INSODUS TECHNOLOGIES

Cyber Security Report

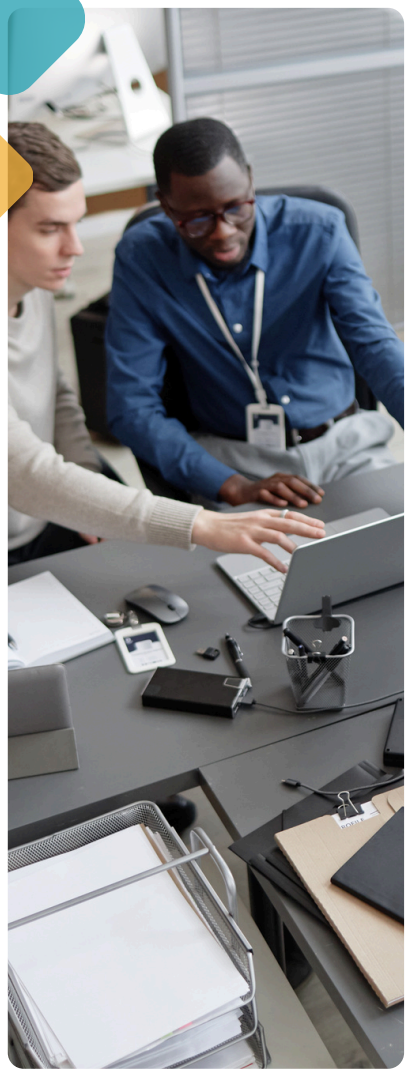
5 Hidden Gaps That Leave 'Secure' Businesses Vulnerable

insodus.tech
info@insodus.tech
+372 64 31310

Cyber Security Report

5 Hidden Gaps That Leave 'Secure' Businesses Vulnerable

Cybersecurity is no longer about protecting a perimeter. It's about understanding your environment well enough to detect and respond to threats before they turn into incidents.



Why This Guide Exists

Many businesses think they're secure because they've "ticked the boxes". They have a firewall. There's antivirus software installed. Maybe there's a password policy and a monthly phishing simulation. But even with all that in place, breaches still happen, often quietly, sometimes devastatingly. The reality is that cybersecurity isn't a checklist. It's a constantly shifting, layered system that requires more than just tools. It demands insight, alignment, and ongoing scrutiny.

This guide was developed to help organisations spot where their security posture may be giving them a false sense of protection. We explore five often-overlooked areas that leave even well-intentioned IT teams exposed. Alongside each risk area, you'll find examples, questions to assess your own situation, and a simple risk impact calculator to help prioritise your next steps.

Cybersecurity is no longer about protecting a perimeter. It's about understanding your environment well enough to detect and respond to threats before they turn into incidents.

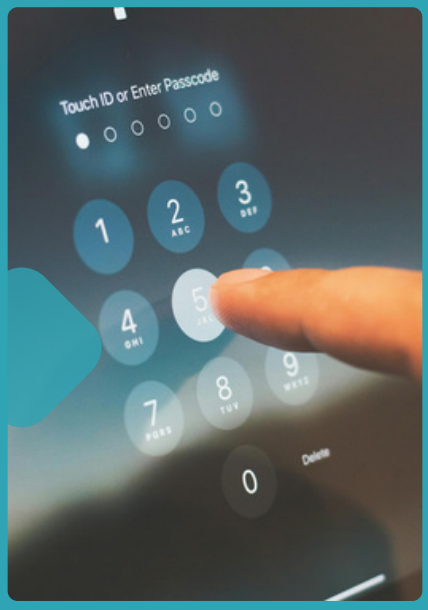
HIDDEN GAP 1: BEHAVIOURAL BLIND SPOTS

What It Is:
Many organisations focus their security efforts on infrastructure such as firewalls, endpoint protection, and email filtering, but neglect user behaviour monitoring. Insider threats, accidental missteps, and subtle deviations in access patterns often go unnoticed until it's too late.

Why It Matters:
Without behavioural analytics, it’s nearly impossible to detect slow-moving or stealthy threats. A compromised employee account may operate normally 95% of the time, but that 5% could be leaking data, probing sensitive areas, or bypassing controls.

Assessment Prompts:

- Do you have systems in place that monitor for unusual user behaviour?
- Are employees’ access logs periodically reviewed for anomalies?
- Have you experienced any insider-related incidents in the past 24 months?



Risk Calculator

If employees have access to multiple unrelated systems or sensitive data without role-based restrictions, and there is no behavioural monitoring in place, the risk of internal misuse or account compromise is high. This is especially concerning in remote or hybrid work environments where oversight is limited.

If access is assigned strictly based on role, reviewed regularly, and supported by user behaviour monitoring (e.g., alerts for unusual login times or data downloads), the risk is significantly reduced. These controls make it easier to detect anomalies before they escalate into incidents.

HIDDEN GAP 2: FRAGMENTED RESPONSE PLANS

What It Is:
It's one thing to have a document labelled "Incident Response Plan". It's another thing entirely for that plan to be usable, current, and embedded into operations. Many organisations either have outdated playbooks or rely on generic templates that aren't fit for purpose.

Why It Matters:
During a breach, the clock starts immediately. If your team isn't clear on who does what, how decisions get made, and who gets notified, every minute costs more. Even minor breaches can spiral into public-facing crises when a response is slow or inconsistent.

Assessment Prompts:

- When was the last time your incident response plan was updated?
- Have you ever run a tabletop exercise or simulation to test it?
- Do key staff know their roles in the event of a breach?

Risk Calculator

If your incident response plan has never been tested in a live or simulated setting, and there is no clearly defined communication protocol, your organisation is likely to struggle in a real breach scenario. This results in longer containment times, delayed responses, and more reputational damage.

If your team has regularly practised simulations, documented lessons learned, and clearly defined roles during incidents, you are much better positioned to respond effectively. Clear communication plans and decision frameworks reduce chaos, preserve trust, and minimise damage.

HIDDEN GAP 3: OVER-RELIANCE ON ENDPOINT TOOLS

Risk Calculator

If your organisation relies solely on endpoint detection tools without supplementing them with broader monitoring solutions like DNS traffic analysis, SIEM, or threat hunting capabilities, you may miss stealthy attacks that bypass EDR coverage. This reliance creates blind spots where attackers can operate undetected.

If your EDR tools are part of a layered strategy that includes network visibility, active threat hunting, and centralised event management, the risk of prolonged undetected breaches drops substantially. These combined capabilities increase detection speed, improve incident response, and enhance overall resilience.

What It Is:
Endpoint Detection and Response (EDR) tools are powerful, but they are not a silver bullet. Many teams mistakenly assume that deploying an EDR system absolves them of the need for broader network monitoring, human review, or layered defences.

Why It Matters:
Threat actors know how to evade endpoint protections. Without complementary measures like DNS monitoring, honeypots, or SIEM (Security Information and Event Management) tools, a determined attacker can still operate undetected.

Assessment Prompts:

- Do you have monitoring systems that go beyond endpoint logs?
- Is your EDR solution integrated into a broader detection strategy?
- Do you regularly review EDR performance and coverage gaps?

HIDDEN GAP 4: SHADOW IT AND ROGUE ACCESS

What It Is:
Shadow IT refers to systems or applications used by employees without formal approval. It also includes legacy accounts, unmanaged devices, and forgotten admin privileges, all of which represent unmonitored entry points.

Why It Matters:
These rogue systems often bypass security protocols and never receive updates or patching. They're invisible to traditional controls, which makes them a dream target for attackers looking for the path of least resistance.

Assessment Prompts:

- Have you conducted an audit of all cloud services and software in use?
- Is there a process for reviewing user permissions regularly?
- Are unmanaged or BYO devices covered under your security policy?

Risk Calculator

If your organisation has not conducted a recent audit of cloud-based services, user accounts, and connected devices, you are likely operating with unknown vulnerabilities. Legacy accounts with elevated privileges, orphaned admin credentials, or unsanctioned apps all represent entry points that attackers can exploit without detection.

If you perform regular audits of all digital access points, enforce centralised control of devices, and remove unnecessary privileges or accounts promptly, you reduce the risk of unauthorised access significantly. Strong governance over these endpoints is key to maintaining visibility and control.

HIDDEN GAP 5: ASSUMED COMPLIANCE = ACTUAL SECURITY

What It Is:
Many businesses operate under the assumption that passing a compliance audit means they are secure. While frameworks like ISO 27001, NIST, or GDPR offer valuable guidelines, they're often the baseline, not the ceiling.

Why It Matters:
Compliance can sometimes create a checkbox mentality that overlooks actual threats. You might pass the audit while still having gaping vulnerabilities because real-world attackers don't care about your certification.

Assessment Prompts:

- Is your security strategy designed to protect your business, or just to pass audits?
- Are your controls reviewed in light of new threat intelligence?
- Do teams understand the difference between compliance and resilience?

Risk Calculator

If your organisation prioritises passing audits over addressing real-world threats, and your security posture is not regularly updated based on emerging threat intelligence, then you're operating with a false sense of security. This approach often overlooks dynamic attack surfaces and leads to gaps that compliance frameworks alone cannot cover.

If your team treats compliance as a baseline and regularly evolves your security strategy to incorporate threat intelligence, behavioural trends, and new tooling, your organisation becomes more agile and resilient. This approach not only satisfies auditors but also strengthens real-world protection.

What Secure Looks Like Now

True security isn't static. It doesn't come from tools alone or from passing a checklist once a year. It's an evolving, living capability that requires attention, alignment, and ongoing investment.

If this report has surfaced even one area where your confidence may be misplaced, that's progress. Use the risk calculators to prioritise where you need to act first. Share this document with internal stakeholders, and open the discussion about what secure actually means in today's environment.

Need help assessing your exposure? Insodus offers full-spectrum cybersecurity reviews, from behavioural analytics and insider threat readiness to response planning and zero-trust implementation. If you'd like an expert eye on your current posture, we're here to help.

Visit insodus.tech or email hello@insodus.tech to book a review.