sumo logic

Endowus gains unified visibility and reduces alert fatigue with Cloud SIEM

Results at a glance

- → 90% reduction in alert investigation time
- → Detected and mitigated phishing incident early on before significant damage was done
- → Eliminated alert fatigue and improved overall employee satisfaction by filtering out noise
- → Greater visibility into cloud-native environments with deep, actionable insights
- → Centralized security operations with a unified Cloud SIEM platform for better threat detection and response

Endowus

PRODUCTS

Cloud SIEM

Sumo Logic Platform

USE CASES

Threat detection, investigation, and response

Challenge

Endowus needed to enhance its security posture, streamline tools, and reduce alert fatigue.

When Endowus began building its security stack three years ago, it quickly experienced significant tool sprawl. With various security tools implemented, including email security and data loss prevention solutions, alerts flooded in from multiple sources, creating an overwhelming volume of pings and notifications. On top of that, the security team had to constantly monitor and fine-tune alerting systems across multiple dashboards, making security management complex and time-consuming.

To regain visibility and improve efficiency, Endowus' Head of Information Security, Alvin Lim, was on the search for a Cloud SIEM solution that could unify its security tools into a single, centralized platform.

Solution

After speaking with three different logging solutions and conducting a proof of concept (POC) with two, they ultimately chose Sumo Logic for three key reasons: its ease of integration, maintenance, and advanced alert tuning.

Easy integration with existing tools

Sumo Logic's cloud-native architecture made it simple for Endowus to integrate its key data sources, including AWS, SentinelOne, Google Workspace, and their secure web gateway. Unlike other vendors requiring complex setups and additional workarounds, Sumo Logic streamlined log ingestion and continuous visibility across their security environment.

"The other vendor we evaluated wasn't cloud-native which meant more hoops to jump through to ingest log data properly. Ever since implementing Sumo Logic, integration has been seamless," Lim says.

Endowus

INDUSTRY

FinTech

ABOUT

Endowus is an award-winning independent fee-only wealth and fund platform. Licensed in Singapore and Hong Kong, Endowus is the first digital advisor in the region to span private wealth and public pension. They proudly serve as a fund investment platform and fiduciary advisor to over 250,000 individuals, family offices, charities, endowments, and institutions.

WEBSITE

endowus.com/#sg

Alert tuning and reduced investigation time

Before Sumo Logic, the team was overwhelmed by alert fatigue and spent roughly an hour investigating each alert. Thinking about the days before implementing Sumo Logic, Lim says, "We'd get flooded with alerts that we didn't know were actionable or not, which gave the team lots of anxiety as we didn't know if it needed to be escalated. With Sumo Logic, we have clear insights into what's happening, and our investigation time has dropped."

Cloud-native flexibility and scalability

As a lean team of two engineers, Endowus needed a solution that was easy to manage without adding unnecessary overhead. Sumo Logic's intuitive Platform, out-of-the-box (OOTB) rules, and automated rule maintenance meant that even team members without deep technical expertise could contribute to security operations.

Strong ROI and justifiable investment

For Endowus, cost-effectiveness was key to choosing the right security solution. Beyond features and capabilities, the ROI needed to be justifiable. Sumo Logic stood out not just for its comprehensive security offerings but also for its reasonable pricing compared to alternatives.

Lim also leveraged Sumo Logic Flex Licensing, so his costs were based on insights and analytics volume rather than data ingestion to scale with his evolving needs. This flexibility allowed them to scale up or down as their use case changed and adapt to new requirements while keeping costs under control.

"Budgetary approvals for new tools can often be challenging. As security leaders, we must advocate for investments we believe in. Sumo Logic made logical sense as we could see the value of the service," Lim said.

CUSTOMER EXPERIENCE

We'd get flooded with alerts that we didn't know were actionable or not, which gave the team lots of anxiety as we didn't know if it needed to be escalated. With Sumo Logic, we have clear insights into what's happening, and our investigation time has dropped.

Alvin Lim
Head of Information Security
Endowus

Results

90% reduction in alert investigation time

With Sumo Logic Cloud SIEM, the Endowus team can quickly identify suspicious activities, reduce false positives, and ensure every alert is actionable. Before, they spent an hour investigating each individual alert. Now, benign alerts are resolved in just five to ten minutes, allowing the team to focus on real threats.

Improved incident detection and response

By eliminating data silos, Endowus has a comprehensive viewof their security landscape, helping them trace attack vectors and identify root causes of incidents.

In one instance, Sumo Logic helped Endowus detect a phishing incident early on before it became impactful. By integrating data from Endowus' various tools, the team quickly identified suspicious behavior and mitigated the threat before it caused any significant damage.

Reflecting on this incident, Lim notes: "Thanks to Sumo Logic, we detected the attack's source early and took action before any real harm was done. Plus, with all the additional tools we had ingesting into Sumo Logic, we also assessed the full extent of the damage and mitigated it quickly."

Sumo Logic's user-friendly, game-like dashboard helps Endowus' security team easily track the progression of incidents and connect the dots between various data points. Even non-technical users can easily navigate the system, making investigations quicker and more efficient.

BY THE NUMBERS

90%↓

alert investigation time

CUSTOMER EXPERIENCE

Thanks to Sumo Logic, we detected the attack's source early and took action before any real harm was done. Plus, with all the additional tools we had ingesting into Sumo Logic, we also assessed the full extent of the damage and mitigated it quickly.

Alvin Lim
Head of Information Security
Endowus

Lim said, "The Sumo Logic Platform is visually appealing and responsive, making it easy to manage, process and analyze large amounts of data. This minimizes lag, which can cause friction in the process. The entire Sumo Logic UI was super responsive, kept us engaged, and helped keep the momentum going."

Customized alert management for tailored risk appetite

Endowus leverages Sumo Logic's customizable alert management features to align security monitoring with its unique needs better. By tweaking thresholds for different data sources, Endowus minimizes alert fatigue and ensures that alerts they receive are actionable and meaningful.

Lim explains, "We wanted to be able to tweak thresholds for each tool and data source to align with our risk appetite. For example, we track user behavior in Google Drive to ensure teams can be flexible without compromising security. If a user downloads sensitive data excessively within a short period, we're alerted and can investigate immediately."

In the future, Lim also hopes to explore Sumo Logic's UEBA and other AI-powered features to enhance their alert management with automation and AI.

"Just from adjusting the thresholds manually, we've already seen improvement in alert quality. We're excited to explore the potential of Sumo Logic's AI features to make our process more efficient. These features will empower our security team to identify, resolve, and remediate potential threats. We want to ensure we increase our coverage and remediate sooner, and I'm extremely happy to see that Sumo Logic is building out features like this to ensure we meet our goals."

Increase in employee satisfaction

Overall, Endowus found that team satisfaction has increased since implementing Sumo Logic. Since the shift to Sumo Logic, Lim notices that security operations are more efficient and there's an increase in team morale.

CUSTOMER EXPERIENCE

We're excited to explore the potential of Sumo Logic's AI features to make our process more efficient. These features will empower our security team to identify, resolve, and remediate potential threats.

Alvin Lim
Head of Information Security
Endowus

"There's less frustration," Lim said. "Before, we'd have to look through six or seven alerts, with five of those being unhelpful. That's no longer the case with Sumo Logic. It's helped uplift the team, who are eager to explore the service's capabilities. It's empowering them to do their jobs better."

Better visibility and peace of mind

Before adopting Sumo Logic, Endowus faced a significant challenge. They had a lack of visibility into AWS security alerts which made it difficult for the security team to conduct thorough investigations, and often, they felt a lingering sense of uncertainty.

"Previously, we were overwhelmed," Lim recalled. "Multiple alerts were coming in, and not being able to address them gave us a sense of unease. Even more worrying was the possibility that there were real threats slipping through that we couldn't detect."

Sumo Logic changed everything. By piping AWS Cloudtrail logs into Cloud SIEM, Endowus has deeper visibility into security events without having to manually maintain complex rule sets. With Cloud SIEM automatically correlating alerts with security frameworks, like MITRE ATT&CK, Endowus receives actionable insights into what has occurred and what could potentially happen, along with remediation steps to mitigate risks.

"Sumo Logic helps us accelerate impact by identifying impactful findings and showing us a clear path to investigation and remediation, all delivered through a streamlined, consolidated Cloud SIEM platform," said Lim.

CUSTOMER EXPERIENCE

Before, we'd have to look through six or seven alerts, with five of those being unhelpful. That's no longer the case with Sumo Logic, and it's made a big difference in the overall happiness of the team. The team is excited to dig into findings and Sumo Logic's capabilities. It's empowering them to do their jobs better.

Alvin Lim
Head of Information Security
Endowus

Simple onboarding and ongoing support

Despite having little prior experience with Sumo Logic, Endowus quickly ramped up with the support of Sumo Logic's customer success team. From the initial POC to full implementation, they benefited from hands-on support, in-person training, and Sumo Logic certification programs, helping them maximize Sumo Logic's full capabilities.

He notes, "We started with little to no experience working with Sumo Logic, but it wasn't difficult for us to learn things with the support of Sumo Logic's customer success team. The customer success team acted as an extended version of our team, helping us fully get up to speed quickly."

Lim highlighted that he recommends Sumo Logic to other security leaders for a variety of reasons, "The ROI with Sumo Logic is extremely high. You get value for every dollar you spend. More importantly, it provides peace of mind, knowing you have the ability to perform deep forensic investigations when needed. It's a powerful tool that helps you achieve your security goals. It's a well-valued tool with a full suite of features, Sumo Logic ensures that your key security success criteria are met."

CUSTOMER EXPERIENCE

We started with little to no experience working with Sumo Logic, but it wasn't difficult for us to learn things with the support of Sumo Logic's customer success team. The customer success team acted as an extended version of our team, helping us fully get up to speed quickly.

Alvin Lim
Head of Information Security
Endowus

Read more about other customer successes — from retail to healthcare to fintech here.

Learn More
Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700

sumologic.com

855 Main Street, Redwood City, CA 94603