jamf

Security 360:

Annual Trends Report

Mobile Devices

Table of contents

Introduction

Jamf's Security 360 provides a thoughtful retrospective on the ever-evolving threat landscape; it is informed by real-world incidents that were identified within our customer base, novel discoveries made by our threat researchers, and observations from global, national, and industry events. This edition of the report is focused on exploring the mobile threat landscape to put a spotlight on the risks that organizations face.

We examine the diverse and impactful attack vectors that attackers use to gain access, pivot from one system to the next, and ultimately compromise data or cause harm. Attackers exploit device and software vulnerabilities, introduce malicious code in apps and web communications, and threaten users, the weakest link in every organization's defenses, all in an effort to achieve their objectives.

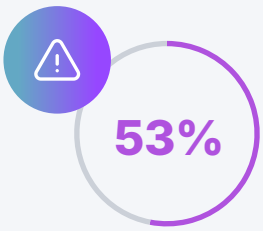
In addition to analyzing these threat trends, the report includes a perspective from Jamf's CISO, providing insight to security leaders and IT practitioners responsible for protecting mobile fleets.

Research methodology

To understand and quantify the real-world impact of the security trends identified in this report, we anonymously examined a sample group of over 1.7 million iOS and Android devices within our customer footprint. Our analysis was carried out at the end of 2025, revisiting the prior 12-month period and spanning globally across multiple countries.

To preserve privacy and maintain the highest standards when gathering and handling data, the metadata analyzed in our research comes from aggregated logs that do not contain personal or organization-identifying information.

Key findings



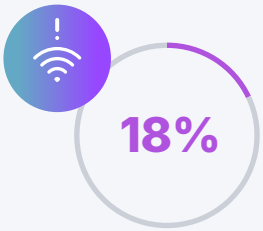
The portion of organizations that had at least one device with a critically out-of-date operating system

An out-of-date OS means unpatched, exploitable vulnerabilities. Automating and enforcing updates goes a long way to protect your devices.

1 in 850

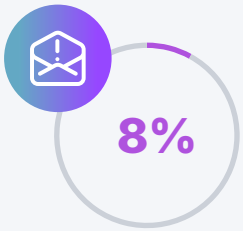
The number of devices used for work — and jailbroken

Jamf detected these devices; context-aware access policies prevented access to company resources.



The share of organizations with employees that connect to risky hotspots

Risky hotspots open the door to infrastructure threats like rogue access points or Adversary-in-the-Middle attacks, especially if devices are not configured to address this risk.



The portion of devices where the user clicked on a phishing link.

Phishing attacks remain a popular tactic for attackers to compromise accounts, with little change year over year. The effects can be devastating without proper protections.

Zero-clicks and browser attacks

Remain popular and effective methods

Vulnerabilities continue to show up in both operating systems and software; they become the key for attackers to harvest sensitive information via multiple spyware families. This report emphasizes the importance of strategically reducing risk on your mobile devices.

Key trends in the enterprise

Mobile devices help employees stay productive wherever they're working. The way we manage and use these devices — and the threats they face — informs how they are secured.

Your organization fights every day to reduce your attack surface. You implement controls and policies and load your tech stack with the best security software, yet attackers evolve and persist.

There are many components that make up your attack surface. In this report, we'll talk about the top risks that organizations struggle to control and attackers commonly exploit — and how to avoid disastrous consequences.

1. Software and device vulnerabilities are part of business.

Despite all the care that goes into developing your mobile devices' operating systems, perfection is impossible. In 2025, more than 48,000 CVE records were published. That's a lot of vulnerabilities to recognize and address.

But developers know this, which is why they release security patches. That's where your teams come in. Are you applying these patches? Keeping operating systems up to date? Following security best practices? The way you configure your devices matters.

Attackers exploit flaws; the attack surface grows.

2. Mobile apps can be a boon or a bane.

Apps are an essential part of mobile work. Your company might deploy dozens — or hundreds — of apps across your fleet. Each app carries its own risks. Mobile malware is relatively rare, but privacy, supply chains and data handling remain potential hazards.

Your apps need to stay up to date as well; their developers are patching vulnerabilities too. Managing the app lifecycle is crucial, and so is ensuring you're balancing security and privacy for your employees.

Apps multiply potential risks; the attack surface grows.

3. Networks and web risks threaten even the most secure devices.

Protecting your data is table stakes, whether at rest or in transit. Achieving this requires understanding your networking infrastructure and user behavior. Employees commonly connect to unprotected hotspots that might be open to Adversary-in-the-Middle (AitM) attacks. Without proper configuration, your data is exposed.

Phishing and other web risks continue to run rampant. Attackers mimic popular sites across multiple categories of online content: entertainment, business, utility and finance. And users fall for them every day, especially as generative AI helps attackers advance their techniques.

User error and external networks offer uncontrolled points of entry; the attack surface grows.

4. Risks multiply and give rise to advanced threats.

Device vulnerabilities, apps, network infrastructure and user behavior can all introduce cracks in your cyber shield. The larger your attack surface, the more difficult it is to cover, and these three risk types are oft exploited for targeted attacks.

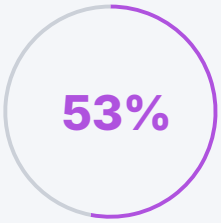
The proliferation of these risks can open the door to more harmful attacks, like Advanced Persistent Threats (APT) and spyware. In 2025, Jamf Threat Labs observed continued exploitation via zero-click and one-click attacks. Executives, politicians, activists and journalists were especially targeted.

We investigated some of the most nefarious zero-click and one-click attacks in 2025. These attacks aim to exfiltrate sensitive intelligence information and exploit multiple components of a device. Later in this report, we'll take a look at our findings.

Device vulnerabilities

Mobile operating systems provide a foundation — secure or not.

The codebase behind your device's operating system is immense and complex. And since humans are fallible and vulnerabilities inevitably find their way into the code. Humans are clever too – attackers are always hunting for potential exploits.



of **organizations** have at least one device with a critically out-of-date OS

What is a CVE?

The Common Vulnerabilities and Exposures (CVE) program acts as a database of vulnerabilities discovered by the cybersecurity community. Each CVE listing identifies the affected software or library, lists a severity score and offers potential methods of exploitation.

Let's look at some prominent examples from 2025, both of which were confirmed to be exploited in the wild. These CVEs were patched in iOS 18.4.1.

CVE-2025-31200

Severity score: 9.8 (critical)

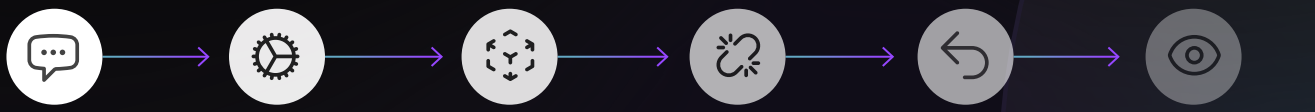
Processing an audio stream in a maliciously crafted media file may result in code execution.

CVE-2025-31201

Severity score: 9.8 (critical)

An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.

Attackers can chain vulnerabilities like these to harvest your data and deploy spyware. Imagine this (vastly oversimplified) scenario:



A high profile target receives a carefully crafted message containing a malicious audio file.

Without human interaction, the mobile device processes the audio message for previewing.

Memory corruption during processing allows arbitrary read/ write capability.

Pointer authentication bypass allows attackers to forge valid code pointers.

Attacker redirects code execution to a malicious payload.

Device is compromised and surveillance begins.

So what does this mean?

- **It's a zero-click, targeted attack:** The user doesn't have to click on anything for their device to be compromised. Targeted users are likely high-profile individuals like journalists, politicians or executives.
- **Vulnerabilities add up:** Attackers are looking closely for possible exploits, and they're good at finding them.
- **Patching matters:** These vulnerabilities were fixed in iOS 18.4.1. If your devices aren't updated, your data isn't protected.

Hopefully, this underscores the importance of up-to-date devices. That's not to say that it's easy to implement. There are a variety of reasons a user may not want to update their device:

- New features/interface they don't want to use
- App incompatibility with new OS version
- Workflow disruption/resource constraints

As we've shown, out-of-date software is extremely common, and staying up to date is a moving target. Enforcing update deadlines and minimum OS versions will protect your device fleet from impactful vulnerabilities, like these analyzed by Jamf Threat Labs in 2025.

Attackers exploit vulnerabilities to implement zero-click vectors like parsing of images and audio files and one-click browser attacks. Even with security patches and vendor effort, attackers are still able to find and exploit new vulnerabilities to build offensive solutions, making regular updates of mobile devices critical to protecting all users from vulnerabilities. Below is a review of the most impactful vulnerabilities in 2025.

Noteworthy iOS vulnerabilities, 2025

CVE-2025-24201 | Severity: 10.0 (critical)	CVE-2025-43300 | Severity: 10.0 (critical)	CVE-2025-31201 | Severity: 9.8 (critical)
DESCRIPTION:		
Maliciously crafted web content may be able to break out of Web Content sandbox.	Processing a malicious image file may result in memory corruption.	An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.
IMPACT:		
This vulnerability allows out-of-bounds writing of data past the end or before the beginning of the intended buffer. This can cause memory corruption or allow an attacker to modify data to execute unexpected code.	This vulnerability also allows out-of-bounds writing of data past the end or before the beginning of the intended buffer.	This vulnerability includes improper access controls, allowing unauthorized access to security-sensitive components. As a result, attackers can modify and read memory and execute unauthorized code.
PATCHED OS:		
iOS 18.3.2 and iPadOS 18.3.2	iOS 18.6.2 and iPadOS 18.6.2	iOS 18.4.1 and iPadOS 18.4.1

Additional vulnerabilities that we confirmed were exploited in 2025 are shown in the following table.

iOS

PATCHED IOS VERSION	DATE	VULNERABILITY SCORING	COMPONENT
18.3.1	Feb 2025	CVE-2025-24200 CVSS score: 6.1 | Severity: medium	Accessibility
18.3.1	Feb 2025	CVE-2025-43200 CVSS score: 4.2 | Severity: medium	Messages
18.4.1	Apr 2025	CVE-2025-31200 CVSS score: 9.8 | Severity: critical	CoreAudio
26.2	Dec 2025	CVE-2025-43529 CVSS score: 8.8 | Severity: high	WebKit
26.2	Dec 2025	CVE-2025-14174 CVSS score: 8.8 | Severity: high	WebKit

Noteworthy Android vulnerabilities, 2025

CVE-2025-10585 | Severity: 9.8 (critical)	CVE-2025-48543 | Severity: 8.8 (high)	CVE-2024-53104 | Severity: 7.8 (high)
DESCRIPTION:		
Type confusion in V8 in Google Chrome allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	In multiple locations, there is a possible way to escape chrome sandbox to attack android system_server due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in uvc_parse_format. This can lead to out of bounds writes since frames of this type were not taken into account when calculating the size of the frames buffer in uvc_parse_streaming.
IMPACT:		
A pointer or other resource is declared as a certain type, but later accesses a resource of incompatible type. This can lead to memory rewrites, crashes and possibly code execution.	Using previously freed memory can corrupt valid data. If attackers introduce malicious data before memory is consolidated, they may be able to execute arbitrary code.	Out-of-bounds writing of data past the end or before the beginning of the intended buffer can cause memory corruption or allow an attacker to modify data to execute unexpected code.
PATCHED OS:		
Chrome 140.0.7339.155	Android 13, 14, 15, 16	Upstream Linux kernel, Feb 2025

Android

PATCHED ANDROID VERSION	DATE	VULNERABILITY SCORING	COMPONENT
12, 12L, 13, 14, 15	Mar 2025	CVE-2024-43093 CVSS score: 7.3 | Severity: high	Framework
Security bulletin*	Mar 2025	CVE-2024-50302 CVSS score: 5.5 | Severity: medium	Kernel
Security bulletin	Sep 2025	CVE-2025-38352 CVSS score: 7.4 | Severity: high	Kernel

*Android does not release OS versions for Kernel updates. Read their applicable Android Security Bulletin for more info.

Chrome

PATCHED CHROME VERSION	DATE	VULNERABILITY SCORING
136.0.7103.125	May 2025	CVE-2025-4664 CVSS score: 4.3 | Severity: medium
137.0.7151.72	Jun 2025	CVE-2025-5419 CVSS score: 8.8 | Severity: high
138.0.7204.63	Jun 2025	CVE-2025-6554 CVSS score: 8.1 | Severity: high
138.0.7204.157	Jul 2025	CVE-2025-6558 CVSS score: 8.8 | Severity: high
142.0.7444.175*	Dec 2025	CVE-2025-13223 CVSS score: 8.8 | Severity: high
143.0.7499.109	Dec 2025	CVE-2025-14174 CVSS score: 8.8 | Severity: high

*The noted version is for Chrome for Desktop.

The way you configure your devices matters.

The modern mobile OS offers a wide range of powerful features, some of which we could only dream of even only five years ago. And you know what they say comes with great power...

You (hopefully) enroll your devices into Mobile Device Management (MDM) to ensure they're appropriately configured. Devices need to balance usability/productivity, security and user privacy — so the right configuration isn't always obvious.

While this will differ based on your organization's risk profile and industry, there are some standard features and setups that introduce a lot of risk, and should therefore be restricted:

- Jailbroken devices circumvent Apple's security restrictions and allow the user to modify their device in unsafe or unstable ways. Each jailbroken device is a potential backdoor for attackers to enter your system.
- Alternative app marketplaces allow users to install apps outside of the App Store or Google Play. Alternative app marketplaces aren't subject to the same security and privacy requirements, increasing the risk of a malicious or problematic app.

YET DESPITE THESE RISKS JAMF THREAT LABS DISCOVERED THAT:

1 in 850
devices used for work were jailbroken

2%
of organizations had devices with alternative app marketplaces.

Thoughts from our CISO

The holistic approach below mitigates the most common threats targeting mobile devices; spyware, compromised or malicious applications, and unpatched apps, all of which can silently expose sensitive corporate data without the user's knowledge.

- **Ensure all mobile devices are enrolled in MDM**, running approved OS versions, updates and meeting security baselines. Any device falling out of compliance should automatically be isolated from corporate resources until remediated. Having a robust framework to manage devices and users on those devices is paramount to stopping potential malware outbreaks before they start.
- **Implement agent-based security** that monitors for jailbreaks, malicious behavior and OS-level threats. Ensure telemetry is feeding into your SIEM so your SOC has visibility into mobile threats alongside the rest of your environment.
- **Enable DNS filtering and phishing protection** that covers all apps on all device, not just email. This should include detection of rogue Wi-Fi and attacker-in-the-middle attacks.

Application risks

Mobile apps are a big part of how your employees get their jobs done. How many mobile apps does your organization deploy? These apps, whether they're third party or developed in house, act as a front door for your sensitive data.

<1%

of organizations are affected by mobile malware.

Mobile malware is uncommon. It exists, but not to the degree seen on computers. This is largely due to the modern architecture used by the major mobile operating systems, where sandboxing and controlled app stores reduce the risk of malicious content reaching the device.

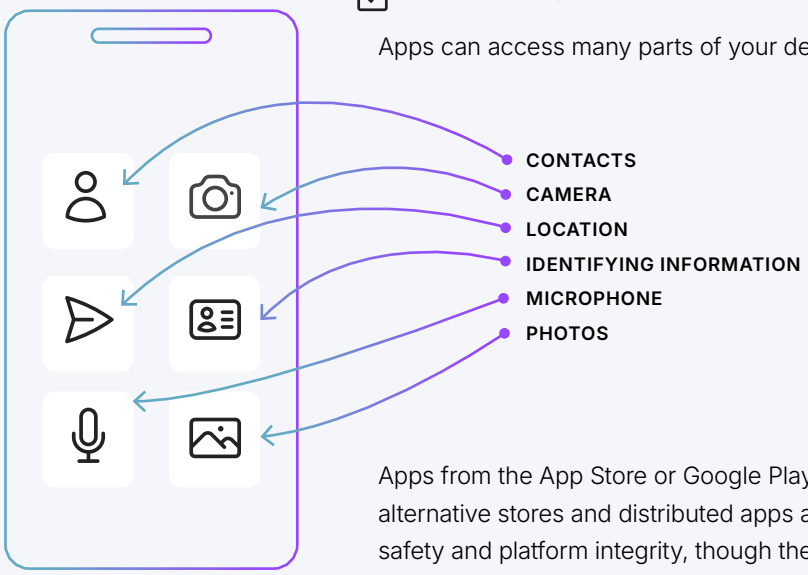
Still, apps expand your attack surface. Consider:

- **How apps handle data storage and transit**
- **What data apps collect and what their privacy policies are**
- **Supply chain concerns, like what libraries the app is built on**

Bad actors leverage app vulnerabilities to implement advanced persistent threats and spyware, so a deep understanding of your apps is crucial. Plus, how apps handle data transfer over networks can introduce risk — more on that later.

App privacy policies dictate data handling.

Apps can access many parts of your device, some more sensitive than others:



Apps from the App Store or Google Play are required to disclose any data collected. All alternative stores and distributed apps are subject to Apple's notarization process for safety and platform integrity, though the approval process is less restrictive than the review process on official App Store.

Security and privacy are difficult to balance.

Whether you give mobile devices to your employees or allow them to bring their own device, allowing access to your company's resources and data requires you to prioritize security and privacy. Security, because you need to protect your data. And privacy, because you need to protect the user.

Finding this balance can be a challenge. For instance:

- Your **data loss prevention** may stray into privacy-violating practices.
- **Locking up a device** for the sake of security can hinder productivity.
- **Improper policies** may enable shadow IT, where users download unsanctioned apps for certain job functions.

To combat these issues, your organization can:

- Require enrollment into **MDM** for access to corporate resources
- Separate personal and company data using hardened containers or partitions on BYOD devices to enforce data loss prevention policies — protecting user privacy by disallowing access to personal data
- Send company network traffic encrypted tunnels to guarantee confidentiality and data integrity
- Educate users about security best practices and policies

Supplement: analyzing app security

Jamf partnered with NowSecure to perform extensive analysis of mobile app risk, particularly in the context of apps that are popular with enterprise deployments. We analyzed 135 of the most popular and widely distributed business and personal mobile apps, using the OWASP standard as a baseline assessment of mobile app risk.

All apps analyzed were on their latest version as of December 31, 2025, reflecting real-world enterprise exposure to current app builds.

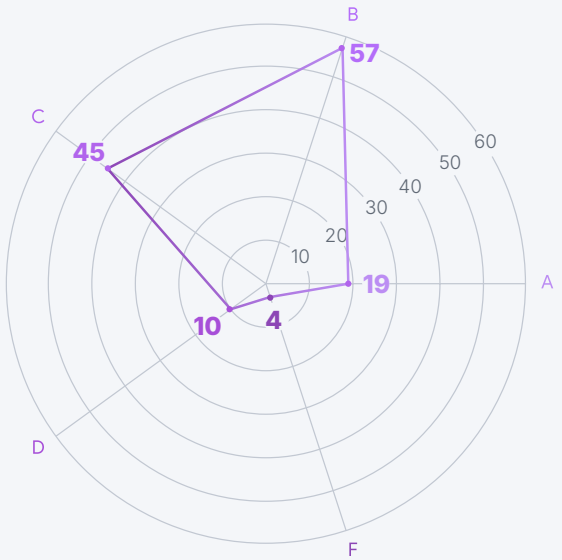
NowSecure helps organizations prevent mobile app vulnerabilities and data leaks from becoming security, privacy, or compliance incidents. By continuously analyzing both first- and third-party mobile apps and embedding results into security, IT and risk workflows, NowSecure gives teams the visibility, evidence and governance needed to manage mobile risk at scale.

Learn more about NowSecure.

App security score

NowSecure provides a mobile app security score from zero to 100 (higher is better) and an **A**-**F** risk rating (**A**=minimal risk, **F**=substantial risk). These scores are based on automated testing that evaluates vulnerabilities, data leakage, insecure coding practices, cryptography weaknesses and networking flaws.

SECURITY SCORES OF POPULAR APPS

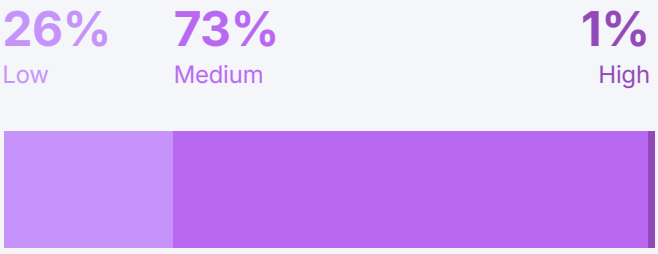


A — F

minimal risk — substantial risk

About **86%** of the 135 apps analyzed have known security flaws, with only **14%** considered to have minimal risk. This implies that risk is prevalent in the most common business and personal apps used daily, even on the latest versions.

VULNERABILITY DISTRIBUTION



Across all the vulnerabilities found in the analysis, most fell into a severity category of medium. As we observe later, the number of vulnerabilities exceeds the number of apps analyzed — implying multiple apps were found to carry more than one vulnerability.

App vulnerability assessment

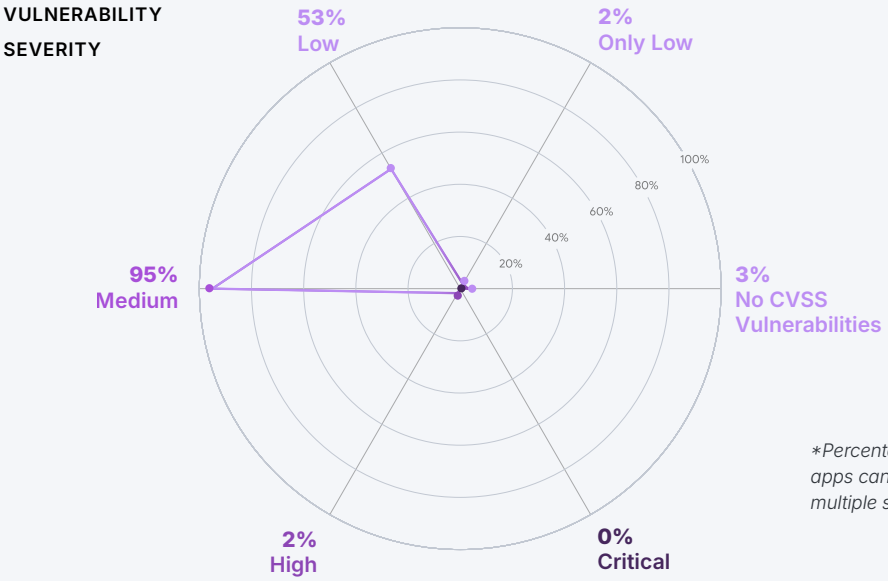
It's important to assess the risk implications that multiple vulnerabilities have on a single app. At the time of assessment, **95%** of apps contained at least one medium-severity vulnerability, and **2%** of the 135 apps had vulnerabilities that are high severity — making them ripe for attacks.

While software makers must remediate vulnerabilities in their applications, enterprises are responsible for understanding their risk exposure and ensuring timely updates. There are different recommendations for patch cadences (for example, CISA recommends remediating critical-severity vulnerabilities within 15 calendar days of initial detection and high-severity vulnerabilities within 30 calendar days of initial detection), but this data shows all organizations should have programs in place to keep apps up to date.

As we mentioned earlier, NowSecure evaluated apps on their current versions. Still, most had multiple vulnerabilities. Managing app risks is a continuous, ever-evolving task, requiring continuous monitoring and enforcement.

But it's manageable if you:

1. Continuously identify vulnerabilities and privacy issues
2. Prioritize remediation based on business impact
3. Enforce policies through mobile device management controls
4. Monitor third-party app behavior over time

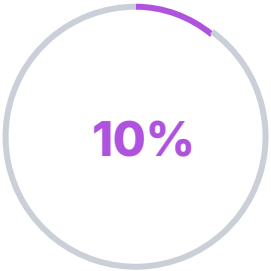


**Percentages may exceed 100% because apps can contain vulnerabilities across multiple severity levels.*

Supply chain

Mobile apps frequently rely on third-party SDKs and libraries that introduce hidden risk.

Your app could have acceptable data collection and privacy policies but use third-party software development kits (SDK) or libraries that have critical flaws. Because enterprises remain accountable for data exposure and compliance failures, they must have visibility into software supply-chain risk.



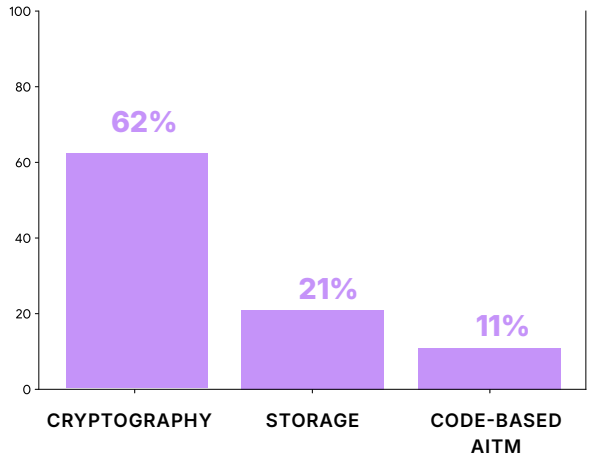
of **apps** used
vulnerable libraries

Data security

Data can leak out of apps in a few different ways.

- **Issues with cryptography:** It's challenging for app developers to secure data, protect communications and verify user identities. Many rely on third-party libraries. Across all the apps they analyzed, NowSecure identified use of two known vulnerable libraries — OpenSSL and libpng.
- **Insecure storage:** How data is managed at rest can make or break your data's confidentiality, integrity and availability. Weak storage protections increase the risk of data exfiltration.
- **AitM risks:** How apps handle data in transit is important too. If communications are not properly encrypted, for example, an adversary can intercept or manipulate sensitive information in transit.
- **Data Access:** Mobile applications have access to cloud and enterprise data that attackers want. Data loss is data loss no matter how it was accessed.

TYPES OF VULNERABILITIES



AI Usage

AI, especially generative AI, remains a hot topic these days. In a January 2026 report, Deloitte states that worker access to sanctioned AI grew by 50% in one year, with 60% of employees using AI tools at work.

It makes sense, since both on-device and cloud-based AIs offer a host of convenient features. For instance, mobile apps increasingly incorporate both:

- **On-device AI:** LLMs enable applications to perform natural language processing tasks, such as text generation and predictive typing, while machine learning models are used for used for features like image recognition, real-time object detection, barcode scanners and augmented reality.
- **Cloud-based AI:** perform various advanced tasks, relying on external infrastructure for processing and computation.

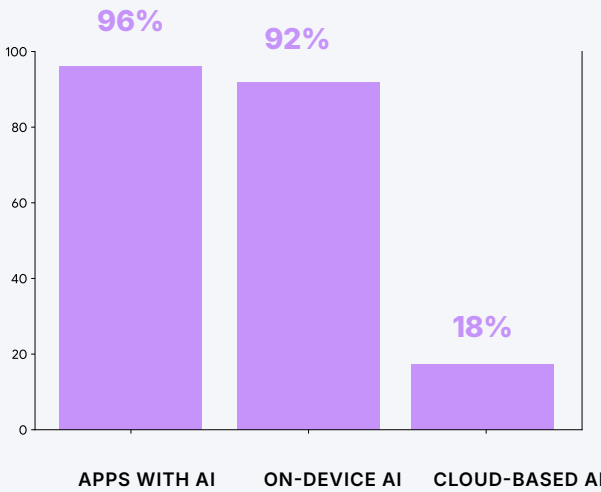
Users and organizations are quick to adopt generative AI, but as fast as the technology evolves, so do the risks.

Consider the risks:

- Users may use shadow AI, unsanctioned and ungoverned AI access that can include **sensitive company data** and violate policy.Cloud-based AI reliance on external infrastructure means your organization may not have transparency into the **potential risks**, including **data exposure**.
- Users may use AI agents to **perform autonomous actions**, beyond intended controls.

It turns out that a lot of common apps use AI, often without clear enterprise visibility.

AI FEATURE PRESENCE IN APPS



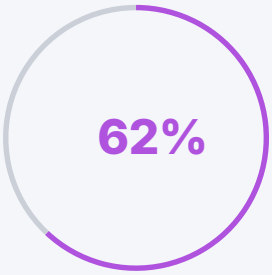
Privacy

We take our mobile devices everywhere. They contain multitudes of information about our personal and work lives, whether it's photos, contacts, sensitive data, financial documents, proprietary information and so on.

For this reason, users and employers prioritize privacy — plus, you might be subject to privacy laws.

This isn't always reflected in our apps though, whether by the developer's intent or neglect. Apps may request dangerous permissions that collect sensitive data, like access to:

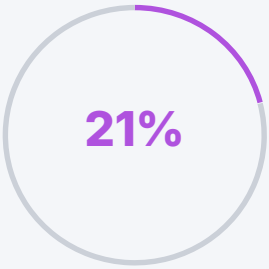
- Device location
- Microphone
- Camera
- Contacts



of **apps** requested dangerous permissions

Beyond requesting information, how do apps handle it? Some data is collected because the app needs it to function. Other data, not so much. Certain app features erode privacy, with privacy-impacting issues like:

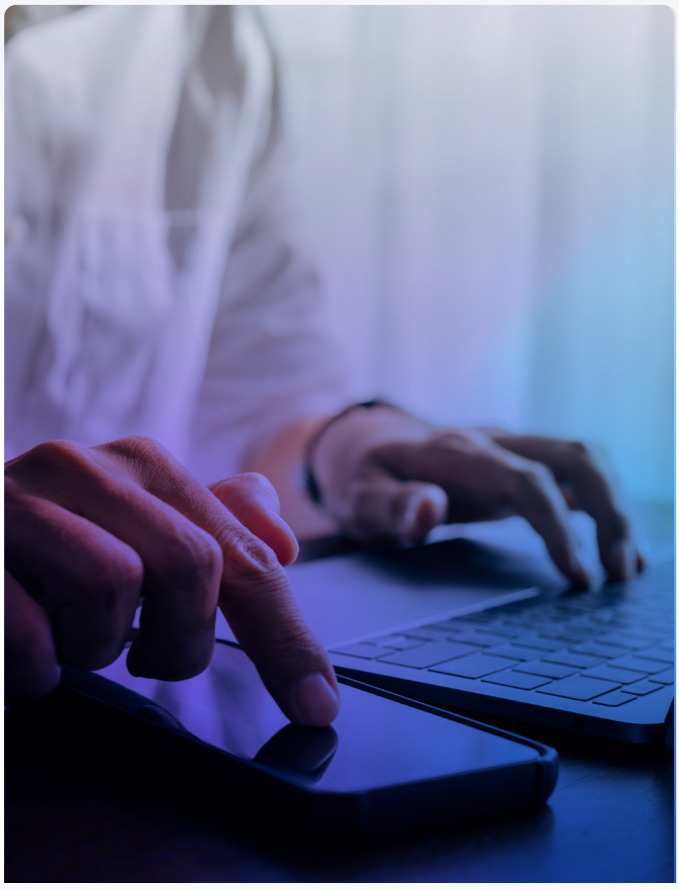
- Tracking and profiling
- Data sharing with third parties
- Contact collection/targeted advertisement



of **apps** contained privacy-impacting behaviors

Thoughts from our CISO

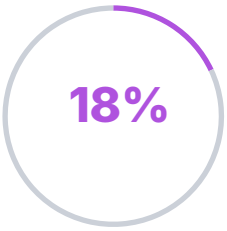
Mobile apps are the front door to sensitive corporate data. To manage this risk, organizations need to control what apps are allowed on devices, protect data as it moves across networks and maintain visibility into app vulnerabilities across the device fleet. With BYOD, the goal is separation. Keeping corporate data containerized and protected without intruding on personal privacy. The result is a balanced approach where security teams have the controls they need and employees have confidence their personal data remains private.



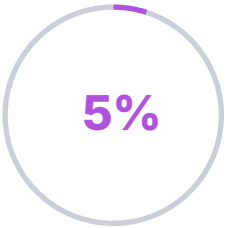
Network and web risks

Like death and taxes, one thing that's certain is that attackers will continue to exploit the weakest link in our security: humans. Attackers are getting more effective, using generative AI to craft increasingly convincing attacks. Users click on phishing links, connect to risky Wi-Fi networks and hotspots, and otherwise let their cyber hygiene slip.

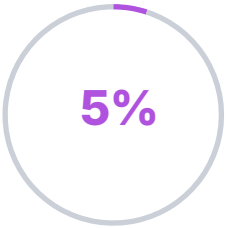
Not all vulnerabilities live on a device; even perfectly secured devices with ideal configurations remain vulnerable to threats that intercept data in transit. Networks are popular means of exploit. This can show up in multiple ways:



of **organizations** have users that connect to risky hotspots



of **organizations** have users that fell victim to infrastructure-based AitM attacks



of **organizations** have devices affected by cryptojacking

Network infrastructure

You can control your own network's configurations but not all third-party networks — including cellular networks — that your users connect to when off campus. Hopefully you're enforcing conditional access, segmenting your network and enforcing Zero-Trust Network Access policies.

If not, your data is at risk. If a user connects to an unsecured public Wi-Fi network — that may have weak encryption or no authentication — attackers can take advantage by stealing session cookies, bypassing certificate validation or other techniques.

Web protocols govern how devices, browsers and servers exchange information. They're a critical component of data security. Attackers can downgrade these protocols to older, less secure versions, making it easier to decrypt and steal data in transit. This opens up your organization to adversary-in-the-middle attacks.

These AitM attacks exploit vulnerabilities in network infrastructure, as opposed to code-based vulnerabilities within an OS or app.

Web risks

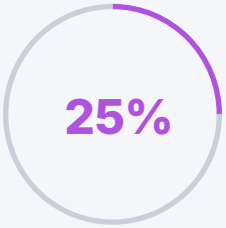
Even on a secure connection, browsing the internet isn't guaranteed to be safe. Devices don't have to be compromised to have problems. Clicking on malicious links/ads or visiting problematic websites can lead to cryptojacking and credential harvesting via phishing. Cryptojacking — where attackers use a device's processing and memory resources to mine for cryptocurrency — can slow down a device into uselessness.

Ah, phishing, our ever-popular foe. Generative AI makes it easier than ever to craft a convincing phishing message. Users can no longer assume malicious messages will be riddled with typos and other classically tell-tale signs.

Top 30 brands used in phishing campaigns

Bad actors like to mimic popular brands. Users are more likely to click on a link from a service they use and are familiar with — attackers take advantage of the trust users place in the institutions they use daily. Attackers are particularly incentivized to target banks and financial services, since compromised accounts are likely to contain both money and sensitive information.

Note that these brands haven't done anything malicious; attackers use their trusted reputation to lure unsuspecting users into a phish.



of **organizations** had a user fall victim to a phishing link.

Entertainment/ networking	Business	Utility	Banking/financial services
Netflix	Microsoft	Optus	Allegro
Facebook	Apple	AT&T	U.S. Internal Revenue Service
Steam	Adobe	Amazon	Rakuten
eBay, Inc.		DHL	Coinbase
WhatsApp		British Telcom	PayPal
		Orange	AEON Card
		Comcast	Sumitomo Mitsui Banking Corporation
		East Japan Railway Company	Navy Federal Credit Union
			Bradesco
			Bank of America Corporation
			HSBC Group
			Raiffeisen Bank
			American Express
			ING Direct

Thoughts from our CISO

In addition to technical controls, its critical to proactively prepare employees to recognize and report phishing and other social engineering threats through awareness programming, training and phish testing. Phish testing should leverage AI to provide testing tailored to the users' abilities and to keep the testing fresh according to new and diverse threats.

The proliferation of risks: advanced persistent threats

So far, we've talked about risks related to:

- Device OS and configuration
- Mobile apps
- Networking and web browsing

Any single risk, say an OS vulnerability, a mobile app with suboptimal data handling or a user connecting to public Wi-Fi, may have a significant impact to your data security. Or it may not, depending on your configurations policies and user training.

But when these risks build, they become a problem. Advanced threat groups stack vulnerabilities to create sophisticated exploits. While the threat actors responsible for these advanced attacks have historically demonstrated restraint by focusing on high-value targets, their toolkits are starting to be released more broadly, potentially putting average citizens in harms way.

Understanding these advanced threats is essential for defending against them. Jamf Threat Labs assessed the multiple exploitation delivery mechanisms (including zero-click and one-click attacks) and operational deployment models used in targeted surveillance operations, to get intelligence data from high-risk users like journalists, corporate executives, politicians, activists, and more. The analysis includes topics like OS and third-party application vulnerabilities, vendor response and more. This is what they found.

How to protect your organization: Implement post-exploitation detection, behavioral telemetry and anomaly-based monitoring, rather than relying on user interaction controls alone.

Zero-click attacks remain highly relevant

Zero-click attacks against Apple and Android devices remain an active threat vector in 2025, particularly for journalists and executive targets. Evidence of this is reinforced by the discovery of attack on WhatsApp users via an imageparsing vulnerability (CVE-2025-43300).

This discovery demonstrates that attackers continue to achieve code execution without any user interaction, bypassing traditional awareness-based defenses. These attacks are generally associated with targeted surveillance or intelligence collection operations.

The continued appearance of in-the-wild zero-click vulnerabilities confirms that motivated attackers retain both the capability and intent to invest in costly exploit development.

Browser attacks persist, including stealth delivery via ads.

Apple and Google published many browser security patches throughout the year. Chrome received 250 security patches; Safari received over 75, indicating ongoing discovery of memory safety issues that can be triggered through crafted web content.

These vulnerabilities are especially attractive because they can be weaponized via JavaScript on malicious websites or advertisements, lowering the operational cost for attackers. Threat intelligence reporting confirms that commercial spyware vendors continue to rely on one-click exploitation chains, combining rendered vulnerabilities with sandbox escapes to achieve full device compromise.

The discovery of Intellexa's operations highlights that such exploits are actively used by intelligence organizations and can be also delivered as zero-click attacks via advertisement network.

HOW TO PROTECT YOUR ORGANIZATION:
Amend your security stack with web traffic inspection, exploit-behavior detection and rapid OS/browser update enforcement within managed mobile environments.

Targeted companies actively fight back, but defensive coverage remains insufficient.

In 2025, platform vendors and large technology companies demonstrably increased their efforts to counter targeted spyware operations, including legal, technical and architectural measures. High-profile legal actions, such as Meta's litigation against NSO Group, illustrate an escalation beyond purely technical defenses into sustained legal deterrence.

At the same time, Apple continues to invest in platform-level mitigations, including the Memory Tagging Extension (MTE) and improvement of lockdown mode. However, successful exploitation chains persist despite these measures.

Advanced attackers continue to adapt their tooling and techniques to operate within or around new mitigations. For example, a possible workaround was recently demonstrated at a private conference.

HOW TO PROTECT YOUR ORGANIZATION:
Complement vendor-level protections with independent detection, forensic visibility and incident response capabilities tailored to targeted attack scenarios.

Spyware to look out for

Predator | Developer: Intellexa

Predator primarily relies on one-click web-based exploits, often delivered via malicious links or web content, including ads. It heavily abuses WebKit vulnerabilities, as reflected in repeated Apple patches. This model is more scalable but more sensitive to patch latency. Predator demonstrates that one-click attacks remain operationally viable.

Graphite | Developer: Paragon

Graphite is a commercial spyware platform linked to advanced iOS exploitation and is assessed to support both zero-click and one-click delivery. In 2025, successful zero-click iMessage exploitation against fully patched iPhones demonstrated Graphite's ability to compromise devices without user interaction. Multiple infections were attributed to the same operator infrastructure, confirming coordinated and deliberate targeting rather than opportunistic activity. These findings establish Graphite as an operational successor within the spyware market, despite increased regulatory and legal pressure on vendors.

Landfall | Developer: N/A

Landfall is a previously unknown, commercial-grade Android spyware family used in a targeted mobile espionage campaign against Samsung Galaxy devices. Operators exploited a critical zero-day vulnerability in Samsung's image-processing library to deliver the spyware via maliciously crafted image files, apparently distributed through messaging applications such as WhatsApp.

The campaign, active from at least mid-2024 until Samsung patched the vulnerability in April 2025, provided attackers with comprehensive surveillance capabilities, including audio recording, location tracking, and contact, photo and call log harvesting. From a defensive perspective, Landfall demonstrates that zero-day-enabled Android spyware operations continue to evolve outside of public visibility, underscoring the need for proactive patch management, anomaly detection and long-term device telemetry across mobile platforms.

Pegasus | Developer: NSO Group

Pegasus is a high-end iOS and Android spyware platform associated with zero-click and limited one-click exploit chains, enabling full-device compromise. It targets a small number of high-value individuals and is optimized for stealth and persistence. In 2025 NSO's business was affected by export restrictions and legal liabilities. The company was since acquired by a group of investors, but the technology is still expected to be used by intelligence organizations, maybe under a different brand.

Dante | Developer: Memento Labs

Memento Labs is an Italian surveillance technology vendor and successor to the controversial Hacking Team, rebranded after its acquisition in 2019. In 2025, tools linked to Memento Labs were used in an advanced cyber-espionage campaign known as Operation ForumTroll with a zero-day Chrome sandbox escape vulnerability (CVE-2025-2783). According to their CEO, they stopped supporting solutions for Windows and shifted their focus to mobile platforms, so this malware family and vulnerabilities are expected to be found on Android devices.

Spyrtacus | Developer: SIO

Spyrtacus is a commercial surveillance spyware family, reportedly actively targeting Android devices in 2025. It was delivered via malicious links and application-layer social engineering. Once resident on a device, Spyrtacus exhibits typical spyware capabilities such as data exfiltration, location tracking, and message and contact harvesting.

Unlike zero-click spyware such as Pegasus or Graphite, Spyrtacus generally requires some degree of user interaction or social engineering to initiate installation. The presence of Spyrtacus in real-world campaigns underscores that not all targeted mobile spyware relies on zero-day exploitation; instead, attackers may combine social engineering with commodity spyware frameworks to achieve similar objectives.

Thoughts from our CISO

Despite significant platform-level mitigations and security hardening by vendors, attackers in 2025 continue to discover and exploit critical vulnerabilities, particularly in high-value components such as browsers (Chrome, Safari) and messaging applications. These components remain attractive targets due to their complexity, frequent exposure to untrusted content and central role in daily user workflows.

The persistence of successful targeted attacks underscores that no mitigation strategy fully eliminates risk, especially against well-resourced adversaries. As a result, rigorous device management and strong update enforcement remain among the most effective and controllable defensive measures available to organizations.

This reinforces that mobile device management is not a supporting function but a core security control. Ensuring rapid security updates, enforcing security baselines, maintaining device visibility and reducing exposure windows are decisive factors in limiting the impact of newly discovered vulnerabilities.

The risks are great — but not insurmountable.

Addressing these risks requires thoughtful architecture. The pillars of secure devices are:

Device management
to apply restrictions, configurations and enforce policies

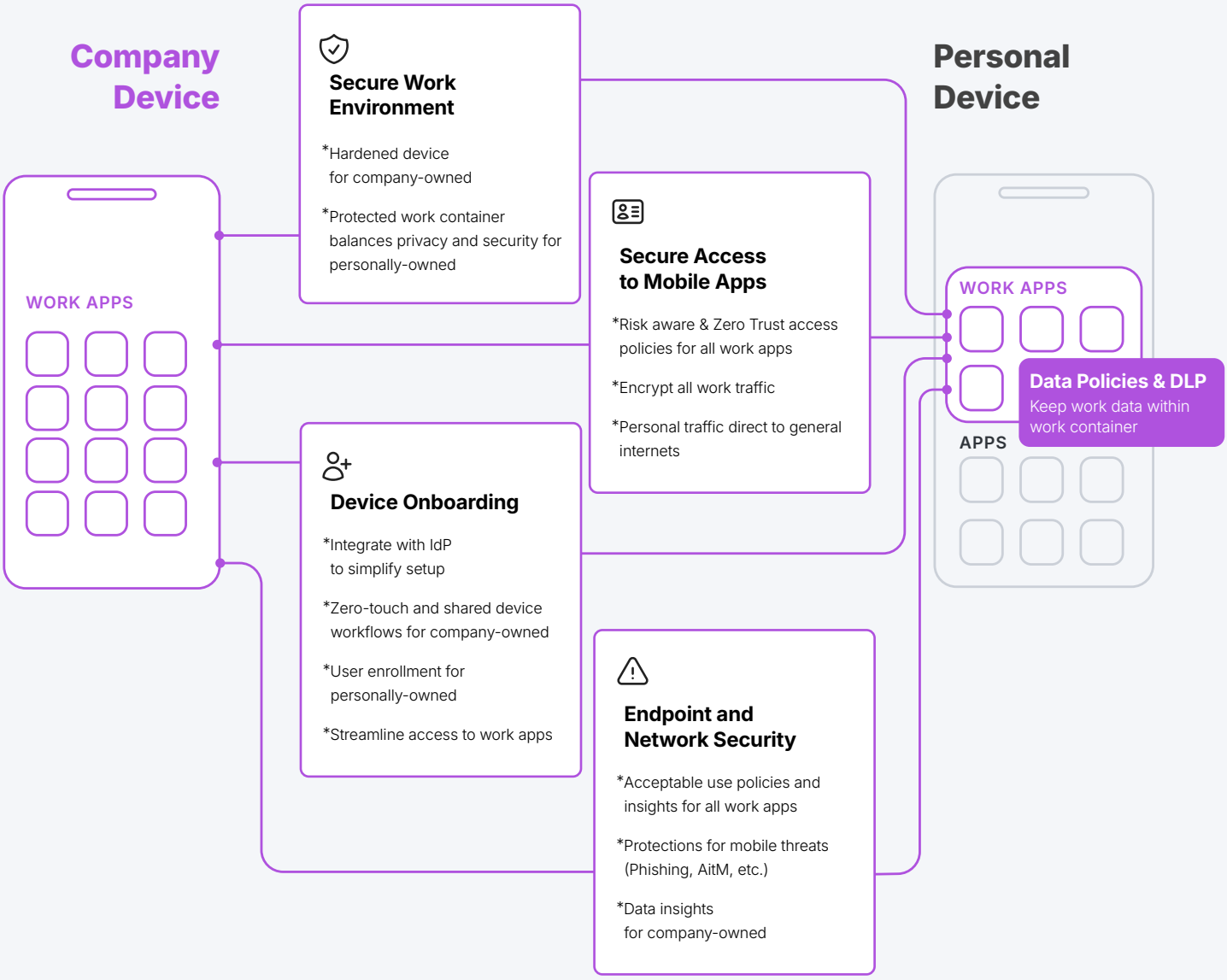
Endpoint security
to monitor device health and behavior, in case of potential compromise

Secure remote access
to govern who and what devices can access company resources

These work together to ensure only a compliant device and authorized user accesses your sensitive data.

This could look a little different, depending on whether a **device is company owned**.

Your devices' configuration can be a risk — or an asset to your security. Automating upgrades, app vetting and behavioral analytics, along with enforcing access policies based on compliance status, puts you well on your way to protected data.



Read the latest mobile research from Jamf Threat Labs

How Predator spyware defeats iOS recording indicators

FEBRUARY 2026

Using a sophisticated technique that exploits Objective-C nil messaging, Predator spyware bypasses iOS recording indicators. The malware hooks a single SpringBoard method that handles all sensor activity updates, then sets the self pointer to NULL, causing the indicator updates to be silently ignored rather than displayed to users. This approach is more subtle than previous techniques, since the device operates normally while providing no visual warning that surveillance is occurring, allowing covert camera and microphone access on fully compromised devices.

OpenClaw: the helpful AI that could quietly become your biggest insider threat

FEBRUARY 2026

OpenClaw is an open-source framework for building autonomous AI agents that can execute shell commands, access files and interact with applications without built-in security boundaries, creating significant enterprise security risks. The framework becomes dangerous through unrestricted system access, data exfiltration potential and vulnerability to indirect prompt injection attacks where malicious instructions are embedded in legitimate business content. Recent security advisories have demonstrated how attackers can exploit various flaws to gain persistent access, making OpenClaw deployments a high-risk insider threat that requires comprehensive detection, prevention and governance strategies to manage safely in enterprise environments.

Predator's kill switch: undocumented anti-analysis techniques in iOS spyware

JANUARY 2026

Predator spyware contains sophisticated anti-analysis capabilities that go far beyond previously documented findings, including an error code system that provides operators precise diagnostic information about why deployments fail. The malware detects developer mode, jailbreak tools, security applications and geographic restrictions, and implements advanced anti-forensics to hide recording indicators from victims.

These mechanisms reveal that operators receive detailed feedback when targeting fails, allowing them to troubleshoot and adapt their approach, demonstrating that commercial spyware vendors invest significant effort into detecting researchers, not just evading security products.

Jamf Threat Labs uncovers mobile app game leaking player credentials

NOVEMBER 2025

World of Warships Blitz, a popular mobile game with over 10 million downloads, was discovered leaking player credentials and session tokens over unencrypted HTTP connections during login and registration. While the credentials were obfuscated, the leak enabled replay attacks where attackers could capture and resend authentication requests to hijack accounts. After responsible disclosure, the developer cooperatively fixed the issue in version 8.4.0.

This investigation emphasizes that even popular apps can contain critical vulnerabilities and that layered security defenses and user education about password hygiene are paramount.

Jamf Threat Labs discovers apps that leak credentials

SEPTEMBER 2025

Two mobile apps were discovered leaking user credentials and personally identifiable information (PII) over unencrypted HTTP connections — a Malaysian healthcare management app serving 15 million users and an Indian jewelry company's "savings" app. Both apps transmit sensitive data in plain text, exposing users to credential theft, identity fraud and unauthorized account access, especially on public networks.

This discovery highlights the critical need for organizations to implement secure data transmission and for users to leverage mobile threat defense solutions, ZTNA and content filtering to block risky apps.

Flekst0re: third-party app store security evaluation

AUGUST 2025

Third-party iOS app stores like Flekst0re pose serious security risks, as demonstrated by a proof-of-concept modified WhatsApp that secretly recorded conversations and transmitted them to a remote server, all while appearing legitimate. These platforms bypass Apple's security review process by re-signing apps with enterprise certificates, and Flekst0re's custom source feature allows users to download unverified apps that could contain spyware or malware.

While third-party stores offer convenience and access to modified apps, they fundamentally undermine iOS security protections, making them dangerous for anyone using sensitive apps like banking, messaging or email.

jamf

Contact us to learn more about the mobile threat landscape.