Media Contact:
Agnes Lamont
Marketingsage
(925) 426-0488, Ext. 112
accelops-pr@marketingsage.net

AccelOps Survey Highlights Need for Better Cloud Security and Performance Monitoring

BYOD and data protection issues top organizations' concerns as they embrace cloud services

SANTA CLARA, Calif. - March 20, 2013 - AccelOps, Inc., the leader in integrated Security Information and Event Management (SIEM), performance and availability monitoring software for on-premise and cloud-based data centers, announced findings from its recent survey of 176 IT security professionals conducted online and at the RSA Conference 2013. While 65 percent of respondents' organizations are using cloud services today, only 46 percent have moved mission-critical applications and data outside the enterprise. Significant inhibitors remain in ensuring effective cloud security and 39 percent of respondents believe that their existing SIEM and infrastructure monitoring tools are not acceptable to support their cloud security and regulatory compliance requirements.

Bring Your Own Device (BYOD), data control and potential data loss top the cloud security concerns identified by respondents, closely followed by enforcing security policies and ensuring visibility across both traditional and cloud infrastructures. Given the inhibitors identified and that less than half of those using cloud services have deployed a hybrid model, there is clearly a need for a single, unified platform that can identify security threats and monitor IT operations across traditional, private and public cloud infrastructures.

“It's a sad indictment of the security industry that, in such a well-established market as SIEM and performance monitoring, 39 percent of those surveyed indicated they could not rely on their existing SIEM and monitoring solutions to ensure cloud security and compliance," said Flint Brenton, President and CEO of AccelOps. “There is much work to be done to ensure that security threats and the risk of data loss associated with cloud environments are minimized. The myriad of cloud services and an ever-changing BYOD landscape means we can no longer simply lock down access to sensitive resources; we have to do a better job of monitoring, correlating and analyzing infrastructure behavior and events to recognize and respond to incidents in real-time."

Unsurprisingly, the survey shows that the responsibility for cloud security remains overwhelmingly with the internal IT staff at 78 percent and only 13 percent of those surveyed hold their Managed Services Providers (MSPs) responsible for cloud security. While 51 percent of respondents indicated that they are moderately to extremely satisfied with the Service-Level Agreements (SLAs) offered around security and access control, a surprising 41 percent indicated they were neither satisfied nor dissatisfied with their SLAs. The survey confirms that organizations must retain ownership and responsibility for their own data, irrespective of the underlying security and processes implemented by the cloud service provider. Accordingly, cloud service providers and their customers need better visibility into cloud resources and a common view of cloud service performance and availability against SLAs to improve customer satisfaction.

Summary of findings:

- 65 percent of respondents said their organizations use cloud services for mission-critical applications and data. Of those, 29 percent are using hybrid clouds and 17 percent have public cloud services.
- 39 percent of respondents rate their organizations' ability to ensure cloud security and regulatory compliance using their existing SIEM and infrastructure monitoring tools as inadequate or fair, and only 29 percent rate them as good or excellent.
- 51 percent are extremely or moderately satisfied with the SLAs their cloud service providers offer.
- 78 percent of organizations retain responsibility for cloud security using internal IT staff.
- In priority order, the issues identified as the greatest inhibitors to effective cloud security are:
  1. BYOD
  2. Data control
  3. Potential data loss
  4. Enforcing security policies
  5. Visibility across all infrastructure resources, traditional and cloud
  6. Real-time analysis of log data
  7. Compliance reporting
  8. Hypervisor vulnerabilities
  9. Rapid incident response

"The promise of cloud computing is to improve agility and deliver greater efficiencies and cost savings," Brenton said. “However, unless risk can be managed and data secured effectively, organizations will not fully benefit from the advantages of the cloud."

AccelOps' software enhances cloud security by providing a “single pane of glass” view of security, performance, and availability information from almost any source across an organization’s entire data center infrastructure – physical, virtual, on-premise, or cloud-based. Patented real-time analytics technology cross-correlates log and event data with context in real time to make sense of complex IT patterns and events as they happen. AccelOps’ scalable architecture and multi-tenancy features enable Managed Service Providers (MSPs) to globally monitor their entire infrastructure yet still provide individual clients with visibility into just those resources allocated to them. AccelOps stores detailed data, including that from cloud providers such as Amazon EC2, in a database to satisfy compliance requirements and for future forensic analysis. The software also provides extensive service-level and compliance reporting for user organizations and MSPs.

Detailed survey findings are available at www.accelops.com/cloudsurvey2013.

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. For more information, visit www.accelops.com.