



Customer: Healthways

Industry/Segment: Healthcare

Products: AccelOps integrated SIEM, performance and availability monitoring software

Platforms/connectivity: Windows, HP-UX, Cisco, Palo Alto Networks

Applications: VMware, Exchange, Oracle and proprietary analysis and communications applications

Results With AccelOps:

- ▶ “Single pane of glass” gives full visibility into what’s going on across the infrastructure for faster problem resolution
- ▶ Comprehensive reporting for all IT operations
- ▶ Unified view into the data center
- ▶ Real-time monitoring and correlation of security events with other types of events

Healthways Monitors and Secures Global Health and Wellness with AccelOps

By combining behavioral science and health and wellness expertise with unmatched data management, analytics and IT capabilities, Healthways has become the largest global provider of well-being improvement solutions. Healthways’ customers include health plans, insurers, employers, communities and government agencies. For more than three decades, the company has helped approximately 40 million patients effectively manage existing health conditions and change behaviors that enable people to stay healthy.

By analyzing claims data for individuals, the company applies science-based research and predictive modeling techniques to tailor specific plans to keep people healthy, address modifiable lifestyle risks and optimize care for the chronically ill.

Thanks to its proprietary technology and extensive IT infrastructure, Healthways connects with millions of people and tailors individual contact using text, chat, telephone and interactive voice response. Its systems architecture is built to make it easy to configure solutions and quickly introduce improvements.

For Healthways, the security, performance and availability of its IT infrastructure are fundamental to its business, and to the well-being of its large, global patient base. All aspects of the infrastructure, including critical databases and custom applications, must be monitored continuously and any problems detected and resolved immediately.

The Challenge: Complete security and compliance, integrated with all facets of the IT infrastructure in a single pane of glass view. Consolidate tools and improve security, performance and availability monitoring, and troubleshooting.

As Healthways has grown, its IT infrastructure and operations also expanded and became more sophisticated. The company has developed an extensive global network, state-of-the-art call centers, maintains more than 350 websites, tens of critical custom applications and multiple Oracle databases running on HP-UX servers. Approximately 90 percent of the infrastructure is virtualized. Over the years, Healthways deployed multiple tools to monitor all aspects of its infrastructure: network; security; servers; storage; databases; and applications. In addition, the company that augments Healthways’ day-to-day

“Our immediate reaction was ‘Wow! This thing is incredible!’”

Russell Butturini, Senior Enterprise Architect, Healthways

operational data center management deployed additional operations management and Security Information and Event Management (SIEM) software. Despite these extensive monitoring capabilities, Healthways found troubleshooting problems time-consuming and cumbersome.

“We had no consolidated view of the data center with all of these tools,” said Russell Butturini, senior enterprise architect at Healthways. “If we needed to troubleshoot an issue, we had to look in five or six different places and correlate data, often by hand, and that is not optimal. We really wanted a single pane of glass that would give us full visibility into what was going on across the infrastructure so we could resolve problems right away and have comprehensive reporting for all of our IT operations. Getting a unified view into the data center was a big driver for us.”

Because Healthways operates in the highly regulated healthcare industry, security and the Health Insurance Portability and Accountability Act (HIPAA) compliance are always top of mind. The company needed its SIEM solution to provide extensive log and security event data collection, real-time correlation, historic analysis and compliance reporting. Healthways wanted to replace RSA enVision and Cisco MARS, which had reached its end of life, with a solution that could provide extensive native device support, including support for Palo Alto Networks firewalls.

Healthways wanted to be able to understand the related impacts on the infrastructure of an incident. If a security incident is recorded, what else happens in the environment? For instance, if an FTP data intake server is being attacked, how does that affect other jobs processing data on that server? Is it knocking out customer connections? What is the overall business service impact?

“With our old tools, all we would see was ‘failed login,’ attempts so finding a tool that could correlate security events with other types of events – correlating what happened on this security device with this network device with this server – was very valuable to us,” Butturini said.

The Solution: AccelOps integrated SIEM, Performance and Availability monitoring software

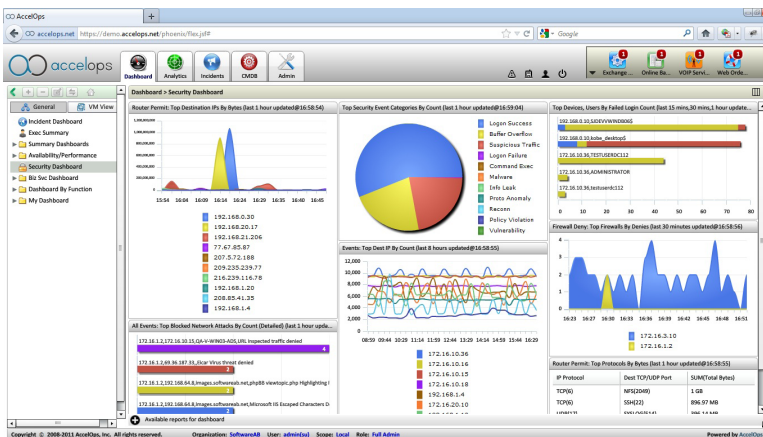
Healthways found AccelOps after searching for a solution that would provide the 360-degree data center visibility and real-time security monitoring it required. AccelOps software is the industry’s first application to monitor security, performance and availability of IT infrastructure and applications on a single platform.

After an AccelOps product demonstration, “Our immediate reaction was ‘Wow! This thing is incredible!’” Butturini said. “That single pane of glass we wanted was right there, so

we could monitor security, availability, performance and everything. AccelOps could give us complete oversight, including that part of our operations management that we contract, so we were sold.”

The AccelOps monitoring application was architected from the ground up to monitor all devices, users and applications. It provides complete visibility across the entire physical and virtual IT infrastructure – on-premise, in the cloud or a hybrid of both – in a comprehensive single application. It seamlessly integrates security, performance and availability monitoring.

AccelOps Dashboard



"The reporting and dashboards are excellent. The visuals are really good and present data in a way that is easy for a deeply technical person to get valuable data, and yet present a dashboard that is useful for an executive. You can really see what's going on and see where it makes sense to make adjustments."

Russell Butturini, Senior Enterprise Architect, Healthways

AccelOps monitors all domains of the data center, including servers, storage, network elements, security devices, users and applications – in real time – to quickly identify and resolve security incidents and performance bottlenecks. From a "single pane of glass," IT administrators can monitor all data center activities and resources, whether on-premise, remote or in the cloud. With multiple critical monitoring functions in a single application, AccelOps accelerates problem identification, helping IT to quickly determine the corrective response: adding compute or storage resources; modifying a firewall rule to eliminate a source of threats; moving competing high-volume traffic sources to different network ports; changing access privileges for a user or group of users.

AccelOps scales readily because it runs on virtual machines that can be easily added or reduced as the number of monitored events changes. It provides a comprehensive view of the information and can be tailored for individual needs, in summary or detailed, drill-down formats. And the AccelOps solution comes with more than 1,750 ready-to-use reports and rules for 200 security threat scenarios that allow users to detect and make sense of complex IT patterns and events in real time.

Healthways had AccelOps installed and running in only six hours, as the application automatically discovered and initiated monitoring on all devices and applications. AccelOps makes it easy to fine-tune and customize alerts, dashboards, reports and user profiles. This allowed Healthways to customize and adjust tool settings to its unique, highly customized environment within a week. In contrast, previous SIEM-only implementations had taken two months to get operational.

The Result: Complete infrastructure security and operational oversight from a single pane of glass tool that's better and more cost-effective than multiple, single function tools

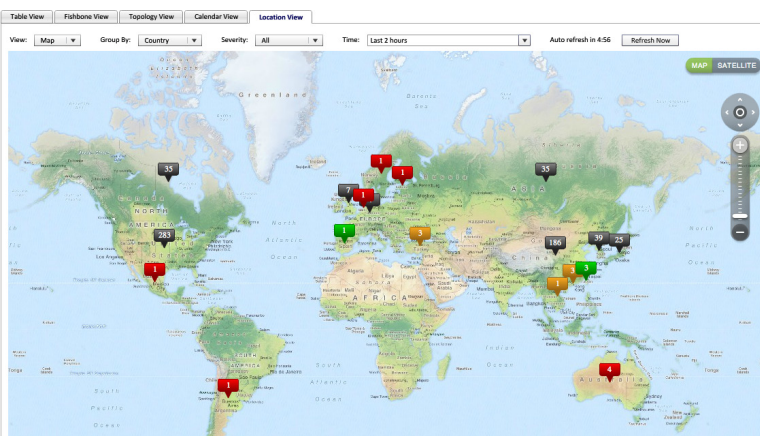
With AccelOps, Healthways has a single pane of glass view across its entire IT infrastructure. The impact of a security event is immediately visible across the network, servers, users and applications. AccelOps' Business Service View provides unique visibility into the impact any given event across the full infrastructure and operational spectrum. Troubleshooting is quicker and easier, facilitated by AccelOps' drill-down dashboard capabilities. Since deploying AccelOps, Healthways has made a noticeable reduction to its Mean Time to Resolution (MTTR).

Using AccelOps, Healthways noticed right away that alerting is more sophisticated than with other tools. Excessive alert chattiness and the potential risk of ignoring a problem event in the midst of too much benign problem reporting is a common problem with traditional monitoring tools. With AccelOps, however, Healthways was able to easily and precisely tune its data aggregation, making it possible to create an alert based on whether a sequence of events occur consecutively or over a number of times in a given

period of time. This makes for greater sensitivity and more meaningful alerts. For instance, rather than triggering an alert every time a server's CPU reaches 80 percent usage, even if only momentarily, and initiating unnecessary interventions, AccelOps allows Healthways to alert operators in the event that the high CPU usage continues and intervention is actually warranted, but not for benign, transient spikes.

"The reporting and dashboards are excellent," Butturini said. "The visuals are really good and present data in a way that is easy for a deeply technical person to get valuable data, and yet present a dash-

AccelOps Geo-Location



“AccelOps delivers phenomenal value. When you need to monitor multiple things, it’s the best tool as far as I’m concerned, and having a single tool saves on annual maintenance fees.”

Russell Butturini, Senior
Enterprise Architect, Healthways

board that is useful for an executive. You can really see what’s going on and see where it makes sense to make adjustments.”

One example of a valuable adjustment for Healthways was being able to analyze overseas Internet activity. AccelOps’ geo-location mapping feature showed that the company was generating millions of connections from countries where it does not conduct business. By using an AccelOps rule to eliminate these connections, Healthways was able to streamline its network traffic and reduce the risk of unauthorized access.

Because of its scope and clarity, AccelOps has become the “go-to” tool for Healthways. Even contracted operations personnel are using it in preference to RSA enVision, HP ArcSight, HP Operations Manager, and System Center Operations Manager. During busy crunch times, such as open enrollment periods, AccelOps has proven itself extremely reliable and scalable.

“AccelOps delivers phenomenal value,” Butturini said. “When you need to monitor multiple things, it’s the best tool as far as I’m concerned, and having a single tool saves on annual maintenance fees.”

About AccelOps

AccelOps provides a new generation of integrated security, performance and availability monitoring software for today’s dynamic, virtualized data centers. Based on patented distributed real-time analytics technology, AccelOps automatically analyzes and makes sense of behavior patterns spanning server, storage, network, security, users, and applications to rapidly detect and resolve problems. AccelOps works across traditional data centers as well as private and hybrid clouds. The software-only application runs on a VMware ESX or ESXi virtual appliance and scales seamlessly by adding additional VMs to a cluster. Its unmatched delivery of real-time, proactive security and operational intelligence allows organizations to be more responsive and competitive as they expand the IT capabilities that underpin their business.

FREE TRIAL DOWNLOAD
www.accelops.com/download

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054
USA

Web: www.accelops.com
Tel: 1 (408) 490-0903
Email: sales@accelops.com

