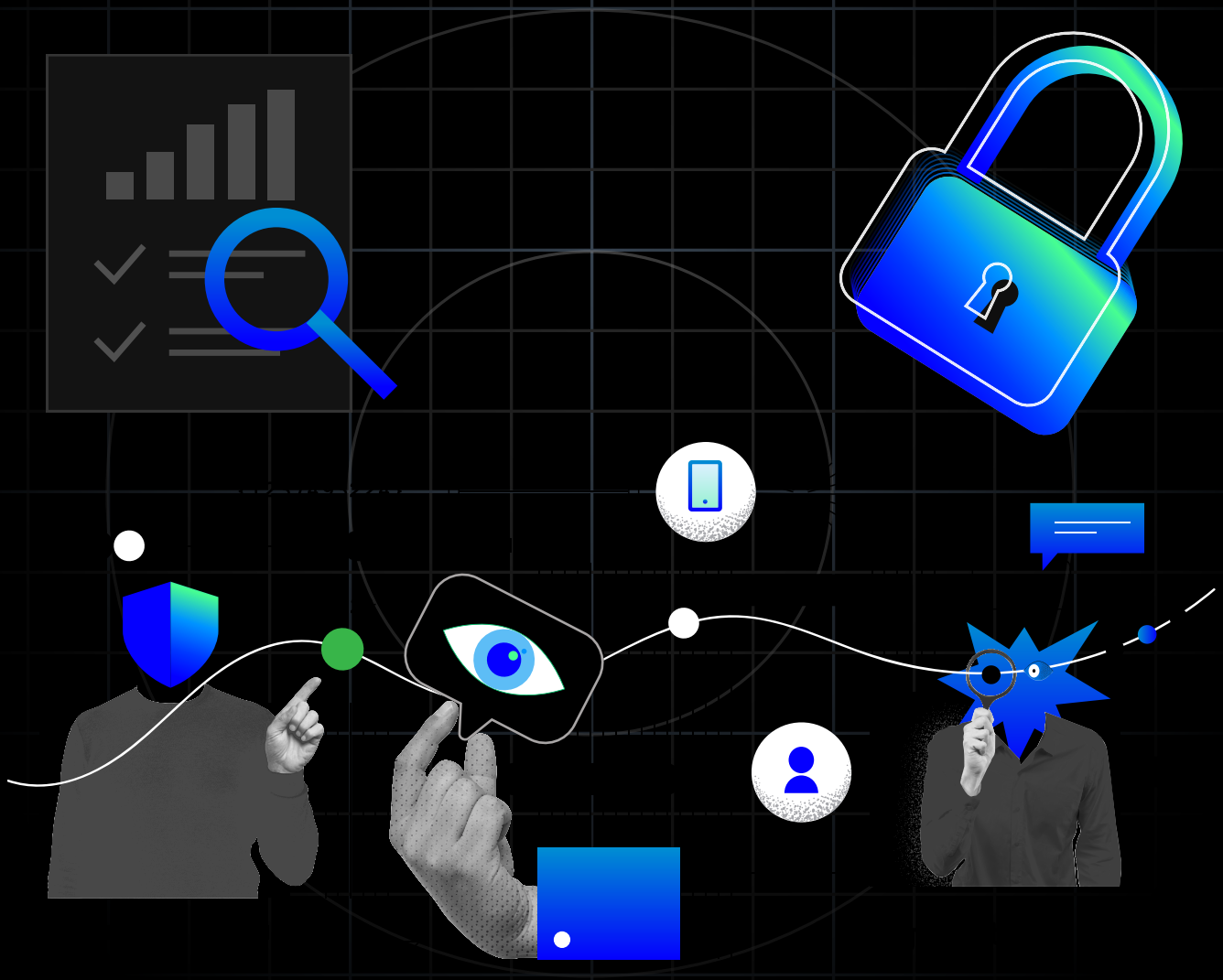
# The Security Paradox:

## Users Want Protection, Apps Deliver Vulnerabilities

What consumers told us about mobile app security — and how their most-used apps failed the test



# Table of Content

# Executive Summary

American consumers have evolved into security experts who know what they want: transparent data practices, minimal permissions, and proof that apps are actually secure.

They read permission requests, delete suspicious apps, and seek alternatives when their trust is broken.

When we tested 35 of America's most downloaded apps against these expectations, the gap was staggering. Every app we tested failed basic security standards that users now demand. Mobile app security is broken.

And it's also the biggest business opportunity you're overlooking.

Our research with 1,000 U.S. consumers reveals a market ready for disruption. More than half will uninstall apps for requesting excessive permissions. Nearly two-thirds will abandon apps that share data without clear consent. When they learn about a breach? Six out of ten users are gone.

Users are actively seeking better-secured alternatives. The demand for independently tested apps has never been higher, creating real opportunities for companies willing to prioritize security transparency.

Think about it: While consumers overwhelmingly demand end-to-end encryption, fewer than half of popular apps actually deliver it. Users reject apps with excessive permissions, yet only one in three apps minimize their requests. These disconnects represent more than a security problem. It's a competitive landscape waiting to be reshaped.

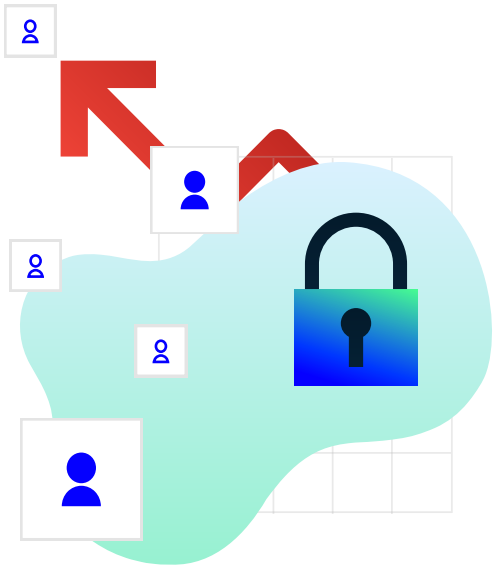
The companies that understand this shift will capture market share from an increasingly sophisticated user base ready to reward transparency with loyalty.

Security Drives Choice

88%

**Prefer apps that are independently tested for security.**

# The Rise of the Security-Savvy Consumer

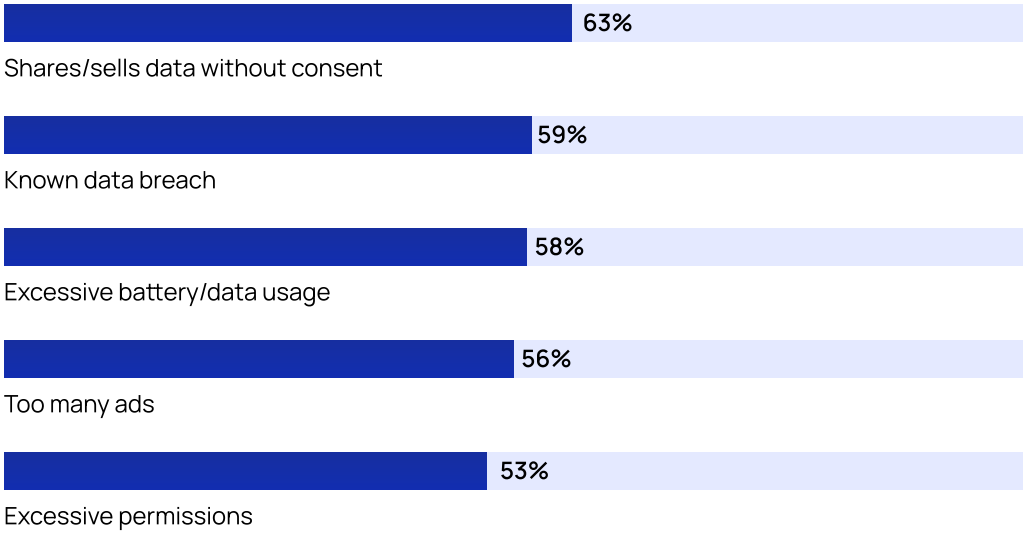


Mobile users aren't just security aware — they're security activated. They no longer passively accept what apps offer.

They're reading permission requests, scrutinizing privacy policies, and deleting apps that don't meet their expectations. This is not a fringe behavior — it's mainstream.

## Top Churn Triggers

**Top 5 Reasons U.S. Consumers Uninstall Apps:**



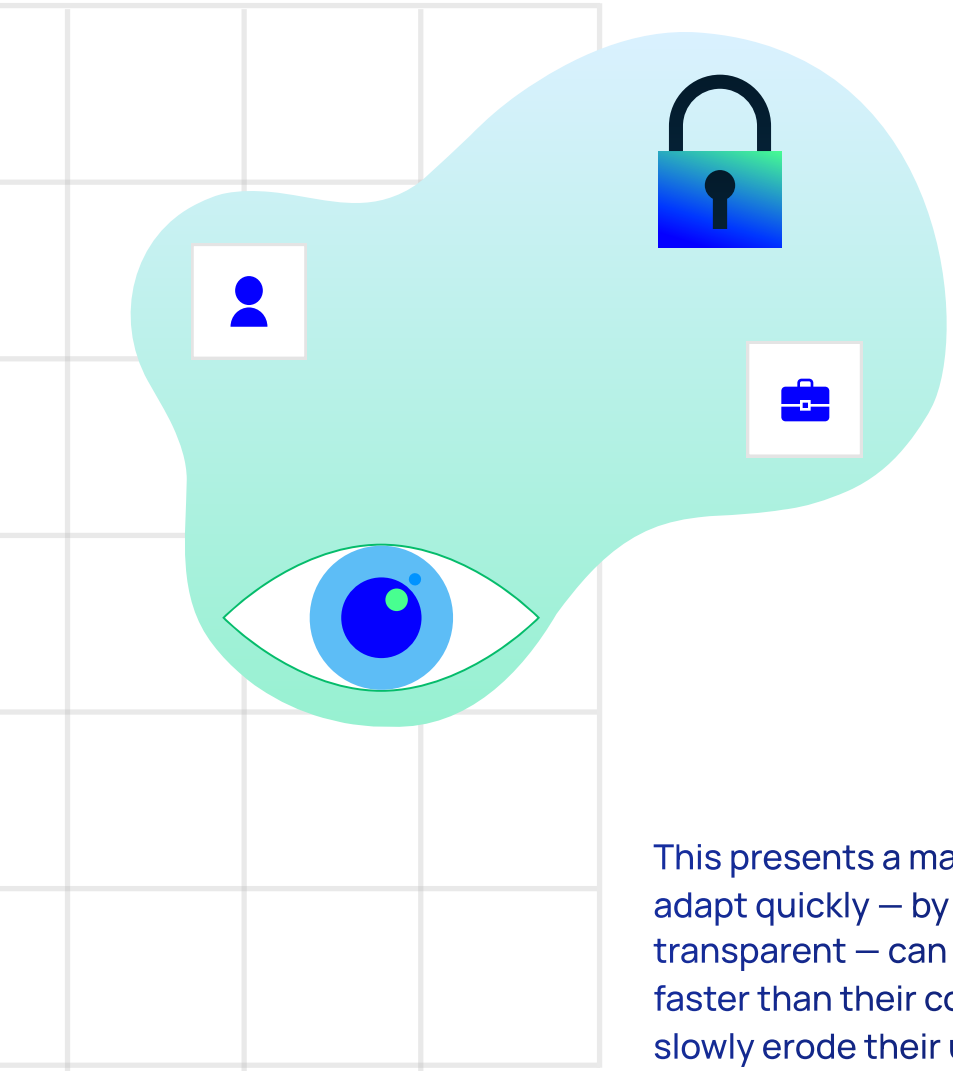

**From App User to App Auditor today's users are more than just digital consumers — they're security gatekeepers.**

- They check permissions
- Review privacy settings
- Track breach history
- Seek independently verified security

**Trust is no longer passively given. It's earned.**

These numbers reflect a wider cultural shift. Years of privacy scandals, data leaks, and silent permissions creep have conditioned consumers. The result is a user base that behaves like informal security auditors. They expect apps to earn their trust, not assume it.

This expectation isn't limited to security-focused apps. It applies across the board — from banking and fitness to e-commerce and dating. Users are bringing a security-first lens to every new app they download.



### What This Means for Businesses

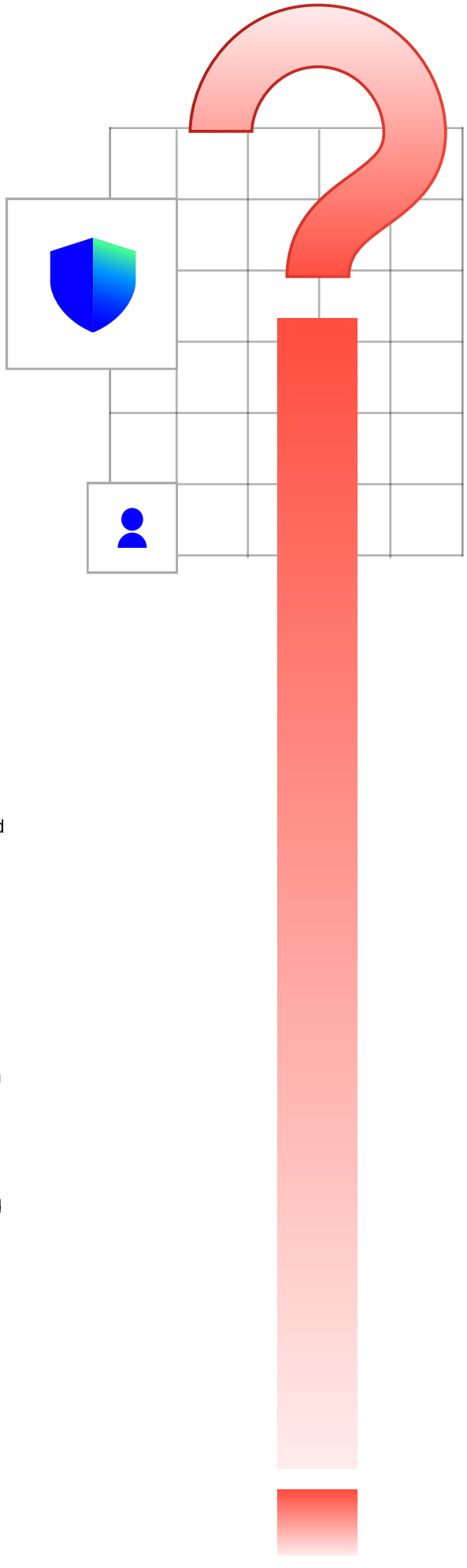
The bar has been raised. Users now measure app quality not just by UI/UX or features, but by how respectfully and responsibly it handles data. The implications are clear:

This expectation isn't limited to security-focused apps. It applies across the board — from banking and fitness to e-commerce and dating. Users are bringing a security-first lens to every new app they download.

- Apps that don't justify their data access get deleted
- Companies that suffer breaches lose long-term user trust
- Users are rewarding visible security features with loyalty

This presents a massive opportunity. Businesses that adapt quickly — by making security visible and transparent — can differentiate themselves and grow faster than their competitors. Those that don't will slowly erode their user base, one uninstall at a time.

# Consumer Security Expectations & Trust Patterns



User trust follows patterns that directly reflect their lived experiences with technology. Every data breach headline, every overly broad permission request, and every unclear privacy policy has taught consumers to evaluate apps with increasing skepticism.

This attitude is based on practical knowledge gained from years of watching companies mishandle their personal information.

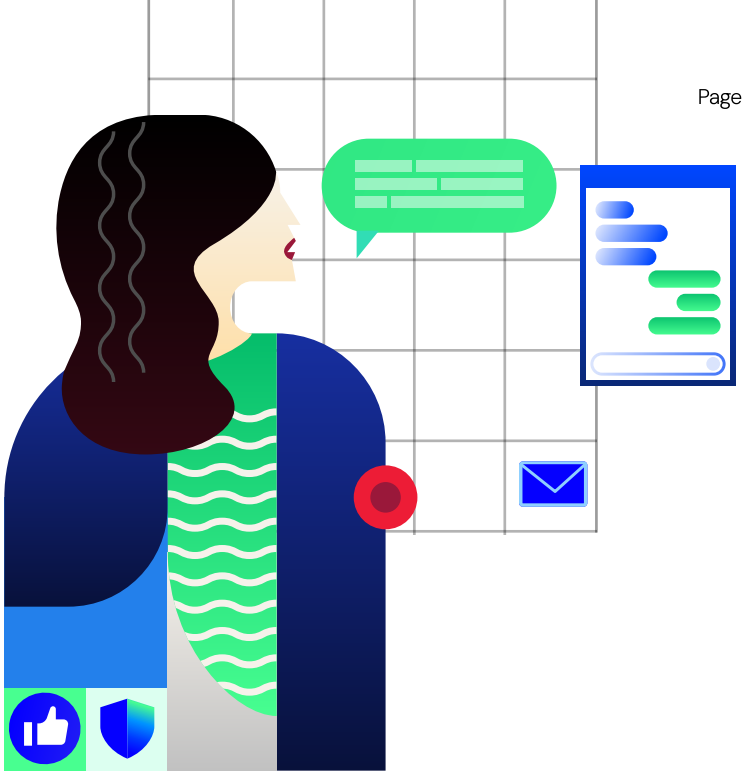
The result? Trust isn't distributed equally across app categories. Users have developed a sophisticated understanding of which types of apps pose the greatest risks to their privacy and security.

### The Trust Hierarchy

When we asked users which apps they distrust the most with their personal data:

- Apps that don't justify their data access get deleted
- Companies that suffer breaches lose long-term user trust
- Users are rewarding visible security features with loyalty

These numbers reflect what users have learned through experience. Social media platforms have faced repeated privacy scandals. Gaming apps often request unnecessary permissions. Dating apps collect intimate personal details and location data. And users have noticed.



## The Social Media Paradox

Here's where behavior gets interesting. **Social media apps are simultaneously the most distrusted and most downloaded category.** Users know these platforms collect extensive data, yet they continue using them daily.

**The lesson here:** Distrust doesn't always equal abandonment. Users make calculated trade-offs between functionality and privacy. They'll tolerate data collection from apps they find valuable, but their tolerance has limits.

**The key insight:** Users aren't asking for perfection. They're asking for honesty about what data apps are collecting and why.

## The Trust Trade-Off Equation

Users don't always uninstall apps they distrust. Instead, they weigh privacy risks against perceived value.

- They may distrust a social app — but keep it for community access.
- They may worry about health data — but use tracking for wellness goals.

## The Lesson?

Apps don't need perfect security. They need visible security efforts to preserve fragile trust.

## What Consumers Actually Want

Despite varying trust levels across categories, 81% of users want end-to-end encryption for their communications and sensitive data. They want clear explanations for why apps need specific permissions. They expect minimal data collection that directly relates to app functionality.

These aren't unreasonable demands. Users understand that apps need some data to function. They object to excessive collection, unclear purposes, and a lack of transparency about how companies are using their information

The trust patterns reveal a market ready to reward companies that respect user privacy while delivering value. Banking apps earn relatively high trust because they've always treated security as a core feature, not an afterthought. They prominently display security measures, require strong authentication, and are transparent about their protections.

Other app categories can adopt this same approach by making their security efforts visible and treating data protection as a user benefit rather than a background process:

- Health apps can highlight data encryption.
- E-commerce apps can showcase payment security.
- Social media platforms can emphasize privacy controls.

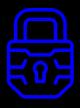
The opportunity exists across all categories

The Encryption Expectation

81%

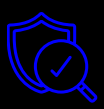
of users want end-to-end encryption for their communications and sensitive data.

## What Builds Trust – Badge Grid



End-to-end encryption

Minimal permissions

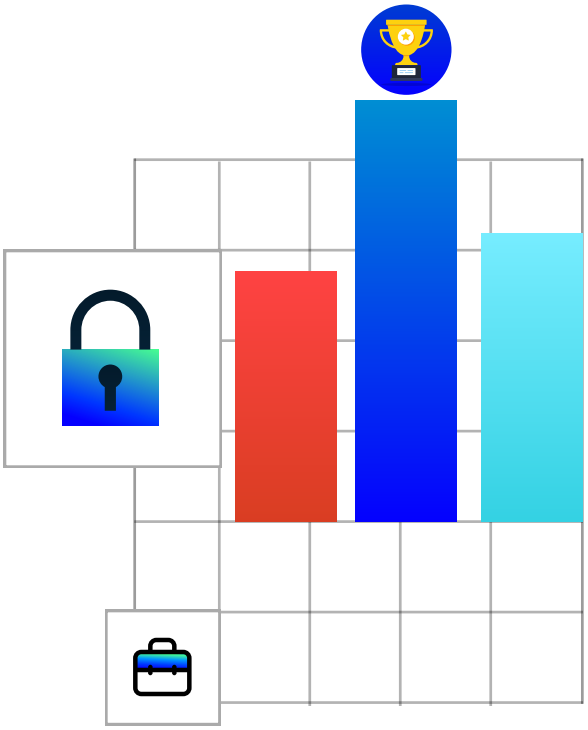


Third-party audits

Transparent privacy policies

Built-in controls (logout timers, anonymous modes)

# The Business Case: Security is the new competitive advantage

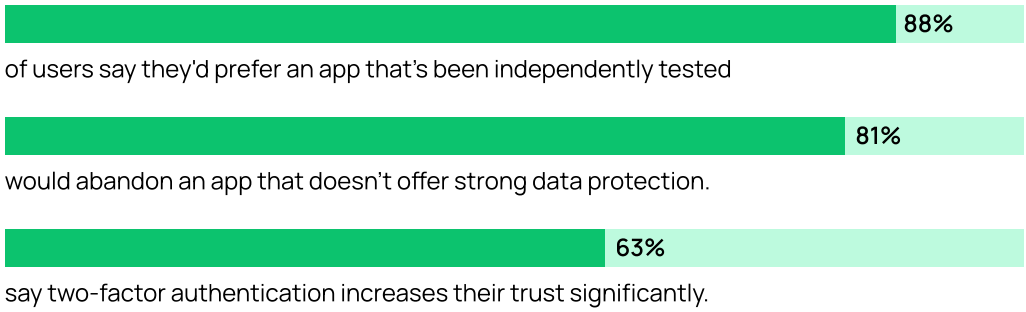


There was a time when mobile app security was treated as a background function — the domain of compliance officers and incident response teams

Not anymore. In 2025, security is a defining part of brand value. Users are making decisions, and switching apps based on how transparently and respectfully their data is handled.

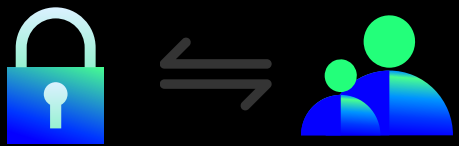
Security has evolved from an engineering challenge into a competitive differentiator.

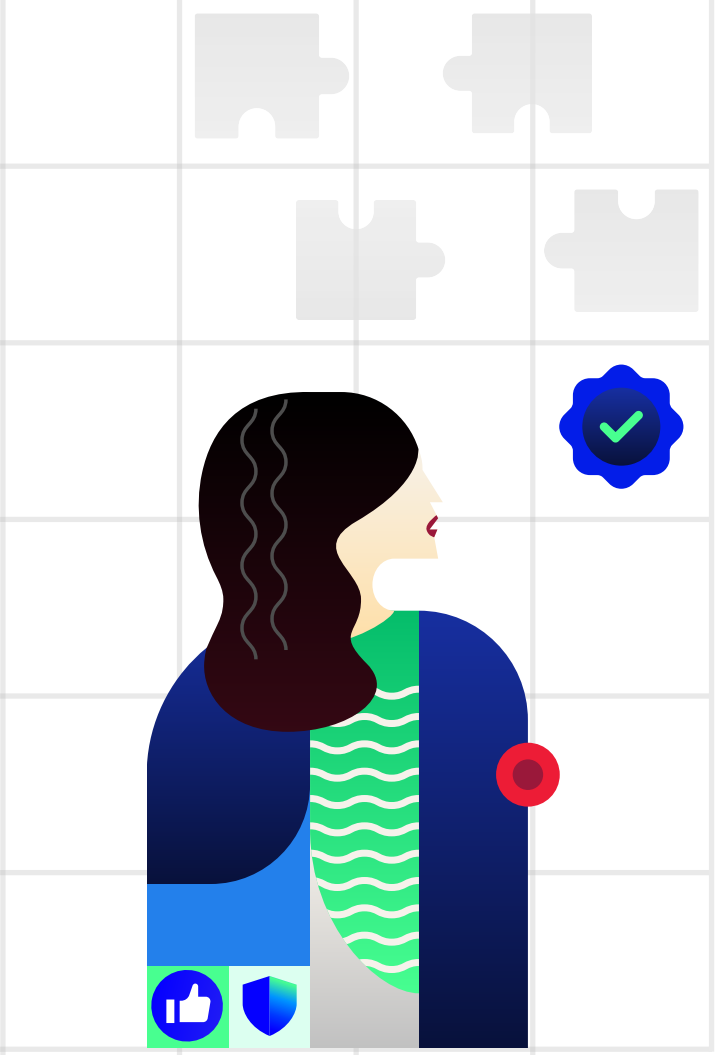
Our survey shows:




**Security = Conversion**

Nearly 9 out of 10 users prefer independently tested apps. This isn't a compliance checkbox — it's a competitive moat.





## What Builds — and Breaks — Trust

Our research exposed a deeper disconnect between the features users believe keep them safe and what apps actually implement. This gap reflects how far security still lags behind user expectations.

- End-to-end encryption for chats and transactions
- Minimal, clearly justified permissions
- Transparency about data sharing and collection
- Security certifications or third-party audits
- Built-in privacy controls like anonymous mode and logout timers

Most of these features are straightforward to implement and don't require a high degree of technical innovation.

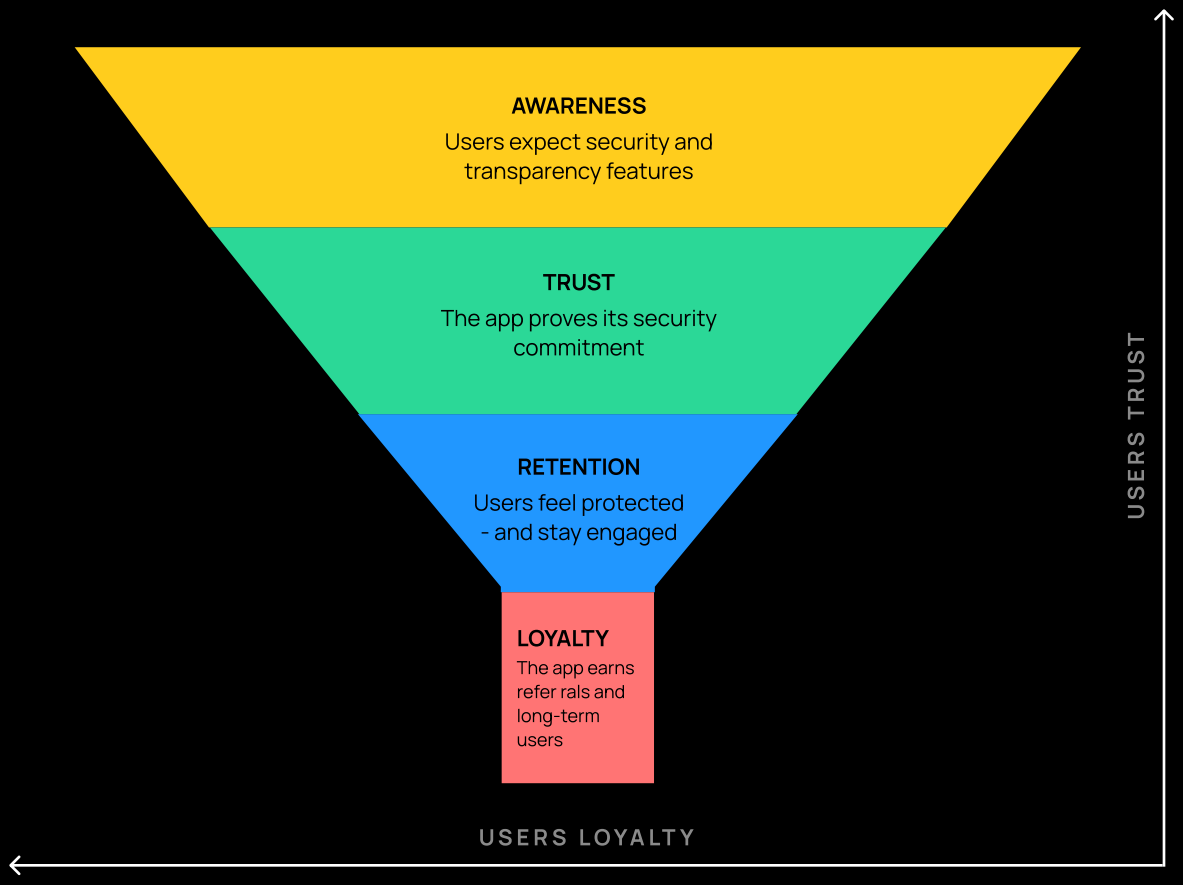
The real challenge is making business decisions that prioritize user trust over operational convenience. For example, minimizing data collection means giving up potentially valuable user insights. Providing clear privacy controls means users might limit what they share.

However, companies willing to make these trade-offs will find themselves preferred by an increasingly security-conscious user base that values transparency over data extraction.

### What Used to Be 'Nice-to-Have' Is Now Make-or-Break

| 2015 | 2025 |
|---|---|
| Security = backend hygiene | Security = user-facing trust signal |
| Audits optional | Audits expected |
| 2FA was fringe | 2FA is table stakes |
| Privacy = legalese | Privacy = product UX |

# Trust-to-Loyalty Funnel




## AWARENESS

Users now expect apps to clearly explain how their data is collected, stored, and protected. Security and privacy are no longer backend hygiene, they are part of the product experience.

## TRUST

Trust begins when users see visible signals of protection: encryption, permission minimization, independent audits. Without these, even the best-designed apps struggle to earn confidence.

## RETENTION

Trust isn't a one-time win. It must be reinforced continuously through secure session management, timely updates, and proactive breach communication. When users feel safe, they stay.

## LOYALTY

Loyalty is the result of sustained transparency. Apps that make security visible and consistent turn users into advocates. They reduce churn, gain referrals, and earn long-term engagement.

*In today's mobile-first market, trust is measurable, visual, and central to retention. Companies that lead with security don't just meet expectations, they outperform them.*

# Reality Check: How Top Apps Actually Perform

To evaluate how top-performing apps align with consumer expectations, we conducted a security assessment of **35 popular apps** across seven high-risk categories: Social Media & Messaging, E-Commerce & Shopping, Digital Wallets & Fintech, Banking, Health & Fitness, Dating, and AI Assistants.

These apps were tested for five key security capabilities users explicitly demand: end-to-end encryption, minimal permissions, transparent privacy policies, third-party audits, and in-app privacy controls.

Shock to the System:

0 of 37 apps met all five user-requested security criteria.Every single app contained at least one critical or high-severity flaw.

## Key Findings from the Scan Results

Each app underwent static, dynamic and API testing using the Appknox platform, aligned with OWASP Mobile Top 10 and industry benchmarks. The results were alarming:

| METRICS | RESULTS |
|---|---|
| Apps tested | 35 |
| Security Checks performed | 3,793 |
| Critical / High issues | 214 |
| Apps with ≥1 Critical / High issue | 100% |

| SEVERITY | COUNT |
|---|---|
| Critical | 57 |
| High | 157 |
| Medium | 385 |
| Low | 315 |
| Passed Tests | 2,879 |

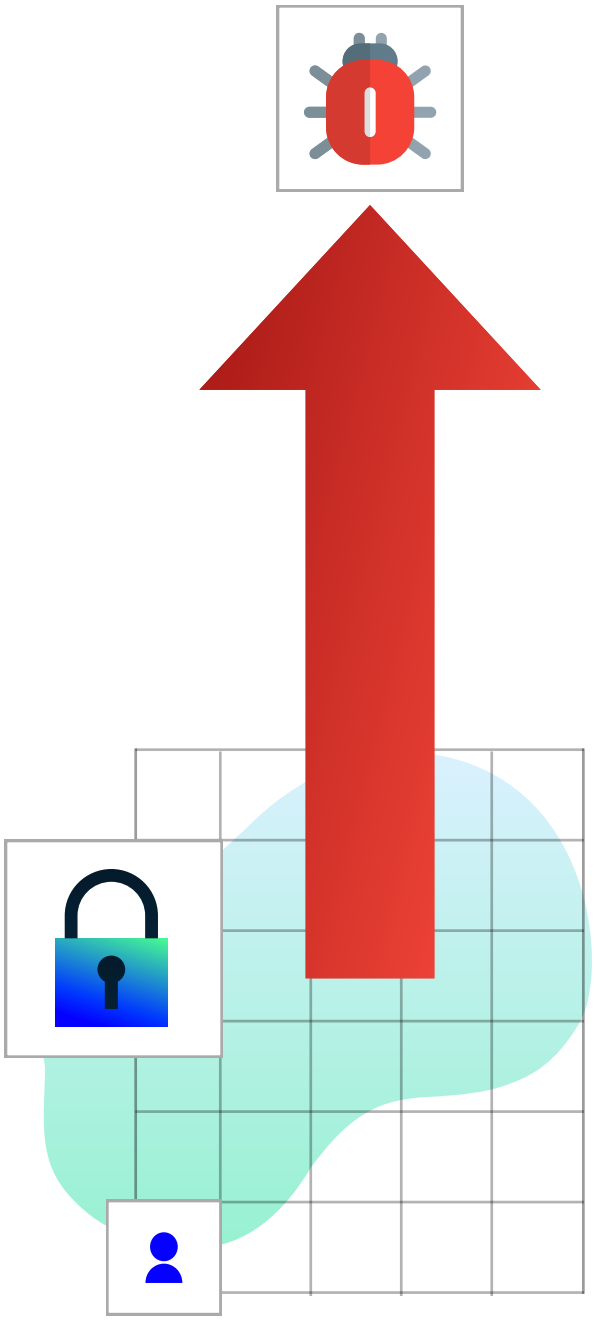
*Table represents Vulnerability Severity Breakdown*

## Most Vulnerable Categories

When we analyzed vulnerabilities by app category, clear patterns emerged. Some of the most downloaded and most trusted categories were among the worst performers. E-commerce and health apps, which handle sensitive data, ranked highest for both total and critical vulnerabilities.

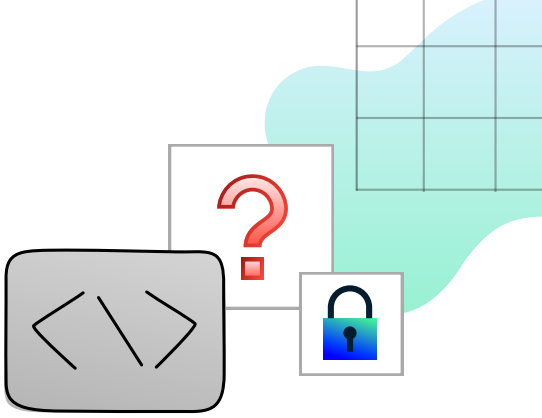
This gives the table context and sharpens the insight that risk correlates poorly with popularity or industry.

| CATEGORY | TOTAL | CRITICAL + HIGH |
|---|---|---|
| E-Commerce | 722 | 52 |
| Health & Fitness | 538 | 30 |
| AI Apps | 527 | 27 |
| Dating | 511 | 23 |
| Banking | 506 | 23 |
| Social Media | 505 | 30 |
| Fintech & Wallets | 484 | 29 |



## Popularity ≠ Protection

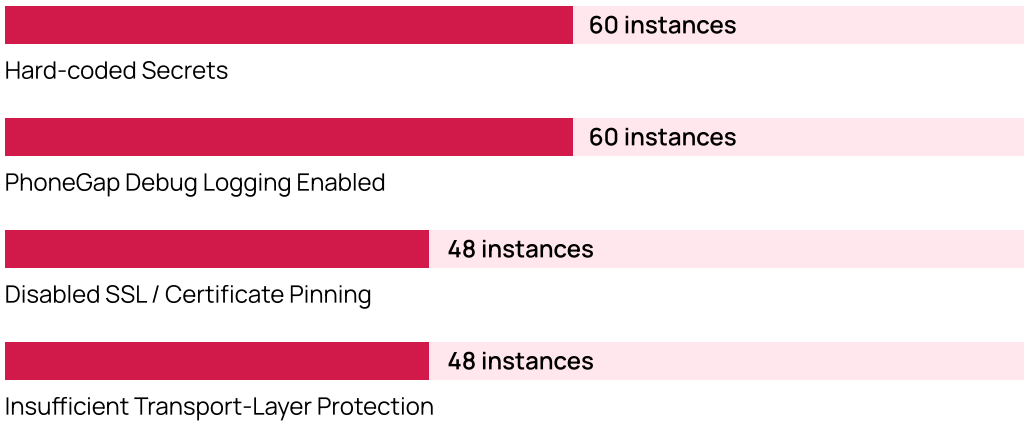
E-commerce apps lead in download volume and vulnerability volume — despite handling payment data.

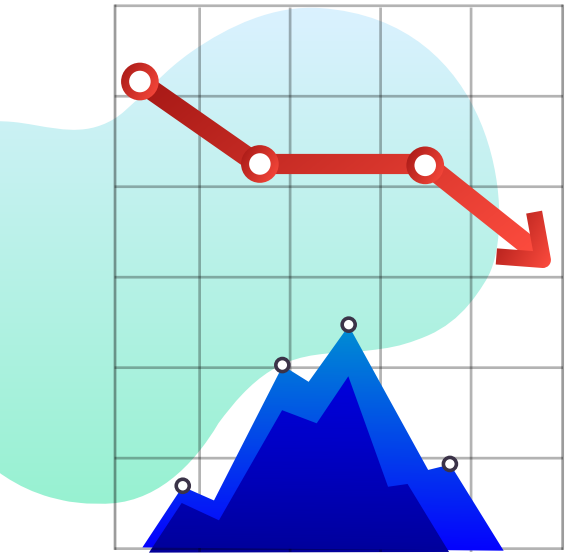


## Most Frequent Threats Developers Miss

Certain weaknesses showed up again and again, indicating systemic oversights in how developers build, test, and ship mobile apps. These recurring issues aren't just bugs — they're signs of insecure engineering practices that attackers regularly exploit.

Graph



## Worst-Performing Individual Apps (critical + high issues)

These aren't fringe or obscure apps - they are some of the most downloaded and trusted in their respective categories. Yet they rank among the worst in our testing, exposing millions of users to serious risks. Their failures are not just technical; they're trust failures that carry long-term brand consequences.

| APP | CRITICAL + HIGH |
|---|---|
| Walmart | 14 |
| Calm | 14 |
| Microsoft Copilot | 13 |
| SHEIN | 11 |

**100%**
of top apps had critical/high vulnerabilities

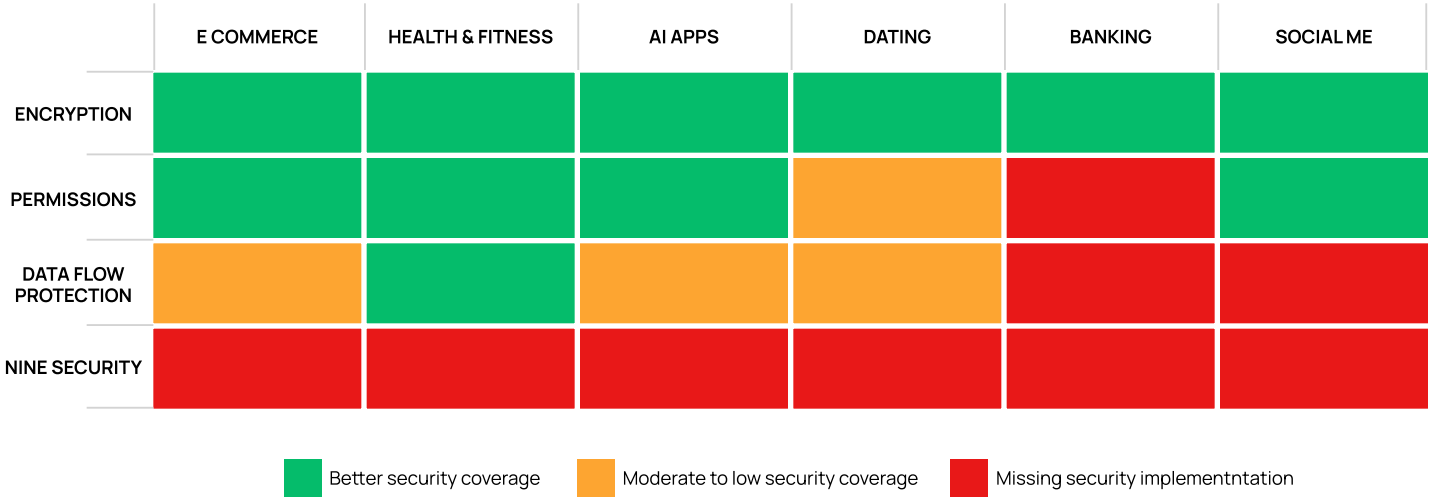
**3,793**
total issues detected in 37 apps

**Zero**
passed all 5 user-expected security tests

## Key Business Insights

- **100 % of apps have security vulnerabilities** — no brand immunity.
- **E-commerce apps** are the most vulnerable, even though they process payments at scale.
- **Banking apps** did relatively better, but still exposed critical issues like session token reuse and lack of TLS certificate pinning.
- **No app met all mobile-security standards**, proving a market-wide maturity gap.

Heatmap of Security Gaps by Category




This heatmap highlights the security performance of each app category across four critical dimensions: encryption, permissions, API/data flow protection, and runtime defenses.

# The Expectations
VS
# Reality Gap

By now, the pattern is clear: users want security, and they're not getting it. But to fix the problem, we have to break it down.

This section dives deeper into the most critical disconnects between what users expect and what popular apps actually deliver. These aren't minor oversights; they are structural failings that lead directly to churn, reputational damage, and regulatory risk.

The contrast between what users expect and what they experience is no longer subtle. It's measurable, wide, and widening — and it's costing companies real loyalty, retention, and competitive advantage. This gap isn't theoretical — it leads directly to user churn, reputational damage, and even regulatory action.

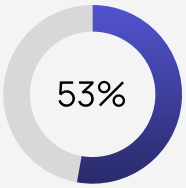
## Permission Failures

**User Expectation:**
Only request necessary data — explain why it's needed.

**Reality:**
Only 34% of apps minimized permissions.

These are real-world behaviors we observed across categories:

- A shopping app requesting access to a user's calendar.
- A fitness app requesting microphone and location permissions without a clear justification.




of users say they uninstall apps due to excessive permissions. It's one of the most visible red flags — and often the easiest to fix.

## What Apps Permissions Reveal?

Permissions aren't just technical requirements. They're behavioral signals. Apps that overreach are often either careless or aggressively harvesting data.

## The Encryption Gap

**User Expectation:**
81% of users expect end-to-end encryption.

**Reality:**
Just 46% of apps actually implement it.

---

Where the gap hurts most:

- Messaging apps that don't encrypt user chats
- Health apps storing emotional and biometric data in plaintext
- AI-powered apps that retain user prompts and chat history in unprotected formats

These failures aren't just risky — they're brand-breaking when exposed.

## Broken APIs and Missing Safeguards

**API Security:**
Several apps leaked metadata or lacked endpoint validation.

**Certificate Pinning:**
Missing in 40% of apps tested.

---

In 2022, multiple dating apps were found exposing user location data via poorly protected APIs. Attackers could use triangulation techniques and exposed coordinates to identify users' real-world locations, posing serious risks of stalking and harassment. The findings triggered public scrutiny and forced several platforms to update their API policies.

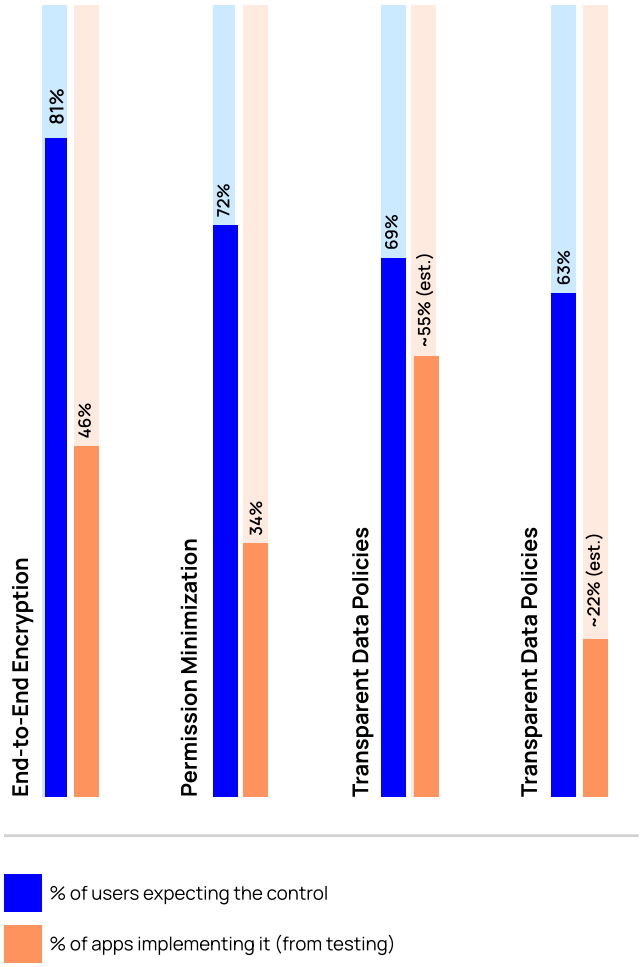
And in the infamous Equifax breach, API-level exposure of sensitive fields helped attackers gain initial access, a chilling example of how "internal" weaknesses quickly go public.

Statistics

In 2021, the Flo period tracker app was caught sharing sensitive user health data with third parties — including Facebook and Google — despite promising users otherwise.

The FTC charged Flo with deceptive practices, leading to a settlement requiring them to revise their privacy practices and undergo regular audits.

Expectation vs. Reality Bar Chart



## Cryptographic Failures and Developer Oversights

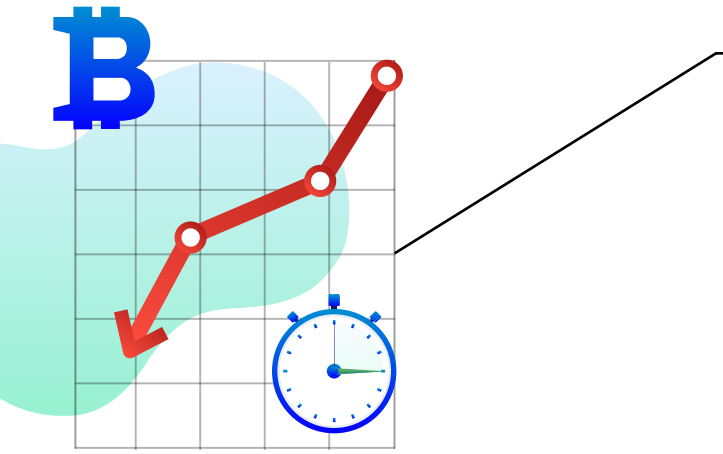
**User Expectation:**
Secure handling of sensitive information

**Reality:**
Widespread cryptographic lapses in production apps

Common flaws:

- **Hardcoded Secrets** – Found in 60+ instances, these expose keys directly in the app package.
- **Derived Crypto Keys** – Weak key derivation logic leaves data decryptable.
- **Improper Encryption Libraries** – Developers using insecure defaults or outdated libraries.

**Real-World Tie-In:**
The Equifax breach in 2017, which exposed sensitive data of over 147 million Americans, was enabled by unpatched software and poor cryptographic hygiene. Attackers exploited a known vulnerability in the Apache Struts framework, gained access through an unencrypted API, and moved laterally due to a lack of network segmentation and weak key handling.



## Weak Runtime and Session Defenses

**User Expectation:**
Session management and tamper resistance

**Reality:**
Apps fail to validate tokens or protect against rooted environments

Common flaws:

- **No Jailbreak/Root Detection –** The Majority of apps don't block rooted device access
- **Session Token Reuse –** Apps fail to properly invalidate tokens after logout, enabling unauthorized access
- **Insecure Logging –** Debug logs left exposed in production (e.g., PhoneGap logging)

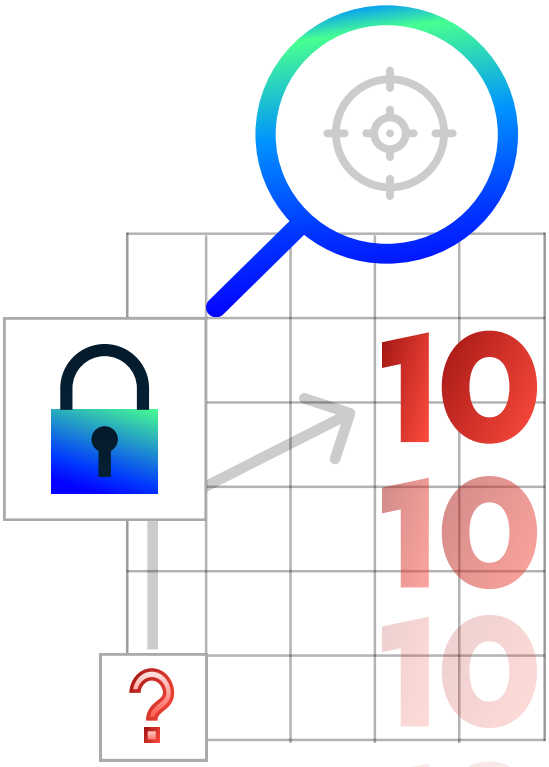
**Real-World Tie-In:**
Multiple banking and fintech apps globally have faced account takeover incidents where session tokens remained valid even after logout. In several cases, attackers reused stale tokens to access user accounts without credentials, prompting urgent patching efforts and new session hygiene standards across the industry.

## Anatomy of a Rooted App Attack

Visual walkthrough of how attackers exploit a weak runtime environment to escalate privileges and extract sensitive app data.

These failures aren't isolated or accidental; they are systemic. The same fundamental weaknesses appear repeatedly across categories, platforms, and use cases.

And users aren't just noticing — they're acting. The trust gap we have outlined here isn't theoretical. It's driving uninstalls, churn, and loss of brand equity. The question isn't whether you can afford to fix these issues. It's whether you can afford not to.




# Category-Specific Security Findings

Our testing revealed that mobile security performance varies significantly by app category — but not always in expected ways.

Apps handling highly sensitive data, like those in e-commerce, health, and AI, ranked among the most vulnerable.

This section breaks down the security posture of top apps across seven high-usage categories, highlighting key risk areas, recurring flaws, and standout cases.

## E-Commerce Apps: Checkout Without Security

| | |
|---|---|
| Total vulnerabilities | **722** |
| Critical/High issues | **52** |
| Top flaws | **Hardcoded secrets, insecure logging, lack of SSL pinning** |

**Why it matters:**
These apps handle payment info, PII, and behavioral data — often without visible protections.

**Notable risk:**
Cart abandonment isn't the only concern. Weak session and API defenses could lead to account hijack or fraud

**Real-World Breach Example:**
In 2022, a major e-commerce platform suffered a breach where its analytics SDK was misconfigured, leaking customer location and purchase history data. This wasn't a malicious attack — it was a failure in update hygiene and oversight. The breach affected over 1.2 million users and triggered lawsuits for privacy violations

## Health & Fitness Apps: Sensitive Data, Weak Defenses

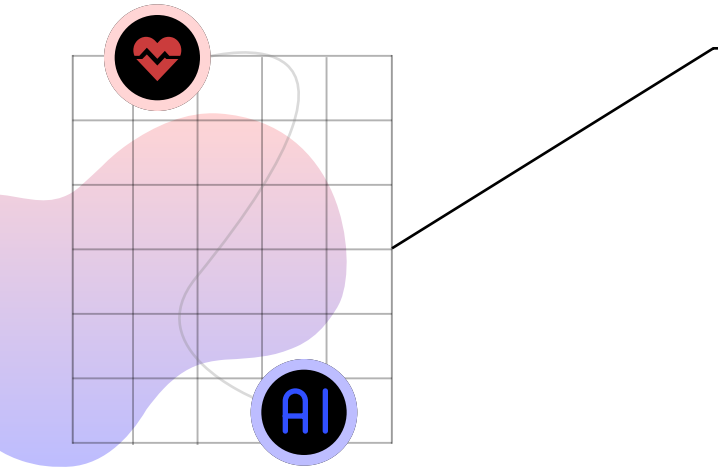
| | |
|---|---|
| Total vulnerabilities | **538** |
| Critical/High issues | **30** |
| Top flaws | **Missing encryption, excessive permissions, rooted device exposure** |

**Why it matters:**
Users trust these apps with emotional, biometric, and medical data. Security lapses aren't just technical — they feel personal.

**Notable risk:**
Health data exposure often triggers regulatory scrutiny and reputational damage.

**Real-World Breach Example:**
In 2023, the mental health app Cerebral disclosed that it had shared the private health data of over 3.1 million users with third-party platforms like Google, Meta, and TikTok — including information on mental health assessments, treatment plans, and appointment details.

The exposure was traced back to tracking pixels embedded in the app and website, used without adequate user consent. The breach triggered widespread criticism, multiple lawsuits, and a federal investigation into HIPAA violations.




## AI Apps: Data-Hungry and Under-Protected

| | |
|---|---|
| Total vulnerabilities | **527** |
| Critical/High issues | **27** |
| Top flaws | **Unencrypted prompt storage, poor runtime hardening** |

**Why it matters:**
AI tools collect rich behavioral and contextual data, often without user clarity on where and how it's stored.

**Notable risk:**
Few AI apps currently disclose how they secure inference data — a looming privacy challenge.

**Real-World Breach Example:**
In January 2025, Chinese AI startup DeepSeek exposed a sensitive database to the open internet — no password required. The leak included over **a million chat prompts, API tokens, system logs, and internal metadata** tied to its generative AI assistant.

Though the database was secured quickly after disclosure, the breach highlighted just how fragile trust can be in AI apps that handle personal and contextual data. With usage growing exponentially and regulation still catching up, AI apps today are flying fast — and often blind — when it comes to security.

**60%**

of tested AI apps failed encryption checks or exposed sensitive metadata.

## Dating Apps: Privacy Roulette

| | |
|---|---|
| Total vulnerabilities | **511** |
| Critical/High issues | **23** |
| Top flaws | **Broken session management, exposed location metadata, no audit trail** |

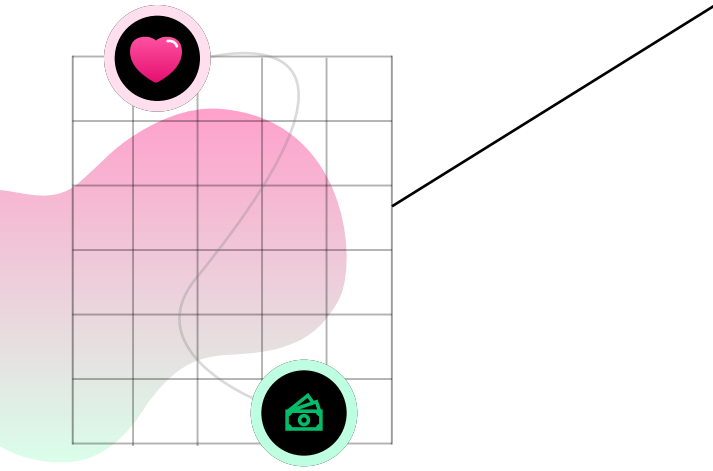
**Why it matters:**
Dating apps combine location, identity, and intent — a potent mix if compromised.

**Notable risk:**
Poor security here can lead to real-world harm, not just digital risk.

**Real-World Breach Example:**
In May 2025, a serious vulnerability in the Raw dating app exposed sensitive user data — including names, birth dates, sexual preferences, and precise GPS coordinates — through an unprotected API.

The data was accessible without authentication, allowing potential stalkers or bad actors to track users in real time.

This breach highlights the unique danger of dating apps: they don't just hold private data, they deal in **real-world proximity**, and when security fails, the consequences aren't just digital.



## Banking Apps: Better, But Not Bulletproof

| | |
|---|---|
| Total vulnerabilities | **506** |
| Critical/High issues | **23** |
| Top flaws | **Debug logging, certificate pinning gaps** |
| Observation | **Banking apps performed better than most, likely due to compliance and maturity, but flaws remain.** |

**Why it matters:**
Banking apps are entrusted with the most sensitive user data — financial credentials, transaction history, and personal identity information. While they generally perform better due to regulatory oversight, even minor lapses like debug logs or token reuse can open doors to fraud and account takeover.

In this space, user expectations are sky-high, and any breach leads to immediate loss of trust and regulatory consequences.

**Notable risk:**
Even one token reuse or exposed log can compromise session integrity.

**Real-World Breach Example:**
In 2021, a major U.S. bank was criticized after a researcher found its Android app logged sensitive transaction data locally, creating a forensic goldmine for malware on rooted devices. No official CVE was issued, but the damage to user trust was already done.

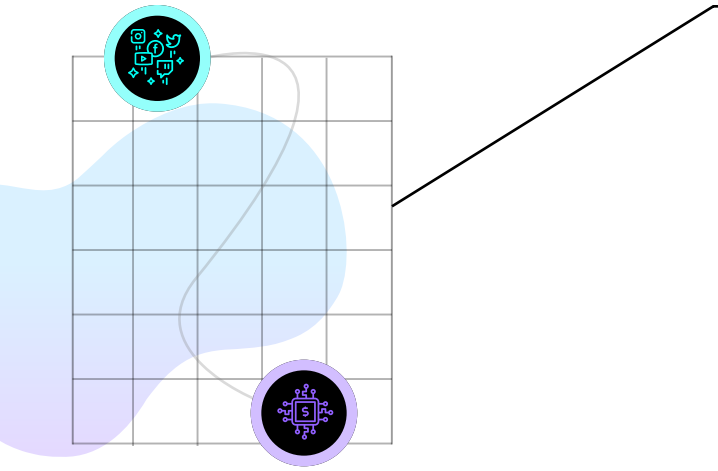
## Social Media Apps: Distrusted, Still Vulnerable

| | |
|---|---|
| Total vulnerabilities | **505** |
| Critical/High issues | **30** |
| Top flaws | **Excessive permissions, insecure communication channels** |

**Why it matters:**
These apps collect the most data and are trusted the least. Our findings reinforce user skepticism.

**Notable risk:**
Messaging channels without end-to-end encryption still persist.

**Real-World Breach Example:**
In 2022, a popular encrypted messaging app suffered a metadata exposure breach. Due to an insecure API, attackers could infer user connections and activity patterns, even though messages themselves remained encrypted. The breach highlighted how **metadata** is often as sensitive as message content.



## Fintech Apps: High Stakes, Mixed Signals

| | |
|---|---|
| Total vulnerabilities | **484** |
| Critical/High issues | **29** |
| Top flaws | **Root exposure, session token reuse, missing encryption** |
| Observation | **Banking apps performed better than most, likely due to compliance and maturity, but flaws remain.** |

**Why it matters:**
These apps promise innovation, but often lag behind traditional banking in controls.

**Notable risk:**
Agile releases without a proper security review introduce avoidable risk.

**Real-World Breach Example:**
In 2023, a popular fintech app was exploited due to missing TLS pinning, enabling attackers to intercept and replay user traffic on public Wi-Fi. The result? Stolen session tokens and unauthorized fund transfers, affecting thousands.

## A Category-Wide Wake-Up Call

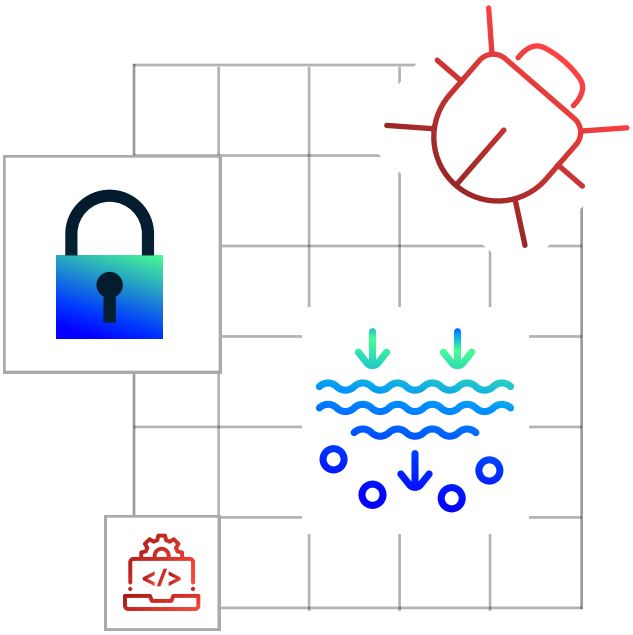
The data is clear: no category is immune. Whether handling health data, financial transactions, or real-time conversations, today's most popular apps are failing to meet basic security expectations. The volume and severity of vulnerabilities — even in apps trusted by millions — reveal an industry still treating security as an afterthought.

Yet this gap isn't just a liability. It's a strategic opening. Businesses that take proactive steps to secure their category, and show it, will differentiate fast. The next section explores how to do just that.

### Risk Profile by Category

| APP CATEGORY | AVERAGE RISK LEVEL | DATA SENSITIVITY | USER TRUST (FROM SURVEY) |
|---|---|---|---|
| Banking | Medium | Financial, identity | Highest |
| Health & Fitness | High | Biometric, wellness | Medium-low |
| Fintech | Medium-high | Financial, session | Medium |
| E-commerce | High | Payment, PII | Medium |
| AI | Medium-high | Behavior, text history | Low |
| Social Media | High | Personal content | Low |
| Dating | High | Location, identity | Lowest |

# Technical Deep Dive: Common Vulnerabilities



Our deep dive into America's most downloaded apps uncovered a sobering reality: popularity does not equal protection. Apps that dominate daily life across finance, health, dating, and beyond still harbor vulnerabilities that put users at risk.

While the nature of risks varied across categories, three systemic flaws stood out across the board:

1. **Surface-Level Defenses:** Many apps lacked deeper protections like runtime hardening, secure storage, or API validation.
2. **Opaque Privacy Practices:** Users had limited visibility into how their data was collected, used, or shared.
3. **Neglected Mobile Hygiene:** From outdated SDKs and excessive permissions to missing encryption, common issues were widespread.

From unencrypted health logs to finance apps leaking API keys, these issues are real, recurring, and deeply preventable. Breaches may make headlines, but it's the silent, everyday failures in mobile app security that erode user trust the most.

Risk Profile by Category

## Red Flags to Watch For: Common Issues Found in 35 Top U.S. Apps

We catalogued the most frequently observed vulnerabilities across the scanned apps:

### Network Security

- No TLS/SSL pinning (40% of apps)
- Unencrypted API endpoints
- Weak or missing certificate validation

### Device & Runtime Protections

- No root/jailbreak detection
- Debuggable builds in production
- No code obfuscation (easily reverse-engineered)

### Data Handling & Storage

- Session tokens stored locally
- Sensitive data stored unencrypted
- Outdated or misconfigured third-party SDKs

### Access & Permissions

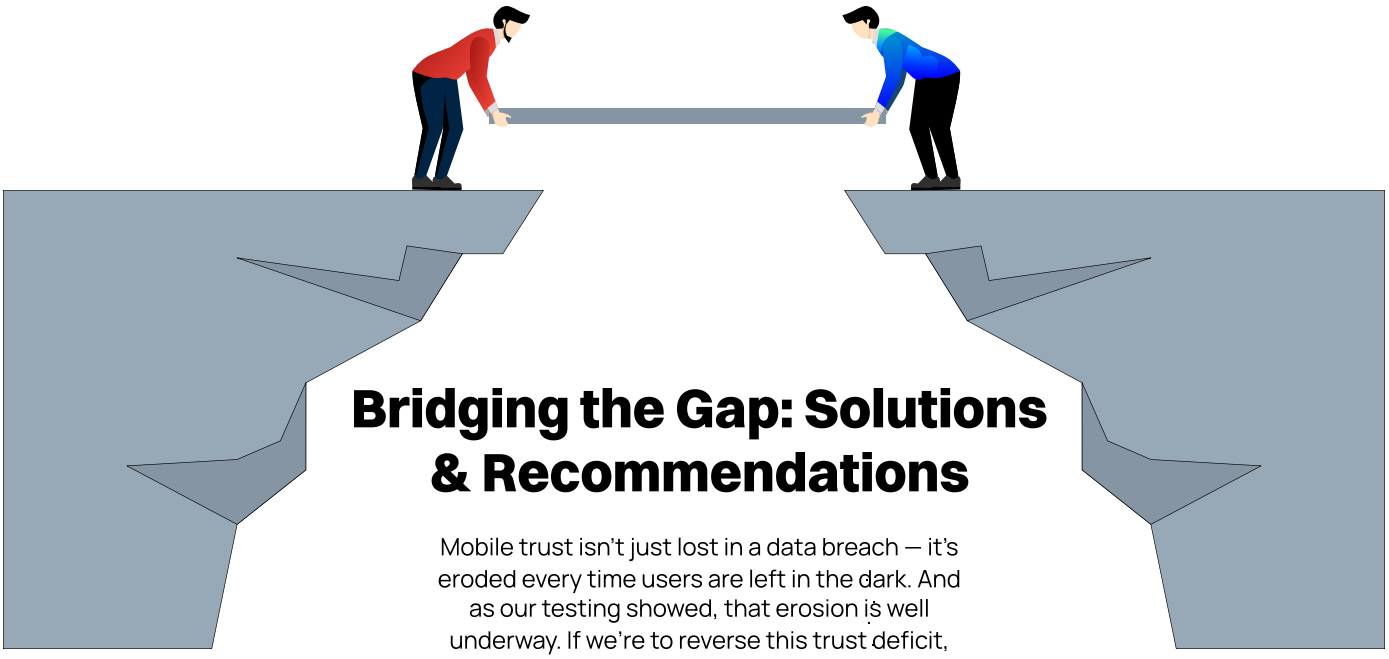
- Over-permissioning (camera, mic, location)
- No explanation for permission use
- No session expiration or auto-logout

## Why It Matters

These flaws are soft targets. Every unchecked red flag is an open door to:

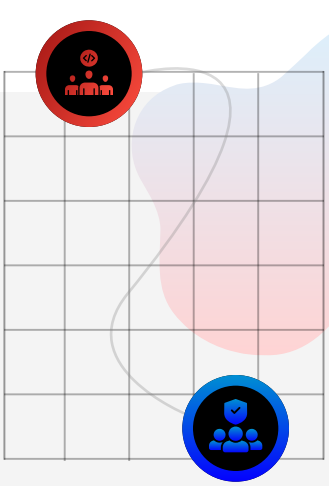
- Unauthorized access to user data
- Exploitation of app logic and infrastructure
- Brand damage, churn, and regulatory action

Most importantly, these are preventable. They signal not a technical limitation, but security deprioritization.



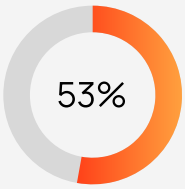
# Bridging the Gap: Solutions & Recommendations

Mobile trust isn't just lost in a data breach — it's eroded every time users are left in the dark. And as our testing showed, that erosion is well underway. If we're to reverse this trust deficit, change must come from within the ecosystem: from the engineers who build apps, the product managers who define user flows, and the security teams who protect data.



### For Product & Engineering Teams

- **Design for privacy from day one:** Adopt privacy-by-design frameworks that embed security into every stage of development.
- **Ask for less:** Limit permission requests to what's strictly necessary. Use just-in-time prompts and explain the 'why.'
- **Make security tangible:** Display visual cues for encrypted communication, give users visibility into what's collected, and enable full data deletion




of users said excessive permission requests would cause them to uninstall an app, yet only 34% of apps minimized permissions.

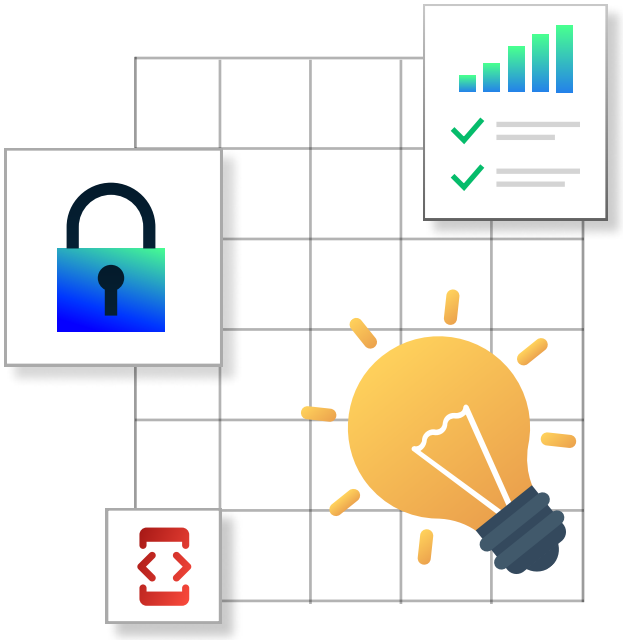
### For Security Teams

- **Elevate trust to a measurable KPI:** Move beyond vulnerability counts. Track real-world trust metrics: user churn after security incidents, uninstall rates post-breach, privacy-related complaints.
- **Audit what users actually use.** Prioritize high-download, high-engagement apps for continuous testing, rather than just relying on internal staging builds.
- **Ensure app store parity:** Regularly verify that published versions reflect your most secure, tested builds, not outdated or debug-heavy variants.


Quick Win: Add a "Security at a Glance" section in your app's store listing, highlighting encryption, permissions, and certifications. When users can see your efforts, they trust them more.

Rebuilding trust isn't a technical fix — it's a cultural shift. But when privacy becomes a shared priority, the reward is lasting: reduced churn, higher loyalty, and apps users actually believe in.

# Conclusion: The Security Opportunity



Mobile app security is no longer just a backend concern; it's a defining element of user experience, brand reputation, and market success.

As our research has shown, users have evolved, but most apps haven't. This final section connects the dots between consumer demand and technical debt, presenting a roadmap to turn security into a competitive edge.

## The Market Signal

Our research reveals a simple truth: users know what they want, and most apps aren't delivering it. The mobile security landscape is transforming from the ground up. Users are no longer passive consumers of whatever apps offer. They're active evaluators who reward transparency and punish overreach.

This shift creates opportunities for companies willing to build differently.

This transformation extends beyond individual app choices. It's reshaping entire business models. Companies that built their success on extensive data collection now face users who question every permission request. Platforms that once competed solely on features must now compete on trust. The old playbook of moving fast and asking for forgiveness later no longer works when users have alternatives at their fingertips.

The companies that thrive in this new environment won't be those with the most sophisticated algorithms or the flashiest interfaces. They'll be the ones that treat user trust as their most valuable asset and security transparency as their strongest differentiator.

## The Technical Reality

The vulnerability data reveals that most apps are still playing catch-up. Poor encryption, over-permissioning, outdated SDKs, and missing privacy controls aren't just lapses - they're indicators of a deeper organizational issue: security is still treated as a compliance checkbox instead of a design principle.

But it doesn't have to be that way. Building secure apps isn't about perfection; it's about visible, credible, user-first security that aligns with real expectations.

The opportunity now lies in leading the next wave of mobile development — one where security isn't a hidden layer but a visible feature. Brands that embrace this shift will not only avoid breaches but also win users for life.

# Appendix

## A. Survey Methodology & Respondent Profile

This whitepaper is based on original consumer research conducted by Dynata, a leading global data and insights platform, on behalf of Appknox in May 2025. The study was designed to understand how U.S. consumers perceive mobile app security risks and how these perceptions drive real-world behavior.

- **Sample size:** 1,000 respondents
- **Geography:** United States (nationally representative)
- **Age groups:** 18 and older, segmented for generational analysis
- **Sampling approach:** Representative of the U.S. adult population
- **Fielding period:** May 2025
- **Margin of error:** ±3.1% at 95% confidence level

The survey examined app install/uninstall behavior, trust factors, security feature awareness, breach response patterns, and category-specific sentiment across mobile app categories, including social media, banking, e-commerce, health & fitness, dating, and AI-powered applications.

## B. App Testing Methodology

To analyze real-world security posture, we selected 35 of the most downloaded apps in the U.S., spanning 7 categories where usage is high, data sensitivity is significant, and user trust is low:

| Category & Sample Apps Tested |
|---|
| **Social Media & Messaging**<br>TikTok, Instagram, Facebook, WhatsApp, Telegram |
| **E-Commerce & Shopping**<br>Temu, Shein, Amazon, Walmart, Capital One Shopping |
| **Digital Wallets & Fintech**<br>Cash App, PayPal, Venmo, Zelle, Coinbase |
| **Banking Apps**<br>Chase, Bank of America, Wells Fargo, Capital One, Citi |
| **Health & Fitness**<br>MyFitnessPal, Flo, Calm, Headspace, Peloton |
| **Dating**<br>Tinder, Bumble, Hinge, Badoo, Ashley Madison |
| **AI Apps**<br>ChatGPT, Gemini, Microsoft Copilot, Character AI, Talkie |

**Note**: Apps were tested in their latest available public version on U.S. iOS and Android app stores as of May 2025. Individual vulnerability results are anonymized to focus on category-level insights.

All security assessments were conducted by the Appknox team using the Appknox Mobile Security Suite

### Methodology:

1. **Approach:** Non-intrusive black-box and dynamic testing (DAST), supported by static and API-level analysis where applicable
2. **Test coverage:** 100+ checks aligned with:
   - OWASP MASVS (Mobile App Security Verification Standard)
   - OWASP Mobile Top 10
   - OWASP API Top 10
   - OWASP MSTG (Mobile Security Testing Guide)
   - PCI - DSS (v4) (Payment Card Industry Data Security Standard)
   - GDPR (General Data Protection Regulation)
   - HIPAA (Health Insurance Portability & Accountability Act)
   - CWE (Common Weakness Enumeration)
   - NIST
3. **Attack surfaces tested:**
   - Permissions abuse and overreach
   - Unencrypted local storage
   - Improper SSL/TLS usage
   - API metadata leakage
   - Lack of runtime security (e.g., no root/jailbreak detection)
   - Insecure SDK or library usage
   - Tampering & Hooking Detection

# About the Authors

Authored by

**Subho Halder**

CEO, Appknox

Subho Halder is the CEO and co-founder of Appknox, a leading mobile application security platform trusted by global enterprises and government agencies. A noted cybersecurity researcher, Subho is the creator of the AFE framework, which has uncovered critical vulnerabilities in platforms built by Google, Apple, and other tech giants.

With a decade-long track record in offensive security, Subho brings deep expertise in mobile threat detection, secure development practices, and AI-led security automation. His research has been presented at BlackHat, Defcon, and other global forums, making him one of the foremost voices in mobile application security.

At Appknox, Subho drives the company's product innovation and strategic vision, helping security-conscious businesses stay ahead of evolving threats. His work continues to influence how the industry builds, tests, and trusts mobile applications.

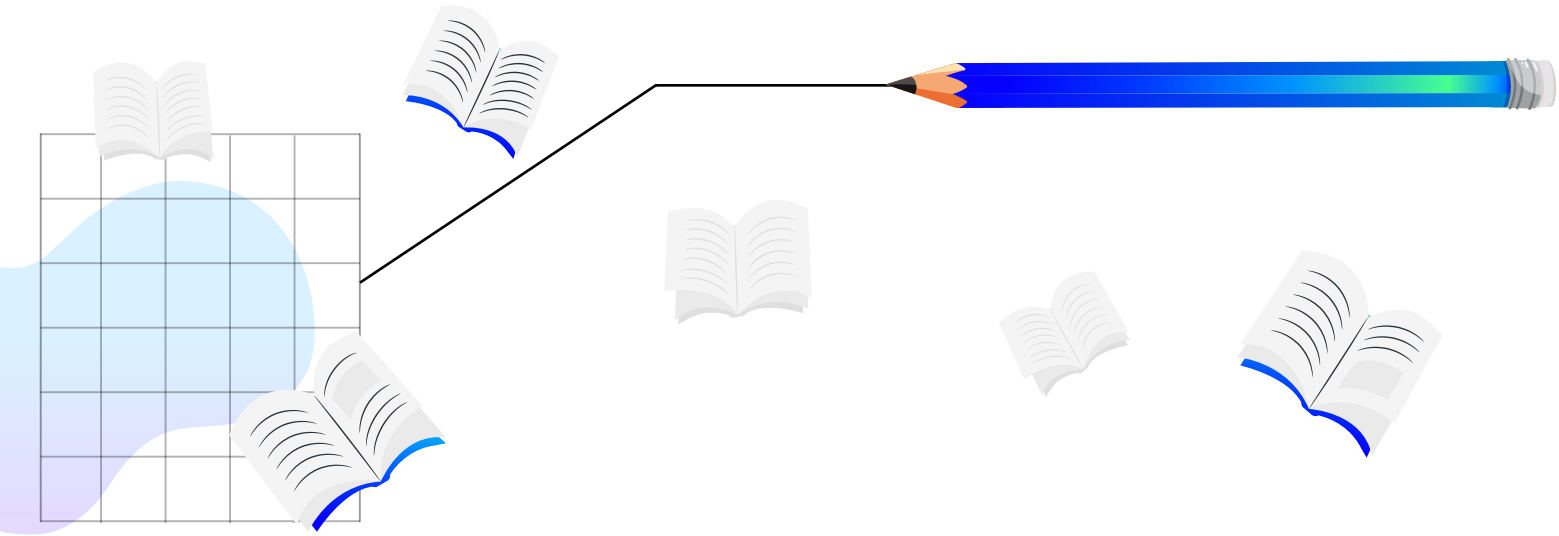
Authored by

**Rishika Mehrotra**

Chief Strategy Officer, Appknox

Rishika is the Chief Strategy Officer at Appknox, where she drives the company's strategic initiatives and growth in the cybersecurity landscape. With a background in technology and business leadership, she specializes in helping organizations navigate the complex intersection of security, technology, and regulatory compliance.

Rishika is deeply passionate about the evolving cybersecurity landscape and plays a pivotal role in shaping Appknox's global strategies, particularly in the Middle East, US, and India. Her vision for secure-by-design digital transformation is transforming how enterprises approach mobile security.



# About Appknox

Appknox is the leading mobile application security platform trusted by over 200 enterprises worldwide, including Fortune 2000 companies and government agencies.

Founded over a decade ago by mobile security researchers, Appknox delivers comprehensive, AI-powered solutions that secure mobile apps throughout their entire lifecycle—from development to app store monitoring. Appknox is designed for scale and compliance, empowering security teams to identify and manage vulnerabilities without compromising speed or agility.

---

With automated testing across SAST, DAST, API, and runtime security layers, Appknox empowers organizations to:

- Identify and remediate vulnerabilities before they reach production.
- Achieve compliance with industry standards, including OWASP MASVS, SOC2, HIPAA, PCI-DSS, and GDPR.
- Continuously monitor live app store versions for security drift and brand abuse.
- Seamlessly integrate security into DevSecOps and CI/CD workflows.
- Deploy both cloud-based and on-premise solutions for maximum flexibility.

---

Headquartered in Singapore and with a global presence in the U.S., Middle East, and Asia-Pacific, Appknox serves enterprises in banking, fintech, healthcare, e-commerce, and government sectors. Gartner recognizes the company as a preferred vendor for mobile application security and maintains an active commitment to the security community through open-source contributions and research.

**Learn more:** www.appknox.com.