ProjectDiscovery

CASE STUDY : factorial

How Factorial Scaled Continuous Security Coverage Across a Fast-Growing Cloud Footprint

Factorial's security engineering team partnered with ProjectDiscovery to keep coverage ahead of a broad and dynamic external attack surface.

About Factorial

Factorial is a fast-growing HR software company headquartered in Spain. As the company has grown, so has its infrastructure, with an external attack surface that spans a broad and dynamic cloud environment. Factorial's security engineering team is responsible for protecting that surface, and it approaches the work the way you would expect from engineers: hands-on, technical, and focused on outcomes.

The Challenge: Keeping Coverage Ahead of Growth

When a company grows quickly, its external footprint grows with it. New services ship, cloud environments expand, and the attack surface becomes broader and more dynamic over time. For Factorial's security team, the priority was making sure coverage scaled proactively alongside that growth, so that visibility stayed ahead of the pace of the business rather than trailing behind it.

Running and maintaining home-grown scanning infrastructure was one way to get there, but it carried overhead the team preferred to avoid. Standing up and securing virtual machines and keeping templates current consumed engineering time that was better spent on security itself. As Factorial's Engineering Manager of Security put it, the question was less about the hours saved by not building the solution in-house, "but more of how much I reduce the window between introduction and discovery."

The team also wanted automated coverage to handle the routine, predictable findings, so that its bug bounty program and its own researchers could concentrate on the novel, higher-value work that automation cannot replace.

What They Were Looking For

Factorial's team evaluated several attack surface management platforms before making a decision. Their criteria were specific, shaped by the fact that they are, at their core, a technical security engineering team.

They wanted low false positive rates, the ability to write their own templates and rules, and full transparency into how findings are generated rather than outputs they could not inspect. They also wanted coverage for new vulnerabilities to be available immediately, not gated behind a vendor's quarterly release cycle. Several platforms fell short on one or more of these points, whether through false positive rates that were too high to be operationally useful or a black-box approach that offered little visibility into how results were produced. For a team that values technical depth, giving up that visibility would have felt like a step backward.

> *For a team that values technical depth, giving up that visibility would have felt like a step backward.*

Why Factorial Chose ProjectDiscovery

What stood out about ProjectDiscovery was not a feature list. It was alignment. ProjectDiscovery's open-source foundation and its transparent, template-driven approach matched the way Factorial's engineers already think about security. Rather than adopting an unfamiliar black box, the team felt like it was inheriting a well-maintained version of something it could have built itself, without the maintenance burden that building it would have required.

> *What stood out about ProjectDiscovery was not a feature list. It was alignment.*

"It was natural," says Factorial's Engineering Manager of Security. "It's the kind of thing that we could have done, but removing all of the inconvenient steps and still giving us the flexibility that we needed."

That transparency was central to the decision. Being able to see exactly how the scanning logic works, and to extend it with their own templates, meant the team did not have to choose between control and convenience. They kept both.

factorial

What Running on ProjectDiscovery Looks Like Today

Today, Factorial runs automated scans across its full external footprint on a continuous, daily basis. When new vulnerabilities are disclosed, scans are triggered automatically with no manual intervention required, and the team receives regular summaries along with proactive alerts when new exploits begin gaining traction.

The impact shows up in two ways. Coverage is broader and more consistent than the team could maintain on its own, and the time between a change appearing on the attack surface and that change being assessed has dropped meaningfully. False positives, while never zero at this scale, are controllable rather than noise that drowns out the signal.

What changed most is harder to quantify. "For me, it was a lot of peace of mind," says Factorial's Engineering Manager of Security. "I don't need to care about maintaining this on a virtual machine and having to update this machine and make sure it's not exposed." The team's confidence in its coverage has shifted accordingly: "I know that if I have something, I will find out as soon as physically possible."

The Outcome

For a security team protecting a broad and fast-growing attack surface, the most important measure is not how many issues you find, but how quickly you find them. Factorial scaled its coverage to stay ahead of that surface as it grew. Its bug bounty program and its engineers now focus on the novel work that matters most, the team spends its time on security rather than infrastructure maintenance, and it has continuous, reliable visibility into an environment that keeps expanding.

That is what trust in your tooling actually looks like.