EBOOK

Essential Planning Guide for Securing Financial Applications

March 2021

verimatrix
DRIVING TRUST

Table of Contents

03

Introduction

04

Mobile Apps: Expanding Fintech & Banking Risk Surfaces

08

Things to Consider Before Deciding on Your App Security Approach

12

Benefits of Outsourcing & Building In-House App Security

13

PCI & PSD2 Compliance: A Checklist of App Security Methods & Techniques

14

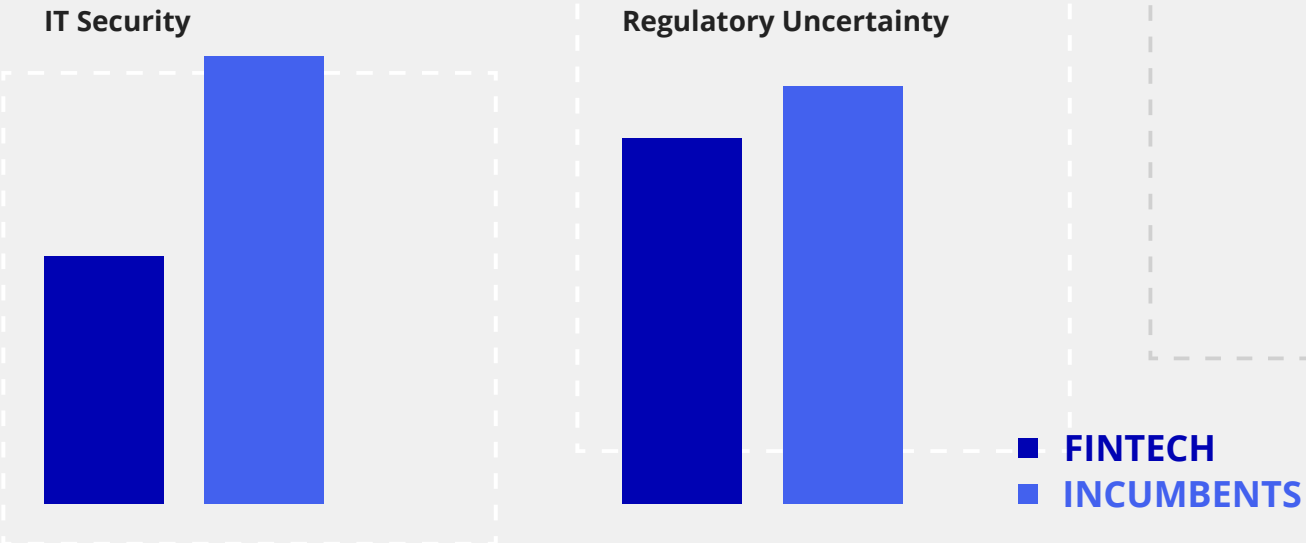
10 Questions You Should Ask in Your App Security RFPs

Introduction

While the fintech and Banking industries have their differences, they share many of the same obstacles. Fintech startups can take a cue from incumbents in the financial services sector who have already learned to navigate their strict regulatory environment. Established financial institutions can also learn from the agility and flexibility of smaller fintech companies.

The landscape of the financial market is evolving along with technology, and getting ahead of new, sophisticated cybersecurity threats is key for both fintech companies and Financial Institutions. In PwC's Global FinTech Report, both players cited that their top two challenges are IT Security and Regulatory Uncertainty.

What challenge did/do you face in dealing with fintech/traditional financial companies?

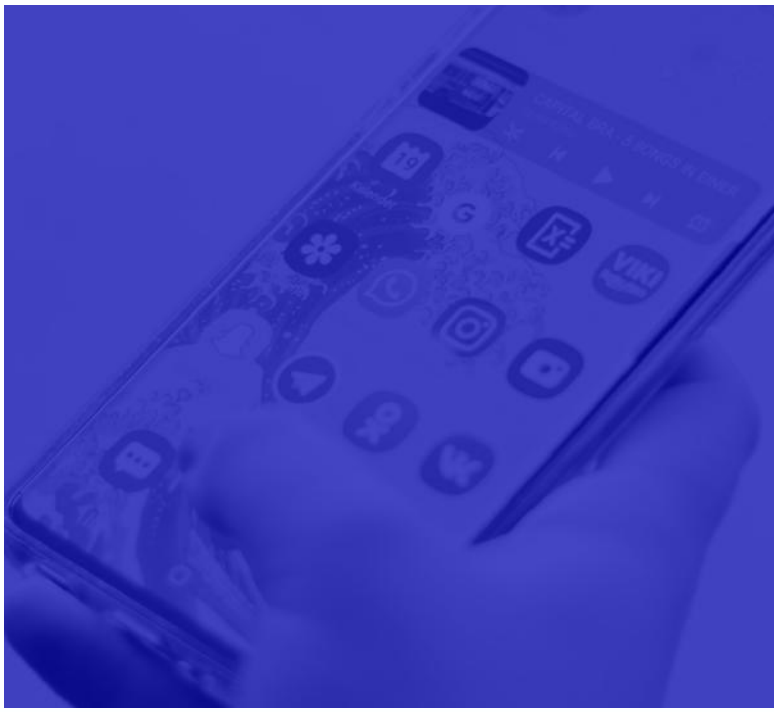


As the line between fintech and banking blurs, one thing remains clear: securing new technology and preparing for ever increasing regulatory requirements in critical.

Mobile Apps:

Expanding Fintech & Banking Risk Surfaces

Mobile devices and applications are one of the fastest-growing risk surfaces in fintech and Banking. **While the traditional security approach is to protect the firewall, mobile devices and apps exist outside of this perimeter.** Cybercriminals are privy to this security oversight, and as more hackers take advantage of app vulnerabilities, it is more important than ever to protect these risk surfaces – not only to meet compliance, but to ensure customer trust and secure valuable intellectual property.



One big challenge is that while banks are heavily regulated, they aren't told how to specifically comply with regulations, which leads to confusion and ill-informed security strategies. (While some countries – like Turkey and Singapore – are paving the way for more definitive rules for compliance, specific app security measures for developers and app publishers are not clearly stated in most countries' regulations.)

Data Privacy Regulations:

The Devil is in the (Lack of) Details

The ambiguity and confusion of the banking and financial services industry also spills over into the burgeoning fintech industry. Players are asking which – if any – regulatory agencies govern fintech companies and which rules they must abide by.

In particular, small players struggle to navigate a complex, ever-increasing regulatory environment as they strive to define their compliance model. Recent years have brought an increase of regulations in the Financial Services industry, where even long-standing players are now struggling to keep up.

THE BEST PLACE TO START IN AN ENVIRONMENT OF AMBIGUITY AND CONFUSION IS TO FOCUS ON WHAT YOU KNOW.

One thing is for certain: any app that processes personal data (and let's face it – they all do) is regulated by governing agencies – and the regulations are tightening every year.

Data Privacy Regulations:

The Devil is in the (Lack of) Details

Worldwide, these data regulations include:

GDPR, an EU regulation that requires controllers and processors of personal data to put appropriate technical and organizational measures in place to implement data protection principles

CCPA, which requires organizations to implement and maintain reasonable security procedures and practices in protecting consumer data

The New York SHIELD Act, a state law requiring any person or business that handles private information of New York residents to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information

Regulations, standards, and directives that more specifically apply to payments, financial services, and banking industries include:

PSD2, an EU regulation that introduces security requirements for the initiation and processing of electronic payments, as well as for the protection of consumers' financial data

PCI, a card industry body which requires businesses to handle credit card information in a secure manner that helps reduce the likelihood that cardholders would have sensitive financial account information stolen

KYC and AML (Know Your Customer and Anti Money Laundering), regulations that require fintechs and banks to make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship.

Here's where things get hazy:

While regulations often address processes and outcomes, they do not tend to list specific technology requirements. Beyond simply implementing reasonable and *appropriate* security measures, there are no real guidelines for how to comply.

Data Privacy Regulations:

The Devil is in the (Lack of) Details

Though regulations will undoubtedly become more defined as technology and markets evolve, even revised versions of directives and standards still lack details and technical clarity.

In fact, after the revised Payment Services Directive finalized the standard on Strong Customer Authentication (SCA) and Common Secure Communications (CSC), the EU Commission stated:

"It is not possible... to anticipate all possible problems with APIs, and to specify... how they have to be addressed. We will therefore have to rely on market players to develop together APIs that work for all sides - banks, third party providers (TPPs) and payments services users."

Thus, fintech and banking companies are left to decide on the nuances and to define their own best approaches for app security. Should you dedicate an in-house team to build cybersecurity technologies or outsource the task to a commercial vendor? An in-house team requires an allocation of time and resources that may reach far out of budget, but many fintech and banking companies are wary of handing over security to an outsider.

Things to Consider

Before Deciding on Your App Security Approach

1 CONSIDER THE COSTS INVOLVED

Many initially (and incorrectly) think that implementing in-house security will save time and money. It's important to consider all costs before deciding in an approach, including:

- Cost of paying your team or a third party to build and customize the tool to your needs
- Cost of developing your teams' skills
- Cost of possible gaps in documentation and lack of warranty
- Cost of support, updating, or additional charges that aren't upfront
- Cost of risks involved in open source software, primarily issues that may arise with special customizations

According to the FBI's Internet Crime Report, cyber crime in 2019 cost U.S. businesses over $3.5 billion, with the average cost of a data breach is 3.92 million according to IBM's 2019 Cost of a Data Breach Report. In contrast, the average cyber security budget ranges from 5% to 20% of an organization's IT budget. **Regardless of if you choose to outsource or internally implement a cyber security framework, you can't afford to cut corners and risk the costly consequences of a cyber attack.**

Things to Consider

Before Deciding on Your App Security Approach

2 CONSIDER THE TIME IT TAKES TO BUILD, IMPLEMENT AND MAINTAIN SECURITY IN-HOUSE.

Depending on your specific app security needs and their complexity, a project to build and implement a solution can take anywhere between 16-21 months (or longer) and consists of multiple phases. Finding a Product Manager experienced in leading such a project can be difficult – and hiring security software architects and developers can have a significant lead time.

And that's all before the show even begins. After hiring, other stages of the build include analysis, design, development, testing, and deployment – not to mention the ongoing maintenance (which also requires retaining experienced developers with a working knowledge of your custom solution).

What's more, any security built during this timeframe will be fixed to your app as is. It can be much more difficult to maintain over time as your app develops and grows.

Things to Consider

Before Deciding on Your App Security Approach

3 CONSIDER YOUR APP'S VULNERABILITIES AND SECURITY THREATS

App security isn't just reserved for big banks. In fact, small businesses account for 43% of all breaches, and when they do get breached, 60% of them will close their doors within 6 months. Banking and fintech apps handle sensitive data, which means they are attractive targets for hackers – and this also makes them subject to stringent compliance regulations.

Security must go beyond the traditional perimeter of backend servers: **Big banks have a long history and a lot of expertise in securing backend systems, but mobile apps are the new kid on the block and their security often falls between organizational cracks.**

Mobile apps access banking services through APIs (Application Programming Interfaces). Attackers can dissect applications to learn how to use these APIs for their own means and to extract the secrets that are meant to stop unauthorized access. Failing to secure APIs can lead to compromise not only of client devices, but also of your entire ecosystem.

Is your team equipped with the knowledge, skills, and tools to defend APIs?

Things to Consider

Before Deciding on Your App Security Approach

4 CONSIDER YOUR DEFENSE IN THE EVENT OF A BREACH

While correctly implemented, robust security solutions will prevent attacks, cyber criminals' toolkits and methods are always evolving. The purpose of these solutions is not only to protect against threats, but to act as a line of defense in the event of a breach. Deploying trusted, recognized tools and partnering with a leader in app security will help you prove that your technology was protected to a reasonable and appropriate degree. Automated, trusted tools will allow you to react quickly to a breach and justify your security choices in the event of a sophisticated attack.

Benefits of Outsourcing vs. Building In-House App Security

OUTSOURCING BENEFITS

Scalability: While your team might understand your needs, risks, and vulnerabilities as they currently exist, a security firm's solutions are built to scale and adapt to the changing needs of your business. They offer solutions that support not only now, but also when they need to accommodate more users, higher network traffic, more power, and changes in hardware.

Guaranteed 24/7 support: It is vital that companies have 24/7 monitoring because security breaches don't always happen during business hours. An attack at 9 p.m. that is not detected until the next morning when your security team arrives at the office could be disastrous.

For highly regulated and sensitive industries like banking and fintech, this means that hiring an in-house team to run a round-the-clock security operation center (SOC) is mandatory.

Easy implementation: After purchasing a cybersecurity solution, proper configuration is a must to guarantee the effective protection of the system and network against cyber threats. This can be mysterious for many organizations as each security solution has its own interface. Without the proper knowledge to configure the tool, the setup process will be time-consuming.

Outsourcing the creation of app security to a third-party vendor relieves you from the responsibility of deploying and configuring complex tools. Partnering with a trusted vendor (especially one that can offer zero code implementation) decreases the burden of your team.

IN-HOUSE BENEFITS

Internal knowledge: Chances are, the people who know the layout and operations of your data flows are those who created the architecture in the first place. Your team intrinsically understands your network and security needs.

However, many fintech and banking companies employ a mix of in-house personnel and outsourced security experts. Your team can focus on nuanced organization-specific issues, while an outsourced team covers a plethora of other threats.

Customization: If your own in-house team develops your application security technology, there is no need to negotiate with a vendor for customization (although a good vendor would be flexible and work with your needs). This offers full flexibility and app security that will truly meet every need.

While customization offers exactly what you want and need, this comes at a cost. If/when employees depart, customized systems may be compromised, inaccessible, or not fully understood.

Visibility & control of data: Perhaps one of the biggest benefits of in-house app security is the ability to remain in sole possession of highly regulated and sensitive data, rather than entrusting it to a third-party.

Regulatory Compliance:

A Checklist of App Security Methods & Techniques

If you outsource – it's important to ask your security partner about the following methods as they relate to compliance with regulatory standards, guidelines, and governing bodies - such as PCI and PSD2. If you hire an in-house security team, it is critical to correctly implement security solutions to ensure that these methods are safeguarding data and payments to a reasonable and appropriate degree:

- **Obfuscation of all critical code**
- **Anti-tamper protection of the application**
- **Network traffic encrypted using TLS 1.3 and downgrade not possible**
- **No sensitive text visible in static analysis of code**
- **Automated environmental checks**
- **Cryptography**

Finding a team to not only implement these security measures but maintain them through every platform upgrade can quickly drive up costs.

In Cisco's Annual Security Report, 53% of respondents who outsource services said that they do so because it is more cost-efficient.

10 Questions

You Should Ask in Your App Security RFPs

1 DO YOU PROVIDE APP SECURITY FOR ANDROID AND IOS APPLICATIONS TO KEEP THEM FROM BEING REVERSE ENGINEERED AND MODIFIED?

If an application's code is not properly hardened, hackers can decompile the application, find its weaknesses, and create an attack. Proper code protection prevents a mobile app from becoming an attack vector. A handful of specific techniques protect applications from reverse engineering and modification, like environmental checks, anti-tamper technology, and obfuscation. It is always best if a vendor's solution implements multiple methods to protect against these threats.

2 DO YOU SUPPORT NEW VERSIONS OF ANDROID AND IOS PRIOR TO RELEASES BEING MADE PUBLICLY AVAILABLE? PLEASE STATE YOUR RELEASE CADENCE IN THE NOTES.

If a new version of Android or iOS becomes available to end users before the application protection software has been modified to address it, the protection will not work with the new version of the operating system. That means that when Apple or Google come out with an upgrade, a large percentage of your user base will get cut off. You need to proactively ensure that the protection works with each new version before users get the OS updates. Stay up to date by looking for a vendor that provides frequent releases that accommodate these developments. Ideally, look for a vendor that provides updates no less than quarterly.

10 Questions

You Should Ask in Your App Security RFPs

3 IS YOUR PROTECTION AVAILABLE AS ON-PREMISE TOOLS THAT WE CAN RUN WITHIN OUR DEVELOPMENT ENVIRONMENT?

Many organizations feel more secure having the tools they use to deliver app protection running on-premise. A solution that provides on-premise tools enables these organizations to maintain control over their application security tools so no applications or data pass out of their environment.

4 IS YOUR PROTECTION AVAILABLE AS A CLOUD SERVICE THAT WE CAN UTILIZE?

While some organizations prefer the control of an on-premise implementation, others may demand the advantages of a cloud solution. Cloud solutions enable more rapid implementation, guarantee that you always have the latest version without the need to upgrade, and run on the vendor's hardware rather than requiring you to purchase, implement, configure, manage, maintain, and upgrade software, hardware, and an in-house data center. A vendor that provides both an on-premise and a cloud-based solution allows you to choose the implementation model that works best for your business; and to swap between them as your business evolves.

10 Questions

You Should Ask in Your App Security RFPs

5 WHAT ARE THE CORE FEATURES OR INNOVATIONS THAT DISTINGUISH YOUR PRODUCT FROM YOUR COMPETITORS?

Discovering a vendor's differentiators should be key when it comes to application security RFPs. Clearly for an in-app protection product, the level of security the product can provide is paramount. Equally important, that security should be easy to apply. Ease of use enables your development team to spend less time on security and more on developing applications. Such a tool will enable better security as well as a faster, smoother product development process.

6 CAN YOU APPLY PROTECTION WITH NO CODE CHANGES REQUIRED? ARE THERE ANY EXCEPTIONS TO THIS?

Many in-app security solutions put constraints on the way application developers perform their coding to take advantage of the solution. A no-code solution can not only simplify use, but it can also give developers the flexibility to work the way they want to. Such flexibility enables developers to protect apps and build the capabilities they need while keeping them happy and on board with the chosen solution.

Of course, most environments are not entirely zero code. There are always exceptions. For example, your developers may want to create a customized response to a particular threat rather than accept the solution's default reaction. The ideal solution will give developers the option to create customized responses, as necessary.

10 Questions

You Should Ask in Your App Security RFPs

7 DO YOU PROVIDE TRAINING IN THE USE OF YOUR SOLUTION?

Some application protection software vendors don't include training with their products. They simply sell you a product, then provide a link to download the manual. While such an approach can be less expensive up front, it can lead to extra, unexpected costs down the road since it may take you some time to learn how to use the software. Alternatively, you may find yourself paying more for training. A vendor that includes training in the cost of the software and gives you everything you need to get started will avoid wasted time, enabling you to budget more effectively and avoid unexpected costs.

8 PLEASE PROVIDE DETAILS OF THE TECHNICAL SUPPORT YOU PROVIDE.

Technical support should be high quality and available when and where you need it. Ideally, the vendor should provide 24/7/365 worldwide customer support, provide agents with deep experience in app protection that can streamline support for implementation, integration, testing and maintenance, as well as high customer satisfaction scores. Ask whether the vendor has awards for excellence in customer service to prove their claims.

10 Questions

You Should Ask in Your App Security RFPs

9 HAS YOUR PROTECTION BEEN USED IN SECURITY CERTIFIED SOLUTIONS OR EVALUATED BY INDEPENDENT SECURITY LABS? IF YES, PLEASE GIVE DETAILS.

Since the nature of application security is low-level and complex, it can often be difficult to validate a vendor's claims about the strength and robustness of their solutions. This means that customers in need of app security may often end up simply choosing the vendor who can tell the best story.

Fortunately, outside evaluators with a high level of expertise provide objective evaluations you can use to compare security offered by different vendors. Organizations like Mastercard and Visa certify mobile payment apps that operate on their networks. This requires extremely high levels of security that must be certified by approved independent labs.

Note that these organizations cannot certify that the tool itself is secure. They verify the security of the application as it uses the tool. So, it's important to find out whether the vendor has multiple customers whose applications (that are secured using their tool) have been certified by one of these organizations. A vendor with no record of going through and passing these independent security reviews should raise alarms.

10 Questions

You Should Ask in Your App Security RFPs

10 HOW MUCH TIME DOES IT TAKE TO DEPLOY THE SYSTEM?

Time is money. If your developers spend too many hours integrating security protections into your product, it's time not spent creating new features that add value for your customers. So, ask your vendor how long it typically takes to add the solution to your application. We recommend that the solution take just one day per application.

Large financial incumbents often struggle to interact effectively with their faster-paced (and less structured) fintech startups. Yet fintechs can develop and deploy too fast, without taking into account rules and regulations that they need to adhere to prior to integrating with institutional banking. Fintech's failure to address these risk points, such as ensuring that the security of their apps meet banking's regulatory standards, can severely delaying time to market, and negatively impacting sales/revenue forecasts.

Forward-thinking organizations are taking proactive measures to test, secure and then deploy their app and API feeds in advance of integration talks to avoid pitfalls that can slow down technical, compliance or partnership approvals.

Conclusion

With data privacy regulations tightening in the financial technology space and as more fintech startups enter the scene, app security will move further toward the front lines and become less of an afterthought. In order to remain competitive in the market, avoid hefty fines, and maintain customer trust, it's imperative that companies choose the right approach to app security.

Sources:
PwC: Blurred Lines: How FinTech is Shaping Financial Services
EU Commission: Letter from Olivier Guersent
IBM: Cost of a Data Breach Report
Small Business Trends: 43% of Cyber Attacks Target Small Businesses
Inc.com: 60% of Small Businesses Close within 6 Months of a Cyber Attack

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners to get to market faster, scale easily, protect valuable revenue streams, and win new business.

verimatrix
DRIVING TRUST