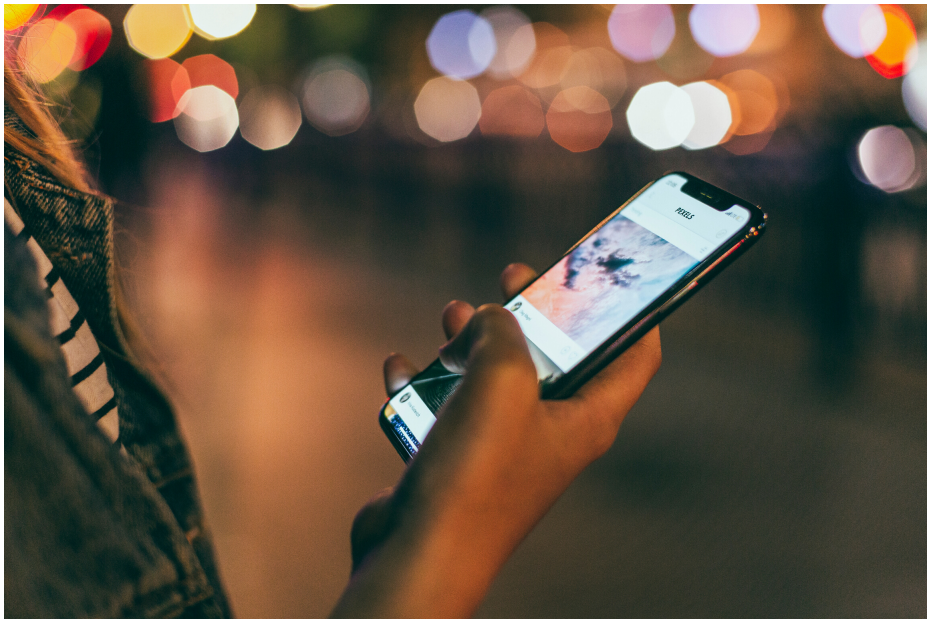
5 WAYS TO PREVENT BANKING APP BREACHES

datatheorem

Prevent AppSec Data Breaches



How can you protect your business, your customer data, and stay informed about your current security posture all at the same time in this age of data breaches? According to a Ponemon Institute Study, companies have a 28% chance of having a data breach incident in the next two years. It's prevalent and if you rely on network or device security to protect your apps, you may want to reconsider your strategy. Web and mobile applications are the most frequently attacked and compromised vectors in a company's security posture, and that includes financial institutions. Traditional IT security measures like firewalls and WAFs won't protect your app from reverse engineering or tampering. But you don't need a Fortune 500 budget or large security staff to tackle this problem.

Understanding the Structural Problems Underlying Banking App Vulnerability

Many, if not all of the most serious vulnerabilities affecting banking apps have to do with the architecture of the app/bank ecosystem and the distributed nature of its various elements. The app is an autonomous piece of software. Most of the time it connects to the bank's back-end systems through standards-based Application Programming Interfaces (APIs). The open, universal connectivity inherent nature of these APIs is great for developers, but it creates security problems that traditional IT security measures like firewalls, endpoint security tools and Web Application Firewalls (WAFs) can't solve. Mobile apps and APIs create encrypted, machine-to-machine interactions on the network. A shadow API won't show up as a compromised endpoint. As a result, the attacker can mask him or herself and appear to be an approved user. Network filters won't catch them.

Who Owns the App Risk?

A further complicating factor in securing banking apps stems from their divided ownership. With traditional banking software, there are usually two owners, both of whom work for the bank. A Line of Business (LOB) manager is responsible for defining the software's requirements. A development team builds it and an IT ops team deploys it. In contrast, most mobile banking apps have a LOB owner, an IT department owner and at least one external entity that develops the app and manages its APIs. This split ownership is problematic for a range of reasons. At a basic level, any time three owners in two or more entities share responsibility for security, there's a strong possibility that something will get overlooked. Then, if there is an incident or a vulnerability discovered, there can be disagreements over who is supposed to fix the problem or the prioritization of the fix.

Prevent Banking App Breaches

Banks need to go beyond relying on network and device security to protect their APIs, apps and customer data. Most banks are under pressure to adopt more robust security countermeasures for their apps without the benefit of huge IT or SecOps teams and at requisite speed. New, automated security tools for apps and APIs make it possible to balance these competing requirements. Recommended practices with these tools include:

1. Protect apps with continuous scanning, vulnerability analysis and automated remediation, e.g. data privacy issues within mobile (iOS and Android) applications. Automation can make up for a lack of staff with specialized skills. Continuous scanning enables SecOps teams to narrow the gap between the discovery of a security issue and its remediation.
2. Participate in the app build and deployment process. This potentially prevents issues before they happen. Regardless of who owns the app, all stakeholders should be involved in the app lifecycle. Security flaws can appear at transition points like the release of a new version of the banking app. In these moments, users can accidentally leave APIs exposed to malicious access and other threats.
3. Get visibility into all relevant APIs and setting alerts to discover shadow APIs. APIs need constant watching, e.g. finding authentication and encryption vulnerabilities in APIs based on their definitions and API specifications. Malicious actors can set up shadow APIs that steal user data by mimicking the bank's real APIs.
4. Go beyond annual or bi-annual audits and have access to security and compliance audit reporting on a continuous basis, i.e. 24/7.
5. Secure the open source and commercial Software Development Kits (SDKs) the app vendor uses to build the app. This may involve the use of specialized toolkits that enable developers to apply secure design principles to open source code.

It is possible to improve the security of banking apps. Getting there involves solving the app's structural weaknesses by securing the app development process along with the connecting APIs. This means bringing people from different organizations into a cooperative mode of working. A common frustration for teams is that many security tools are limited in function and only allow security or IT or engineering to have insights into vulnerability management. New, automated app and security tools are growing beyond this.

"Data Theorem has helped Provident secure our mobile banking app and catch potential vulnerabilities prior to end user release."

John Haggarty, Vice President at Provident Credit Union

How Data Theorem Can Help

Data Theorem tools provide a common platform for establishing and monitoring app security. Our tools also give developers the ability to implement security practices that they may not know how to do on their own—or have time to do.

- **Audit-ready**: Allows anyone in the company to pull a report, at any time, to prove or analyze regulatory compliance statusTrue
- **True DevSecOps**: Integrates with Jira, Bugzilla, etc to send alerts, analyzes the best way to resolve quickly and safely, and provides secure code samples and recommendations for remediation
- **Beyond Pen Testing**: Continuous (24/7), automated dynamic and static analysis of vulnerabilities and app store blockers

Our customers include five of the seven largest banks in the United States as well as dozens of credit unions, so we understand that a bank's reputation is a critical piece to their business and avoiding a data breach is its highest priority. This is why security automation is necessary to not only find the vulnerabilities, but also prioritize them, and offer remediation options. The end result is worth it: Banking customers will be more secure and the bank will have fewer security risks and lower odds of a data breach.

Data Theorem is a leading provider of modern application security. Its core mission is to analyze and secure any modern application anytime, anywhere. The Data Theorem Analyzer Engine continuously scans APIs and mobile applications in search of security flaws and data privacy gaps. Data Theorem products help organizations build safer applications that maximize data security and brand protection. The company has detected more than 400 million application eavesdropping incidents and currently secures more than 4,000 modern applications for its Enterprise customers around the world.