Forcepoint

Customer Story

At This Cutting-Edge Automotive Supplier, Intellectual Property Protection Has Kicked into High Gear

GG Group heads off the risk of losing not just its own intellectual property, but that of its high-profile automotive clients.

The highly competitive automotive industry is now in the midst of an even more heated race—toward the newest and most effective electric technologies for connected cars and autonomous driving. With a history as a rich target for corporate espionage, the auto industry has many documented examples of employees exchanging trade secrets for personal gain. GG Group, a global manufacturer of automotive and industrial technological solutions, has chosen Forcepoint amongst peers to safeguard data and intellectual property in order to retain customers' trust as they innovate.

CUSTOMER PROFILE:
One of the leading suppliers of cables and wires across several sectors, including automotive, industry, and elevators, and has more than 4,000 employees in nine countries.

INDUSTRY:
Manufacturing

HQ COUNTRY:
Austria

PRODUCT:
Forcepoint Data Loss Prevention

Rapid advancement and increased competition in the electric vehicle market is putting leading automotive companies' intellectual property (IP) at risk. Third-party suppliers like GG Group, which automakers rely upon for some of the most critical components of their proprietary technologies, have more than just their own IP to protect. As a trusted partner, GG Group has access to and collaborates with high-profile clients on highly valuable proprietary schematics and development plans.

With collaboration on a global scale, this sensitive, proprietary data is frequently on the move. Realizing data in motion can be difficult to see and control, GG Group needed a better way to secure it. And as the company expanded into countries with a known high risk of IP theft and corporate espionage, it wanted to ensure proprietary data was locked down. The breach of just one client's IP could mean the loss of every clients' trust—hurting GG Group's reputation and its bottom line.

> "Identifying the vendor that understands the value of IP and offers innovative, scalable, and adaptive data loss prevention was key."
>
> **CHUKS OJEME,** CISO, GG GROUP

"You can imagine that if critical data stored in GG Group custody is compromised, the company would lose its reputation with the customer and in the marketplace, " said Konrad Langhammer, Forcepoint Account Executive. "Announcing that the data has been stolen would mean other car manufacturers would know, putting GG Group's business at great risk."

The company's security team knew it needed to double down on data protection for its own benefit as well as its clients'.

"For me as the CISO, it is very important that we understand the internal requirements to protect our critical information. Identifying the vendor that understands the value of intellectual property to a manufacturing company and offers innovative, scalable, and adaptive data loss prevention was a key success criteria for the project," explained GG Group CISO, Chuks Ojeme. "We found that Forcepoint is that vendor."

Catching risky users and spies on a global scale

To meet these challenges, GG Group explored several data loss prevention solutions. However, only Forcepoint's solution was able to meet the requirements the company deemed necessary to catch risky users in action and stop corporate espionage. In particular, Forcepoint demonstrated its data loss prevention solution could be tuned specifically to discover data types such as source code, engineering drawings, sensitive trade secrets, and other data the company identified as "crown jewels".

To address the risks of international expansion, Forcepoint's solution provides encryption for data as it moves outside the organization and across more than 80 countries. For example, with Forcepoint's centralized policy management, GG Group is able to increase international control by applying customized policies from a single console, even to distributed locations.

Challenges

Protecting its valuable IP and that of its high-profile clients across its corporate and international locations.

Visibility to risky activity, indicating corporate espionage.

Approach

Gain greater visibility and control of critical data with Forcepoint Data Loss Prevention (DLP).

Implement pre-defined policies with the DLP to help IT team meet compliance needs.

Forcepoint expert support in developing organizational policies to guide DLP customization.

Reducing voluntary data movement to decrease risk

GG Group is now confident with the precautions in place to keep automakers' proprietary data safe. But, to be truly effective, data protection policies can't revolve around technology alone—they have to be a part of a larger organizational strategy for data protection, specifically, and cybersecurity in general.

Forcepoint worked closely with GG Group to develop the organizational priorities and strategies that would guide, and serve as the foundation for, customized data protection policies that meet the company's unique needs.

For example, Forcepoint helped GG Group build in features such as self-remediation to educate users on good data hygiene and monitoring their resulting data interactions. This enables the organization to identify its riskiest users in seconds—providing early warning of data sharing policy violations and potential instances of corporate espionage.

Elevating data security to a business strategy with continued partnership

With the initial roll-out focused on high-risk geographic areas, Forcepoint will continue to support a broader deployment to additional locations to further enable secure collaboration among GG Group's staff and its clients. The organization is also exploring the addition of web, email, behavioral analytics, and mobile agent integration technology.

"A holistic, integrated cybersecurity portfolio with Forcepoint would provide GG Group with a full compliance picture," explained Langhammer. "This can be audited and can show the organization's partners that the company is a big player."

And a continued partnership between the enterprise and Forcepoint will support GG Group as it further develops its organizational policies and fine-tunes the DLP solution to match. "A DLP project is never really finished. You have to create new rules, follow policy changes, new requirements within the company and for customers, and so on," said Langhammer. "So Forcepoint will be there as a trusted partner to help the organization keep the DLP product aligned with the business."

Results

DLP policies customized for GG Group's data protection and compliance needs, constantly fine-tuned in response to organizational policy changes.

Ability to apply different policies to different locations, all from a single console.

Reduced data movement with educational pop-ups that educate users on good data hygiene—thereby reducing risk.