what is the user location and how to remediate the situation. AccelOps provides answers to these questions by combining security, performance, configuration, change and user identity data on a single unified platform, ensuring critical information necessary to solve problems is just two clicks away. 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.

The patent-pending Elastic Monitoring Capability of AccelOps ensures that MSSPs can easily scale their systems to handle changing customer loads by simply adding or removing virtual appliances to the cluster adding virtual machines eliminating expensive data loads, transfers and hardware upgrades.

"The AccelOps architecture accommodates bursts without forcing service providers to change their licenses and management of different components as things change on the fly"

Susana Schwartz
Connected Planet

How it works

After deploying the virtual appliance based AccelOps product, you need to simply provide the range of IP addresses and appropriate access credentials. AccelOps automatically discovers and categorizes your entire infrastructure including servers, storage, networks, applications, etc. and maps their inter-relationships. The information is gathered in an agentless manner.

With this auto-discovered knowledge, the product immediately captures the right information such as log files, configuration metrics, network flow data etc. from the appropriate 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 installing the product. With the built-in XML-based parsing engine, new sources can be added without waiting for product updates — enabling MSPs broad market opportunity and supporting custom enterprise applications.

How AccelOps helps grow your business

Minimize upfront and recurring costs

The AccelOps product has been built from ground up for service provider requirements. Unlike traditional approaches of building solutions around specific hardware and software requirements, the AccelOps solution is a virtual appliance solution. MSSPs can quickly get the AccelOps product up and running on existing VMware or Linux environments eliminating the need to buy expensive hardware. MSSPs can remotely manage customer environments by deploying AccelOps on virtual machines in the customer's environment, this enables MSSPs avoid expensive installation services and hardware management challenges. Since the AccelOps product can run on the free ESXi version of VMware, there is often no cost to

the customers to install the virtual environment on existing hardware with excess capacity. For the MSSPs, the virtual solution also allows them to offer redundancy and high availability services to clients at very low incremental costs.

Protect your investment: grow your profit margins

As the customer scaling requirements change, MSSPs can increase or reduce coverage simply by using license keys. In contrast, most traditional approaches require MSSPs to start with a sized-approach and start anew with yet another oversized hardware and software replacement every time the need to scale occurs. AccelOps' out of the box industry leading multi-tenancy capabilities allow MSSPs to manage multiple customers with a single AccelOps software deployment to further drive down infrastructure and incident management costs. AccelOps' unique ability to easily codify even the most complex rules and scenarios enables MSSPs to bake into the product the human knowledge component of operators. This reduces ongoing costs and minimizes risk of knowledge leaving the company when key personnel exit.

These capabilities allow you to protect your initial investment and obtain one of the quickest times to value and ROI in the industry allowing profit margins to grow over time. Some of AccelOps' MSP customers currently support over 200 enterprise customers with the AccelOps platform.

Our differentiated lines of services

The AccelOps product enables MSSPs to grow their revenues by adding new lines of services as their customers' business growth results in increasingly complex and expanding IT environments. MSSPs can start managing a few critical services for their customers and then quickly expand their footprint with customers by offering and managing more complex services over time without incurring additional costs of adding and integrating new tools.

MSSPs can grow their businesses beyond Firewall, IDS/IPS and IAM with complete log management, SIEM and compliance automation offerings. AccelOps offers full log aggregation, real-time event correlation and online data retention with rules and reports mapped to leading management and compliance standards such as PCI, SOX, COBIT and HIPAA.

The integration of Security Information and Event Management (SIEM) and Availability and Performance Management (APM) capabilities on a single platform, in-memory real-time analytics and the ability to present them in a unified interface enables MSSPs to provide unique differentiating services to their clients. The white labeling ability allows MSSPs to offer all these service offerings as a fully branded MSSP solution to their clients and increase their brand value over time.

AccelOps enables MSSPs to meet individual Customer SLAs at varying levels of customer requirements. A single click allows you to manage customer environments at the service or individual IT component levels. The ability to manage more than a thousand auto-discovered metrics across servers, storage, network and applications combined with numerous out of the box business services, dashboards and reports allows you to quickly and efficiently prioritize incidents based on importance and criticality of business services allowing you to provide the appropriate service level agreements (SLAs) demanded by different customers.

"As a provider of e-Discovery solutions, assuring the integrity and protection our company and clients' information assets are paramount. We continue to invest in proven processes and leading-edge solutions to achieve service reliability and maintain operational integrity. 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

Reporting Capabilities

AccelOps ships with an extensive knowledgebase of security, compliance, change, performance, availability and service management rules, dashboards and over 1000 report templates mapped to best practices and standards. AccelOps also provides MSSPs the flexibility to quickly create or customize analytics to monitor or report on almost any service level, operational threat or policy violation.

"We've been truly impressed by AccelOps' differentiation, how elegantly and powerfully both security and performance and availability monitoring have been integrated into a single solution. Not only does the AccelOps platform create new sell-through opportunities for channel partners, but it helps transform them into operationally efficient MSPs and MSSPs offering margin-rich, differentiated services."

Ken Lewis
Vice President of sales and marketing at CMI

About AccelOps

AccelOps virtualized, cloud generation software monitors performance, availability and security (SIEM) of IT infrastructure and applications in highly dynamic and scalable data centers. Anchored by patent-pending technology for distributed real-time analytics, AccelOps software works across private clouds, public clouds and traditional data center environments, to bring proactive and comprehensive service health visibility.

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

FREE TRIAL DOWNLOAD
www.accelops.com/download

FREE TRIAL DOWNLOAD

Download the 30 day trial
www.accelops.com/download

© 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.