iVerify.

WHITE PAPER

Beyond MDM

Why the Mobile Device is the Enterprise's Biggest Blind Spot

iVerify Inc.

iverify.io

TABLE OF CONTENTS

Executive Summary

The mass adoption of mobile devices for work-related tasks is rapidly expanding the corporate attack surface and significantly impacting an organization's security posture. Mobile devices have become the center of digital life, serving as the primary hub for authentication and access to corporate data. This shift, coupled with pervasive Bring Your Own Device (BYOD) policies, has created a fundamental security gap where personal risk becomes a corporate liability.

Attackers have capitalized on this vulnerability. They are moving away from historical, PC-focused exploits like EternalBlue and increasingly targeting mobile as an easier, less-protected access point. This includes the proliferation of sophisticated, zero-click spyware, such as the Coruna and DarkSword exploits, and high-volume mass threats like smishing and SIM swapping. These identity-centric attacks bypass traditional network and endpoint security controls, resulting in “the Enterprise Blind Spot”.

Mobile security has long been an afterthought, with enterprises under-investing and relying on the false assumption that devices are "secure by default" or that management tools (MDM) are sufficient. Since MDM is not a threat-detection or response solution, **90% of mobile devices** remain without adequate protection. This has created a massive detection gap: a fully patched phone can report a clean security posture even while it is actively being used to compromise the organization through credential or token abuse.

With financial cybercrime losses exceeding **$16.6 billion in 2024**, and the risk of catastrophic breaches constantly growing, organizations can no longer afford to ignore the rapidly growing mobile device threat landscape. Enterprises must strategically address mobile's centrality and close this liability before they are breached.

The Evolution of Mobile Security

Mobile: The Center of Digital Life

Mobile devices have become the core of digital life, spanning both professional and personal spheres. According to one recent survey,[1] Americans check their phone an average of **186 times a day**. Our phones are now the primary access point for nearly all digital communication—email, Slack, encrypted messaging, and social media—and, critically, serve as the central hub for authentication. Whether through Multi-Factor Authentication (MFA) codes, specialized apps, biometric identifiers, or password managers, the mobile device holds the 'keys to the kingdom' of the broader digital world. This ubiquity makes it easy to access corporate networks and resources 24/7 from anywhere.

While this shift significantly enhances productivity, this centrality has created a massive, lucrative target. Online attackers have not only noticed; they are actively exploiting this shift, making it crucial for organizations to secure this endpoint as they would any other.

The Shifting Threat Landscape

Instead of attempting to exploit and compromise individual devices with purely technical exploits, attackers are now focused on using stolen account credentials to quietly access systems. This pivot to credential theft is increasingly enabled by the combined power of AI tools and sophisticated social engineering techniques, making the attack identity-centric rather than device-centric.

Organizations have noticed. **85% percent of security professionals**, regardless of their organization's size or industry, say they think mobile attacks are on the rise. Additionally, while 34% said they worry about the increasing sophistication and scale of AI-powered attacks, human user behavior was the factor most often cited by them as a data breach contributor,[2] with 44% saying it was a factor.

Why Are Attackers Targeting Mobile Devices

Where the money and data go, the attackers go, too, and mobile devices offer the greatest return on effort with the lowest friction.

- **Credentials and Access:** The average person's phone is a treasure trove of sensitive information, including passwords, MFA codes, authenticator apps, and biometric data. Access to those could open up the gates to all kinds of personal and professional accounts.
- **The Trust Factor:** Users are more likely to click on links and respond to messages when they appear on familiar, personal devices. Unlike phishing emails, users are less conditioned to spot malicious texts, making mobile-based social engineering highly effective.

1 Cell phone Usage Stats 2026, Reviews.org
2 2025 Mobile Security Index, Verizon.

- **Blurred Boundaries and BYOD:** With **82% of companies** now having a “bring your own device” (BYOD) policy,[3] an increasing number of people are using the same device for their personal banking as they do for their corporate email. It also means they’re using personal devices for work without proper security measures in place. **70% of mobile devices** affected by cyberattacks are personal, rather than company-issued[4].

The Security Gap

Smartphones have long been viewed as closed ecosystems, protected by strong operating system controls, curated app stores, and hardware-backed security. This secure-by-default mentality has meant that enterprise security investments at many organizations haven't kept pace with the real growing threat from mobile devices. What focus there has been has centered on device management, not on device compromise.

Mobile device management (MDM) software is a well-established best practice, especially in BYOD environments, but it’s not a replacement for dedicated mobile security. MDM tools can enforce policies like password requirements, push configurations, and enable remote wiping if a device is lost. What they cannot do is detect threats or respond to active attacks. It's the difference between locking your doors and having an alarm system. Both matter, but one won't do the other's job.

Advanced exploit chains, such as the recently discovered Coruna and DarkSword exploits, target the operating system itself, bypassing user interaction, application sandboxes, and many of the signals that enterprises traditionally rely on to detect compromise. Without advanced mobile security solutions, these threats would easily go undetected.

iVerify had been conducting an independent technical analysis of the Coruna exploit kit several weeks before Google published its findings. It is one of the most significant examples of sophisticated spyware-grade capabilities proliferating from commercial surveillance vendors in the hands of nation-state actors we’ve observed. It also marks a major shift in the mobile threat landscape; tools once reserved for targeting heads of state are now being deployed against ordinary iPhone users. Yet despite the growing threats, many organizations treat MDM as their mobile security strategy, leaving a significant blind spot with implications far beyond the C-Suite.

Read the technical findings from the iVerify Research Team on:

- **The Coruna exploit**
- **The DarkSword exploit**

3 Top BYOD Security Risks & How Mobile Virtualization Preserves Privacy, Hypori.
4 2025 Mobile Security Index, Verizon.

The Threat Spectrum

Targeted Threats: Nation-State Actors and Advanced Spyware

The traditional threat spectrum draws a clear line between nation-state actors and financially motivated cybercriminals. On mobile, that line is increasingly blurred.

Advanced exploit kits, like Coruna, demonstrate a level of sophistication historically reserved for state-sponsored operations: zero-click delivery, kernel-level access, long dwell times, and deliberate operational security designed to avoid detection.

What has changed is not only who can deploy, but how they're used. Advanced techniques are filtering downward, reused, repurposed, or adapted for broader objectives. This collapse of the threat spectrum has profound implications for enterprises.

Zero-Click Exploitation and Commercial Spyware

Commercial spyware products such as Pegasus and Graphite have become increasingly popular among nation-state attackers because they don't require a target to click a link or actively download a malicious file to their device.

There have been several recorded instances where Pegasus software has been used against human rights activists, journalists, and political-opposition leaders, including in 2023 when iVerify found that it had been deployed against political opposition leaders in India.[5]

But enterprise leaders and those connected to them are being targeted, too. A May 2024 iVerify investigation of 2,500 self-scanned devices in its user base discovered seven new Pegasus infections, amounting to 2.5 infections per 1,000 scans.[6]

For a 10,000-employee organization, that rate would translate to roughly 25 compromised devices across the fleet. And because most organizations have never scanned their mobile devices for advanced threats, these infections typically go undetected indefinitely. In late 2024 and early 2025, iVerify continued to detect activity consistent with zero-click mobile exploitation, indicating the threat is not diminishing.[7]

And in November of 2025, the Cybersecurity & Infrastructure Security Agency[8] warned that threat actors were actively using commercial spyware to target users of messaging apps. The threat actors used both phishing techniques and zero-click exploits to compromise their targets' accounts and devices.

In short, mobile compromise is no longer a hypothetical reserved for diplomats or dissidents. The same techniques can be applied where the return on access justifies the effort — including corporate environments.

5 India Targets Apple Over Its Phone-Hacking Notifications, The Washington Post
6 iVerify Mobile Threat Investigation Uncovers New Pegasus Samples, iVerify.
7 iVerify Uncovers Evidence of Zero-Click Exploitation in the US, iVerify
8 Spyware allows cyberthreat actors to target users of messaging applications, CISA

Man-in-the-Middle (MiTM):

State-sponsored groups, such as the China-allied Salt Typhoon, use sophisticated techniques to compromise telecom network infrastructure,[9] making unencrypted traffic vulnerable to interception, surveillance, and data manipulation. Attackers also get access to jumping-off points for MiTM-enabled endpoint attacks.

While enterprises that do business in Asian countries that use China-backed telecom infrastructure are most at risk, it's worth noting that infrastructure built by Chinese companies ZTE, Huawei, and TP-Link is present in U.S. telecom networks, representing potential risk.

As with commercial spyware, enterprises must recognize that the risk extends far beyond the C-suite. A single compromised phone, whether it belongs to a senior executive or an administrative assistant, provides access to the same corporate email, Slack channels, and authentication tokens. Adversaries don't need to target the CEO when targeting an IT administrator or finance team member who can deliver the same credentials and access. The threat is not who carries the device, it's what the device can access.

Mid-Range Threats: Physical, Insider, and Data Loss Risks

Mid-range threats range from possible physical device access by governmental authorities to local network manipulation and malicious insider risks, to possible data leakage by negligent employees.

Border crossing device forensics: The number of electronic services searched at crossings by US Customs and Border Protection has risen steadily over the last couple of years. More than 55,000 devices were searched in fiscal year 2025,[10] though that represents less than 0.01% of arriving international travelers.

Commercial tools can do full-file system imaging and can extract all personal data, photos, and messages from devices. It's not just happening in the US; almost every country has the authority and capability to search and seize data from electronic devices.

Fake Cell Towers (IMSI Catchers): These are used by law enforcement and governments, along with cyber criminals, to mimic legitimate cell towers, tricking nearby mobile devices into connecting.[11] This allows them to track phone locations, intercept or disrupt communications, spy on foreign governments, or even install malware.

Insider threats: Several security firms[12] have documented campaigns backed by the Democratic People's Republic of Korea (DPRK) to infiltrate US companies by posing as remote IT workers. They gain legitimate access to companies' systems, then exploit that access for data theft and extortion purposes.

9 Counterping Chinese State-Sponsored Actors, CISA
10 Border Search of Electronic Devices At Ports of Entry, US Customs & Border Protection.
11 Apple and Google Are Introducing New Ways to Defeat Cell Site Simulators, EFF
12 Global Companies Are Unknowingly Paying North Koreans, Unit 42.

Data leakage risks: Mobile devices, especially in a BYOD environment, can increase the risk of accidental data leakage and unauthorized access. Specifically, this can happen through unsecured cloud storage, messaging apps, and email.

Mass Threats: Social Engineering, Smishing, and SIM Swapping

While these attacks may not be as sophisticated or specifically target organizations, they're still a serious threat because of their massive volume. The low level of technical ability required to pull them off allows many more criminals to become attackers. And regardless of skill, the goal of those attackers remains the same: compromise a mobile device and use it to gain access to the broader computer systems.

Smishing (SMS Phishing): This is the dominant method attackers use to steal credentials, with **80% of companies** reporting smishing attempts on their employees.[13] While many people now know how to spot traditional phishing emails, they're less likely to spot scam texts. The common use of Tiny URLs in texts further masks malicious links.

SIM Swapping: Attackers trick mobile carriers into porting phone numbers to a new device, ultimately allowing them to intercept MFA codes sent by SMS text messages and hijack a target's account. According to the FBI, there were 982 complaints involving SIM swaps filed in 2024, accounting for nearly $26 million in losses.[14]

The trend is accelerating globally. In the UK, fraud-prevention service Cifas[15] reported a staggering **1,055% year-over-year surge** in unauthorized SIM swaps in 2024, jumping from 289 cases to nearly 3,000. Australia saw a 240% increase in SIM porting fraud over the same period, with 90% of cases occurring without the victim's engagement. Nearly half **(48%) of all account takeovers** in 2024 involved mobile phone accounts.

Victims often don't realize anything is wrong until their phone suddenly shows "No Service" and their accounts have already been drained.

Social Engineering: Attackers will leverage the immediacy and trust that comes with mobile communication to trick their targets into thinking they're someone they're not, like a company executive, a colleague from IT, a vendor, or even a family member. The informal nature of text-based communication makes people more likely to respond quickly without verifying the request, prompting them to hand over money, account credentials, or other sensitive information. Any employee with access to corporate systems or financial accounts can become a target.

As mentioned previously, these techniques are used across all attack levels and are becoming increasingly popular among attackers. For example, vishing attempts, where cybercriminals call targets on the phone and attempt to trick them into handing over information, jumped 442% from the first half of 2024 to the second half of the same year.[16]

13 2025 Mobile Security Index, Verizon.
14 2024 Internet Crime Report, FBI
15 1,055% surge in unauthorised SIM swaps as mobile and telecoms sector hit hard by rising fraud, Cifas
16 2025 Threat Report, CrowdStrike.

The rise of AI-powered tools, including those that enable the creation of audio and video deepfakes, has also made it easier for attackers to launch sophisticated social engineering campaigns at unprecedented scale. More than **4 million mobile-focused social engineering attacks** were detected in 2024.

77% of organizations believe AI-assisted deepfake and SMS phishing attacks are likely to succeed.[18]

Mobile banking trojans: These are malicious software programs that steal financial and sensitive data from mobile devices. They often masquerade as legitimate apps or hide within seemingly benign programs. In 2024, the number of mobile banking Trojan encounters more than tripled from the year before, while malware attacks against PCs dropped.[19]

Trojan banker attacks on Android: Researchers are warning of a new Android banking Trojan known as Sturnus.[20] First spotted late last year, this malware has a wide variety of capabilities, including the ability to fully take over a device.

Notably, it can bypass encrypted messaging. By capturing information directly from the device screen after decryption, it can monitor communications via WhatsApp, Telegram, and Signal. It can also gather banking credentials through legitimate-looking fake login screens that replicate real banking apps.

18 2025 Mobile Security Index, Verizon.
19 2024 Financial Cyberthreats report, Kaspersky.
20 Sturnus: Mobile Banking Malware Bypassing WhatApp, Telegram & Signal Encryption, Threat Fabric

TARGETING INDIVIDUALS FOR FINANCIAL GAIN

The Scale of Financial Cybercrime

Cybercrime is on the rise because it pays, creating an immensely profitable and rapidly escalating industry for threat actors. The sheer scale of financial loss underscores the urgency of the mobile threat.

Financial losses reported to the FBI's Internet Crime Complaint Center totaled **$16.6 billion in 2024** (the most recent figures available), marking a catastrophic 33% increase from the year before.[21] Nearly 860,000 complaints were filed with the FBI in 2024.

The vast majority of the losses (83%) stemmed from cyber-enabled fraud, where criminals used technology to steal money, data, or identity information. The largest contributors to these losses were:

- **Investment Fraud:** $6.57 billion
- **Business Email Compromise (BEC):** $2.77 billion
- **Tech-Support Scams:** $1.46 billion

In terms of complaint volume, **phishing** remains the most common form of attack (193,407 complaints), but newer, high-volume mobile scams are also on the rise. For example, fraudulent road toll scam texts accounted for 59,271 complaints and $129,624 in losses in 2024.[22]

The Cryptocurrency Accelerator

This jump in losses is part of a broader trend, accelerated by the increased availability and use of cryptocurrencies. Designed to be anonymous and untraceable, cryptocurrency enables cybercriminals to scam larger amounts of money with little hope of recovery. Of the 2024 reported crimes, cryptocurrency was involved in 149,686 complaints and accounted for **$9.32 billion in losses**,[23] demonstrating its critical role in funding the global cybercrime economy.

Mobile as the Critical Entry Point

As attackers increasingly monetize individual access, mobile devices become the preferred entry point. The result is a growing category of financially motivated attacks that never touch the corporate network, yet directly impact corporate risk.

Mobile phishing is increasingly becoming a problem for businesses. As noted before, 80% of organizations say their employees are being targeted with mobile phishing attempts.[24] Additionally, researchers say phishing attacks targeting mobile devices increased by **25% to 40%** compared to desktops in 2024, with that trend continuing into 2025.[25]

21, 22, & 23 2024 Internet Crime Report, FBI.
24 2025 Mobile Security Index, Verizon.
25 250+ Phishing Statistics and Trends You Must Know in 2025, Keepnet.

Unsurprisingly, the attackers continue to go where the money and data are. The same researchers noted that financial services continue to be the most targeted, accounting for 27.7% of all phishing attacks globally.

It's important to note that while mobile devices are the hardware used to deliver the messages, those messages aren't just coming by SMS text. Encrypted messaging services like WhatsApp, QR codes, social media direct messages, and mobile device emails are also regularly used for mobile phishing attempts.[26]

The Human Element: Social Engineering in Practice

Despite defenders' best efforts, cybercriminals have been successful in using social engineering to target organizations and their employees. Here's a look at how they do it.

Help desk manipulation: Attackers will impersonate employees, using information gathered from LinkedIn and other social media to convince IT staff to reset passwords or enroll new MFA devices, thereby gaining access to corporate accounts.

Executive impersonation attacks: Attackers impersonate a company leader and create a sense of urgency via text or mobile messaging, claiming they need immediate access to systems or that funds must be sent via wire transfer right away.

AI boosts sophistication and scale: AI tools are making all of these attacks quicker and easier to pull off, as well as more convincing. Instead of combing through social media by hand to harvest personal details about a potential target, cybercriminals can now automate the process.

Meanwhile, audio and video deepfakes are now being used to realistically mimic real people's likenesses, increasing the likelihood that targets will fall for impersonation attacks. That has companies worried. **77% of organizations** believe AI-assisted deepfake and SMS phishing attacks are likely to succeed.[27]

This shift reflects a simple reality: compromising the right person often yields faster and more valuable outcomes than attacking an organization head-on.

26 250+ Phishing Statistics and Trends You Must Know in 2025, Keepnet.
27 2025 Mobile Security Index, Verizon.

Scattered Spider Case Study

Young, English-speaking attackers, often posing as company IT and help desk workers, used techniques including SMS phishing, vishing, and SIM swapping to obtain login credentials, install remote access tools, and bypass multi-factor authentication to access company systems.[28]

They both infected enterprise systems with ransomware and extorted sensitive data. Some of their first victims were massive casino companies, including MGM Resorts International and Caesars Entertainment, before moving on to retailers like UK department stores Harrods and Marks & Spencer, along with the grocery store chain Co-op Group.

The same group also claimed responsibility for the cyber attack on automaker Jaguar Land Rover,[29] widely considered to be the U.K.'s most costly of all time, with a financial impact of 1.9 billion pounds ($2.55 billion).[30]

Demographics of Victimization: "Anyone, Anywhere."

People say that they'd never fall for a social engineering attack, but the truth is, anyone can.

While the raw numbers show that older demographics bear the largest financial burden—people ages 60 and up reported **$4.88 billion** in losses and filed **147,127 complaints** in 2024[31]—attackers do not discriminate. Any and all employees are potential targets.

The blurring of professional and personal boundaries means that, as more employees access work files on personal devices, both are at equal risk.

28 Scattered Spider Advisory, CISA.
29 30 M&S hackers claim to be behind Jaguar Land Rover cyber attack, BBC.
30 Cyber Monitoring Centre Statement
31 2024 Internet Crime Report, FBI.

DATA LOSS PREVENTION AND INSIDER RISK

The Mobile DLP Challenge

Enterprise Data Loss Prevention (DLP) and insider risk programs are fundamentally built on an assumption of visibility and control. They are designed to monitor, log, and govern sensitive activity on managed endpoints and within enterprise applications. Mobile compromise fundamentally breaks this assumption.

While many companies still issue their workers laptops, BYOD has become the norm with smartphones, so often the same personal device handles work and life data, leading to inevitable data blending. When corporate data resides on a personal smartphone, it exists outside the corporate security perimeter. It can easily migrate to unsecured personal cloud storage, consumer messaging apps, or personal email, all of which are blind spots for traditional DLP. Even low-tech theft, such as an employee taking a photo of a document, leaves no digital trace for current systems to follow.

The most critical gap arises when an attacker obtains OS-level access via an advanced exploit, such as the Coruna zero-click exploit. In this scenario, the attacker can observe and exfiltrate sensitive data outside the reach of all traditional DLP and EDR tools. Encrypted messaging apps, personal email, cloud storage, and authentication flows all become pathways for massive data loss. Crucially, these situations do not resemble traditional malicious insider threats. The employee remains unaware; their device behavior appears normal, and enterprise controls register no anomaly. Yet, sensitive corporate information is continuously exposed, highlighting the failure of traditional DLP to account for the mobile attack surface.

Insider Threats: Malicious and Negligent

Advanced mobile threats highlight a blind spot in insider risk strategies: not all data loss is intentional, and not all compromise originates within enterprise systems. While it’s far more likely that a company will experience a data leak because of a negligent employee rather than a malicious one, threat actors are looking to infiltrate a company’s employee ranks and use that access for their own benefit.

Experts say the risk is real, growing, and the attacks have the potential to inflict serious damage on targeted organizations. Meanwhile, mobile devices, especially employees' personal ones, complicate detection because they can put data outside the reach of corporate security professionals.

DPRK Case Study

Operatives backed by the Democratic People's Republic of Korea (DPRK) have successfully infiltrated US companies by posing as remote IT workers. Researchers have tracked the activity back to at least 2022.[32]

Typically, the North Koreans would create fake workers with fabricated names, resumes, and even personalities in attempts to get them hired at major companies across a variety of industries. They would also pay non-North Korean people, known as "facilitators," to do things like launder money and cryptocurrency, receive and monitor company laptops at their homes, or stand in for the North Koreans during video interviews to make it look like someone else was applying.

While the North Koreans' initial goal was to raise money for their regime, the scope of the operations has recently expanded. North Korea is now targeting companies outside of the U.S., in places like Europe, and they're looking to do more than just earn paychecks. They're also using their privileged access to corporate systems to steal data and launch cyberattacks[33]

Location Intelligence and Sensitive Travel

Employees traveling through high-risk parts of the world face additional threats from government surveillance. This is particularly true for politicians, diplomats, and journalists, with the former being at high risk due to their access to potentially sensitive information. If a country's telecommunications infrastructure is compromised, location and other sensitive data, along with unencrypted communications, could be intercepted.

Border crossings also represent potential risk. If authorities confiscate a device at a crossing, it could be forensically examined and its data extracted.

32 DPRK IT Workers Expanding in Scope and Scale, Google Threat Intelligence.
33 The ultimate insider threat: North Korean IT Workers, Google Threat Intelligence.

Salt Typhoon Case Study

China-allied Salt Typhoon used sophisticated techniques to compromise telecom network infrastructure.[34] And because carriers in countries like Japan, South Korea, and New Zealand are actively routing telecom traffic through China-backed infrastructure, unencrypted traffic became vulnerable to interception, surveillance, and data manipulation.

The attack provided ample opportunities to surveil unencrypted communications and countless jumping-off points for MiTM-enabled endpoint attacks, including on mobile devices, which iVerify has observed on numerous occasions.[35]

Law enforcement and intelligence officials from the US and around the world said that the years-long, coordinated attack likely compromised almost every major American telecommunications network, targeted more than 80 countries, and possibly stole data from every American.[36]

Despite the best efforts of governments and security professionals, Salt Typhoon remains active in the U.S. and elsewhere. According to media reports, the group recently hacked the emails of U.S. Congressional committee staff.[37]

34 Counterping Chinese State-Sponsored Actors, CISA
35 iVerify Uncovers Evidence of Zero-Click Mobile Exploitation in the U.S., iVerify
36 Counterping Chinese State-Sponsored Actors, CISA.
37 China hacked email systems of US congressional committee staffers, FT reports, Reuters.

THE ENTERPRISE BLIND SPOT

The Security Investment Mismatch

Despite the central role mobile devices play in enterprise operations, security efforts and spending to secure them haven't kept pace. Enterprises spend heavily on endpoint detection, network, and cloud security, but mobile devices are often forgotten, ignored, or treated as a compliance checkbox. There's also the critical misconception that any deployed MDM solution is enough; it's not. MDM solutions help companies regulate the mobile environment, but they're not designed to detect or stop attacks.

81% of enterprises have not incorporated MTD into their current cybersecurity stack[38]

OS & Device Makers ≠ Enterprise Defense

Many organizations assume that modern smartphones are "secure by default" because they run iOS or Android. That assumption has become a critical enterprise blind spot.

Mobile Operating Systems are designed to preserve platform integrity; they do not detect or stop the identity-centric attacks that compromise businesses today.

They will not catch:

- Targeted smishing and mobile social engineering
- SIM-swap–enabled MFA bypass
- Zero-click and fileless spyware
- Authentication token theft and session hijacking
- Identity-led intrusion campaigns that never install malware

These attacks do not break sandboxing rules. They do not require malicious apps. They do not trigger consumer malware protections. And in many cases, they leave no visible indication to the user. From the operating system's perspective, everything appears normal.

38 Modern Mobile Device Protection: Why Legacy Approaches Fall Short, Zimperium

A fully patched, non-jailbroken phone can still be:

- Receiving and responding to malicious messages
- Relaying valid MFA codes
- Holding active session tokens
- Authenticated into corporate email, cloud apps, VPNs, and admin portals—all while the device reports a clean security posture.

This is not a corner case. It is now a primary access path used by attackers.

As long as the kernel looks intact and apps behave within expected boundaries, the OS considers the device "secure", even if it is actively being used to compromise the organization. In practice, this means the phone can be secure while the enterprise is already breached.

When organizations rely on only MDM to enforce policy and OEMs to "handle security," they gain compliance visibility, not threat detection. They can see OS versions, passcodes, and configuration states, but they cannot see:

- Active exploitation
- Credential and token abuse
- Session misuse
- Targeted surveillance or spyware activity

This is why attackers have moved to mobile. Not because phones are unpatched, but because enterprise defenses stop at the operating system boundary.

Apple and Android were never designed to protect enterprises from:

- Smishing-driven credential theft
- SIM-swap attacks
- Zero-click exploitation
- Identity-centric intrusion operations

Enterprise mobile security is not about whether a device is "safe." It's about whether the device is being used as an attack surface.

The Detection Gap

Whether you're talking about mobile or traditional computing devices, data breaches can be hard to detect, especially as threat actors move toward less technical attacks powered by social engineering.

On average, in 2025, it took organizations **241 days** to identify and contain data breaches. That may seem like a long time, but it marked a nine-year low and continued a downward trend that started with a peak of 287 days in 2021.

39 Cost of a Data Breach Report 2025, IBM.

Data breach costs also dropped from the year before. Organizations worldwide paid an average of about $4.44 million per breach, marking a 9% drop from 2023 levels.

Part of the decline is due to increased security spending. But mobile defense hasn't been forgotten — it's been systematically ignored, receiving only a small fraction of the investment and attention devoted to other parts of the enterprise.

When it comes to social engineering-powered phishing, it's important to note that iOS and Android devices are equally susceptible. While malware may be designed to attack a specific operating system, no OS is immune to human attempts to trick employees into handing over their credentials.

And people are often apt to do that. About **60% of the data breaches in 2025** involved a human element.[40]

Why Traditional Approaches Fail

The shift to mobile work—combined with the attacker's strategic move away from technical exploits toward social engineering—means security leaders need to completely rethink their priorities and defenses. Current approaches fail to secure the enterprise because they are built on outdated assumptions.

1. Obsolete Mobile Threat Defense (MTD)

Old-school mobile threat defense solutions are built primarily to detect attacker attempts to jailbreak or root mobile devices. However, threat actors have largely shifted away from these detectable attempts. Modern exploits, such as the Coruna zero-click exploit, operate at the kernel level without requiring a jailbreak, rendering this foundational MTD strategy unreliable for contemporary mobile threats.

2. The Limits of Containerization

Containerization, which isolates certain corporate processes and resources, provides only limited protection. It is ineffective against kernel-level exploits and is completely useless against social engineering. The attacker's focus has shifted to credential theft, which bypasses the container and the application sandbox entirely.

3. The Human Barrier

Human perspectives on mobile security have also failed to keep up with the times. Employees are understandably protective of their personal devices and information, creating a security/privacy tension. Their resistance to having company eyes or security software on personal phones creates massive, unmanaged security gaps in the BYOD environment.

39 Cost of a Data Breach Report 2025, IBM.
40 2025 Data Breach Investigations Report. Verizon.

4. The Endpoint Misconception

Many security professionals still treat mobile devices as just another endpoint and a secondary concern to laptops or servers. In reality, the mobile device is now a primary endpoint, the authentication hub, and a main access point to corporate resources. Until this strategic reality is acknowledged, enterprise security will continue to operate with a fundamental blind spot.

THE ERA OF NEGLECT IS OVER

The Forcing Functions

The era of neglecting mobile security is over. Change is being forced upon organizations by undeniable market pressures, escalating costs, and mounting regulatory scrutiny. The question is no longer if a breach will happen, but when, and the financial and reputational consequences are now too great to ignore.

The forces driving this change include:

- **Escalating Costs and High-Profile Breaches:** The financial consequences of inaction are escalating rapidly. While the average global cost of a data breach fell 9% to $4.44 million last year, the average cost of a data breach in the U.S. rose 9% to a record **$10.22 million**, driven in part by higher regulatory and legal costs.[41]
- **Board-Level Pressure:** High-profile, costly breaches attributed to the compromise of mobile devices, such as the 2023 cyberattack against MGM that cost the company about **$100 million**, are now commanding board-level attention.
- **Regulatory and Compliance Pressure:** Regulatory pressures and compliance requirements are increasingly extending their scope to explicitly address mobile devices and security.
- **The Cyber Insurance Imperative:** Cyber insurance companies have taken decisive notice of the mobile threat. They are now extending their endpoint-control requirements to mobile devices, making demonstrable mobile security a future prerequisite for maintaining adequate coverage.

Mobile is no longer a secondary concern. It must become every enterprise's top security priority because it is already an attacker's primary target. Everyone's access is valuable, and every phone with corporate access is now a strategic target.

What Organizations Must Do

To close the Enterprise Blind Spot and protect against the current threat landscape, organizations must implement a strategic shift in their security posture. The new mandate requires five core actions:

1. **Acknowledge Mobile's Centrality:** Move beyond the "just another endpoint" mindset. Recognize that the mobile device is a primary authentication hub, communication center, and access point to corporate resources. This is a strategic shift, not merely a technical one.

2. **Close the Security Investment Gap:** Treat mobile security with the same rigor and dedicated funding as desktop security. Security professionals must have the visibility, detection, response capabilities, and resources necessary to protect company systems from a mobile-first attack landscape.

41 Cost of a Data Breach Report 2025, IBM.

3. **Move Beyond Device Management (MDM):** MDM enforces policy but offers no threat detection or response. Real mobile security is a requirement, not a feature. It must include behavioral analysis, active-threat detection, and incident-response capabilities to counter modern exploits.

4. **Integrate Mobile into Core Security Operations:** Mobile device health and threat telemetry must be seamlessly integrated into Security Operations Center (SOC) workflows, Conditional Access policies, and Zero Trust architectures. Mobile intelligence is now mission-critical intelligence.

5. **Protect the Entire Fleet:** Recognize that every employee is a target. Because the threat is what the device can access, not who carries it, all mobile devices with access to corporate resources must be protected.

CONCLUSION

Securing mobile devices is no longer optional for organizations. These devices are not merely secondary endpoints; they are one of the primary means by which business is conducted, and they function as the authentication hub and main conduit for corporate data. This centrality has made them the path of least resistance for attackers, allowing them to operate entirely outside of enterprise awareness.

An advanced compromise can leave a device enrolled in MDM, with applications functioning normally, and the user noticing no disruption. From the organization's perspective, no alarms are triggered, even as sensitive data is continuously accessed and abused. This is the mobile blind spot: the gap between where risk actually exists and where enterprises can see. As attackers increasingly target individuals rather than infrastructure, this gap becomes a strategic liability.

Enterprises can no longer afford to treat mobile security as a secondary concern or a solved problem. The threat landscape has shifted. Visibility must shift with it. The risk is too great not to.

ABOUT iVERIFY

iVerify Enterprise: Mobile EDR for Real Threats on Every Device.

iVerify is the pioneer in Mobile Endpoint Detection and Response (EDR), delivering advanced, comprehensive protection against the modern mobile threat landscape.

The iVerify Difference

Unlike legacy mobile security products—which are often limited to signature-based detection and lack response capabilities—iVerify provides a complete EDR solution:

- **Advanced Threat Detection:** We employ heuristic-based threat hunting, including the industry's most sophisticated Pegasus detection capability, to identify zero-day and end-day exploits, fileless malware, and infected devices.
- **Comprehensive Coverage:** Our security platform defends against mass threats like smishing, malicious apps, ransomware, and identity-centric attacks resulting from credential theft. This coverage is extended by our SmishGuard feature, which moves beyond static intelligence to a content, behavior, and intelligence-driven model capable of identifying both opportunistic and targeted smishing attacks. SmishGuard utilizes on-device inference and federated learning to analyze linguistic patterns and sender behaviors, ensuring strong privacy by avoiding centralized access to private user data.
- **Complete Enterprise Response:** iVerify is the only solution that detects threats and quickly responds to eliminate the impact of compromised BYOD and corporate-owned mobile devices, greatly reducing the likelihood of a corporate breach.

Protecting Your Enterprise

Used by leading banks and government institutions, iVerify's solutions secure the entire organization, spanning consumer, enterprise, and government sectors with privacy-focused BYOD and enterprise-grade security.

We also offer special protection for journalists and civil society at iverify.org.

Request a demo to experience our advanced features firsthand.