accelops

AMERICAN SYSTEMS Takes Security Information Management and IT Service Management to the High Ground with AccelOps

AMERICAN SYSTEMS, one of the largest employee-owned companies in the United States, provides system engineering, technical and managed services to government and commercial markets. The company located in Chantilly, Virginia, offers a bevy of services spanning consulting, professional IT, logistics and acquisitions, design, development and integration, custom solutions, as well as staffing and operations.

AMERICAN SYSTEMS, which has been in business for nearly 35 years, is a mid-tier enterprise with 1,500 employees in 16 office locations and more than 125 field sites to support its nationwide clientele. An IT staff of 30 operates 9 datacenters and 17 remote facilities led by CIO Brian Neely. The company uses a variety of IT management tools, such as BMC, Cisco, Microsoft, Solarwinds and open source utilities, to manage their diverse infrastructure comprised of a bevy of Cisco, Juniper, EMC, Microsoft, VMware, McAfee, RSA and Symantec products.

The company is known for anticipating and responding rapidly to their customers' present and future needs. With equal precision, the IT staff determined that they needed to advance their current infrastructure protection and source a new Security Information Management (SIM) system. The company had converged their NOC/SOC organization and sought a solution that offered: broad coverage and visibility, the means to extend operational and security controls, as well as means to retain and readily analyze event, log and other operational data as necessary.

"*AMERICAN SYSTEMS is all about being responsive, efficient and thorough when it comes to solving customers' needs. Our IT organization operates under these same principals. Having the majority of our business serving government clients, we needed to build-out our security management capacity. Since security is part of operations, we required broad event correlation, monitoring and instrumentation that could be easily implemented, customized and scaled*," said Brian Neely, CIO/CTO of AMERICAN SYSTEMS.

The evaluation process was led by the CIO, IT Infrastructure Services Group and the information security team. Primary test criteria were ease of use, feature set, security, operations and compliance requirements.

Among commercials SIMs that were assessed, such as EMC (RSA Envision), LogRhythm and Symantec, AMERICAN SYSTEMS selected AccelOps. The company evaluated vendors against a multitude of SIM requirements. AccelOps met or exceeded these requirements and offered advantages in regards to: usability, discovery, automated event, log and configuration data capture, breadth of correlation and anomaly detection, built-in rule set and reports, topology and search functionality, and identity and location management. AccelOps gives users immediate access to massive purpose of root-cause analysis, investigation, reporting and audit. The company also praised AccelOps' powerful analytics engine that enables custom rules with Boolean logic and the report flexibility to easily slice and dice data.

"*AccelOps auto-discovery and automatic CMDB population enabled broad data collection and the ability to have more relevant and categorized information, such as Switch, Firewall, system configurations, directory objects, virtualization and applications - all current and managed within the same GUI. The dashboard is very intuitive and interactive to allow us to see infrastructure and security issues and problems, topology, as well as drill-through on any details. We can adjust or make new dashboards on the fly including the ability to quickly search incidents and raw events. A very useful, unique feature, was the association of user identity and location to events. This allows us to immediately know the primary login name and location (such as the wireless AP, VPN or nearest layer-2 switch) for a given event. Great for cutting down the time to do investigations, monitor for acceptable use and report accuracy*," said Wesley Ward, Information Security Engineer at AMERICAN SYSTEMS.

Enterprises are most concerned about service delivery and means to improve operational efficiencies. Most security and log management systems offer basic event capture, analysis and alerting, but have limited to no context on the infrastructure, identity, location or service impact. Today's datacenters are more complex. The lines between what is a security violation, a change management incident, a network anomaly or an application problem are becoming more blurred. Threats and attacks are more sophisticated. Given these challenges, enterprises require a new, a more holistic approach to datacenter management that is IT cross-functional and service intelligent. Likewise, organizations need to have more timely operational oversight and complete information at their fingertips to preempt threats, identify issues and triage problems quickly and effectively.

Challenge

Drivers

- Comprehensive Security Information Event Management
- Advance converged NOC/SOC operational capabilities
- Event cross-correlation, consolidation and retention

Considerations

- Usability, effort to implement, customization and scale
- Rule extensibility, event filtering and accuracy, and reporting
- Validate approved changes and business impact in real-time
- Centralize IT instrumentation to fortify ITIL and SOX compliance

Results

- Comprehensive security monitoring and controls with full online operational details
- Centralized IT Service, security and operations instrumentation
- Proactive management and service monitoring
- Virtual appliance; simplified procurement and allows for broad coverage and scale

accelops

"The SIM products had different degrees of event data collection, but they were solely security-oriented and the breadth correlation such as configurations, network flows and logins varied. AccelOps went beyond conventional security management by also integrating service, performance, availability and change management. The business service definition is exceptional and allows us to easily map applications, services and network components as a service. We then can monitor and view high-level status of our services, and understand the details of problems and incidents as related to severity, IT function issue, and business impact. We have not seen a feature like this before and it allows our team to have a uniform means to respond to business issues more efficiently. We have set up and will expand defining our services so we can be proactively notified on critical environments and systems. Since all the operational data is there, we can create and deliver reports more efficiently and inform different groups regarding trends, metrics, potential issues and changes in performance," added Ward.

AccelOps links the physical and virtual infrastructure directly to the business and business services to enable proactive management, efficient root-cause analysis and service intelligence. The solution combines IT management breadth and depth with state-of-the-art discovery, analytics, monitoring and alerting, CMDB, service mapping, SLA tracking, identity access and compliance. AccelOps cross-correlates operational data from configurations, network flows, logins, events, system logs and other sources across network devices, systems, applications, security devices, virtualization, users and directories without agents. A dynamic web GUI offers extensible dashboards, topology maps, reports, rules and metrics aligned to best practices.

"We found AccelOps to be very easy to use - the web GUI is attractive and intuitive. We were trained remotely in two hours and felt confident in a couple of days. Deployment went very smoothly and what monitoring we had in place prior, such as SNMP and syslog, could be quickly brought online. AccelOps took advantage of our VMware investment, where by expansion simply requires adding more processing or virtual machines running the AccelOps application and provisioning storage. We liked the fact that the data management was embedded and optimized for long term access to all the collected data," concludes Wesley Ward.

"Value was seen after day one when we had to find exactly who, where, what and how someone changed certain permissions on a File Share server. AccelOps' query capability searched through thousands of events with iterative filtering to quickly 'find the needle in the haystack'. AccelOps' true identity and location management came in to play big-time," concludes Wesley Ward.

Key Likes

- Easy to use and implement with comprehensive analytics / reports
- Robust Security Information Management feature-set that also offers service, performance, availability and change management
- Extensive cross-domain correlation and IT service instrumentation
- Virtual Appliance: simple to procure, configure and scale

Innovative Features

- Auto-discovery, interactive topology map, and complete CMDB
- Statistical profiling of network behavior, systems and user activity
- Business service definition, monitoring, alerting and reporting
- Captures broad operational details with all real-time and historic information readily online and accessible.

"We were looking to centralize IT business instrumentation and to extend our event correlation, performance monitoring and security information management. We assessed name brand options, but then we came upon AccelOps. We have not seen any solution that ties the network, system and security information together and offers service-level insight. AccelOps provides my team instant intelligence on our business posture, security threats and operational issues through an integrated, easy and dynamic web GUI. The degree of automation and level of operational analytics and security controls are powerful, extensive and scalable - truly enabling proactive, service-oriented management," concludes Brian Neely.

AccelOps provides an integrated datacenter monitoring and cloud service management solution. The result delivers unprecedented infrastructure oversight and operational intelligence to advance service reliability and quality across availability, performance and security objectives.

See how AccelOps can help your IT accelerate business at www.accelops.net.

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