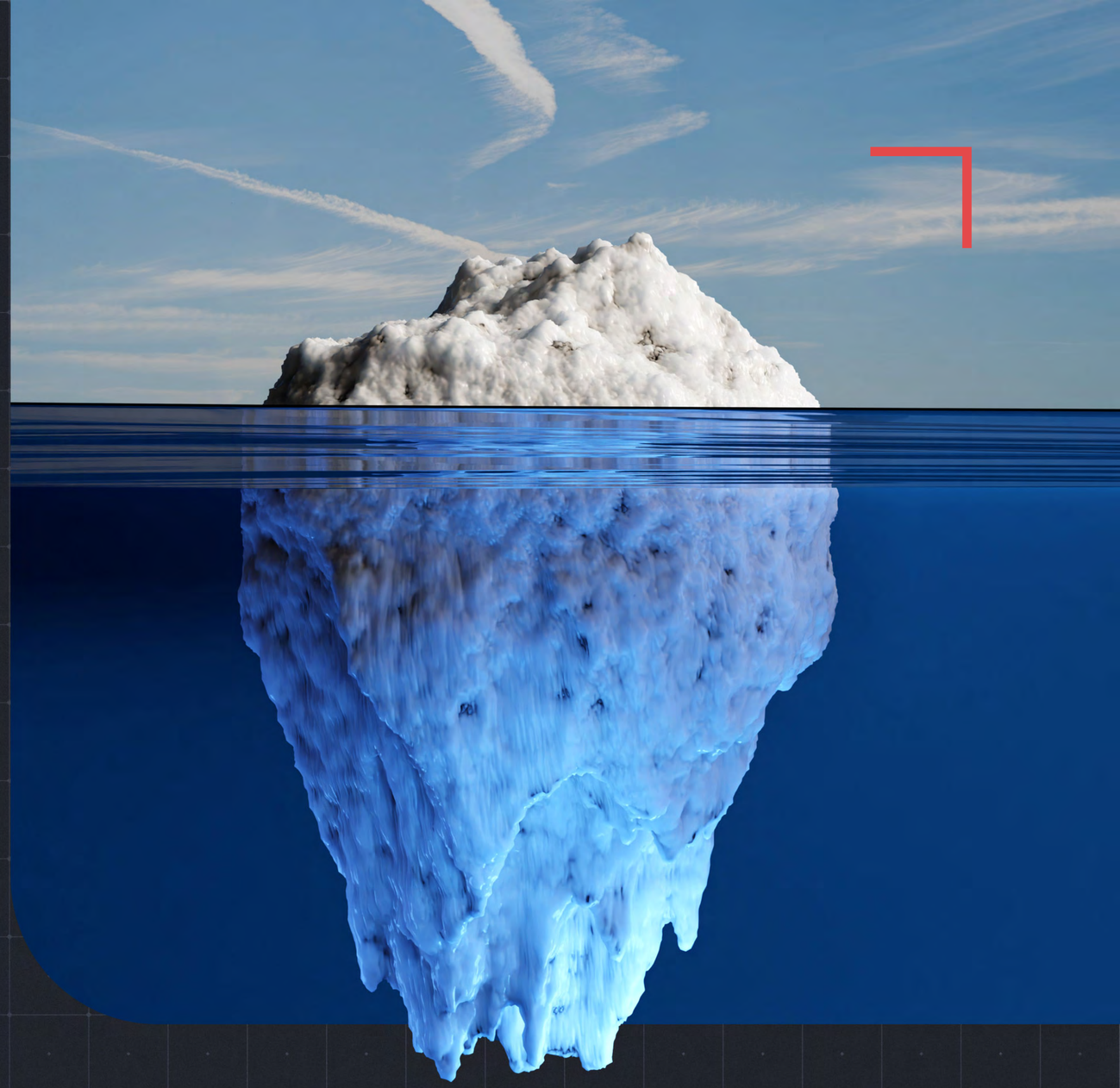
The hidden cost of legacy

Why application delivery needs a rethink—now



Standing still, is no longer an option

Why today's leaders must address spiraling renewal costs and rising risk exposure crippling growth.

If renewals don't fix exposures when delivering applications, why stay?

For all enterprise organisations across Australia, budgets are tight, but application resilience is mission critical. This is no longer just an IT concern: legacy platforms create financial and operational exposure. Renewal invoices arrive heavier each year, but value doesn't improve. For Australian business and tech leaders the pressure is immediate: keep critical apps resilient without locking your organisation into another low value renewal cycle.

Why no action is riskier

Over the past two years, high-profile exploits of legacy platforms have left critical systems wide open, forcing organisations to maintain and patch vulnerabilities rather than invest in more productive work. In Australia, over half of major outages are still security related*. The NIST National Vulnerability Database confirms that CVEs published as far back as 2018 remain actively exploited, many now marked as "Deferred" with no remediation coming from the vendor. For organisations locked into multi-year contracts, every renewal builds in not only higher costs but also compounding exposure.

Standing still now costs more than change. The cost of inaction (downtime, breaches, regulatory fines, reputational damage) far outweighs the cost of migrating to new Application Deliver Controllers (ADC). This alternative brings business and tech leaders greater availability, policy enforcement, identity, and traffic security, delivering a smooth, seamless migration to a new platform with less vulnerability and specialised application delivery that enhances user and customer experiences.

Standing still isn't peaceful

Renewals don't fix cracks, they widen them.

Paying more for less

Australian IT leaders are under pressure to keep systems alive on shrinking budgets. When systems fail, it's business and tech leaders who are first in the firing line. Stuck in contracts with global vendors that cost more and deliver less, they feel trapped. Frustrated, they are constantly firefighting and lacking control as the hidden costs of downtime, inefficiency, and reputational damage continue raging. It's vital to choose your next partner correct, because you will be stuck with them for the duration of the contract.

How ADC vulnerabilities erode what business and tech leaders are devoted to most

Slicing revenue, obscuring competitiveness, repelling customers

Service interruptions

ADCs often act as traffic managers, remote access gateways, and load-balancers. If compromised or forced offline, key customer services (web portals, remote access, VPNs) instantly become unavailable and unreliable.

Data exposure and privacy risks

Vulnerabilities allow attackers to steal credentials, session tokens, and other sensitive data. This leads to customer data breaches that undermine trust.

Regulatory and legal consequences

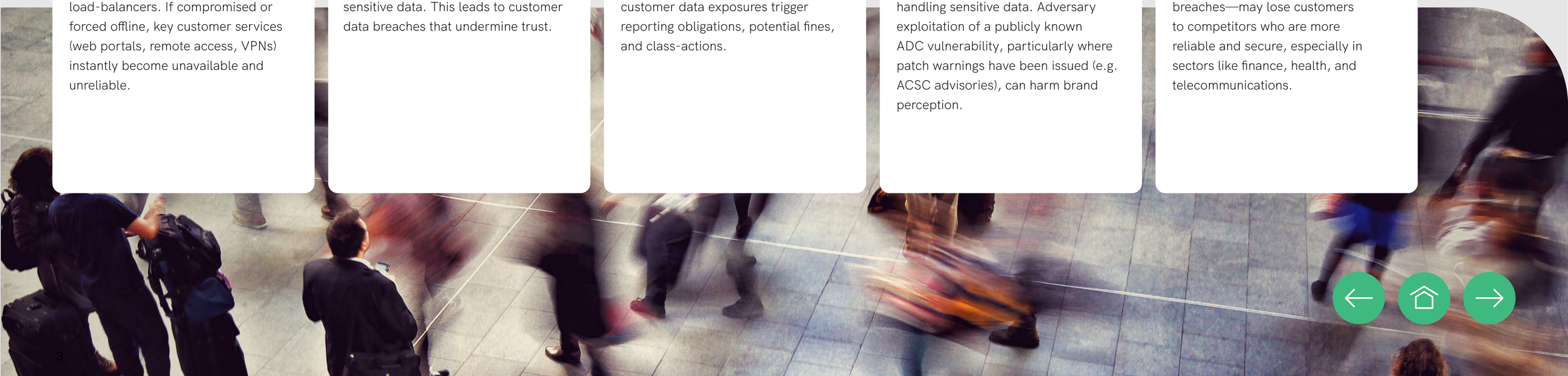
Under privacy laws (Privacy Act, Notifiable Data Breaches Scheme), customer data exposures trigger reporting obligations, potential fines, and class-actions.

Reputational damage

Customers expect their information to be secure, especially in sectors handling sensitive data. Adversary exploitation of a publicly known ADC vulnerability, particularly where patch warnings have been issued (e.g. ACSC advisories), can harm brand perception.

Competitive disadvantage

Organisations handling vulnerabilities poorly—or suffering outages and breaches—may lose customers to competitors who are more reliable and secure, especially in sectors like finance, health, and telecommunications.



How customers react and what sketchy service delivery impacts

Availability and uptime

When ADCs are compromised or under attack, customer-facing applications often degrade or go offline. Customers can't log in, it's slow, and there's service errors. Even a brief outage will degrade trust.

Latency and performance degradation

DoS attacks or misconfiguration makes everything slow when customers are expecting fast responses (web, mobile, remote services). Performance issues like these push customers away (shopping carts abandoned, users switching to competitor services).

Security incidents visible to customers

If a breach is public, customers feel their data is unsafe. Even a perceived risk, like a report in the media, can lead to churn. Particularly in sectors with sensitive data, the consequences of data exposure are magnified.

Remote access confidence

Many businesses rely on remote access (VPN, Gateway). If vulnerabilities affect these services, experience for employees, partners, and customers (e.g. telehealth, remote support) suffers and trust in accessing services safely declines.

Regulatory disclosures demand transparency

Under the NDB scheme, organisations must disclose data breaches and exposure, which can publicly harm reputation, sometimes more than the technical incident itself.

Today's toll, tomorrow's pain.

Direct costs

of implementing emergency patches, system downtime, deployment of monitoring or logging, forensic investigations, staff overtime or external consultancy can run into hundreds of thousands to millions of AUD.

Strategic loss

low to no customer loyalty and brand erosion, making winning new customers difficult and partnerships challenging. Trust is vital and this kind of damage can have long-term effects.

Competitive positioning:

Organisations that demonstrate strong security with resilient ADC infrastructure differentiate themselves. Conversely, organisations with repeated incidents and weak posture also stand out.

Insurance and market risk

Cyber insurance premiums increase after incidents, requiring stronger patching and security hygiene. Investors and partners look unfavourably at organisations who have vulnerabilities or past incidents.

Lost revenue and opportunity

If web services are down, customers can't transact. In retail, e-commerce, and finance, even small hours of outage can translate to lost sales. Also, delays or inability to deliver services (e.g. remote learning, telehealth) could incur penalties and loss of contracts.

Regulatory penalties and legal fees

If personal data is breached, there's fines under the Privacy Act, plus costs of complying with investigations, possible class actions, and compensation. Also, there's the non-financial costs of legal reputation, board scrutiny.

Regulatory and compliance backlash

Organisations that suffer breaches due to known vulnerabilities (especially where ACSC has issued advisories) may be seen as failing due diligence. Under Australia's Privacy Act and the Notifiable Data Breaches (NDB) scheme, personal data exposed through an ADC vulnerability can trigger a requirement to notify customers and regulators.The Essential Eight expects organisations to patch known high-risk vulnerabilities promptly.

Non-compliance with patching or failing to act on ACSC advisories attracts scrutiny, possible penalties from regulators and affect government contracts, certifications, and partnership deals. Customers may also seek recourse if data or service loss is traced back to vulnerabilities that could have been prevented.

Modernisation pays for itself, fast

With Nexon and F5, transitioning is simple and seamless

Despite these great tangible benefits, some organisations see migration as a complex hurdle that stands in the way. Yet, with Nexon's local delivery and support, and F5's global expertise, you'll confidently modernise in a safe, low-risk way that lowers cost and strengthens resilience, they are boldly freeing teams from the patching treadmill.

Less risk. More ROI.

Australian IT leaders are under pressure to keep systems alive on shrinking budgets. When systems fail, it's business and tech leaders who are first in the firing line. Stuck in contracts with global vendors that cost more and deliver less, they feel trapped. Frustrated, they are constantly firefighting and lacking control as the hidden costs of downtime, inefficiency, and reputational damage continue raging. It's vital to choose your next partner correct, because you will be stuck with them for the duration of the contract.

Where global strength meets local power

Your digital future to the power of Nexon, amplified by F5 application delivery

The status quo is unsustainable. Business and tech leaders need to simplify complexity and have expertise backing them up. This is where Nexon and F5 come in. Together, they give organisations a proven, low-risk path out of the legacy trap.

Nexon's deep local consulting, migration, and managed services remove the bandwidth burden from internal teams. F5 is a global leader whose entire business is built around application delivery and security. It's the best of both worlds: the confidence of global innovation combined with the accountability of a trusted local partner. They are the specialist you turn to when the generalist fails.

Application delivery isn't a bolt-on. With Nexon and F5 on your side, it's front and centre-engineered for performance, resilience, and security. F5 delivers global scale, resilience, and recognition. Nexon provides local trust, migration expertise, and managed services.

Large Australian healthcare provider cuts renewal costs by 40% and migrates under 30 days.

The outcome? A safe and seamless transition as you migrate, stronger resilience and security posture against the very CVEs making headlines. Lower total cost of ownership, achieved without disruption. You don't have to get caught out. You don't have to bleed at renewal. With Nexon and F5, you can modernise with confidence and move boldly forward.

Don’t just renew, review

A clear, low-risk assessment giving executives certainty and leaders relief

Business and tech leaders want an experienced partner to lead the migration without downtime and risk. They want confidence that change won’t blow out costs or timelines. A way to reduce risk, not commit to it. This isn’t about rushing to migrate-it’s about clarity before you renew. Having a clear picture of costs vs change before contracts lock them in.

Get clarity before committing

One blueprint. One timeline. No surprises.

Before renewing, leaders need to know their options. To move forward with clarity, Nexon and F5 demystify costs, risks, and timelines. By reviewing your renewal cycle, your current infrastructure, and dependencies, we provide a tailored blueprint. It’s a safe, low-risk step—designed to give you confidence in your decision, whichever way you go.

Book your discovery assessment now!