sumo logic

CASE STUDY

Using Sumo Logic and machine data to deliver a more secure ecommerce experience

VAIMO
CORE OF COMMERCE

Industry

eCommerce technology

Headquarters

Stockholm, Sweden

Size

400+ employees

Use cases

Security analytics

Compliance

Challenge

Among other vital responsibilities, Vaimo is tasked with safeguarding its clients' eCommerce operations. This means relentlessly applying creative techniques to thwart persistent, malicious behaviors that include spam, identity deceit, and bogus user creation, all while attempting to restrict access to key infrastructure resources to a core group of authorized specialists. Concurrently, the company eagerly sought new ways to satisfy an ever-increasing set of regulatory requirements.

Solution

Vaimo deployed Sumo Logic's cloud-native machine data analytics platform to extract the hidden value contained in the log files produced by its ongoing operations. This entailed capturing, aggregating, and taking action utilizing the raw data generated on more than 1,000 servers in its hybrid-computing environment.

Results

With Sumo Logic in place, Vaimo has been able to shrink the number of personnel permitted to interact with its sensitive resources and is far better positioned to manage security-related incidents. The company has also improved its compliance with current and upcoming regulations such as the Payment Card Industry Security Standards Council (PCI) and the European Union's General Data Protection Regulation (GDPR). Vaimo has even been able to use its newfound mastery of machine data to strengthen its competitive stance.

> **"By adopting Sumo Logic, we've demonstrated to our clients that we're serious about protecting their eCommerce resources so they can deliver the best end user experience."**
>
> **Wilko Nienhaus**
> CTO

For more than a decade, Magento has been a well respected, widely adopted open source eCommerce platform that powers hundreds of thousands of stores. In 2018, Magento was acquired by Adobe as a key ingredient in a much larger computing initiative. As Magento's Global Elite partner, Vaimo is delivering commerce solutions exclusively on the Magento platform, PIM solutions on either inRiver Product Marketing Cloud or Akeneo open source platform, and also delivers solutions within Adobe Experience Cloud. Vaimo has hundreds of clients representing the eCommerce arms of world-class, renowned consumer brands such as Jack Daniel's, Dyson, Helly Hansen, TOUS, and Jaguar — to name just a few. Vaimo's international staff — distributed among 21 global offices in 13 countries — is composed of highly knowledgeable professionals with expertise in

commerce strategy, design, and technology.
To support such an extensive client array, Vaimo fields a hybrid cloud-computing architecture comprised of more than 1,000 Linux servers spread among numerous global data centers. These servers run a variety of open source software solutions such as Apache and MySQL. Vaimo is also integrating its computing environment with Cloudflare to provide a reliable, faster, and more secure user experience. All of these assets generate tremendous volumes of machine data, chiefly representing operational and diagnostic details.

Vaimo continually seeks to improve all aspects of its operations, especially security. With operations in many countries, Vaimo is also subject to increasingly stringent regulatory obligations. Vaimo's executive leadership understood that applying state-of-the-art technology – including solutions that could unlock the potential of machine data – would not only address these challenges, but could also supply a competitive advantage versus rivals that did not share this strategic vision.

Vaimo's evaluation team evaluated a number of solutions over a two-month period and concentrated on these key factors when scrutinizing potential machine data management products:

- **Flexibility.** Vaimo has a unique environment and it was important that any chosen technology be capable of conforming to it.
- **Direct access to machine data.** Authorized users needed to be able to construct powerful queries without soliciting assistance from IT.
- **Reporting and visibility.** Pre-built dashboards, reports, and other visual aids would give Vaimo a head start towards identifying and correcting issues.
- **Integration with other tools.** The company uses a battery of technologies to manage its operations, such as Frenzy for filtering; the selected solution needed to work well with other packages.
- **Automation.** Vaimo wanted to specify events that would in turn automatically trigger scripts to resolve the issues uncovered by these incidents.
- **Ease of adoption.** The company was insistent that the new solution be smoothly and quickly deployed, with no user impact or disruption.

Upon concluding this comprehensive appraisal, Vaimo's experts determined that Sumo Logic satisfied these criteria better than the other alternatives that had been under consideration.

Vaimo launched its Sumo Logic rollout to address two initial use cases:

- Collecting alerts that would then trigger automated reactions.
- Troubleshooting potential problems by monitoring deviation from standard operational patterns.

Choosing Sumo Logic has been a successful, positive experience for Vaimo. It's benefited diverse constituencies, both within the company as well as for its clients. From the clients' perspective, Vaimo's improved machine data utilization has bolstered the defenses for their eCommerce implementations by hindering spam and other security breaches.

Internally, the automation offered by Sumo Logic has resulted in far fewer time-consuming, manual tasks. Vaimo's administrators and developers now enjoy a clearer, more logical view of the company's machine data that yields advantages throughout the organization. For example, when software developers recognize that something has gone awry with an application, they not only examine their application logic, but now also consult Sumo Logic to evaluate the contents of critical logs. Prior to Sumo Logic, this would have required laboriously connecting to multiple production servers and then combing through individual log files to help uncover the problem.

> **"We're no longer flying blind: applying Sumo Logic to our machine data has given us much better insight into what's happening on our clients' eCommerce sites."**
>
> **Fred Vaurs**
> Security Officer

From the administrative perspective, Sumo Logic has revolutionized the issue detection and correction process. Its machine learning-based pattern recognition makes it possible to compare a given user's historic interaction with a key resource and provide an alert if a deviation takes place. Sumo Logic's graphs, dashboards, and other visual evidence have eradicated extensive manual procedures, delivering actionable results more quickly and efficiently. It's also now much harder for spammers to disrupt Vaimo's clients: Sumo Logic can detect spikes in unusual activity from the same IP address and then automatically take countermeasures, such as blocking that address. The same automated evaluations are applied when consumers create accounts on Vaimo's clients' websites, eliminating the need to annoy them with CAPTCHAs.

Vaimo's operational security management is also more effective than before. Since machine data has been captured and centralized within Sumo Logic, there are notably fewer instances where an administrator must connect to a production server to examine logs. In those cases where it is necessary to work with a live server, Sumo Logic reports on the specific actions taken by the user. This means that Vaimo's security team is no longer "flying blind": they have full insight into what's happening on their servers as well as all alerts that are generated by Sumo Logic.

Today, Vaimo's security team is the primary Sumo Logic user, with the IT organization employing it to a lesser extent. However, this has laid the groundwork for more ambitious undertakings later. Going forward, Vaimo may elect to track additional security-centric events and then eventually ingest and maintain application logs. This would further cement Sumo Logic's role as a single point of truth that would be relevant for both application and security concerns. Finally, Vaimo may ultimately incorporate third-party cloud providers; Sumo Logic is already well equipped to cope with these new platforms and machine data formats without disrupting any users or internal processes.

About Vaimo

Vaimo is one of the leading solution providers on Magento Commerce and the core of our offer is drawn from the platform. As a Magento Global Elite Partner we can guarantee you'll be working with some of the most knowledgeable experts within omnichannel, webshop, and commerce. Our focus on strategy, design, and technology makes Vaimo a first class partner for digital solutions and commerce within both B2B and B2C. For more information visit www.vaimo.com.

About Sumo Logic

Sumo Logic is the leading cloud-native, machine data analytics platform that delivers continuous intelligence across the entire application lifecycle and stack. More than 1,600 customers around the globe rely on Sumo Logic for the analytics and insights to build, run, and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value, and growth. For more information, visit www.sumologic.com.

su
mo
sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com