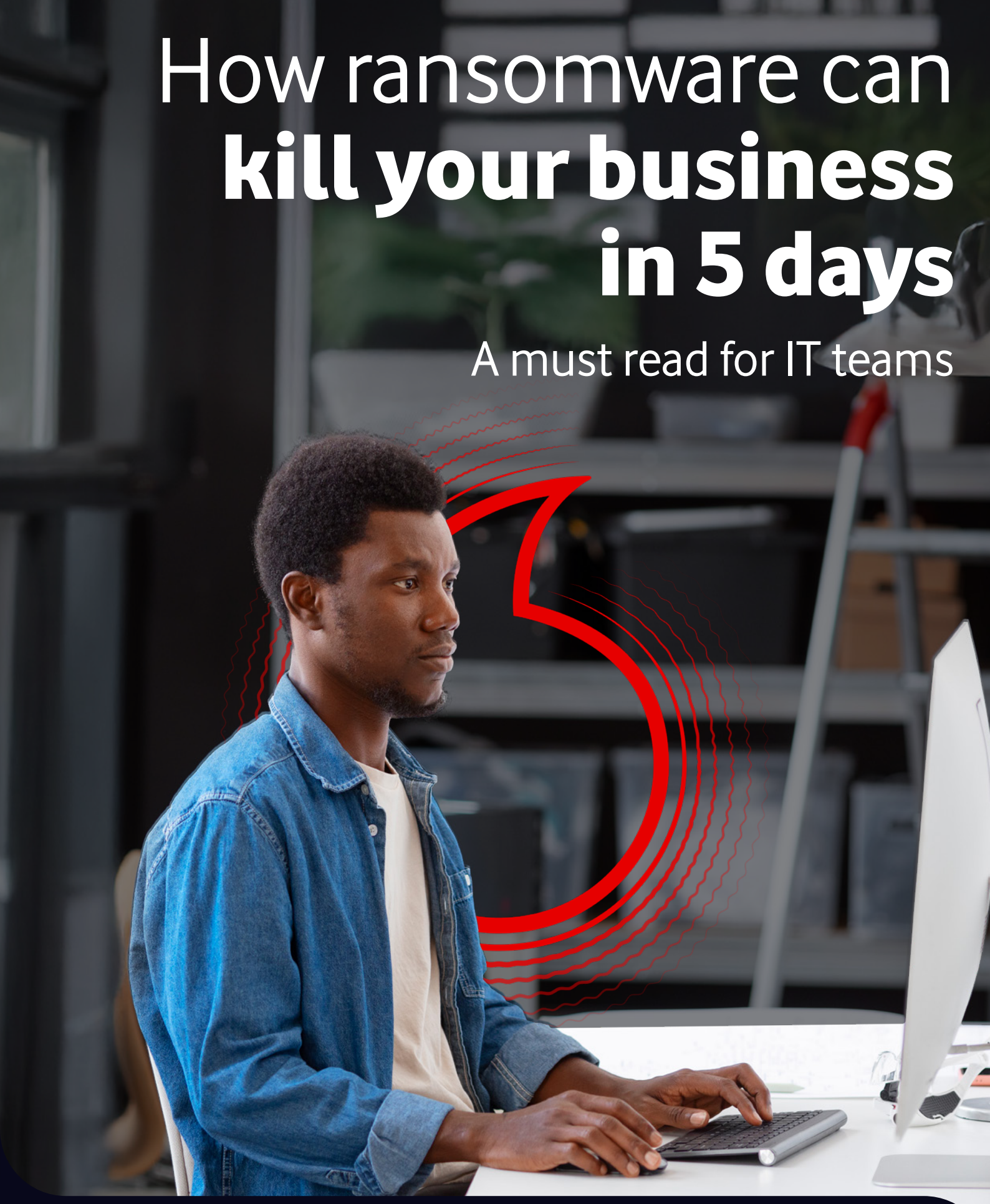
How ransomware can **kill your business in 5 days**

A must read for IT teams



Microsoft | vodacom business

Ransomware **doesn't** discriminate

Ransomware isn't just targeting big businesses anymore. Small and mid-sized companies are now the preferred victims — **because attackers know your defences are thinner and your teams are stretched.**

They also know that once your data is locked, **you'll be desperate to get it back.**

In South Africa, the average cost of a data breach has hit R53 million. For most SMEs, that's not just a financial hit — it's a business-ending event. **And it doesn't take weeks to reach that point. It takes days.**

This **guide** walks you through what those five days look like — **and how to make sure you don't go through them.**

The 5-day disaster: What ransomware really looks like

Day 1: Infection

It starts quietly — **a click on a fake invoice, a compromised login, maybe just a missed patch on an old system.** You won't know it happened. Nothing crashes. Nothing breaks. But in the background, the malware is already scanning your network, mapping your drives, quietly infecting every system it can reach.

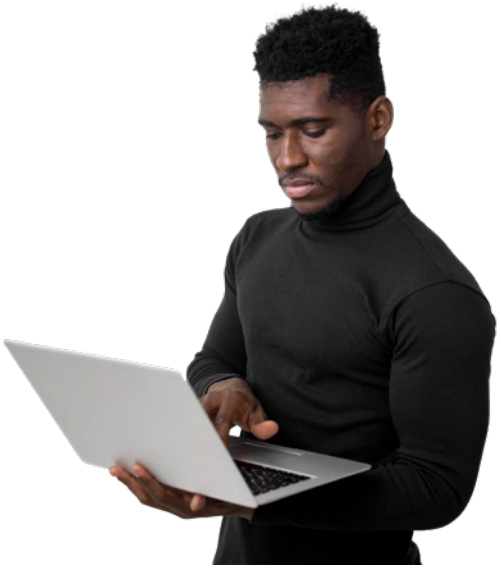
It even starts corrupting your backups — the same ones you were relying on for recovery. And because everything still seems fine, no one raises a flag.

Day 2: Lock-out

Overnight, everything changes. You arrive at work and suddenly no one can access their files. Email is offline. Your finance system's dead. Support tickets can't be pulled up. A ransom note appears:

"Your files have been encrypted. To restore access, send $100,000 in Bitcoin to the wallet below."

Your business has just been taken hostage — and every hour you spend offline is costing you money, clients, and credibility.

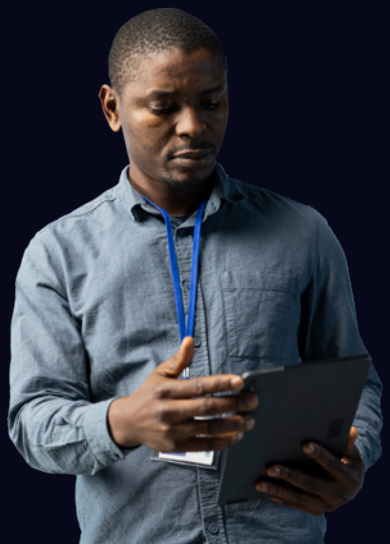


Day 3: Chaos

Now the scramble begins. Your IT team is trying to assess the impact, but the attackers have done the damage — **and worse, your backups aren't clean. They've been compromised too. You're stuck.**

Then leadership starts asking uncomfortable questions: Should we consider paying? Is that even legal? How did this happen?

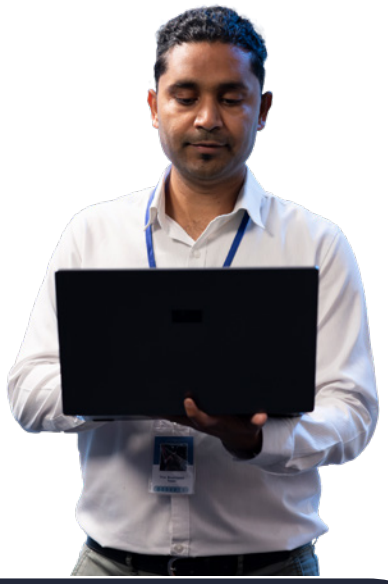
Meanwhile, clients are waiting on deliverables. Staff are stuck without access to critical systems. People start to panic — not just about the systems, but about their jobs.



Day 4: Escalation

The ransom note changes tone. Now they're not just threatening to keep your data — **they're threatening to publish it.** Client data. Financials. Internal HR files. Your business is looking at potential POPIA violations, and the legal team is suddenly front and centre in every meeting.

The board wants answers. Your clients want reassurance. And your team is exhausted, trying to contain something that's already gone too far.

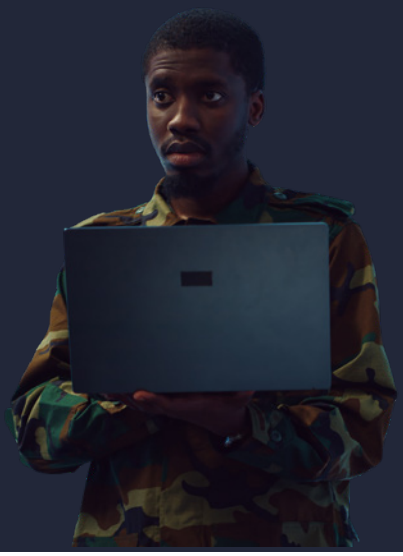


Day 5: Fallout

Even if you manage to get systems back online, the damage is done. You've lost revenue. You've lost trust. You've racked up recovery costs — from forensic experts to legal advisors — **and you still don't know exactly how much data was taken, or how far it spread.**

Some clients may never return. Your leadership team is shaken. And as the weeks go by, the costs just keep coming.

Could your business survive this long without access to its systems, data, or clients?



South African examples

If you think ransomware only targets the big guys — think again. **These mid-sized South African businesses were hit hard:**

Lombard Insurance

In 2020, Lombard Insurance experienced a ransomware-esque cyberattack that disrupted its systems and forced emergency recovery.

"Lombard Insurance Company Limited regrets to confirm that it has been the victim of a cyber attack on some of its systems by criminals targeting its data."
-ITWeb

Tracker South Africa

In 2020, Tracker was hit by ransomware that encrypted customer-facing systems, cutting off access to essential services.

"Tracker has been targeted by a cybercrime attack in the form of ransomware that encrypted information on some systems, disrupting customer access to its services."
-Tracker

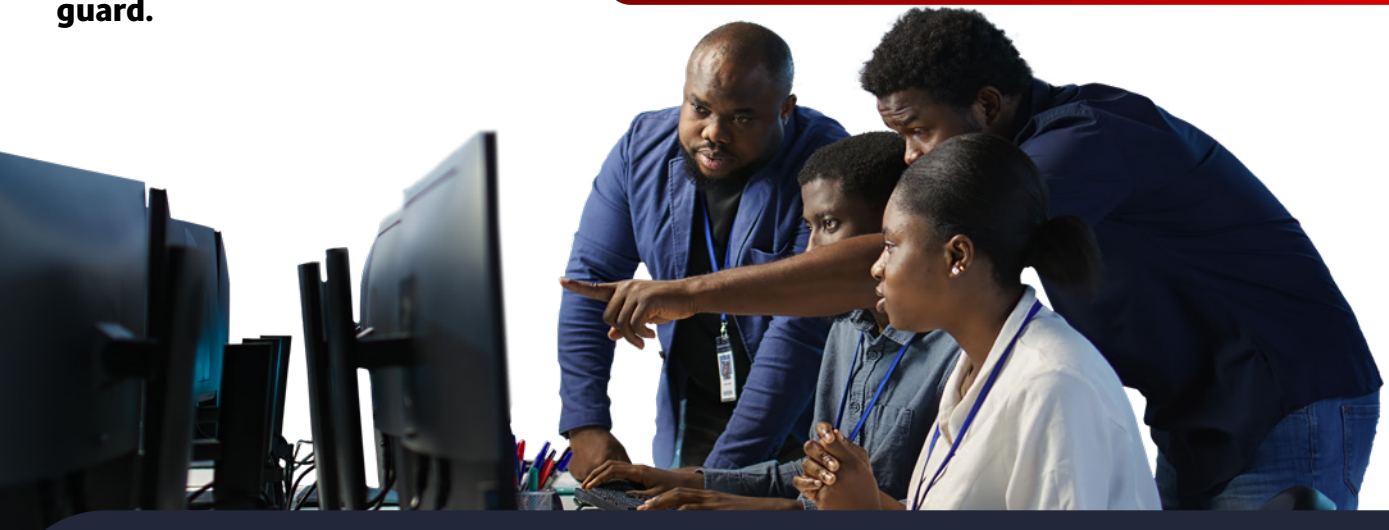
Debt-IN Consultants

In 2021, Debt-IN Consultants suffered a ransomware breach that led to personal records being leaked online.

"It is suspected that consumer and personal information of more than 1.4 million South Africans was illegally accessed from Debt-IN servers in April this year, but this breach only came to light last week with the discovery that confidential consumer data and voice recordings of calls between Debt-IN debt recovery agents and financial services customers had been posted on hidden internet sites that are only accessible by a specialised web browser."
-Debt-IN

These incidents show how even established mid-sized businesses can find themselves caught off guard.

So, it's worth asking: **if they struggled, how would your business cope?**



How to survive (and recover)

If the five-day timeline worried you, good — **it means you know preparation matters.**
And you don't need a massive budget to do it. Just the right tools in the right places — **many of which you might already have.**

Here's how to build your defence, layer by layer.

Stop the attack before it starts

Most ransomware slips in through a single weak point — **usually a user clicking on something they shouldn't, or an attacker logging in with stolen credentials.** That's where the first line of defence comes in.

Microsoft Defender for Office 365 and Endpoint helps you catch malicious links, files, and attachments before they ever reach your users. And when someone tries to log in with a stolen password, Entra ID's Conditional Access and Multi-Factor Authentication steps in — **blocking access unless the identity checks out.**

With these in place, you're not just hoping users don't make a mistake — **you're giving them a safety net.**

Limit the damage if they get in

Even with good defences, you should still be extra cautious. The next step is making sure that if something does get through, **it can't spread freely.**

Microsoft Intune gives your team the power to instantly lock or wipe any compromised device — **even if it's not in the office.** And with Privileged Identity Management, sensitive systems are protected by default: no one gets access unless they absolutely need it, and even then, only for as long as they need it.

It's not about trusting your users less — **it's about giving attackers less to work with.**

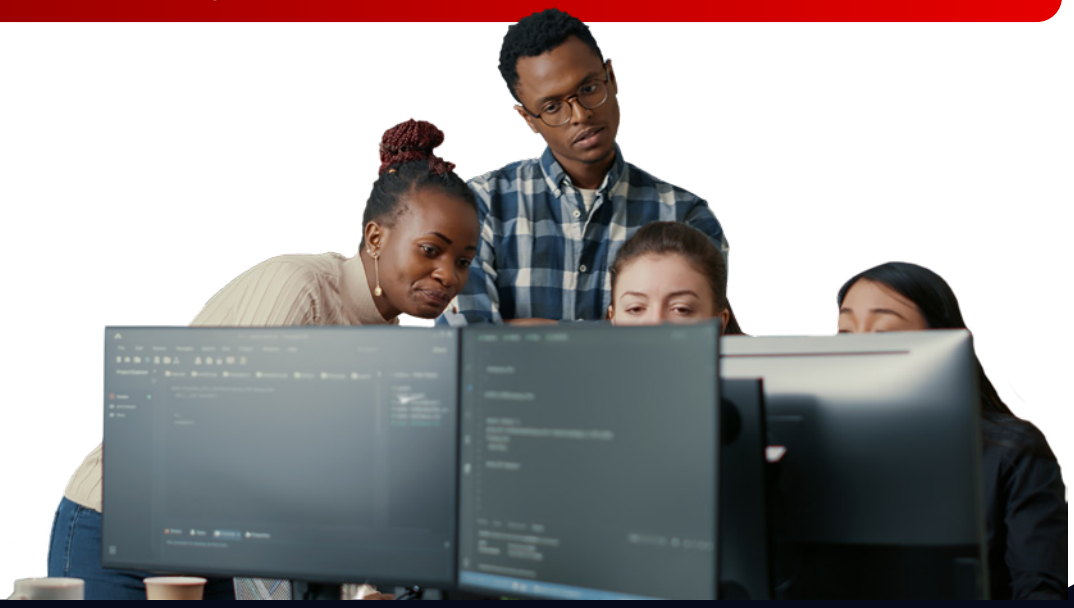
Recover fast — without paying the ransom

Let's say the worst happens. Files are locked, operations are down. **This is where recovery speed makes all the difference.**

Azure Backup and Site Recovery let you restore clean, pre-attack versions of your systems — **so you can skip the corrupted files entirely and get back online faster.** And for everyday files, OneDrive and SharePoint's versioning features give you a fast way to roll back to safety, without needing to start from scratch.

With the right layers in place, ransomware becomes something you're ready for — not something you're scrambling to survive.

And you don't need to purchase all these solutions to start. If you're running on Microsoft, it's likely that you already have access to some of these tools. So instead of getting overwhelmed by new products, start with what you own — and build a solid defence from there.



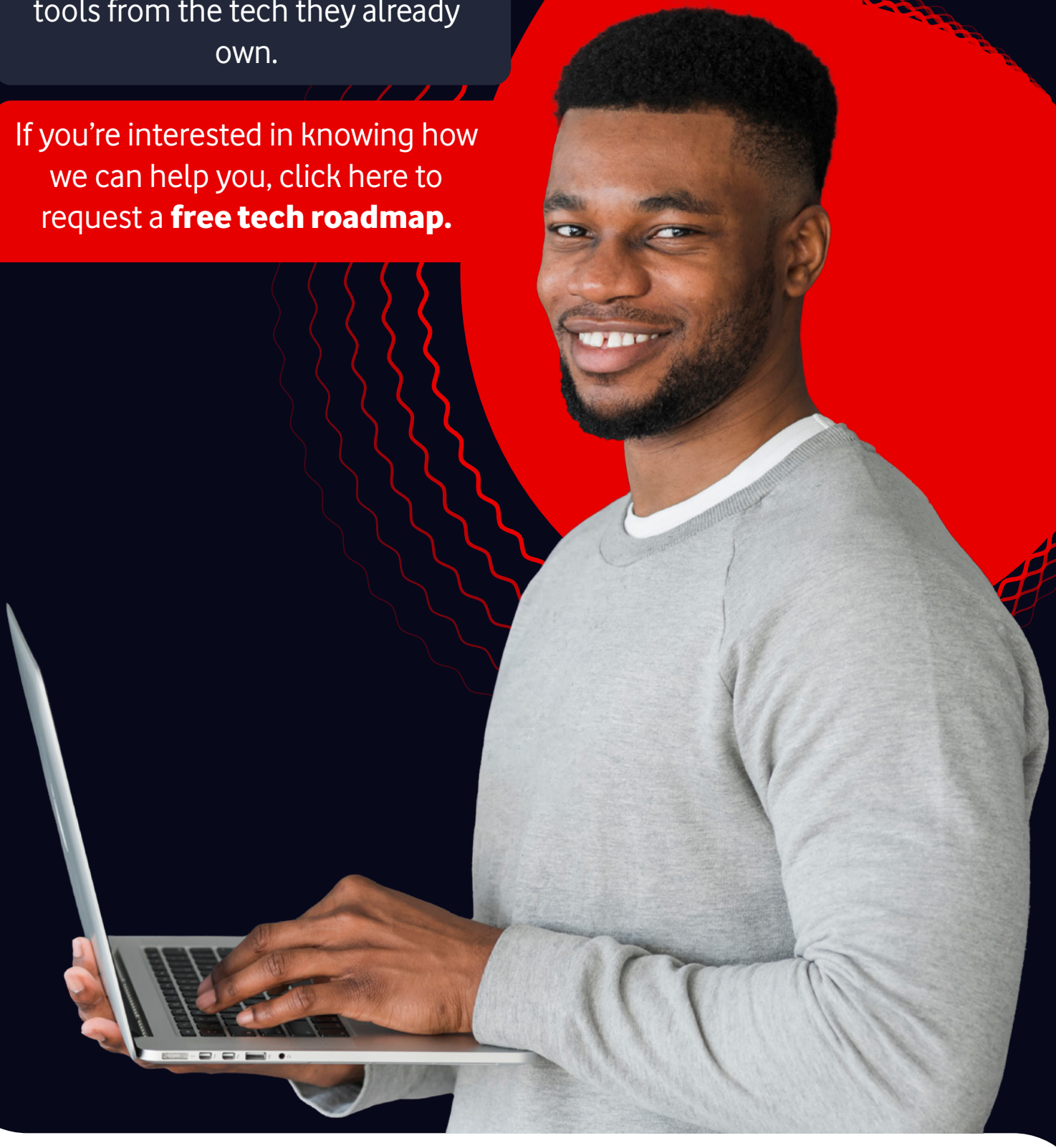
Don't wait for the ransom note

Once the lock screen appears, your options shrink fast. That's why the smartest move is to prepare before anything happens — when your systems are still clean, your team is in control, and the choices are yours to make.

Microsoft's security stack gives IT teams everything they need to stop ransomware before it spreads — and bounce back fast if it does. But getting those tools set up the right way, at the right cost, takes more than just a product list.

That's where **Vodacom Business** and **Microsoft** come in. We're working together to help growing business access more powerful tools from the tech they already own.

If you're interested in knowing how we can help you, click here to request a **free tech roadmap.**



Microsoft | vodacom business