As one of the longest-standing carmakers in the world, CarCo has a proven pedigree amongst consumers and auto enthusiasts for quality and performance. And despite manufacturing cars for over 100 years, it is still one of the most innovative car manufacturers today. As evidence, the company is rapidly addressing global carbon neutrality goals with the introduction of CarCo AUTO DigiLab, an innovation hub which focuses on next-stage mobility and digitalization.

The team is helping CarCo expand its line of electric compact vehicles, family SUVs, and electric scooters via its subsidiary. This expansion to a modern model portfolio has not only transformed the company’s engineering prowess, but also ignited a digital transformation to deliver additional value and service to their customers. However, as most enterprises quickly discover, digital transformation isn’t achieved without risk.

CarCo Turns to Noname Security for Comprehensive API Protection
The Problem

Though apps get most of the credit, application programming interfaces, or APIs, provide the underlying connectivity in this new era of devices, applications and online services. APIs enable organizations to streamline workflows, develop new ways to support customers, and pursue new avenues to drive profit. And when you consider this breadth of connectivity, it’s easy to see how APIs also unfortunately expand an attack surface. The evidence clearly illustrates just how lucrative an attack vector APIs can be.

In 2022, 76% of cybersecurity professionals admitted to experiencing an API security related incident. And according to Imperva’s Quantifying the Cost of API Insecurity report, US businesses incurred upwards of $23 billion in losses from API-related breaches in 2022. This reality can be attributed to the fact that APIs present unique vulnerabilities that traditional tools like API gateways and web application firewalls can’t address. Which is why CarCo partnered with Noname Security.

Though fortunately not the victim of an attack, CarCo wanted to get a firmer grip over their API landscape. Given how vital APIs are to their product and service roadmap, the company saw this endeavor as equally vital to business growth as it was to maintaining current operations. And rightly so. On average, Noname Security uncovers 30% more hidden APIs than customers originally anticipated. Which illustrates the critical role API discovery plays in maintaining a robust security posture.

The Solution

After engaging with the Noname Security team, the two sides agreed to conduct a pilot with the subsidiary, with the goal of cataloging and classifying their APIs. The scope also included monitoring their environment for any notable misconfigurations, vulnerabilities, traffic anomalies, or exploitable external attack paths. The company required a self-hosted deployment in their AWS environment, a feature which many API security vendors don’t offer. Within just 30 minutes the Noname API Security Platform was deployed, and within 20 minutes after deployment, the platform was fully integrated with the subsidiary’s AWS API gateways.

As anticipated, the Noname API Security Platform was able to provide complete visibility into the subsidiary’s API landscape. With this dynamic inventory, the company has a single source of truth and can detect dormant, legacy, and zombie APIs across its digital ecosystem. The subsidiary can now also track API changes and user access, plus get alerts when changes violate company-defined policies or industry best practices. This includes authentication. The Noname platform identifies the authentication methods for each API, as well as the absence of authentication or misapplication when compared to best practice.
Ultimately, the platform provides the subsidiary with actionable insights and more control over its API security posture.

In terms of vulnerabilities, the platform uncovered a few abnormal behaviors and unfamiliar users that prompted the CarCo security team to conduct further investigation. Despite these minor security flaws, there were none that would cause immediate alarm or infer that they had been exploited. And though the pilot did not reveal a compromise, it is safe to say that it was still extremely valuable. The Noname platform located hundreds of both production and pre-production APIs, as well as classified tens of data types throughout the environment.

Moving forward

The subsidiary pilot was a testament to the forward thinking and market leadership CarCo has exhibited during the last hundred years, as API security is emerging to be a top priority for automakers. As evidence, a team of researchers led by revered bug-bounty hunter Sam Curry, recently discovered critical API flaws across the automotive industry. The list of offenders included world-renowned automakers, such as KIA and Ford. Unsurprisingly, Sam’s team found APIs that exposed sensitive customer data, such as their address, credit card info from sales quotes and VIN numbers—information with obvious implications for identity theft.

These exploited API vulnerabilities could also expose vehicle location or enable hackers to compromise remote management systems. Meaning cybercriminals would have the ability to unlock vehicles, start engines or even disable starters altogether. With that said, Noname Security is encouraged by the partnership with CarCo thus far and look forward to expanding our relationship as their API security needs evolve.

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope — Discovery, Posture Management, Runtime Protection, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in Tel Aviv and London.