accelops

Case Study

A private Cloud-based approach to being a Managed Security Services Provider

Integrity
SECURITY | RISK | COMPLIANCE

Company name:
Integrity Technology Systems, Inc.
Industry: Cloud Services Provider

Results with AccelOps:

- Cloud Based MSSP Offering
- Customer Onboarding — Quick Deployment And Time to Value
- Elastic Monitoring — Scales on Demand
- Rich Feature Set and Capabilities
- Native Multi-Tenancy
- White labeling Capability for Branding
- Competitive Advantage due to Cost Savings

About Integrity Technology Systems

Integrity Technology Systems (Integrity) is a consulting firm that offers a variety of information security, IT risk management and compliance services in the financial services, technology and manufacturing industries. These services include security penetration testing, disaster recovery, audit and control review, audit liaison, and policy and security architecture reviews.

"Beyond being a superior SIEM platform, we feel that we have a competitive advantage with AccelOps. AccelOps gave us a positive ROI in less than 3 months per subscription year. As we add more customers, the positive returns can be realized even faster based on economies of scale and AccelOps' overall lower on-going costs. We do not have to buy and manage additional appliances for each client or retire older appliances. This has allowed us to realize a positive ROI faster, which in turn freed up capital to help drive expansion of our business — a very big win. So it was worth the expenditure."

Business Requirements

Integrity's clients are typically multi-site organizations with at least one internal data center or co-location hosting facility as well as secondary sites. Their customers have a broad range of systems including Microsoft, IBM, Oracle, Linux/Unix, Cisco, VMware and others. Beyond monitoring security operations, many of Integrity's clients have compliance requirements that they must document and demonstrate to adhere to government or industry mandates.

Dave Nelson, President of Integrity, sought to improve service offerings for his clients and expand into new markets. He wanted to provide a Software-as-a-Service model to his clients that would collect their event logs and analyze it in a remote environment so that the clients wouldn't have to hire and retain specialized individuals. By being the Managed Security Service Provider (MSSP) for their clients, Integrity would be the security expert for those clients who didn't have the resources to do it themselves.

Primary Requisites for a SIEM MSSP Platform

Integrity needed a SEIM solution that offered log and security event data collection, real-time correlation, historic analysis, compliance reporting and data management. In addition, the SEIM solution needed to have native multi-tenancy, be easy to install, customize and scale easily. Per Dave Nelson, "*We needed a solution which would allow us to use a single monitoring foundation for our clients while maintaining operational segmentation. This solution had to afford quick implementation with little on-site overhead. We wanted a pre-defined knowledge base (e.g. dashboards, portal, alert rules and various reports), but also the ability to tune and customize the solution to offer additional engagement options. We also needed to give our clients a robust portal so our clients could run their own queries, reports and dashboards. The solution needed to scale easily for us to add enterprise-level clients without a long and costly upgrade process.*"

Private Cloud-based approach

Integrity decided on a private cloud approach instead of running a traditional SIEM operation driven by several factors. First, Integrity wanted to eliminate upfront hardware and software costs that a traditional SIEM implementation would cost them. Second, traditional SIEMs developed for enterprises with well-defined implementation sizes, would make it expensive for Integrity to scale with increasing customer demands. Third, Integrity needed to be able to provide guaranteed uptime and availability based on client Service Level Agreements (SLAs) contracts.

Prior tools

Integrity was using open source tools OSSIM and Splunk prior to selecting AccelOps.

Integrity found the professional version of OSSIM to be costly and operationally unviable. OSSIM had too many moving collector parts and the overall administration and on-going maintenance was cumbersome. According to the Integrity technical team, support from OSSIM was not very responsive making it hard to effectively support its MSSP clients.

Integrity had deep concerns with other vendors hardware based models. Looking at the future, Integrity knew it would need to constantly ditch old hardware and start from scratch for each capacity increase.

"With Splunk, we had reliability and scalability issues that made us reluctant to roll out an MSSP service based on Splunk. We found Splunk to be a solid general-purpose query utility but not really a fully packaged solution — it was more of a search tool with a log repository. The event correlation was manual and not cross-correlated. We would have to customize everything out of the box and rely on a general community to build out capabilities."

Selection process and alternatives

Integrity's selection criterion was simple — beyond having a strong SIEM feature-set, the solution had to securely and operationally support a multi-tenant environment, provide a positive ROI within 3 months, scale from mid-sized business to large enterprise organizations and support an accelerated cost effective deployment.

Based on their past experience, open source tools and Splunk were ruled-out. They evaluated AccelOps, IBM (Q1Labs), McAfee (NitroSecurity), and SolarWinds (TriGeo). The technical team found that IBM Q1Labs's multi-tenancy had issues with address space overlap and it needed a variety of hardware resources to support different SIEM attributes like NetFlow. It would be increasingly cumbersome to scale out per customer and across multiple customers due to manual and administrative costs in terms of maintenance. McAfee's NitroSecurity product was costly and not flexible — the multi-tenancy mechanism using Collectors was not elegant and the functionality and scale provided by Nitro required administering multiple boxes. With SolarWinds (TriGeo), the technical team could not determine if the product had true multi-tenancy. The solution had physical appliance limitations and did not offer rule and reporting flexibility Integrity required as well as lacked cross-correlation and rule sophistication capabilities.

"We considered alternative solutions from IBM (Q1 Labs), McAfee (NitroSecurity) and SolarWinds (TriGeo). Most of them were built around the tenet of placing their solution in a single enterprise. The feature sets were good, but our service provider needs were different and we didn't feel like they were baked in quite as well. We observed deployment, scale and on-going administration deficiencies, as well as high overall costs. AccelOps was the only solution that met all our criteria."

Why AccelOps?

After spending six months looking at different solutions, Integrity selected AccelOps for two major reasons.

First, the AccelOps solution was developed from ground-up for a service provider model. Other vendors were built for traditional enterprises with service provider features overlaid on top which wouldn't scale for Integrity's needs as it would cause data redundancy, segmentation and multi-tenancy issues.

The second was that other vendors were designed around a specific piece of hardware or a specific size of software to be placed on the customer's hardware. But with AccelOps, Integrity could quickly deploy the virtual appliance in a VMware environment or on a basic Linux environment and simply use license keys to increase or decrease the licensing needed for each of their clients.

Results with AccelOps

Cloud Based MSSP Offering

Integrity's approach to build a cloud based solution eliminated upfront investment costs. Using AccelOps, Integrity was able to build a highly redundant and highly available solution to limit customer downtime. Even if a particular device failed, they could go in and manage it through multiple devices and failover to another device. Going with a traditional SIEM environment would have meant duplicated hardware costs across the board and building highly scalable and redundant infrastructure. By going to a cloud model, Integrity leveraged a single highly redundant infrastructure across the board for all its clients.

Customer Onboarding — Quick Deployment and Time to Value

AccelOps delivered on its promise to provide a quick time to value for new clients that Integrity signed on. It was important for Integrity to shorten the onboarding period for each client as well as start monetizing its investments quickly. Integrity found AccelOps easy and quick to implement and were able to onboard their current clients in less than a day. They deployed the AccelOps virtual appliance collector which automatically took in logs and NetFlow, ran a discovery, obtained configurations and events, and became fully operational in hours — versus days and weeks with alternatives they had used in the past.

The AccelOps' virtual appliance cluster and remote virtual appliance collector that uses standard server equipment helped Integrity reduce customer installation and on-going maintenance costs.

"The benefit of AccelOps is that it runs on ESXi, a free version of VMware. As long as the customer has a server of some type that has the capacity to run a virtualized environment, they can install AccelOps. In this day and age, almost every customer that we come across, no matter how large or small, has the capacity to run a virtualized environment. Most of them prefer to have their own server hardware so that it matches the rest of their infrastructure — it can be monitored and maintained versus us doing that on their behalf."

Elastic Monitoring — Scales on Demand

The AccelOps Virtual Appliance solution has helped Integrity grow capacity as needed and eliminated the cost of deployed appliances becoming outdated. Integrity has been able to set up new collectors on client sites, finish many tasks remotely and begin monitoring and analysis for existing clients within hours. Since the AccelOps virtual appliance supports clustering, the system handles peak event loads without dropping excess data, a limitation with other SIEM vendor hardware appliances. Dave shared, "*This is very useful during critical incident response periods. If we go over peak capacity at any time, the system still supports the increased load as long as it is not extended beyond average monthly load — other systems literally fall down or drop event records. We don't pay for excess monitoring capacity or lose client data. This peak monitoring feature is a material benefit for us, as well as our clients.*"

Rich Feature Set and Capabilities

The Integrity technical team has seen tremendous productivity gains through the Accelops solution allowing them to focus their efforts on monitoring customer environments rather than managing the tool itself. The ability to do on-the-fly updates, upgrades or migrations with minimal effort has let Integrity focus their resources on monitoring services.

"The AccelOps product has almost every conceivable bell and whistle. The discovery, scope of capabilities, incident management, query, rule development, reporting and event data management are top notch. The AccelOps web interface is tremendous; very intuitive, easy to configure and maintain — we don't have to be onsite."

Native Multi-Tenancy

The in-built multi-tenant capabilities of AccelOps have helped Integrity monitor events across all its customers or focus on particular customer incidents. Dave said, "*We believe the way that AccelOps has implemented their multi-tenant functionality is the most progressive in the market. We can monitor configurations, systems, virtualization, users, system integrity, malware — you name it, the data is being monitored by AccelOps — available when and wherever we need it.*"

White Label Capability for Branding

Integrity leveraged the ability to white box their solution so that when their customers log into the portals, they don't see the AccelOps license, logo or software — they see a complete end to end Integrity branding. That has helped integrity strengthen their brand and provide legitimacy to the services and offerings that they provide.

Assessing AccelOps ROI

Integrity found its return on investment (ROI) in AccelOps to be very quick. Integrity was able to avoid the typical upfront and large capital investment required by other security monitoring products. The mature knowledge base allowed them to get up and running quickly and onboard clients with minimal administrative overhead, capacity costs and operational risks. As AccelOps offers MSSPs a flexible licensing model based on aggregate resource monitoring, Integrity was just able to add additional AccelOps virtual appliance instances and update the appropriate license keys as they onboarded additional clients or upgraded current client capacities.

The benefit of being able to offer additional services to their clients also differentiates Integrity from other security providers making it a great value proposition for them.

Transforming to being a MSSP with AccelOps

AccelOps enabled Integrity to quickly become a MSSP in terms of offering extensive SIEM services and log management to their customers. AccelOps' SIEM platform enables complete log management capability, NetFlow analysis, real-time security monitoring and compliance-based reporting for their customers. The extensive event correlation, responsive web GUI, alert management and knowledgebase enables Integrity to get full visibility and offer an independent view and situational awareness of their clients' security requirements.

The easy to customize built-in rules, reports and dashboards enable them to provide clients direct visibility into their organization's security through tailored portals and reporting. By being an external monitoring entity, Integrity also provides stronger proof and objective validation for client auditors.

Dave Nelson said, "*An MSSP offering has added to our revenue stream. The operational and security visibility that AccelOps affords us also enables us to establish a more strategic relationship with our customers. AccelOps better enables us to identify risks and gaps beyond interview processes and has opened up additional consulting service opportunities.*"

"We estimate at 50% savings or more by leveraging virtual appliances. By not being locked into priority hardware, we have lower procurement costs using off-the-shelf hardware and storage. We gain economies via AccelOps' virtual appliance cluster and reference storage. We can also eliminate costs using our clients' existing VM infrastructure. AccelOps has lower ongoing costs. Over a 3-5 year period, even with EPS growth and new features, we won't have to retire our hardware investment."

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.

accelops

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