SOLUTION BRIEF

Build38 Mobile Application [Security] Platform

>Opportunity unlocked: Strengthening mobile app security with extended detection & response_

Securing revenue through mobile app protection

The evolving landscape of mobile app security requires a comprehensive, cloud- augmented approach that protects against increasingly sophisticated threats, and frees organizations up to focus on their business, app development and customer relationships. Our increasing transition to digital platforms and the ubiquity of smartphones means that we depend on mobile technologies to assist us with everyday tasks now more than ever.

For businesses, this means that mobile applications are no longer a nice-to-have—they are an absolute necessity for acquiring and retaining users, and generating revenue. However, the business or product managers charged with delivering their organization's mobile services on time and on budget face considerable challenges, not the least of which is ensuring the security of the apps they develop, while at the same time complying with an expanding list of regulations across different industries and geographies.

>Research indicates that 90% of all mobile applications are vulnerable to advanced security attack vectors_

Revenue streams at risk

Mobile apps are an attractive target for cyber criminals because they store valuable information such as user credentials, passwords and payment information. The consequences of a cyber attack or data breach can be devastating, including regulatory fines, reputational damage, legal action and revenue loss—particularly if the business relies on the app as a revenue source. As a result, revenue stream protection is an important driver for businesses investing in mobile app security.

Widening the attack surface

Integrating innovation & multi-layered defenses

Finding and implementing the right mobile app security solution today is a formidable challenge, the complexity of which is compounded by the need to ensure seamless integration with development teams, maintain the continuous release of innovative services, and manage the intricate task of securing apps across various operating systems and devices. However, these are not the only concerns making life difficult for mobile app decision-makers. Hackers are also becoming increasingly sophisticated. While in the past, they focused solely on targeting either apps or devices, today, they are increasingly aiming at one, a combination, or all three of the following technology layers:

The app or device itself

Hackers target the mobile device or the app itself.

The network

Attackers may intercept data as it travels between mobile device and backend system.

The app's back-end APIs

Attackers may unlawfully access an app's back-end APIs. This is often done by employing the app as a Trojan horse, often via repackaged apps that can easily fool traditional security systems and web application firewalls (WAFs)

Navigating the mobile security maze

Within a network, hackers may intercept data as it travels between a mobile device and back-end systems. In the backend, attacks are often carried out by employing an app as a Trojan horse, usually via repackaged apps that can deceive traditional security systems and web application firewalls. Powerful, effective mobile app security is necessary to fend off these kinds of attacks, but finding the right solution and implementing it can be a time-consuming, resource-heavy, and costly process for organizations. They often struggle with certification processes, high lab testing costs, and device diversity and maintenance. And to make things more complicated, they also have to support numerous operating systems, deal with fragmented security solutions, and navigate the complexity of open-source security solutions, such as root detectors.

The biggest risks to mobile application security

Data breaches

Mobile apps often store sensitive information such as user credentials, passwords and payment data. If this data is compromised in a breach, it can have devastating consequences for users and the app provider.

Malware threats

Malicious apps can infect your device with malware, granting attackers access to personal information. These malware-infused apps can wreak havoc on users' personal data and financial accounts, and can even lead to identity theft. They may steal or delete vital data from users' phones, including passwords, contacts and other sensitive information.

Inherent vulnerabilities

Not all mobile applications are developed with the best security practices in mind. This not only increases the likelihood of inherent security flaws and loopholes, but also jeopardizes user security and a business' overall integrity.

Unauthorized access

This occurs when malicious actors gain entry to your mobile app through various means, such as exploiting weak passwords or vulnerable code. Insecure apps can also fall prey to manipulation by malicious third parties, enabling them to access confidential data or manipulate the app for their own purposes. Without robust authentication measures, hackers can access sensitive data, pilfer customer information, and even seize control of the entire application.

Delegating mobile app security to specialized professionals

Bridging skill gaps & embracing expertise

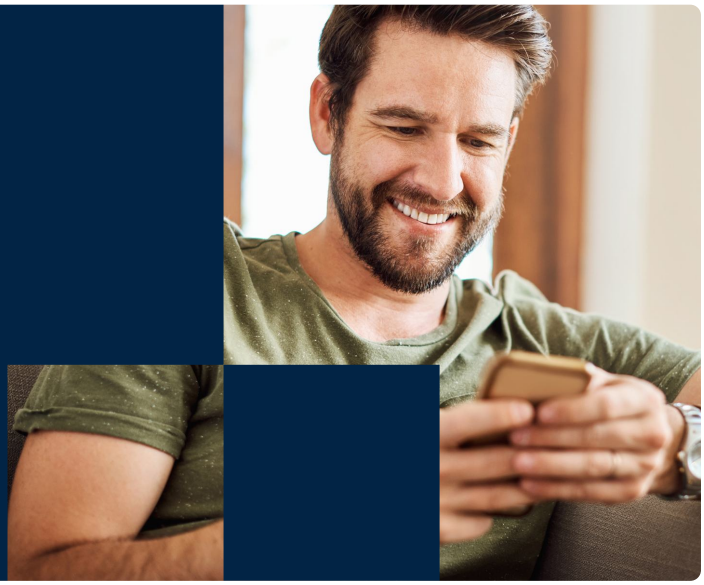
Many organizations are also struggling with an ongoing skills shortage. Companies find themselves lacking (and unable to recruit) the in-house security expertise they need. As a result, they are choosing to outsource their mobile app security requirements to third-party experts.

Addressing the challenge
The evolving landscape of mobile app security needs a comprehensive and integrated approach that leverages local and cloud-based resources to safeguard against increasingly sophisticated threats.

Head of Mobile Banking Solutions `BANKING APP SOFTWARE LEADER`

>What's fantastic about Build38 is that it handles much of the thinking about the types of attacks we need to defend against. This is where their value truly shines. It frees up our mental capacity, allowing us to focus more on our core business, rather than constantly worrying about security_

>Meet Build38
One platform. Three layers of threat protection. Unparalleled mobile app security_



The biggest risks to mobile application security

There's a pressing demand for a system capable of seamlessly integrating advanced mobile in-app protection with cloud-based mobile threat intelligence, detection, and response (XDR). This is why Build38 takes a multi-layered approach to mobile app security, providing mobile businesses with a comprehensive cloud-augmented mobile app security platform that enables them to strengthen their apps against data breaches and unauthorized access.

What the ideal mobile app security platform looks like

Leveraging AI, cloud, and multi-layered defense

The ideal mobile app security platform should combine the strength of an application's ability to defend itself locally on a device with the capabilities of the cloud, leveraging artificial intelligence (AI) to enhance security. This can be achieved with a mix of human-controlled and automated monitoring and response mechanisms. Moreover, the platform should transcend the limitations of basic runtime application self-protection (RASP), which relies solely on apps to safeguard themselves in the field. Instead, it should encompass multiple layers of in-app and cloud-based security.

Layers of in-app and cloud-based security

Superior mobile in-app protection

Mobile apps often store sensitive information such as user credentials, passwords and payment data. If this data is compromised in a breach, it can have devastating consequences for users and the app provider.

Augmented cloud-based security modules

Companies should not depend solely on mobile app self-protection. Instead, they should augment their local protection with AI- driven, cloud-based security modules. Every app instance should be fortified through cryptography, X.509 certificates and robust device binding. In addition, they should leverage the continuous stream of security telemetry data collected from all application instances and use machine learning to extract meaningful insights into mobile app threats. This approach enables the delivery of exclusive automated, operator- assisted or programmable threat detection and response capabilities.

Build38: Reinventing mobile application security

Pioneering an advanced zero-trust technology stack

Build38 goes beyond device and app security to safeguard the entire mobile environment. It guarantees zero-trust security across your whole mobile technology stack, encompassing apps, networks, and backend infrastructures. Our comprehensive platform offers cloud-based threat intelligence options for enhanced security, and three flexible in-app self-protection options.

Cloud-augmented mobile app threat intelligence

Comprehensive intelligence and response

Exclusive cloud-based Threat Intelligence options provide three additional layers of security for your mobile app. These comprehensive services provide mobile businesses with a range of AI-powered automatic, human-monitored, and programmable features for mobile app detection and response.

Build38 Active Hardening

Installed by default. The server hardens all mobile app instances through cryptographic-key-based individualisation, and AI technology transforms security data into deep threat insights.

Build38 Threat Intelligence

A user-friendly web console empowers business teams with real-time visibility and control over mobile app security, so they can monitor for threats and shut them down as soon as they appear.

Build38 Threat Intelligence & Response API

REST APIs enable back-end developers to seamlessly integrate fine-grained mobile threat detection, intelligence, and response actions into server-side applications.

Build38 Attestation & Response

A user-friendly software-as-a-service (SaaS) interface empowers non-technical teams to establish automated remote security responses and attestations, including real-time confirmation of compliance with emerging industry standards such as PCI MPoC and eIDAS 2.

Multiple layers of [protection]. One streamlined solution.

Build38: Business benefits

Build38 is a comprehensive, fully integrated, and flexible mobile app security solution that provides robust protection against evolving threats, while simplifying your security architecture.

Elevate your mobile app security with Build38

With mobile app cyberattacks on the rise, staying on top of increasingly sophisticated security challenges can be an ongoing battle. Build38 allows businesses to secure their mobile applications—and safeguard their revenue—in the shortest time to market, and at a lower cost than developing an in-house solution.

With Build38, businesses can accelerate their time to launch, deployment, and certification. They benefit from future-proof threat protection and substantial total-cost-of-ownership savings. Moreover, enhanced—yet frictionless—user security on even older devices fosters higher engagement and loyalty, resulting in increased customer satisfaction. This leads to a greater return on investment and improved onboarding success.

In any modern organization, mobile apps have become a necessity. Build38 empowers organizations to focus on their business, customer relationships, and app development, secure in the knowledge that their apps are shielded from malicious attacks and comply with regulations. The result is expedited development and ongoing security awareness—without the weight of security concerns.

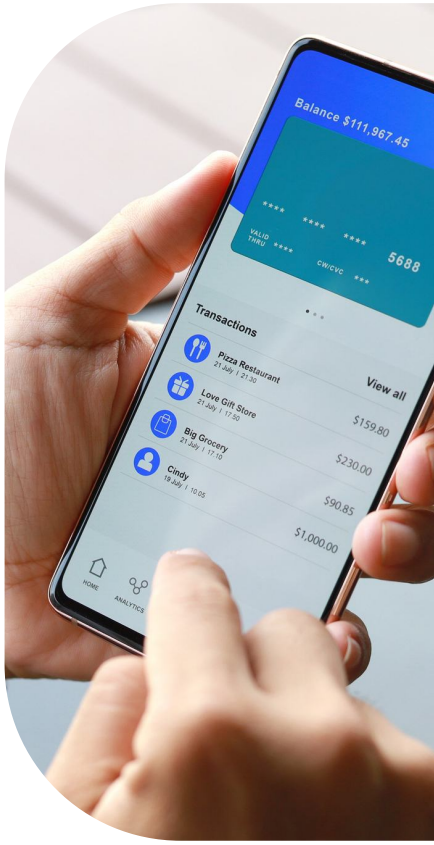
Driving business and security success on mobile app ecosystems

Build38 empowers countless organizations worldwide with unparalleled mobile app security, safeguarding their mobile applications from a myriad of threats and partnering with them to ensure robust protection and security across a multitude of industries and use cases.

CASE STUDY

Implementing dynamic mobile app security at a top 10 global bank

Revolutionizing mobile banking security for eight million consumers



Industry

Financial services
Mobile banking

Working under the strictest safety standards, our client, a top ten global bank, prided itself on having the most innovative technology on the market for preventing and detecting cyberattacks, ensuring the confidentiality, integrity and availability of entity, client and employee information at all times.

Build38 worked with them to ensure the optimal implementation and maintenance of these strict security standards, and provide a fine-tuned user experience for more than eight million mobile app customers.

Head of mobile banking solutions BANKING APP SOFTWARE LEADER

>What's fantastic about Build38 is that it handles much of the thinking about the types of attacks we need to defend against. This is where their value truly shines. It frees up our mental capacity, allowing us to focus more on our core business, rather than constantly worrying about security_

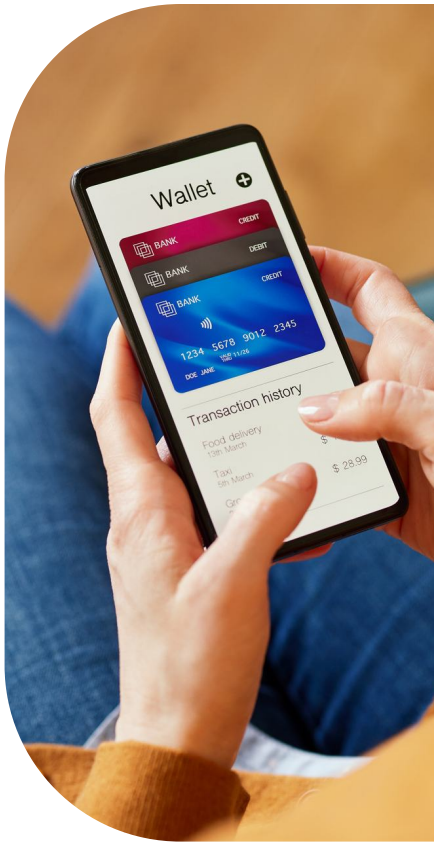
CASE STUDY

Enhancing mobile app security in 70 retail banks

Banking app software leader boosts security with best-in-class mobile app security platform

Industry

Software development
Payment security
Digital banking



This strategic implementation involved not only a 'mobile-first' approach but also a 'mobile-only' banking strategy. Users were given the option to exclusively access their bank accounts via a mobile app, eliminating the need for browser-based access or visits to a physical branch.

The company's security team partnered with Build38 to ensure they met stringent security measures. Build38 also provided them with powerful mobile app security via runtime application self-protection (RASP), and real-time monitoring and defense that allowed them to detect and respond to security threats and vulnerabilities within their application during runtime.

CASE STUDY

Safeguarding a top mobile car key app

Leading Asia Pacific auto maker ensures security and convenience for drivers with Build38

Industry

Auto manufacturing

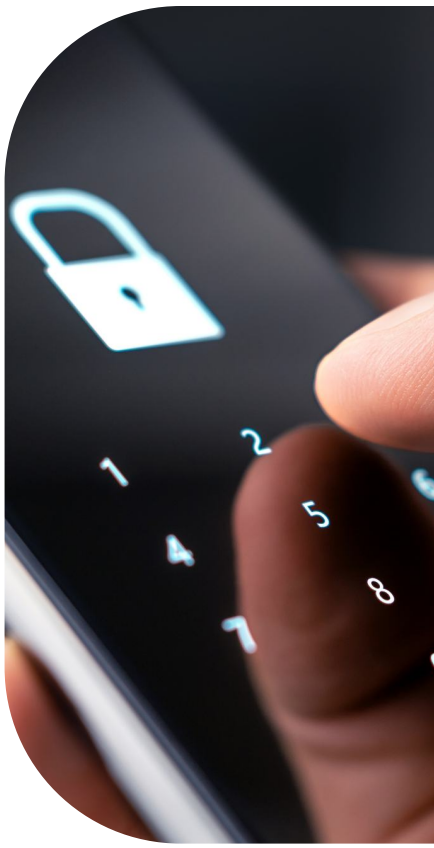
Our client, a leading Asia Pacific auto manufacturer, has a strong presence in both domestic and global auto markets. They offer a wide range of vehicles, including passenger cars, commercial vehicles, and electric models. Through strategic partnerships, they've expanded worldwide.

The automaker is dedicated to research, especially in electric and hybrid tech, to ensure top-notch safety and quality in their vehicles. They actively support their country's green transport efforts by innovating to meet customer demands and environmental goals.

CASE STUDY

Protecting users' most valuable online information

digital identity app partners with Build38 to ensure end-to-end mobile app security

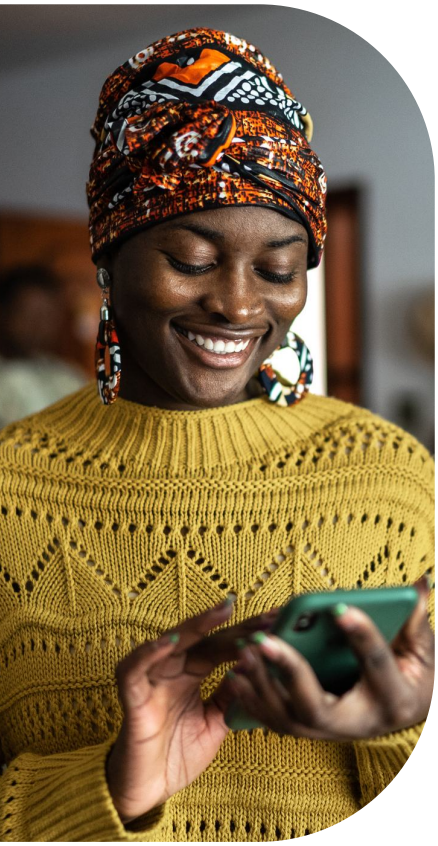


Industry

Software Development
ID Management
Financial Services

A leading digital identity app company needed to safeguard the personal information and authentication credentials of its users, and ensure compliance with the stringent eIDAS 2 regulatory frameworks mandated by the European Union (EU).

It embarked on a search for a security partner that would help it achieve its goals. After an exhaustive assessment of the leading vendors in the mobile app security market, the company chose Build38 to secure its digital ID app.



CASE STUDY

Eradicating mobile banking app fraud in Africa and the Caribbean

Prominent African and Caribbean mobile bank overcomes security crisis with Build38

Industry

Financial services
Mobile Banking

Facing a significant security incident of unauthorized withdrawals executed via their mobile banking app, a prominent African and Caribbean bank required an urgent solution and response to their security emergency.

The bank obtained a temporary license for Build38 and implemented the mobile app security platform as quickly as possible. As soon as it was deployed, all attacks ceased immediately. For the next four months, the security conducted an in-depth survey of security solutions on the marketplace and found Build38 to be the most comprehensive, confirming they had made the right decision and prompting them to acquire a permanent license for Build38.

About Build38

Your trusted mobile application security partner

The Build38 Mobile App Security Platform empowers businesses to effectively counter security attacks targeting their mobile apps. The platform stands out with its advanced Mobile App Self-Protection, cryptography and AI-driven Active App Hardening, and cloud-based Mobile Threat Intelligence.

Build38 streamlines compliance requirements, expedites certification processes, and eliminates the need for extensive security expertise within mobile app teams. It uniquely caters to the rigorous security requirements of various mobile applications, including mobile-first banking apps, SoftPOS apps, digital ID apps, digital wallets, car key apps, eHealth apps, crypto wallets, and many other application types.

Trusted by industry-leading mobile app companies, the integrated, yet modular, system guarantees zero-trust security across the entire mobile technology stack, encompassing the app, network, and backend infrastructure.

For more information, visit www.build38.com.