sumo logic | Continuous Intelligence Platform™

CASE STUDY

Cloud SIEM is central to PACCAR's mission to modernize security operations

Challenge

PACCAR is a Fortune 500 company and a global technology leader engaged in the design, manufacture, and customer support of premium light-, medium- and heavy-duty trucks under the Kenworth, Peterbilt, and DAF nameplates. PACCAR also designs and manufactures advanced diesel engines, provides financial services, information technology, and distributes truck parts related to its principal businesses. PACCAR serves customers worldwide through an extensive dealer network in over 2,200 locations in 100 countries. Half of their revenue comes from outside the United States, and they are constantly expanding—now rolling out their dealer network into Asia and the rest of the world. In 2020, the company grossed $18.7 billion and netted $1.3 billion.

Scott Ashlock, SOC Manager, PACCAR discusses security modernization using Cloud SIEM. Watch now

As a technology leader in their space, security is top of mind for PACCAR. They have a sophisticated security organization divided into three divisions—Global Security Operations, Global Information Security, and Vehicle Security.

PACCAR's Global Security Operations division comprises their North America and Europe Security Operations teams and the Access Management and Information Security teams.

Company

PACCAR

Industry

Manufacturing

Environment

Hybrid with a mix of on-prem and public cloud

Sumo Logic Products

Sumo Logic Cloud SIEM

Use cases

Modernizing Security Operations

Results

Gained go-to strategic partner for security modernization and digital transformation

Increased security operations efficiency through powerful search and log management tools

Reaped cost savings from cloud-native SIEM solution

Over the past several years, PACCAR has been on a mission to optimize and grow its security program. They've been hard at work consolidating vendors and tools, and improving security capabilities to protect org and customer data. One of the key goals was to reduce their tooling without compromising security. PACCAR identified overlaps that cost them money and resource availability for their team. They reduced vendors and tooling for web proxy replacements, enhanced detection and response, and identity and access management, allowing them to standardize their global process, improve security and save on costs. The introduction of passwordless pilots through Windows Hello also helped them mature their security program, improve their security posture, and provide options for their internal customers.

Among the primary initiatives in their campaign to optimize their security program was searching for a new Security Information and Event Management (SIEM) solution. In 2015, PACCAR engaged a provider to implement an on-premises SIEM solution alongside managed SOC services for their on-premises environment. After six years with this legacy SIEM provider, several pain points couldn't be overcome. Replacing aging infrastructure would be costly, and through the years, they needed one full-time employee (FTE) in each of their North America and Europe locations just to maintain the environment. Above all, they wanted a strategic relationship with a vendor, not just a service provider. The vendor they were using didn't fit that profile.

They evaluated seven cloud-based SIEM solutions in the market, including the one offered by their existing on-prem SIEM provider.

> **"What set Sumo Logic apart from the rest was the speed at which we could search. It was incredible, and Sumo Logic beat out every other vendor by a large margin. The speed alone increases the efficiency of our investigations and saves us countless resource hours."**
>
> **Scott Ashlock**
> North America Security Operations Manager, PACCAR

Solution

After conducting an extensive proof of concept process with seven cloud SIEM providers, PACCAR chose Sumo Logic Cloud SIEM.

Cloud SIEM checks all the boxes for PACCAR: cloud-native, integrated with their environment and existing tools, reduced the need for disparate SIEM tools, met all their use cases, and provided value from the beginning. "Sumo Logic hit all of our needs, wants, and desires hands down. It was pretty much a no-brainer," Scott Ashlock, PACCAR's North America Security Operations Manager, shared.

Results

PACCAR now uses Sumo Logic as their cloud-native SIEM solution.

Scalable and flexible cloud-native solution
PACCAR's decision to switch to Sumo Logic Cloud SIEM eliminates the need to allocate significant resources to hardware due to aging and as their needs evolve. This is in line with PACCAR's overarching goal of consolidating their tooling and reducing the assets they need to maintain on-site with corresponding FTEs. Sumo's scalability also affords them flexibility as they grow their business worldwide.

Integration with existing tools and architecture
With their detailed campaign to modernize their security program, Sumo Logic's ability to integrate with PACCAR's existing tools and architecture is critical. With Sumo Logic's API-first product principle and broad integration with solutions in the market, PACCAR is assured they can continue to reap the benefits of Cloud SIEM as they make improvements in their tooling and environment.

Strategic partnership and stellar customer service
PACCAR specifically wanted a vendor with whom they could form a strategic partnership. From the POC process to onboarding and implementation, Sumo Logic has gained PACCAR's trust by providing excellent support every step of the way. PACCAR now counts Sumo Logic as a go-to partner in maintaining the security of their systems and as a trusted resource for recommendations in improving their security program and environment. Transparent and constant communication has been key to this strong relationship.

Improved efficiency with modern log management and powerful search capabilities

Using the log management capabilities of Cloud SIEM, PACCAR boosts productivity through automated security workflows that eliminate the need to conduct manual tasks like data collection and correlation. Sumo's deep search capabilities and robust integration with PACCAR's existing response platform save them valuable time and resources in parsing logs, and drastically shortening the time to action compared to their previous practices.

Pricing value that fit PACCAR's strategy

Sumo Logic's pricing aligned with PACCAR's budget criteria, which was a crucial piece in their decision-making. However, beyond the immediate cost savings of moving to a cloud solution at the end of life of their previous on-prem SIEM hardware and software, PACCAR enjoys immense value in Sumo Logic's capabilities as a solution provider and as a strategic partner. Cloud SIEM lines up with its goal of consolidating and streamlining security tools. Sumo's domain expertise in modern security and cloud analytics provides an important source of knowledge in PACCAR's digital transformation.

Next steps

PACCAR's Security Operations team is in the process of maximizing their use of Cloud SIEM's advanced features and will be looking at utilizing Sumo Logic to aid with additional logging functions across the broader organization. Sumo Logic is committed to providing value as a strategic partner as PACCAR continues its digital transformation and fine-tuning its security program to find points for improvement and modernization.

> **"Sumo Logic Cloud SIEM drives value. It's a great product that leverages our existing environment and integrated well with everything."**
>
> **Scott Ashlock**
> North America Security Operations Manager, PACCAR

About Sumo Logic

Sumo Logic is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy.

For more information, visit www.sumologic.com

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

www.sumologic.com