The Unpatchable Fleet

Why South Africa's mobile-first enterprise is dangerously exposed to the patch apocalypse, and what to do when patching is no longer the lever

Greg Strydom, CEO, Think Tank Software Solutions

The short version, for the board

The gap between a vulnerability being disclosed and being weaponised used to be measured in weeks. It is now measured in hours, and the people whose job is to track it say the old patching model is finished. That is the global story, and it is well evidenced.

The South African version is more specific and gets less attention. We are one of the most mobile-dependent economies on the continent, we bank through apps rather than cash or cards, and most of the devices doing that work are personal phones the organisation does not own and cannot see. Our corporate fleet is mostly Samsung, which is better supported than the budget Android that dominates the rest of Africa, so the local problem is rarely that a patch does not exist. The problem is that the patch never reaches the device, because nobody is managing it.

Once you accept that, the question changes. It stops being how fast you can patch and becomes what you do about the devices you cannot. The answer is to govern the endpoint itself: know what is connecting, block what is unsafe, separate company data from personal data, and quarantine anything you cannot fix. This paper sets out the case and ends with a short self-assessment, so you can place your own organisation on the curve before a regulator or an attacker does it for you.

1. The window closed

Patching used to run on a calendar. A flaw was disclosed, a fix shipped, and an administrator scheduled it for the next maintenance window. Thirty days was respectable and ninety was defensible, because the attacker worked at roughly the same speed as the defender. That balance has gone.

On 10 June 2026 the United States Cybersecurity and Infrastructure Security Agency issued Binding Operational Directive 26-04. It threw out calendar-based deadlines and replaced them with a four-factor risk test that scores a vulnerability on exposure, known exploitation, automation potential and impact. A flaw that scores on all four now has to be fixed in three days.

CISA was blunt about why: artificial intelligence has compressed the time between disclosure and exploitation to the point where a thirty-day service level agreement is a liability rather than a control. The directive only binds United States federal agencies, and it has no force in South Africa, but CISA went out of its way to tell everyone else to follow, and similar guidance has already appeared in the United Kingdom and India.

The research behind that decision is sobering. The Cloud Security Alliance has documented AI systems producing a working exploit for a freshly disclosed vulnerability in ten to fifteen minutes, for about a dollar a go. Mandiant's M-Trends 2026 report puts the average time-to-exploit for high-value targets at minus seven days, which is to say the attack is often under way before the vendor has finished writing the advisory. A record 48,185 vulnerabilities were catalogued in 2025, and that curve is bending upward in step with the AI tools that find them.

Verizon's 2026 Data Breach Investigations Report, built on more than 22,000 confirmed breaches, caught the moment the theory became the pattern. For the first time in the report's nineteen-year history, exploiting a vulnerability passed stealing a credential as the most common way in, at 31 percent of breaches. It happened while defenders were losing the race to fix. Only 26 percent of the flaws on the United States known-exploited list were fully remediated last year, down from 38 percent, and the median time to close one had stretched to 43 days. Attacks got faster and patching got slower in the same twelve months.

Read the directive as a signal rather than a rulebook. The most heavily resourced security apparatus in the world looked at the new speed of attack and concluded the old model cannot keep up. If that is true for a federal agency with a forensic triage team on standby, it is more true for a Cape Town logistics operator running four thousand handsets in the field with two people in IT. The patch apocalypse is not a forecast. It is here, and it is a problem of speed. In South Africa, as the rest of this paper argues, it is also a problem of physics.

2. South Africa runs on the phone

Most writing about endpoint security is really writing about laptops. The Western enterprise runs on managed Windows machines, refreshed every three years and patched on a schedule, and that is the fleet the global tools were built around. It is not how South Africa works.

Here the phone is not an accessory to the computer. For most people it is the computer, the bank branch and, increasingly, the till. South Africa also has one of the most banked populations on the continent, so unlike Kenya and much of the region, the money does not move through telco mobile-money wallets. It moves through the apps of the established banks, on personal smartphones, which is why South African fraud looks the way it does later in this paper.

The make-up of the fleet is its own story, and it is a more flattering one than the continental average suggests. Samsung holds just over half the South African market, more than every other brand combined, with Apple second at around one device in six and a real premium tier above it. The cheap Transsion handsets, Tecno and itel, that dominate Nigeria and Ghana barely register here, below two percent each. Most of the mass market sits on mid-range Samsung Galaxy A-series phones bought on instalment, and Samsung now supports those for

five to seven years. So at the median, the South African corporate device is reasonably well patched, and the naive version of this argument, that the whole fleet is rotting, simply does not hold.

The risk has not gone away, though. It has moved. In South Africa the danger is seldom that no patch exists. It is that the patch exists and never lands, on a device the organisation cannot see. It collects in four places. The first is the personal-device long tail, where staff run company email, WhatsApp and line-of-business apps on whatever phone they happen to own, governed by no one. The second is the large second-hand and refurbished market, where a handset is often halfway through its security life on the day it changes hands. The third is the older and grey-market tail that economic pressure keeps in service well past its support date, with unemployment near a third and replacement a luxury.

The fourth is particular to this country, and it is about the cost of data. The Competition Commission has repeatedly found the prepaid pricing structure to be anti-poor, with people who buy small bundles paying disproportionately more per gigabyte, and South Africa still sits 31st of 45 African countries for the price of a gigabyte. A Capitec poll of thousands of South Africans found 87 percent feel high data costs limit their access to work and education. Most people buy capped prepaid bundles that expire, so a several-hundred-megabyte security update is a real and visible expense. On a R150 ten-gigabyte bundle, a 500 MB update is roughly R7 of data that the user would rather spend on something else, so the prompt gets dismissed. The patch is available, the user declines it to protect their airtime, and the device stays exposed while nobody in the organisation is any the wiser.

That is the local shape of the problem. Not a fleet that cannot be patched, but one that is patchable in principle and unpatched in practice, scattered across devices the company neither owns nor watches. The rest of the continent makes it worse rather than better, which matters because South African firms operate across it. By usage, the Transsion brands make up about a quarter of the African market, and in Nigeria the two biggest, Tecno and Infinix, are close to half. These are devices built to a price, and software support is the first cost cut. Transsion's published policy gives its budget lines around two years of security patches, often with no operating system upgrade at all. A phone bought today across much of Africa can be out of support inside two years while staying in daily business use for five. Anyone running a regional fleet inherits both problems at once.

> **Sidebar: the device is the battlefield, even when the bank app is sound**
>
> The stakes are concrete. The South African Banking Risk Information Centre recorded an 86 percent rise in digital banking fraud in 2024 and a 74 percent jump in losses, to R1.888 billion, with digital banking now the dominant channel at 65.3 percent of reported incidents. The detail that matters most is that SABRIC attributes the bulk of this to social engineering rather than any technical breach of the banks' apps. Phishing, vishing, SIM-swap, fake apps and smishing do the work.
>
> That is exactly why the endpoint is where the fight is lost. The unmanaged phone is where a fake banking app gets sideloaded, where a smishing link is tapped, where a one-time PIN is read off the screen, and where an out-of-date operating system lets overlay malware sit on top of the real app. One South African investor lost more than R6 million to a fake app posing as a JSE trading platform. SIM-swap is a named SABRIC method, with average losses around R10,000 and individual cases running into hundreds

> of thousands of rand within hours. Managed devices give a bank levers the unmanaged ones do not: SIM-replacement and smishing controls that flag or block the attack, and conditional access that keeps a compromised handset away from the banking app in the first place. None of this stops a customer being talked out of an OTP, but it shrinks the device-side surface that turns a clever message into an empty account. For a board operating under the FSCA and Prudential Authority Joint Standard, that surface is now a governance question, not an IT footnote.

3. Patching is not the lever

The instinct after reading Section 1 is to patch faster. Buy a quicker tool, build a tighter pipeline, shorten the approval queue. For a fleet of company laptops that is the right instinct. For South Africa's mobile reality it answers the wrong question.

You cannot patch what the manufacturer no longer patches, and you cannot patch a phone you cannot see. The first case bites hardest across the rest of Africa, where the vendor has simply stopped shipping updates. The second is the South African case, where the update exists but never reaches a personal device sitting outside any management. A flawless patch operation, fully staffed and automated, deploys nothing to a handset it has no visibility of and no authority over.

Verizon's breach data shows where the exposed credentials actually sit. In its 2025 report, of the devices found holding corporate logins in infostealer logs, 46 percent were unmanaged against 30 percent that were managed. Close to half the leaked corporate credentials in the set came off devices the organisation did not control. That is the visibility gap stated as a number, and no patch reaches into it.

So the useful question is not how quickly we patch. It is what we do about the devices we cannot. That is a different discipline, and it rests on four things. Visibility, because you cannot govern what you cannot see, and for most organisations the personal phone holding customer data is completely dark. Conditional access, so that a device on an unsupported operating system, or missing critical patches, or rooted, does not reach the mail server or the banking app. Containerisation, which keeps company data in a space you control on a device you do not own, so you can wipe the work container and leave the family photos. And quarantine, the ability to spot a non-compliant device and wall it off automatically, across a real fleet, without a person ruling on each case. This is what the industry calls zero trust: access turns on the device's current state, not on who owns it or where it sits on the network.

None of that is patching. All of it is management. The shift this paper asks for is from a patching mindset, which assumes the hole can always be closed, to a containment mindset, which assumes it sometimes cannot and plans for that. The unpatchable phone is not a problem you solve once. It is a risk you contain continuously, and containment is a capability an organisation either has or does not.

4. The governance gap

There is a second reason this belongs in the boardroom rather than the server room. The law has already moved, and it does not wait for a breach to create liability.

The Protection of Personal Information Act requires every responsible party to take appropriate and reasonable technical measures to protect personal information against loss and unauthorised access. A phone holding customer records falls squarely inside that duty. POPIA does not ask whether you were breached. It asks whether your safeguards were reasonable, and a fleet of unmanaged, unpatched, unencrypted personal devices carrying customer data is hard to defend as reasonable on any ordinary Tuesday, breach or no breach. The penalties are not trivial, running up to R10 million or, on the relevant test, ten percent of turnover, alongside civil claims and, in the worst cases, criminal exposure for responsible parties. The first major fine has already been issued, R5 million against the Department of Justice. Breach notifications to the Information Regulator have climbed sharply, and since April 2025 they must be filed through the Regulator's online portal, which has firmed up both the reporting and the scrutiny that follows.

For financial institutions the bar is higher again. The FSCA and Prudential Authority Joint Standard 2 of 2024 on Cybersecurity and Cyber Resilience took effect on 1 June 2025. It is principle-based, it puts ultimate accountability on the governing body, and it makes third-party and vendor risk an explicit board responsibility. It reaches banks, insurers, market infrastructures and pension funds. For any of them an ungoverned mobile fleet is no longer just a POPIA exposure. It is a Joint Standard exposure, and the Joint Standard reports to the board, not the help desk.

The gap, then, sits between what the law now assumes you can demonstrate and what an ungoverned fleet can actually show. Demonstrability is the word that matters. Both POPIA and the Joint Standard increasingly reward the organisation that can produce evidence of its controls, and an endpoint management console is precisely an evidence machine: which devices exist, what patch level each is on, which are compliant, which were denied access and when, all logged. This is not a theoretical mapping. Endpoint vendors already align their controls to national cybersecurity frameworks line by line, and the same exercise maps cleanly onto POPIA and the Joint Standard. Newer platforms push it further, with continuous-compliance features that catch a device the moment it drifts out of policy and remediate it out of band rather than waiting for the next scheduled scan. The organisation that cannot produce that evidence is not only less secure. It is less defensible.

5. The category, on its merits

When patching stops being the lever, management becomes it, and the category that does this work has a name and a current scorecard. Both are worth knowing before any conversation about products.

Gartner published its first Magic Quadrant for Endpoint Management Tools on 5 January 2026, evaluating sixteen vendors. Omnissa, the former VMware end-user computing business that became independent in 2024 and was widely written off as a Broadcom casualty, came through

as a Leader and scored highest across all four use cases in the companion capabilities report, including a near-perfect mark for autonomous endpoint management. Workspace ONE, in other words, is not the orphan some people still assume. Tanium and Adaptiva also landed as Leaders. Microsoft sits at the front for any organisation already living inside its stack, because Intune is part of the Microsoft 365 estate they already pay for. Jamf remains the specialist for Apple-only environments. Ivanti, ManageEngine, IBM and others hold the multi-platform and mid-market ground.

A word on Intune, because it is where most South African boardroom conversations begin. The common assumption is that a Microsoft 365 subscription already covers the endpoint, and for a Windows-and-identity estate that is often a fair reading. Intune is a capable tool and it is the natural fit when the fleet is managed laptops tied to corporate identity. Its design centre is Windows, though. Support for deep Android Enterprise management, for rugged hardware, and for the budget-device and personal-device long tail is thinner, and those are exactly the parts of the fleet that define the South African problem. The point is not that Intune is weak. It is that "we have Intune" answers a narrower question than most people think, and the gap between the two is shaped like the African enterprise. Knowing where that line falls is the first real test of competence in this market.

The scorecard itself carries a quieter caveat. It is weighted for a fleet you may not have, because it rewards deep Windows laptop control, which is what the Western enterprise runs. The vendor that wins a Windows-weighted ranking is not automatically the right answer to an Android-first, BYOD-heavy, abandoned-hardware question. Buy against your own reality. In practice that reality reduces to four capabilities once patching has failed: genuine Android Enterprise depth, so you can govern a personal phone you do not own; containerisation and mobile application management, which is the practical line between a POPIA incident and a non-event; conditional access, which is the control you keep when the patch you need does not exist; and automated quarantine, so an unpatchable device is seen and isolated at scale without a person adjudicating each one. Score any vendor against those four, in your own environment, and most of the marketing falls away.

> **Sidebar: the endpoint that is not a phone or a laptop**
>
> Two of the verticals that matter most here, logistics and retail, do not run on phones or laptops at all. They run on rugged scanners, handhelds, point-of-sale terminals and kiosks, and a warehouse scanner should not be managed like a laptop. These devices also sit closer to revenue than a laptop does, so when a scanner fleet drops offline or falls out of compliance, the first thing anyone notices is stalled operations and lost productivity, not a security alert. The security event comes later. The hyperscaler tools are weakest exactly here, which is where the specialists earn their place. Ivanti's lineage is a useful example: its cloud product descends from MobileIron, its on-premise sibling EPMM from MobileIron Core, and its Wavelink and Velocity heritage runs deep in rugged and supply-chain devices, with native support for Android Enterprise and the major rugged manufacturers. For an operator managing thousands of rugged endpoints across a distributed estate, breadth across traditional, rugged and smart devices from one console is the difference between a single platform and a swivel chair between four. The principle holds regardless of vendor: rugged is a real category with real specialists, and a serious endpoint strategy has to account for it.

The honest conclusion is that there is no single correct product, and anyone who opens with one is selling. The right answer governs the device you actually hold, enforces a policy you can actually defend, and isolates the device you cannot fix. Several vendors can clear that bar, Ivanti among them, depending on the estate. The bar is the point.

6. The autonomous turn

If the window has closed and people are too slow, the obvious move is to take the person out of the loop, and the industry has a name for that too. Autonomous endpoint management describes a progression. Reactive is an administrator noticing a problem and fixing it. Proactive is the platform spotting it and raising an alert. Autonomous is the platform detecting, deciding and remediating with nobody waiting in the middle. Gartner expects more than half of organisations to fold in autonomous endpoint management by 2029, up from almost none in 2024, and every serious vendor now claims some version of it.

The logic is sound, because when exploitation arrives in hours a human approval queue is itself the weak point. Take the person out of routine patch decisions, let risk-based rules push the critical fixes immediately, and route the rest through staged workflows. The continuous-compliance features now shipping do exactly this, catching a device that misses its maintenance window and remediating out of band. For a laptop estate, that is real progress.

On the South African fleet, the job quietly changes. Autonomy cannot save a phone the manufacturer has abandoned, because there is no patch to apply, and it cannot patch a personal device the company has chosen not to manage. What it can do is the containment work from Section 3, at machine speed. The valuable autonomous action here is not "deploy the update" but "find the device that cannot be updated, judge it non-compliant, and isolate it from the data without waiting for a person". That is a sharper and more defensible claim than the glossy version of the pitch, and it is the one that fits the country.

A note of caution so we do not oversell it. Autonomous is the most inflated word in the category. The sober reading, which buyers reach on their own, is that these systems do not automate the decision so much as the execution of decisions a person is still accountable for. Security keeps a human in the chair because only a human can be held responsible by a regulator, a board or a court. Be wary of any vendor offering to remove the human from accountability rather than from the routine. The aim is to automate the work, not to launder the responsibility.

7. Sovereignty, and the on-premise option

There is one more turn, and it is the one most often skipped in the rush to autonomy. A modern endpoint platform is a control plane with total authority over every enrolled device. It can wipe a phone, lock it, locate it, install software on it, read its certificates and report its state. Hand that plane an autonomous mandate, as Section 6 describes, and you have delegated standing command over the whole fleet to a system that can act without a human veto. The question nobody asks in the procurement meeting is where that control plane lives, and under whose law.

For a cloud-hosted platform run by a foreign provider, the answer is uncomfortable, and it is not just about where the data physically sits. The United States CLOUD Act lets American authorities compel a US-based provider to hand over data wherever in the world it is stored, so a German data centre operated by a US company does not, on its own, put the data beyond American reach. Residency is not the same as sovereignty. What decides sovereignty is the jurisdiction and ownership of whoever operates the platform. The vendors have started to concede the point in their own product lines. In April 2026 Ivanti launched a Sovereign Edition of its MDM cloud for the European Union, run not by Ivanti but by an independent European operator, sector27, on a certified data centre in Germany, sold explicitly on jurisdiction, auditability and resilience. Europe was offered a sovereign option. South Africa, so far, has not been.

That does not leave the local board without a lever, and this is the practical part. The same technology has an on-premise deployment that the EU cloud edition does not require you to wait for. Ivanti's EPMM, the on-premise descendant of MobileIron Core, runs on hardened appliances inside your own data centre, under your own jurisdiction, with no foreign control plane in the path. For an organisation that takes the sovereignty exposure seriously, an on-premise deployment is the option available in South Africa today, and it is worth weighing against the convenience of a foreign-operated cloud. The point is not that the cloud is wrong. It is that the choice has a sovereignty dimension that belongs on the evaluation sheet next to Android depth and quarantine. Ask where the control plane sits. Ask whose law governs the operator. Ask what happens to your fleet if that jurisdiction and ours fall out. The absence of a local sovereign cloud is a gap, but on-premise control is a real answer to it, and asking the question early is cheaper than asking it after the fact.

8. Where do you sit? A board self-assessment

This paper has argued that South Africa faces a patch problem it cannot patch its way out of, under laws that assume controls most organisations cannot yet demonstrate, answered by a category of management most have not properly adopted, and shadowed by a sovereignty question almost nobody asks. The next step is not to buy anything. It is to find out where you actually stand.

Score your organisation on each of the five pillars below, from 1 to 5, and be the pessimist in the room. The value is in the gaps it exposes, not the comfort it offers.

Visibility. A 1 means you have no idea how many devices touch your data or what state they are in. A 3 means you can see company-owned devices but personal ones are dark. A 5 means real-time inventory and compliance state across every device that reaches corporate data, owned or personal.

Patch and support posture. A 1 means you do not know which of your devices still receive security updates. A 3 means you track it for laptops but not for the mobile fleet. A 5 means you know the support status of every device class and have a defined response for those that have fallen out of support.

Conditional access and containment. A 1 means any device reaches your data regardless of its state. A 3 means you have some access rules but cannot reliably enforce or quarantine. A 5 means out-of-date, rooted or non-compliant devices are denied access and isolated automatically.

Demonstrability. A 1 means that if the Information Regulator or a Joint Standard auditor asked you to prove your endpoint safeguards tomorrow, you could not. A 3 means you could assemble the evidence with effort and delay. A 5 means your controls, access decisions and compliance state are logged and auditable on demand.

Sovereignty awareness. A 1 means you have never asked where your endpoint control plane lives or under whose law. A 3 means you know but have not assessed the exposure. A 5 means you have weighed jurisdiction and foreign-access risk as a documented procurement decision.

Add the five. Twenty to twenty-five and you are ahead of almost every peer in the country, and this paper is a confirmation rather than a warning. Twelve to nineteen and you have a real but bounded programme of work, and you roughly know where it sits. Below twelve and the fleet that runs your business is, in governance terms, running without you, and the distance between your exposure and your evidence is the first thing a regulator, an auditor or an attacker will find.

The patch apocalypse is a global event. The unpatchable fleet is a South African condition. The first cannot be stopped. The second can be governed, but only by an organisation honest enough to score itself a two before circumstances score it a one.

Sources and notes

This paper draws on public sources current to June 2026. Key references, by publisher, for verification and linking:

- CISA, Binding Operational Directive 26-04, "Prioritizing Security Updates Based on Risk", 10 June 2026.
- Cloud Security Alliance, "The Collapsing Exploit Window", April 2026, on AI-speed exploitation and the ten-to-fifteen-minute exploit figure; Mandiant M-Trends 2026 on time-to-exploit; published 2025 CVE totals.
- Verizon Business, Data Breach Investigations Report, 2026 edition on vulnerability exploitation overtaking credential abuse as the leading initial access vector and on remediation shortfalls against the CISA known-exploited list; 2025 edition on the share of corporate credentials found on unmanaged versus managed devices.
- SABRIC, Annual Crime Statistics 2024, on digital banking fraud volumes, losses, channel share, SIM-swap and social engineering.
- Statcounter and Intelpoint on South African and African vendor market share; market reporting on Galaxy A-series financing and the South African premium and second-hand segments; Transsion and Tecno published software-update policy.
- South Africa Competition Commission, second Cost of Living Report (1 April 2026), on mobile data pricing; Capitec Connect consumer polling on data affordability.

- Protection of Personal Information Act, sections 19, 22 and 72, and Information Regulator enforcement and breach-reporting practice; FSCA and Prudential Authority Joint Standard 2 of 2024 on Cybersecurity and Cyber Resilience (effective 1 June 2025).
- Gartner, Magic Quadrant for Endpoint Management Tools, 5 January 2026, and the companion Critical Capabilities report; vendor statements from Omnissa and others on their positions.
- Ivanti materials on Neurons for MDM, the EU Sovereign Edition (April 2026) and EPMM on-premise deployment; commentary on the US CLOUD Act and data sovereignty.
- G. Strydom, The Token Reckoning, 2026, on token cost governance and AI sovereignty risk.

Figures are quoted as reported by their publishers, and the more conservative figure has been used where sources differ.

Greg Strydom is CEO of Think Tank Software Solutions, a South African technology advisory and enterprise software firm and Ivanti Premier Partner serving the South African and broader African market across banking, telecommunications, retail, logistics and insurance. *This paper is a board-level briefing and does not constitute legal advice. Organisations should confirm their obligations under POPIA and applicable financial-sector standards with their own advisers.*

Internal version 1.2 | 1 July 2026