Jason Schriner

Compliance

7/27/25

Some sectors of technology must be regulated in order to ensure the safety of the public. This includes industries such as Healthcare and Banking. These companies must demonstrate they are following these regulations to auditors. This act is referred to as compliance. Today technology is shifting toward cloud computing, and this is having an effect on how companies are able to demonstrate compliance.

One of the biggest challenges in regulated industries today is keeping up with how quickly infrastructure changes. In cloud environments, systems can spin up and disappear within minutes. That makes it hard to prove to auditors that everything was compliant especially when the system you're being asked about no longer exists. To solve this, organizations need better ways to track what is happening in real time. That’s wheretelemetry comes in. By collecting data as systems run, telemetry gives teams a way to look back and see exactly what was happening at any point in time.

Telemetry is data collected from systems while they’re running things like logs, metrics, and events. It’s become a powerful tool not just for monitoring performance, but also for supporting compliance. By capturing detailed records of how systems behave over time, organizations can provide auditors with a complete picture of operations, instead of relying on limited snapshots.

A case study in the DevOps handbook demonstrated how “Regulators often put too much reliance on code reviews to detect fraud. Instead, they should be relying on production monitoring controls, in addition to using automated testing” (Kim et al., 2017). Telemetry plays a central role in this approach by offering real-time insight into system behavior and making it easier to catch issues that slip through traditional safeguards.

The case study demonstrated how telemetry data was able to uncover an issue before any other means was an incident involving ATM systems. In that case, a developer placed a backdoor into the system and was able to sneak it past code reviews and have it deployed into the production environment. The breach wasn’t discovered through traditional means. Instead, it was found at a daily meeting when reviewing the telemetry data. Someone noticed that all of the atm's in a particular area had been placed in maintenance mode outside of their scheduled maintenance window. This abnormal behavior led to an investigation that uncovered the backdoor. This story highlights a key point compliance and security don’t stop at deployment. Just because code passes review and testing doesn’t mean it’s safe or compliant once it’s live. Telemetry allows teams to see what’s really happening in production, detect issues early, and respond quickly capabilities that are increasingly expected in regulated environments.

To meet these expectations, many organizations are building dashboards that give auditors direct access to telemetry data. Instead of requesting log files or reports, auditors can view real-time and historical data across the entire system. They can see who accessed what, when it happened, and whether it aligned with policy all without relying on manual sampling or delayed reporting.

Compliance in the modern era requires visibility, traceability, and agility. Telemetry provides all three. It doesn’t just help organizations stay in line with regulations; it helps them prove it, with evidence that’s complete, current, and verifiable. As infrastructure continues to evolve, production telemetry will remain a key part of any serious compliance strategy.

References:

Kim, G., Debois, P., Willis, J., Humble, J. (2017). The DevOps handbook : how to create world-class agility, reliability, and security in technology organizations. It Revolution Press, Llc.