digital.ai™

THIRD ANNUAL

2025 Application Security Threat Report

Quantifying the evolving risks shaping modern application security

Contents

Introduction

Imagine a scenario where an unknown actor systematically examines the security of four out of five houses in your neighborhood, checking to see if the doors are locked. Some houses are merely observed, while others with unsecured entries are explored, potentially leading to stolen blueprints or other goods. In the most egregious cases, the actor takes everything of value and ransacks the rest.

In January 2025, 83% of the client-side apps monitored by Digital.ai had their front door "checked" (Figure 1).

What does this mean? These apps[1] were either run in an unsafe environment—such as a jailbroken or rooted phone, or worse, in a debugger or emulator—or they were probed for weaknesses. In the worst-case scenarios, they were actively tampered with.

If 83% of the homes in your neighborhood were subjected to such systematic security probing, most homeowners would respond with immediate action. You would ensure locks are in working order, invest in a video doorbell, or even install a comprehensive alarm system.

"Threat actors are not only picking locks, they're systematically checking every digital front door, and they're armed with increasingly sophisticated technologies."

Our digital neighborhoods are growing at an unprecedented rate, and they are under constant threat. In the face of such intrusions, and with the cost of a data breach approaching 5 million USD[2], organizations cannot delay in fortifying their investments. With an explosion of freely available tools and AI-powered capabilities, threat actors can now effortlessly reverse-engineer, analyze, and exploit applications at an alarming scale. Threat actors are not only picking locks, they're systematically checking every digital front door, and they're armed with increasingly sophisticated technologies.

Digital.ai's *2025 Application Security Threat Report* casts light on these shadows and aims to empower organizations to build stronger barriers around their digital properties. With hundreds of customers across nearly every vertical and continent, Digital.ai maintains a unique vantage point from which to track attacks on client-side applications. This report expands upon previous years' findings, incorporating industry-specific trends, regional differences, and a new focus on attack perspectives from both enterprises and users.

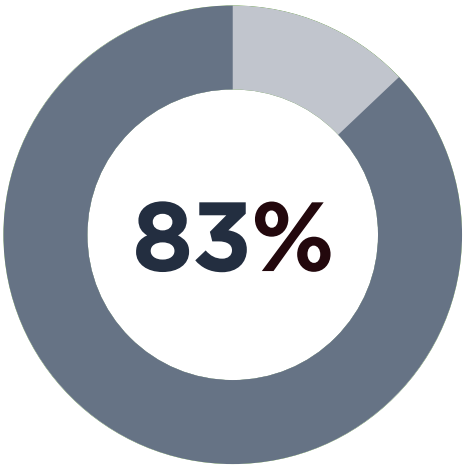


Figure 1: *In January 2025, 83% of Digital.ai-monitored client-side apps were attacked*

1. A "client-side app" refers to a software application where most of its code runs on the user's device (the "client"), meaning the app's functionality is primarily processed within the user's browser or operating system, rather than on a remote server.

2. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Key Findings

1 Rising Attacks on Client-Side Apps

The percentage of apps experiencing attacks has surged from 65% in February 2024 to 82.7% in January 2025, with mobile platforms (iOS: 88.1%, Android: 90.4%) being even more frequently targeted (Figure 2).

2 More Apps Are Released More Frequently

Organizations continue the frenetic pace of delivering apps to their customers. This trend is most obvious in the mobile application app space— **Apple's App Store® and the Google Play™ store offered nearly 4 million apps**[3] with 137.8 billion downloads in 2024—while desktop and web apps also remain popular.

3 Threats Are not Limited to FinServ Apps

While financial services have traditionally been a primary target, new data highlights significant attacks in the Telecom (91%) and Automotive (86%) industries, showing that threats continue to broaden across sectors (Figure 3).

4 Urgent Need for App Security

Organizations must prioritize resilience against reverse engineering and tampering, ensuring that security protections are continually updated to mitigate expanding and evolving threats.

Organizations that have implemented app protection measures are staying ahead of increasingly sophisticated attacks, while those without these defenses remain vulnerable targets. There are simple-to-implement application security solutions in-market today that provide enterprises with remarkably effective protection, saving businesses millions of dollars, reducing risk, and increasing the most valuable asset of all: customer trust.

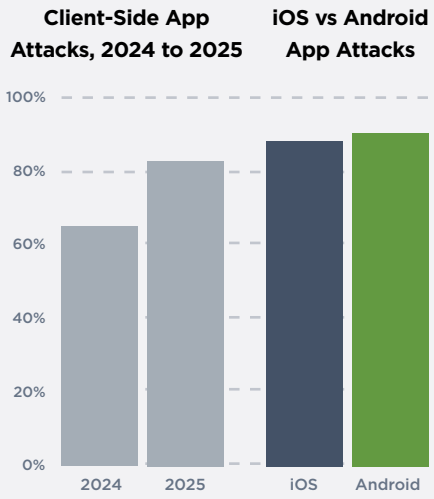
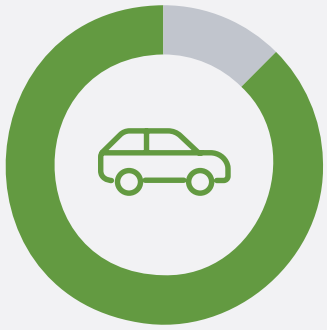
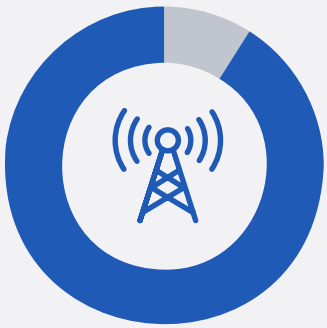


Figure 2: *Attacks rose on client-side apps from 2024-2025 across device types*



Automotive • 86%



Telecom • 91%

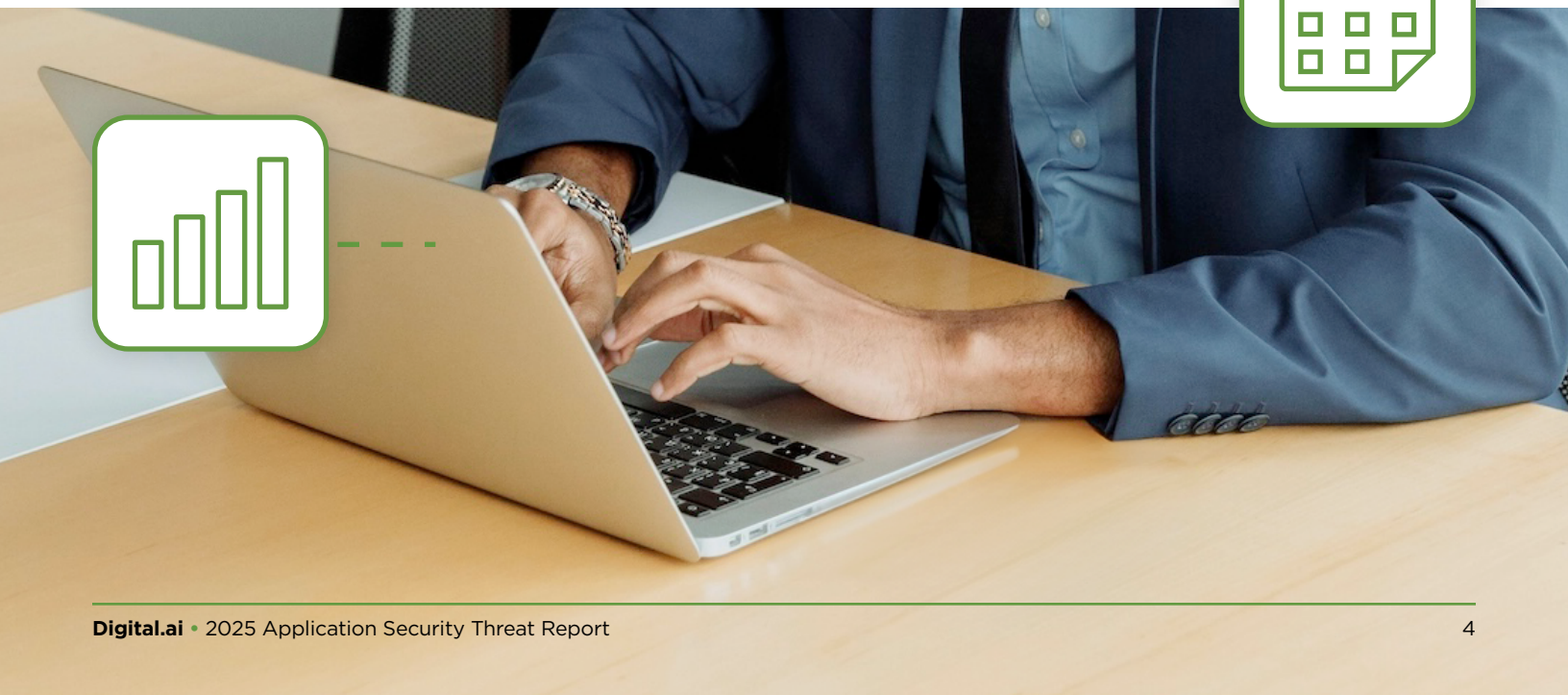
Figure 3: *Significant attacks in the Telecom and Automotive industries in 2025*

3. https://42matters.com/stats

Methodology

The report is based on data collected between January 1–31, 2025, from select customers of Digital.ai's Application Security offerings around the world. Digital.ai monitors and protects the surveyed customer applications from attacks occurring in the wild across the globe and in every major industry, including banking, media, telecom, manufacturing, gaming, and cyber security. The attack types discussed in this report (integrity, environment, and instrumentation) are the threats identified by the Organization of Worldwide Application Security Professionals (OWASP®) and documented in the OWASP Mobile Application Security Verification Standard (MASVS)[4]. More information on OWASP® and the MASVS can be found here.

4. "The OWASP® Word Mark and OWASP & Design™ Logo are registered or unregistered service marks of OWASP Foundation, Inc. in the United States and other countries. All rights reserved. Unauthorized use strictly prohibited.



Market and Industry Trends

Market Trends

From schools to global enterprises, more organizations are building their own mobile apps to be more connected globally and make it easier for customers to engage with their businesses through a quick tap on their smartphone's screen.

Why? Because mobile apps provide organizations with a direct, data-driven channel to understand, personalize, and enhance customer interactions in real-time.

Mobile apps have increasingly taken over our lives, brands, and interactions with customers to a significant degree. **Consider that the Apple's App Store® and the Google Play™ store together offer nearly 4 million apps for download[5], with 137.8 billion downloads in 2024.**

We live in an app-obsessed world. While organizations and consumers both embrace this trend, threat actors are arguably even more enthusiastic. The cost of a breach is approaching 5 million USD[6] and any app in the wild is a potential threat vector.

Temptation

Applications represent a juicy target for attacks, and threat actors are increasingly tempted to claim that prize. Apps contain more business logic than ever before as organizations migrate critical operations to client-side platforms for better customer engagement. This shift creates an expanding attack surface with vast potential gains for those with malicious intent.

Mobile, web, and desktop apps continue to attract outsized attention from threat actors in 2025. Across industries and across the globe, threat actors are attacking apps with an even greater frequency. In January of this year, 82.7% of apps monitored by Digital.ai experienced attacks. AI-assisted attacks, as well as a renewed willingness to share attack tactics and scripts, have made threat actors more efficient and prolific than ever before.

"Mobile apps provide organizations with a direct, data-driven channel to understand, personalize, and enhance customer interactions in real-time."

5. https://42matters.com/stats

6. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Industry Trends

Digital.ai has expanded coverage of industry-specific data this year to include attacks on apps in the telecom, healthcare, and automotive industries. These stats are ultimately representative of the app market as a whole, so even organizations that are not in one of these four industries should find this report meaningful.

Telecom

Telecom continues to evolve at a frenetic pace. The continued push to include more control and functionality on the client side of Telecom apps (including account management, digital wallets, and device security features), is most relevant to the data on attack trends. At the same time, mobile carriers are increasingly integrating eSIM activation, network switching, and roaming management into their apps, reducing reliance on physical SIM cards and in-store visits.

What does this mean for security? Essentially, more apps equal more attack surface. As Telecom apps become essential gateways to content, connectivity, and financial transactions, they become more attractive targets for credential theft, fraud, and app manipulation. Concurrently, 5G and Edge Computing expand the attack landscape. The shift to distributed computing reduces central chokepoints and increases potential points of failure and client-side risks.

Financial Services (FinServ)

Second only to Telecom in terms of the pace of innovation is likely the Financial Services sector. One of the key changes driving the FinServ industry forward is a trend towards embedding finance and "Banking as a Service" (BaaS) into what were traditionally non-FinServ apps.

More non-financial companies (retailers, tech firms, automotive manufacturers) are embedding financial services into their platforms, making FinServ more decentralized and providing a ripe target for threat actors. Telecom companies, for example, might provide payment services to their apps. Automotive companies might provide the ability to purchase maintenance or parts.

Traditional FinServ, meanwhile, has picked up the pace of adding generative AI and predictive analytics to hyper-personalize banking, a trend that contributes to the growing footprint of client-side banking apps.

"As Telecom apps become essential gateways to content, connectivity, and financial transactions, they become more attractive targets for credential theft, fraud, and app manipulation."

Automotive

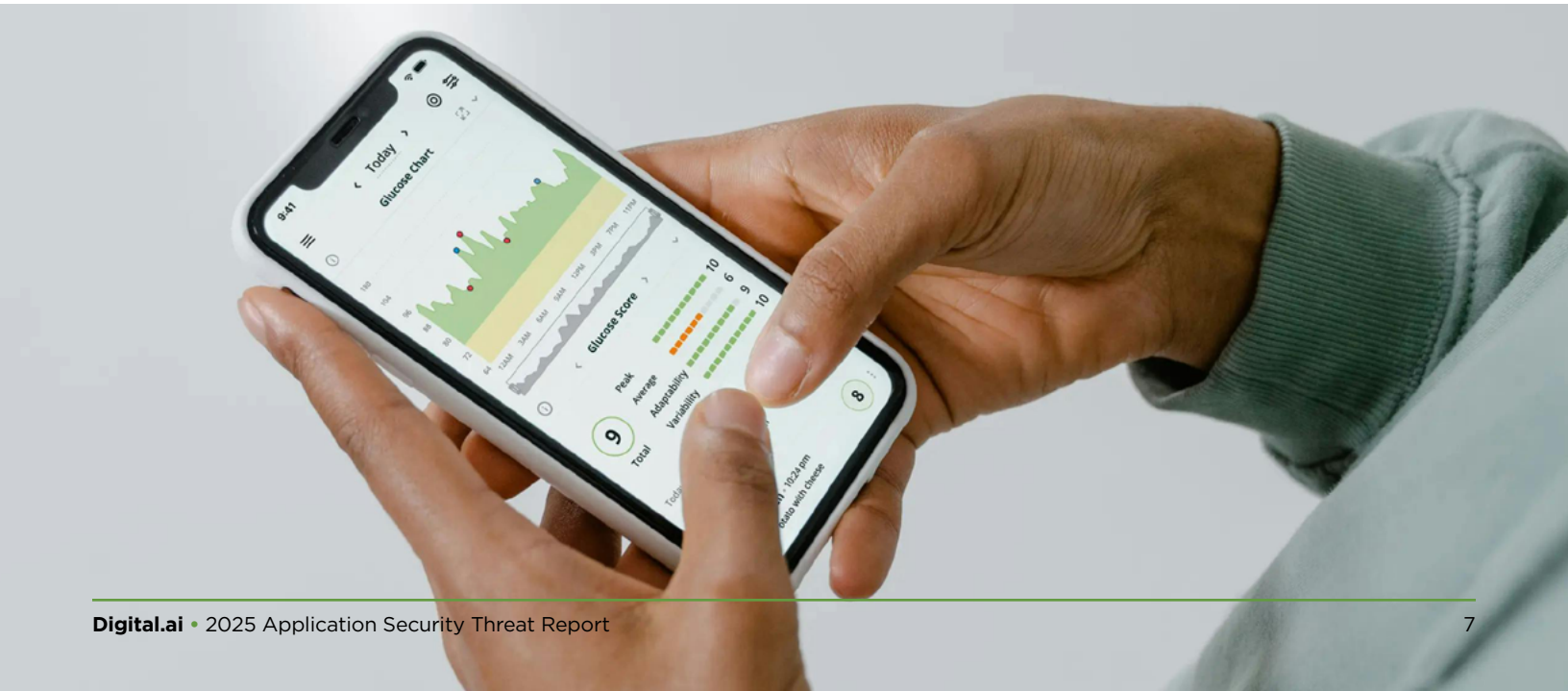
In the early days of the mobile phone industry, analysts often compared the social status of smartphone owners to that of car owners. Today, Automotive software applications have brought the comparison full circle, with Automotive companies now racing to integrate increasingly sophisticated apps into vehicle dashboards and to enhance phone apps with functionalities such as unlocking, starting, and even servicing cars remotely.

The shift from hardware centric to software-defined vehicles is ongoing, with over-the-air (OTA) updates, AI-powered driver assistance, and cloud-connected vehicle services rapidly becoming the norm rather than the exception. Every one of these advances, though, is a prime opportunity for threat actors—some of whom are simply curious as to whether they can drive from the backseat of their car, while others are looking to wreak havoc and cause harm.

Healthcare

AI-powered diagnostic tools and virtual health assistants are transforming patient care, especially with predictive analytics improving early disease detection. In an increasing number of cases, patients access these insights via their mobile phones. Meanwhile, the rise of digital health platforms—like telemedicine, remote patient monitoring, and digital therapeutics—is seeing widespread adoption, integrating wearable tech with mobile health-tracking apps and cloud-based health ecosystems.

These Healthcare mobile apps are all susceptible to reverse-engineering; sometimes merely by curious, tech-savvy patients looking to modify their own self-care, and in worst-case scenarios, by threat actors intending to cause physical harm.



Attack Data

This section presents an aggregated look at the likelihood of any app being attacked. Aggregated, in this context, indicates the combined data across all industries, geographies, and platforms protected and monitored by Digital.ai Application Security offerings.

As mentioned before, 82.7% of apps experienced attacks in January 2025—a 27% increase from 2024 (Figure 4).

Why is this happening?

1. First, tool democratization—reverse-engineering tools (Frida, Ghidra, etc.) continue to proliferate and attract large communities of users who are likely to share ideas, tips, and tricks.
2. Second, the growing proliferation of AI tools used by threat actors. Generative AI assists in both malware development (more malware is being created faster) and in source code analysis.
3. Finally, the growing attack surface not only leads to an increase in the total number of attacks but also provides fertile ground for threat actors to thrive. Both white hat and black hat hackers typically learn by doing, and our app-centric world offers ample opportunities for them to hone their skills.

What's different in 2025? Attack rates have surged across all industries. No sector is immune—even previously less-targeted areas like healthcare and automotive are now under significant threat.

"Attack rates have surged across all industries. No sector is immune—even previously less-targeted areas like healthcare and automotive are now under significant threat."

2024-2025 App Attacks

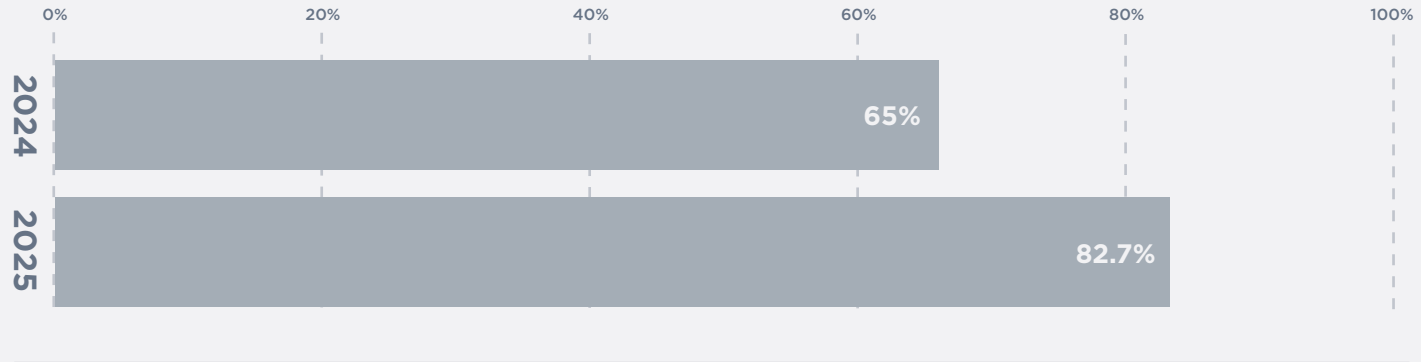


Figure 4: *Client-side app attacks increased by 27% between 2024 and 2025*

Attacks by Industry

Financial services and gaming apps have historically been the most targeted sectors. However, due to limited data availability this year, gaming was not included in our analysis. Meanwhile, telecom and automotive applications are now experiencing similar levels of attacks as those previously seen in financial services. Greater regulation in some sectors has led to improved security controls, which may also contribute to better detection and reporting of attacks.

Financial services apps had an 87.5% attack rate (Figure 5A). Attackers target digital banking, fintech, and payment platforms to intercept data, reverse-engineer authentication mechanisms, and automate fraud. Man-in-the-middle attacks and API exploitation remain common. Despite regulations like the Revised Payment Services Directive (PSD2), attackers continue to subvert identity verification and bypass multi-factor authentication.

Healthcare applications saw attacks on 78.5% of monitored apps (Figure 5B). The industry's rapid digitization, telemedicine adoption, and reliance on mobile apps for patient management create new attack surfaces. Patient data theft, ransomware targeting healthcare APIs, and manipulation of remote monitoring systems are key threats. Strict regulations like Health Insurance Portability and Accountability Act (HIPAA) in the United States and the EU's General Data Protection Regulation (GDPR) drive stronger security and improve the visibility of attacks.

Automotive applications experienced an 86% attack rate (Figure 5C). Software-defined vehicles rely on mobile apps for remote access, telematics, and OTA updates, making them attractive targets. Attackers manipulate remote unlocking, abuse charging infrastructure payment systems, and intercept vehicle control data. Security controls in connected car ecosystems remain inconsistent, with APIs often exposed to tampering.

Telecom applications had the highest attack rate at 91%, though our sample size for this industry is small relative to the others (Figure 5D). Nevertheless, some factors lead us to believe telecom will remain a target for threat actors. The integration of mobile identity management, carrier billing, and eSIM activation into telecom apps has increased their value as targets, while SIM-swapping fraud, fake telecom apps, and API exploitation are major attack vectors. As telecoms adopt stricter security measures, they may also uncover and report more attacks than less regulated industries.

While all industries saw a rise in attacks this year, telecom surpassed financial services in attack frequency, and healthcare and automotive applications are now top targets. As regulations tighten, better security may improve attack detection, giving enterprises clearer insight into the risks they face.

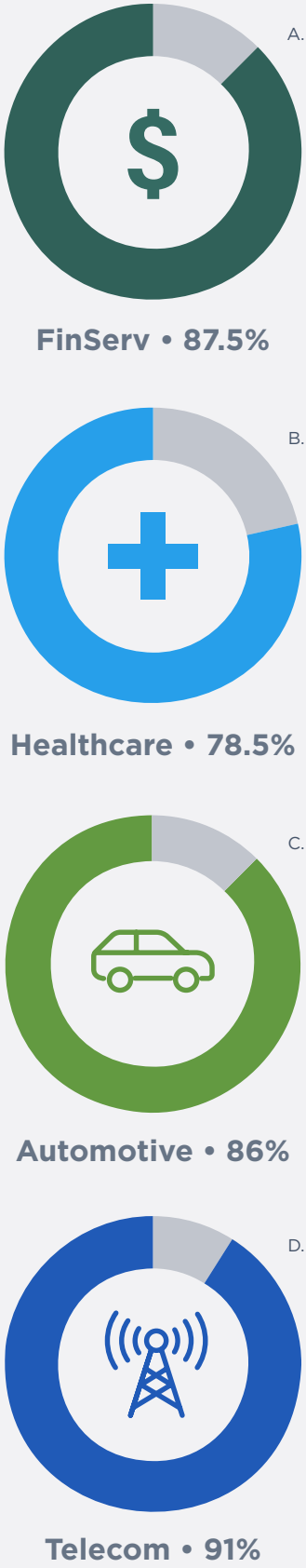


Figure 5 (A-D): *Attacks on client-side applications increased across all industries in 2025*

Attack Likelihood: Android vs. iOS

In 2025, attack rates on mobile applications remained high, with 90.4% of monitored Android™ platform apps and 88.1% of apps made for the iPhone® mobile device experiencing attacks. While Android has historically been targeted more often, the gap has narrowed as iOS attacks increase, likely due to a rise in jailbreaking and advanced exploitation techniques. To face these new threats, Digital.ai has improved jailbreak and root detection capabilities, which has resulted in an increase in jailbreak and root reporting.

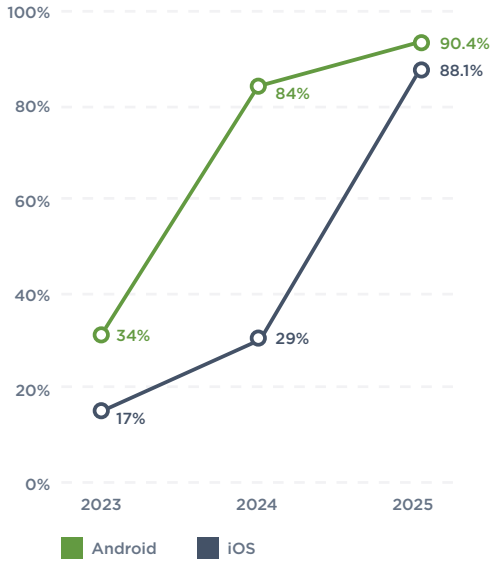


Figure 6: *Increase in attacks across device types between 2023 and 2025*

Environment attacks, where apps run in compromised conditions such as rooted or jailbroken devices, affected 84.2% of Android™ platform apps and 79.8% of iOS apps (Figure 7). The widespread availability of rooting and jailbreaking tools continues to erode platform security. In the house analogy, an environmental attack is akin to checking the doorknob to see if it is locked. It does not necessarily imply ill intent, but it is surely something a homeowner will want to be aware of if it happens.

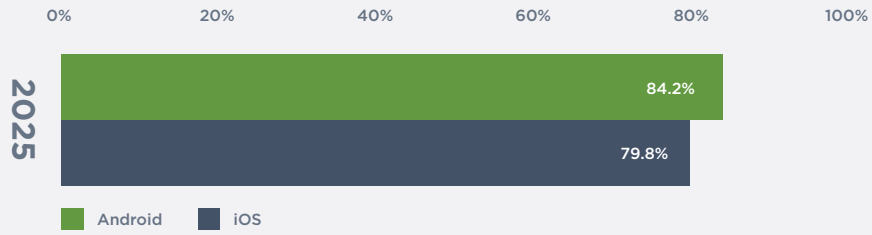


Figure 7: *Environment attacks in 2025*

Instrumentation attacks, which involve dynamic code modification or hooking frameworks like Frida, were significantly more common on Android, occurring at a rate of 81.5% compared to 44% on iOS—nearly twice as much (Figure 8). Android's open architecture makes it more susceptible to runtime manipulation, whereas iOS has stronger built-in restrictions. In the house analogy, an instrumentation attack is more invasive than simply checking locks. It's roughly equivalent to an intruder walking through an unlocked door, scoping out the house to locate valuables, and perhaps taking a few notes before departing through the unlocked door.

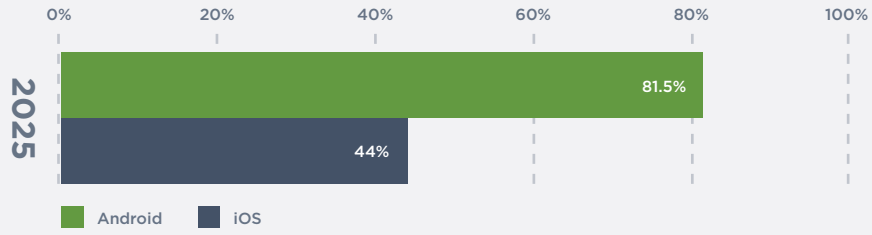


Figure 8: *Instrumentation attacks in 2025*

"While Android has historically been targeted more often, the gap has narrowed as iOS attacks increase."

Integrity attacks, where app code is modified or repackaged, affected 51.4% of Android apps and 23.3% of iOS apps (Figure 9). Android's app distribution model and third-party app stores make it easier for attackers to distribute modified apps, whereas iOS benefits from stricter app store controls. In the house analogy, integrity attacks are the equivalent of somebody changing something in the house, almost always with malicious intent. They might leave with a TV, take a drawer full of jewelry, or perhaps vandalize the property.

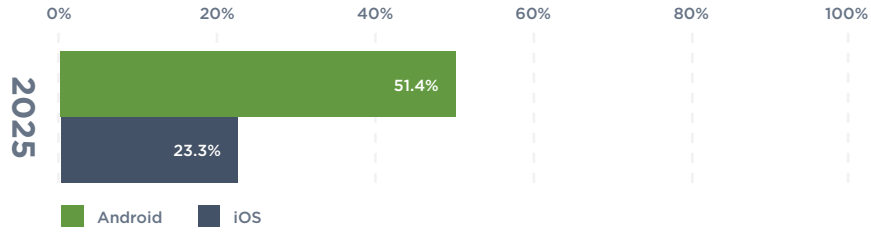
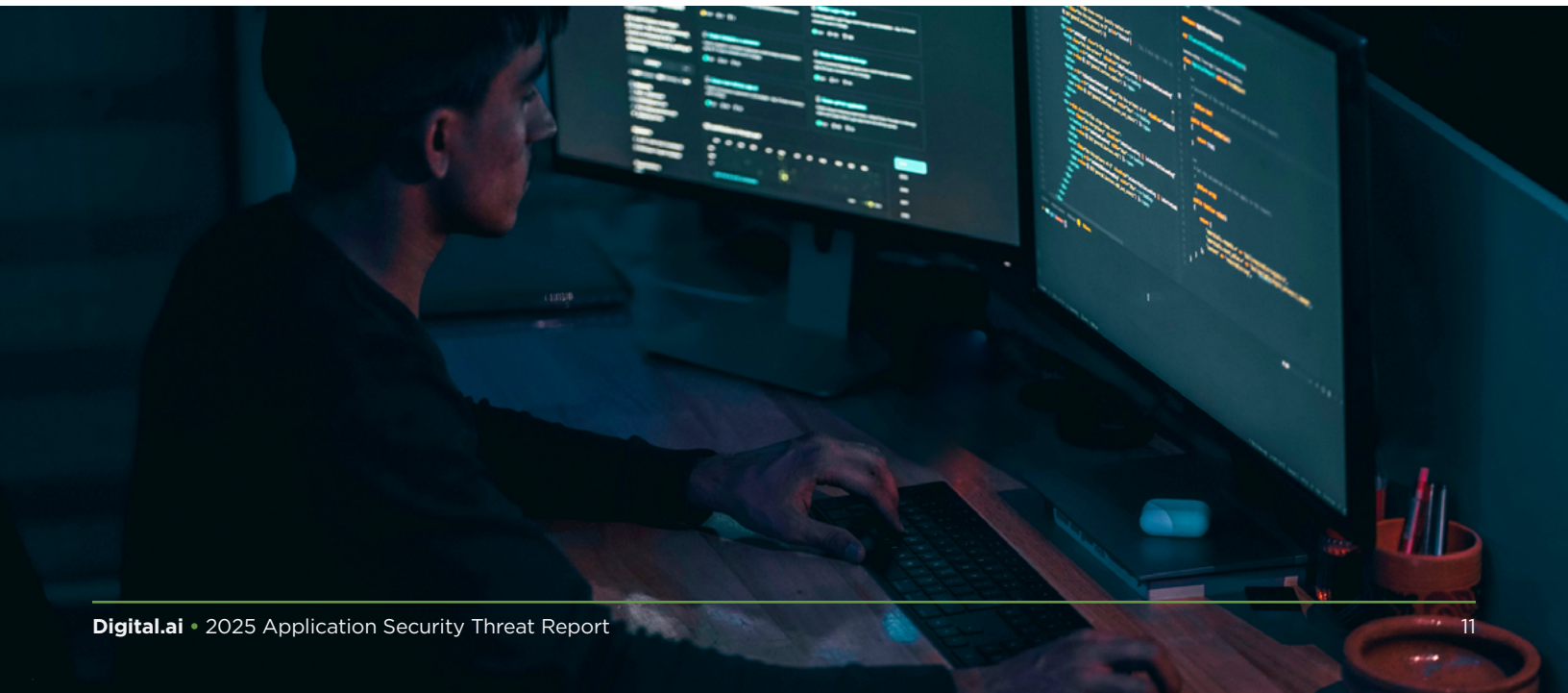


Figure 9: *Integrity attacks in 2025*

"Integrity attacks are the equivalent of somebody changing something in the house, almost always with malicious intent."

Ultimately, both platforms face persistent threats, but differences in architecture and security policies affect attack techniques. As a result, organizations apply different levels, layers, and types of protections to apps running on the two different operating systems.



Threat Perspectives

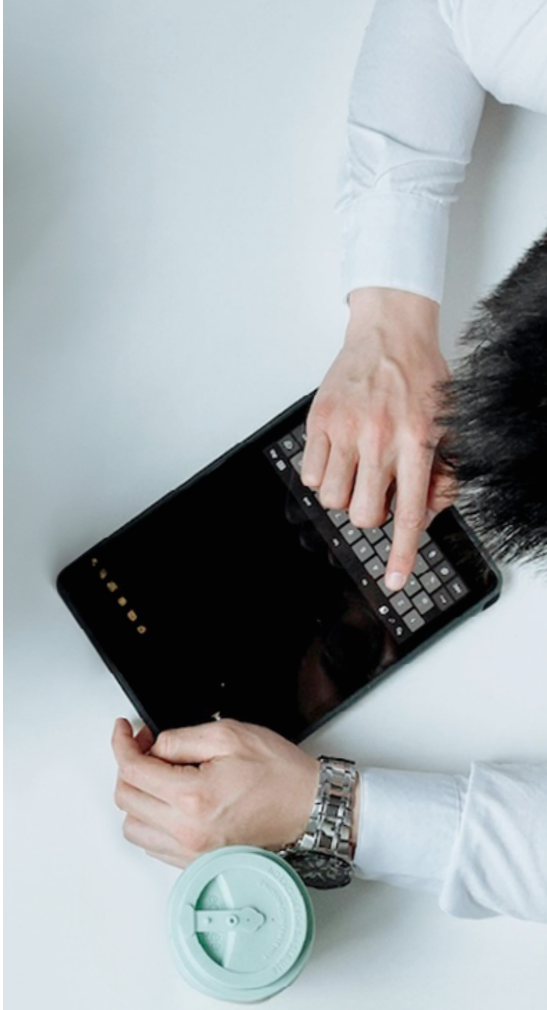
This section explores critical nuances in Digital.ai's threat assessment, examining the measure of attack likelihood from both enterprise and end-user perspectives, and focusing on the frequency of threats across individual app instances rather than the number of mobile apps deployed by Digital.ai customers.

Enterprise Perspective:

This method considers the threats based on the number of organizations or enterprises that develop mobile apps. For instance, if two different organizations each develop one mobile app and one of these apps is compromised, the data would show that 50% of the organizations' apps were attacked. *This approach focuses on the proportion of affected apps relative to the total number of apps developed by these organizations.*

User-Level Perspective:

This approach measures threats by examining the scale of user exposure to security incidents. Imagine the two apps developed by these organizations are used by 10 million customers each, resulting in 20 million total app instances deployed. If 400,000 of these instances are attacked, the data would show that 2% of the app instances were attacked. *This method provides insight into the overall threat landscape by measuring the impact across the total number of app instances actively used "in the wild."*



While the enterprise perspective is meaningful—highlighting that a single breached app can compromise an entire organization—***examining the absolute number of attacked app instances provides a more comprehensive view of where, how, and how frequently applications are attacked.***

User attack stats are also helpful because these attacks can significantly damage user trust, which is obviously of vital concern to an organization. For instance, if news of a breach becomes public or a user is warned individually about an attack, their perception of the enterprise with which they are interacting may be negatively affected.

User Perspective (iOS vs. Android) Across OS Versions

This section presents an analysis of user perspective attack statistics observed during January of this year, based on the overall number of app instances monitored by Digital.ai.

From both enterprise and user perspectives, it is useful to think about attacks based on the categories assigned by OWASP® using their MASVS resilience categories. The following list is an aggregated account of app instances attacked during our observation in 2025, organized by MASVS category:

- Overall attacks: 0.40%
- Unsafe environment: 0.35%
- Integrity: 0.03%
- Instrumentation: 0.04%

Attacks on Android™ Platform Apps Across Versions

Readers of Digital.ai's 2024 Threat Report have requested data on the number of attacks across mobile OS versions. An initial hypothesis was that the data would exhibit an inverted bell curve (Figure 10).

This assumption was based on the notion that older OS versions have had more time for researchers to identify vulnerabilities, particularly those enabling threat actors to root devices. Rooted devices are more susceptible to environmental attacks and, consequently, to integrity and instrumentation attacks. Conversely, the newest OS versions might contain vulnerabilities not yet identified by security testing and are often targeted by curious users exploring the system's defenses.

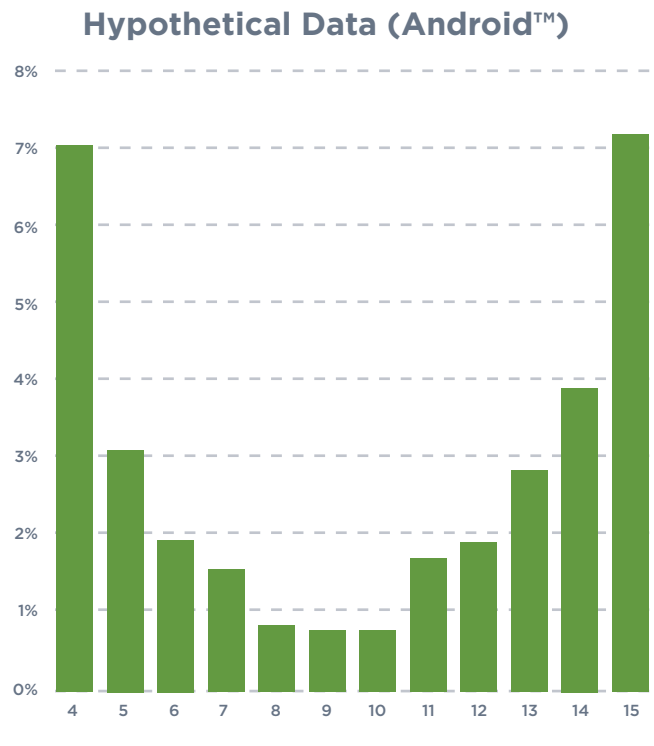
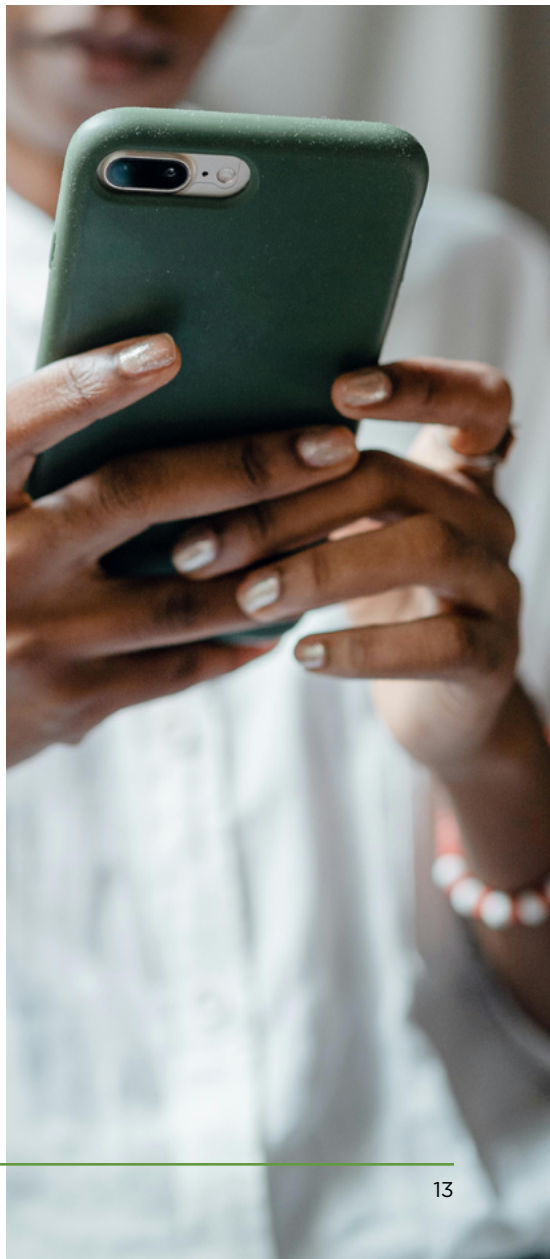


Figure 10: *Hypothesized attack % across versions*



However, the real-world data presented a more complex picture (Figure 11). Android 6 is likely an anomaly, due to a localized attack reported numerous times. Excluding this version, the data revealed a bell curve of attacks, with higher frequencies in the middle Android versions (7,8,9,10,11) than at either end of the spectrum. Several factors may contribute to this pattern:

1. OS developers, such as Apple and Google, have progressively improved the security of their systems. Newer OS versions are typically more challenging to compromise, necessitating greater innovation from threat actors. This phenomenon is discussed in this blog post. Consequently, newer OS versions attract significant attention until effective attack techniques and tools are developed.
2. Threat actors aim to create tools that are usable across the widest range of OS versions. However, they face similar challenges to application developers in supporting older versions. Procuring devices running outdated OS versions becomes increasingly difficult over time, and maintaining support for these devices yields diminishing returns as user numbers dwindle.

Attacks on iOS Apps Across iOS Versions

Apple® devices exhibit a similar curve to Android™ devices, although there are fewer maintained release versions for both threat actors and developers to support. Apple's efforts to ensure that all users, including threat actors, adopt the latest OS versions are evident in the data.

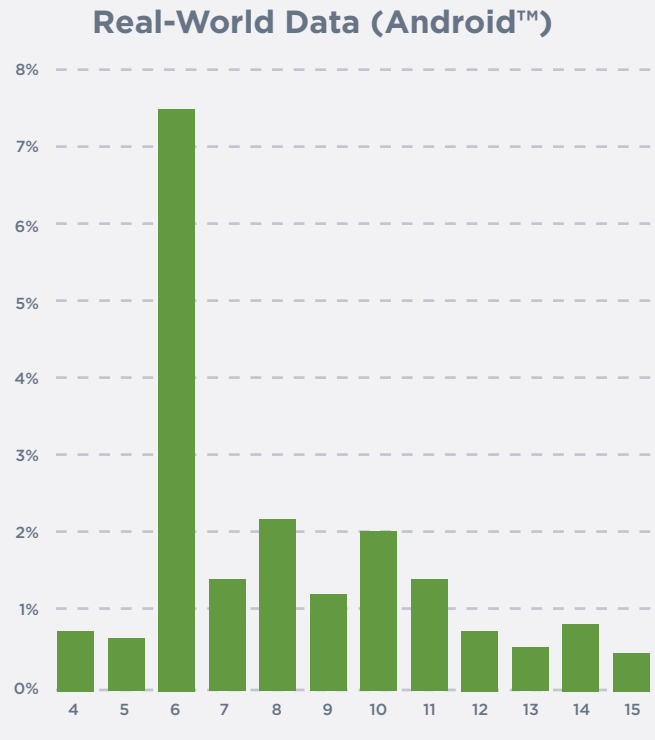


Figure 11: *Attack % across versions*

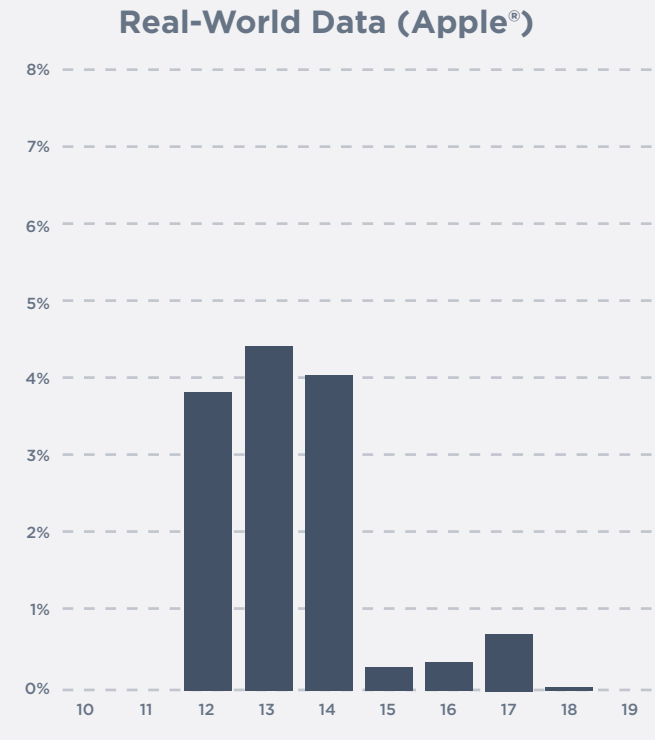


Figure 12: *Attack % across versions*

Regional Differences in Attack Rate

Attack rates vary by region, with EMEA experiencing the highest rate at 0.69% of all app instances reporting an attack, followed by North America at 0.64%, LATAM at 0.58%, and APAC at 0.42% (Figure 13).

- EMEA's high attack rate is likely influenced by its strong fintech adoption and stringent regulatory requirements. Regulations such as GDPR have heightened awareness of privacy and security concerns, leading to more mature security programs and improved attack detection.
- North America's high attack rate is likely driven by its concentration of financial services, healthcare, and technology firms. Despite significant security investments, frequent attacks on high-value targets keep overall risk elevated, justifying these investments.
- Lower attack rates in APAC and LATAM are encouraging but may also indicate a lack of visibility due to underdeveloped cybersecurity practices. Regulatory environments play a crucial role in attack visibility. EMEA and North America have well-established cybersecurity laws increasing incentives to enhance protection and detection capabilities. In contrast, LATAM and APAC, having different reporting and data security requirements, may have comparable attack volumes but lower visibility into threats.

"Better detection and reporting provide a clearer understanding of the threat landscape."

Figure 13: *Attack rates by region*

While experiencing more attacks is not desirable, better detection and reporting in regions like EMEA and North America provide a clearer understanding of the threat landscape. This perspective suggests that higher observed user attack rates may indicate more robust security practices and better preparedness.

Regulatory frameworks influence the detection of cyber threats. *EMEA and North America benefit from well-established cybersecurity laws and data protection requirements, motivating regulated entities to enhance protections and, consequently, improve detection capabilities. LATAM and APAC, however, may experience similar attack volumes but have lower visibility into these threats due to differing regulatory frameworks found there.*

This paradoxical situation suggests that while a higher number of detected attacks is not inherently desirable, it may indicate better detection and reporting mechanisms. Therefore, regions with fewer reported attacks, like LATAM and APAC, might not necessarily be safer but rather less visible in terms of threat detection. From this perspective, EMEA and North America may be viewed as well-positioned as compared with LATAM and APAC and one could additionally argue that the telecommunications sector is better positioned than the financial services sector due to its higher visibility of attacks.

Malware

Until now, this report has been discussing a very specific kind of threat, one which the vast Fortune 500® companies are taking steps to defend against and which OWASP® has labeled a threat to the "resilience" of apps.

Unfortunately for organizations who are creating apps for their end users, the threat landscape includes a wide variety of threats, most of which are helpfully labeled within OWASP's MASVS.

Among these additional threats is malware running on the endpoint. Malware poses numerous problems for end-users, many of which have been chronicled by security vendors. These vendors produce reports that describe these varied threats. This report, by contrast, focuses on the threat of malware interacting with apps created by Digital.ai clients.

Digital.ai tracks this malware using a feature called "Malicious Package Detection."

Throughout January this year, Digital.ai found that 1.2% of monitored devices were infected with some type of malware; which can be further dissected into the following categories:

Threat Level	Percentage
High	6.94%
Medium	10.65%
Low	83.77%

Malware classified as having a *high* threat level encompasses various types, including banking trojans, spyware, viruses, and worms.

What this means: As a creator of applications, you are also facing malicious code running on some of the same Android devices that are running your apps. That malicious code can be innocuous or dangerous. Our research shows that 6.94% of the malware is highly threatening and and includes banking trojans, spyware, trojans, viruses, worms.

Conclusion

Not everyone who checks for an unlocked door is an intruder; locksmiths, for example, might check to see if the lock is working appropriately. However, if the vast majority of locks in a neighborhood are being checked, residents may prefer to know more about who is doing the checking and what their intentions are.

Attack rates on apps have reached unprecedented levels, with 82.7% of monitored apps experiencing attacks in January 2025, highlighting the persistent and evolving nature of these threats.

> **"Organizations can no longer afford to leave their doors unlocked or rely on subpar locks."**

While financial services and telecom remain prime targets, healthcare and automotive applications are now equally at risk as industries embrace mobile-first and software-defined ecosystems. Android™ platform and Apple® iOS attacks continue to rise, with adversaries leveraging runtime instrumentation, environment manipulation, and integrity compromises to bypass security controls. Regional differences suggest that regulation and security maturity may influence attack detection, with EMEA and North America reporting higher attack rates than LATAM and APAC.

In the vulnerable digital neighborhood of mobile apps, organizations can no longer afford to leave their doors unlocked or rely on subpar locks. Just as a comprehensive neighborhood defense requires vigilant residents, resilient barriers, and advanced surveillance, mobile security demands a multi-layered and proactive approach. Sophisticated attackers—like persistent burglars—will probe every weakness, requiring organizations to deploy advanced obfuscation, anti-tamper techniques, strong encryption, runtime protections, and continuous monitoring to fortify their digital perimeters against increasingly frequent and calculated intrusions.

Digital.ai's Application Security solutions deliver cost-effective, simple-to-implement, and remarkably effective protection against these attacks. As threats evolve, Digital.ai continuously expands its protection capabilities, identifies emerging attack vectors, and streamlines implementation—making robust application security not just necessary, but accessible to all.

Appendix

The data in this report was collected during the month of January 2025 from the apps protected by Digital.ai, representing customers across the globe in every major industry, including banking, media, telecom, manufacturing, gaming, and cyber security. For questions or comments, please contact Daniel.Shugrue@digital.ai

About Digital.ai

Digital.ai is the only AI-powered software delivery platform purpose-built for the enterprise, enabling the world's largest organizations to build, test, secure, and deliver high-quality software. By unifying AI-driven insights, automation, and security across the software development lifecycle, Digital.ai empowers enterprises to deliver innovation with confidence. Trusted by global 5,000 enterprises, Digital.ai is redefining how enterprises build better software in an AI-driven world. Additional information about Digital.ai can be found at digital.ai and on LinkedIn, YouTube, and X.