code42

Company name

Banked

Industry

Technology

Company size

150 employees

Use case

Source Code Protection & Compliance

Banked :

CASE STUDY

Safeguarding Source Code, Productivity, and Trust: How Banked Uses Incydr

Put yourself in the shoes of an innovative tech company aiming to disrupt a highly regulated space, while also keeping their data secure. Sound like a tall order? With Code42 Incydr™, **Banked** has found the sweet spot - gaining total visibility to keep their source code safe and retain their competitive edge, without disrupting employee productivity.

About Banked

When Banked was founded in 2018, they aimed to solve the problem of an archaic payment infrastructure that placed an expensive burden on merchants. Since then, they've focused on making strategic partnerships with banks and the broader fintech ecosystem, building tools to provide a fairer, faster, and more secure payment system for merchants and consumers alike.

Protecting Source Code and Ensuring Compliance

Being a tech company, Banked has always prioritized security, but data protection, from both insiders and external actors, took on a more critical level of importance given their work in the financial industry. Jamal Issouquaein, IT Engineer at Banked, explains, “We work with a number of international banks and financial institutions and they have requirements on some of the technologies we use and the protections we have in place, not only for their data but our own data as well.”

On top of regulatory compliance needs, they also knew they needed to be sure their most important data was well protected. For Banked, that meant making sure they had full visibility over the source code that powers their real-time payment platform so they know where it moved, whether to trusted or untrusted destinations. Jamal explains, “Being in the financial services space, [losing source code] could open up the product to significant security breaches with financial information. It's also reputational as well - if people are going to trust using our products with their own financial information, we need to make sure that we don't have significant security events like source code leaking.”

> *“Being in the financial services space, [losing source code] could open up the product to significant security breaches with financial information. It’s also reputational as well - if people are going to trust using our products with their own financial information, we need to make sure that we don’t have significant security events like source code leaking.”*
>
> \- Jamal Issouquaein, IT Engineer at Banked

Changing the Game with Incydr

In looking for a solution, Jamal and his team knew their main requirement would be visibility over known and unknown risks without overstepping employee privacy, especially in a global, remote workforce that allows for personal use on corporate devices.

“There are solutions out there that offer an extreme amount of control and an extreme amount of oversight, but often it’s too much. We have to make sure that we’re not overstepping those bounds and that if we are installing anything on the devices that tracks activity,” says Jamal, “Incydr surfaces genuine security risk, rather than becoming some sort of employee tracking system.”

When evaluating Incydr, Jamal and the team at Banked discovered the visibility and context in the console were exactly what they were looking for. “One of the aha moments we had while going through the proof of value (POV) process was our visibility over AirDrop traffic. We’re a Mac-based company and we recognize that there’s a lot of Mac-specific features, like AirDrop, that could be vectors for data loss.” Jamal continues, “[With Incydr] we no longer had a concern about leaving that sharing option open because we can see exactly what’s happening.”

What’s Next for Banked

With the risk of source code exfiltration successfully mitigated, Jamal and his team look forward to using Incydr to address additional use cases, such as securing data moved by departing employees. The Banked team plans to integrate Incydr with their HR system to “automate a key part of our offboarding process and ensure we have the right oversight for that extra peace of mind.”

For others in need of a data protection solution, Jamal offers this advice: “Consider the oversight you have on your employees and think ‘what’s the minimum that we need to collect from their devices to do data loss prevention appropriately, without turning into Big Brother?’ We have trust in our people, so all we needed was something to confirm there’s no exfiltration and Incydr could provide that for us.”

Gartner Peer Insights

50+ Verified Security Reviews

★★★★★

4.8 out of 5 stars

About Code42

Code42 is the leader in Insider Risk Management. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss and speeds incident response without inhibiting employee productivity. Amplifying the effectiveness of Incydr are the Code42® Instructor™ microlearning solution, and Incydr’s full suite of expert services. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. Innovative organizations, including the fastest-growing security companies, rely on Code42 to safeguard their ideas.