VYFORITY

Cyber security and business architecture advisory

Your dashboard says green. *We read what it is hiding.*

The Posture Reality Check is a two-day, read-only diagnostic that proves the gap between your stated security policy and your actual technical reality. No agents, no exploitation, no disruption: we read the configuration your own systems already hold, and hand your board the deltas in plain numbers. Fixed fee, $4,500 ex GST.

Two days, one answer

Not a maturity survey and not a roadmap. One question, answered with evidence: where does what you have been told diverge from what is actually configured?

Read-only, no disruption

Configuration review, directory extracts and architectural observation only. Nothing is touched, exploited or broken. Your IT team's objection to being tested disappears.

$4,500 ex GST, fixed

Agreed before we start. The lowest-risk way to find out whether the green on your dashboard is real, before an insurer, an auditor or an attacker finds out for you.

WHY THE DASHBOARD LIES

The watermelon: green on the outside, red within

Your IT team reports **100% coverage**, **MFA enforced**, **servers isolated**. They believe it, and they are reporting in good faith. But coverage has silent exceptions, enforcement has quiet exemptions, and isolation has forgotten firewall rules. The reporting is **green** because it measures intent; the reality is **red** because attackers exploit configuration, not intent. Ransomware does not hack in. It logs in, through exactly these gaps.

WHAT YOUR BOARD RECEIVES

The stated-versus-actual table. A short, stark comparison: what you were told, beside what the configuration shows. "MFA enforced globally" against the count of accounts silently exempted. This one table ends the debate.

The material deltas, quantified. Not four hundred findings: the specific, countable gaps that matter, in numbers a director understands without translation. A figure, not an adjective.

A board-ready one-pager. Plain language, defensible, tabled as-is. Plus the raw evidence behind every number, so the finding survives challenge from the team that reported green.

Why it must be independent. The team that configured the environment cannot be the team that grades it, and the MSP that reports green earns nothing by finding red. Vyfority holds no vendor margin and did not build your stack, so the numbers carry no agenda. This is the check your own people cannot mark for you.

THE FOUR DOMAINS WE READ · WHERE RANSOMWARE OPERATORS LOOK FIRST

01

Identity

The blast radius. Where privileged access has quietly accumulated, where enforcement has exemptions, and how far a single compromised login could actually reach.

02

Endpoint

The coverage reality. Where "100% protected" meets the machines with no working agent and the exclusions that quietly switch protection off exactly where it matters.

03

Network

The highway. How freely an infection could move once inside, whether critical systems are truly isolated, and, for industrial sites, whether a phishing email can reach the production floor.

04

Backups

The kill switch. Whether your last line of recovery would survive the attack that targets it, or fall with the same credentials, turning an incident into a ransom payment.

Two days to know what your dashboard won't tell you

Read-only, non-disruptive, and done inside a week. You receive the stated-versus-actual table and the evidence behind it: enough to know whether the green is real, and enough to decide what, if anything, to do next. $4,500 ex GST, fixed, led personally by a former enterprise CISO.

Dean Kastelic · Founder, former enterprise CISO
dean.kastelic@vyfority.com.au
linkedin.com/in/deankastelic · vyfority.com.au