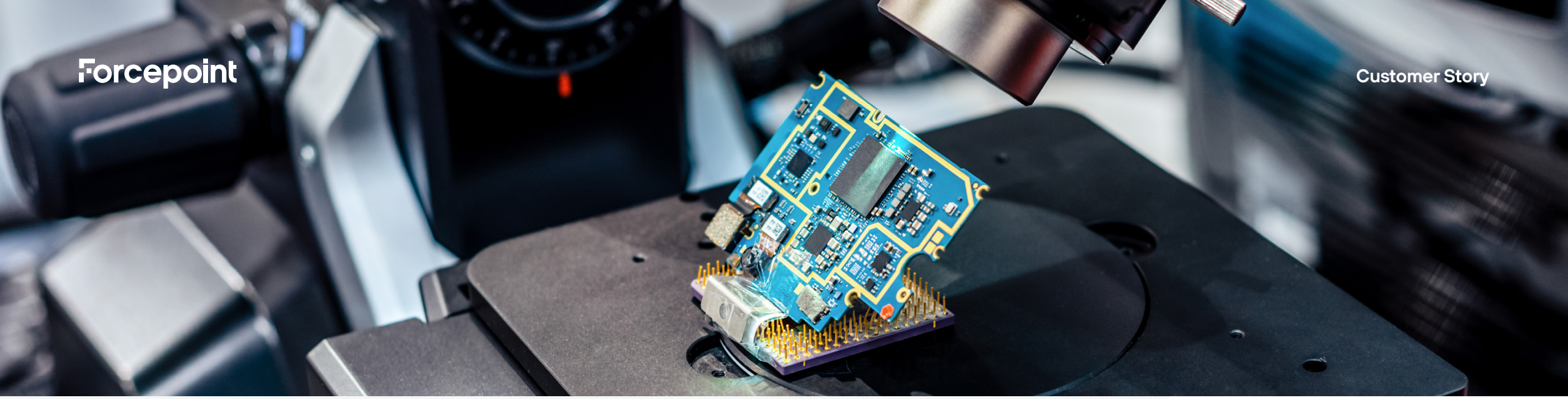

Forcepoint

Customer Story

Semiconductor Company Relies on Forcepoint to Keep the Competition Guessing About Next-Gen Mobile Devices

This leading maker of AMOLED display driver chips must keep its product designs, roadmaps, and foundry contract information away from prying eyes to keep thriving in the semiconductor market.

This semiconductor company runs a billion-dollar computer chip foundry while also specializing in designing its own analog and mixed-signal non-memory semiconductors. The chip maker must protect its own intellectual property (IP) and product roadmap plans from theft or leaking by internal threats, while also safeguarding critical information about what its processor and foundry customers are planning for their own product portfolios. The theft of even a snippet of information about future products is a risk this company must take seriously, so the company depends on Forcepoint to protect against data loss.

CUSTOMER PROFILE:
Designer and manufacturer of analog and mixed-signal semiconductor platform solutions.

INDUSTRY:
Manufacturing

HQ COUNTRY:
South Korea

PRODUCTS:
- Forcepoint Data Loss Prevention (DLP)
- Forcepoint Insider Threat (FIT)

The semiconductor business is tricky to navigate in the best of times. The upfront costs of running a chip foundry like this chip maker's fabrication facility in South Korea are immense—billion-dollar plans for upgrading equipment and retooling process technologies must be greenlighted and paid for years in advance of any return on investment. A steady stream of customers must be kept on board to ensure that capacity manufacturing doesn't flag or losses could run into the tens of billions.

The stakes couldn't be higher when it comes to ensuring that information about its own product plans and those of its customers aren't leaked to competitors or the press. The company counts some of the most high-profile makers of market-leading smartphones and tablets among its clients. It can take months and even years to bring a coveted consumer device like a new iPhone or Galaxy smartphone from the drawing board to a gala unveiling in front of an excited audience. There must be secrecy each step of the way, and the company does not want to develop a reputation as a weak link in the process.

The chip maker also has its own design business to protect from prying eyes. The company has an ongoing partnership with major mobile device makers to invent the next generation of touchscreen display technologies, with applications expected to extend further to areas like automotive and Internet of Things (IoT) user interface (UI) designs.

Countering insider threats

In the past, companies focused on external breaches as the main threats to their data security. But in recent years, this chip maker came to realize that protecting its data from outside threats wasn't enough in an industry where even small snippets of privileged information can be worth their weight in gold. The company was increasingly concerned about exfiltration threats—the risk of data loss through accidental or malicious actions by employees inside the company.

It wanted to address the threat of data loss by insiders in two ways:

- → To better identify and block exfiltration events in a preventative fashion.
- → To produce forensics for better identification of how exfiltration events happened after the fact.

At the same time, the information security team required a data loss solution that would "play well" with the rest of its security software products and minimally interfere with employee productivity and workflow, explained the company's business solution team lead.

"The most important consideration was to find a system that can monitor user systems to predict potential data loss incidents, be compatible with existing PC security software, and not undermine company-wide workforce performance," he said.

An exfiltration solution that ticks off all the boxes

The company tasked security vendors with providing a proof of concept (POC) to demonstrate their data loss prevention capabilities and ability to catch and record activities by insider threats. The South Korean chip maker selected Forcepoint Data Loss Prevention (DLP) and Forcepoint Insider Threat (FIT) to safeguard against data exfiltration.

The major reasons for the selection included:

- → Forcepoint's high performance scores in the POC compared to rival vendors.
- → The compatibility of DLP and FIT with other IT platforms, apps, and tools in use.
- → The intuitive dashboard UI for managing DLP, which enables an administrator to assess risk factors at a glance with Incident Risk Ranking (IRR) and adjust policies as needed.
- → The minimal impact of DLP and FIT on employee communications and workflow.

Challenges

Better identify and prevent data exfiltration.

Produce forensics to record and document exfiltration activity.

Approach

Implement Forcepoint DLP and Insider Threat.

> "Forcepoint's solutions truly stand out due to the human-centric management interface design."
>
> **TEAM LEAD,** SEMICONDUCTOR COMPANY

"Forcepoint's solutions truly stand out due to the human-centric management interface design. As user risk is analyzed and prioritized, we can manage each user differentially by risk level, saving time and effort for our security admins," the team lead said.

Analyzing human behavior to dynamically deter data loss

The company was also convinced that the combination of Forcepoint Insider Threat and DLP would provide the granular visibility into high-risk activity to help identify indicators of compromise such as stolen user credentials, privileged credential abuse, and even unintentional user mistakes that could lead to data loss.

One recent example of how the solution has protected the company occurred when an employee accidently clicked on an email link leading to a ransomware attack. Using FIT's forensic features, the chip maker and Forcepoint were able to identify the user and discover the root cause and context of the accident, enabling the company to make adjustments and prevent another similar incident.

Security products from other companies typically apply permission/blocking policies for user and device actions based on a whitelist/blacklist system. Unlike its competitors, Forcepoint DLP provides a behavior-based basis for decisions to flag or block activities with adjustable, pre-set policies for user and device actions according to a ranking of how risky an incident is via the IRR feature.

Smartphone secrets kept safe

The end result is that the company has leveraged Forcepoint's solutions to implement a system that can predict and respond to potential data loss incidents in advance by monitoring user systems, while also providing forensics to better understand how such events occur, a crucial tool for preventing data loss in the future. The compatibility of DLP and FIT with existing systems added even more value, according to the company's IT security team.

"Thanks to Forcepoint, we were able to implement a solid security control system with limited resources. Although there are a wide variety of endpoint environments at our company, we succeeded in applying the solutions with almost no conflict or noise," the team lead said.

"There have been almost no issues with compatibility, performance, business delay, or conflict. Both our IT administrators and users are satisfied, and based on this exemplary case, we are considering applying it to our other operations around the world."

Results

A solid security control system implemented with almost no conflict or noise, with limited resources.

Forcepoint