**Introduction**

Following the rules in highly regulated industries can be tough, especially with new technology. Two case studies, "Proving Compliance in Regulated Environments" and "Relying on Production Telemetry for ATM Systems," show how companies can handle these challenges. They point out how old methods of checking compliance don't work well anymore and how automation and real-time monitoring help keep things safe.

**Proving Compliance in Regulated Environments**

Bill Shinn, a security expert at Amazon Web Services (AWS), helps companies follow regulations while using cloud computing. In the past, auditors would check compliance by manually reviewing servers, taking screenshots, and looking at logs. But in today's age, cloud systems constantly change. This makes those old methods not effective.

Shinn suggests a better way to do this, which is by using automated tools that collect data all the time. Instead of auditors requesting proof manually, they can log into tools like Splunk or Kibana to see real-time data. This approach makes compliance faster and more accurate.

AWS also created the DevOps Audit Defense Toolkit, which explains how businesses can show they are following the rules. It helps companies document their compliance, use automation to gather proof, and make sure security measures meet legal requirements.

The AWS case study teaches us important lessons. One is that automation is helpful. Manually checking compliance is slow and can have mistakes. Automated systems make it easier. Another one is that auditors need easy access to data. It should be possible to check compliance data anytime and not have to wait on reports.

The case study also shows that teamwork is important. Security teams, compliance officers, and developers must work together to make compliance smooth and effective. Using these ideas, companies can stay compliant while enjoying the benefits of cloud technology.

**Relying on Monitoring for ATM Security**

Mary Smith, a leader at a big financial company, believes that simply reviewing code is not enough to catch fraud. Instead, companies should also monitor their systems in real-time. She shares an example of fraud in ATM software. A developer secretly added a backdoor to ATM machines, letting them enter maintenance mode at specific times so they could take out cash illegally. The fraud wasn't caught through a code review or approval process. It was found when someone noticed that ATMs were going into maintenance mode at odd times. This proves that real-time monitoring can catch issues that classic security checks might miss.

The ATM case study shows us a few key lessons as well. One major one is that checking the code isn't enough. Reviewing code is useful, but it won't always catch everything. The case study shows that real-time monitoring is necessary. Watching systems for unusual activity helps catch fraud early. Actively looking for strange patterns also helps. Being able to spot unusual behavior can help stop security threats before they cause damage.

**Conclusion**

Both case studies show that businesses need modern ways to stay compliant and secure. Old auditing methods don't work well in today's world. Companies should use automation, real-time monitoring, and teamwork to stay compliant and prevent security risks. These new approaches help businesses follow the rules while keeping operations smooth and safe.