The Security Paradox Facing Mid-Market Organisations

You face enterprise-level threats. Ransomware. Nation-state actors. Supply chain compromises. But you lack enterprise resources to defend against them. Cyber insurance demands Zero Trust. Compliance frameworks require continuous monitoring. Breach costs are climbing.

Yet you can't justify enterprise security teams, can't operate the complex security platforms vendors sell you, and can't afford to leave critical gaps unaddressed.

When businesses can't access the security they need because it's too expensive or too complex to operate, something's wrong. Vendors sell software-as-a-service platforms without operational capability. You're left managing the gap yourself or hoping nothing goes wrong.

Two Assumptions are Dead

Traditional network security assumed:

- X Users worked inside corporate walls
- X Applications lived in data centres

Both assumptions are dead. Enterprise tools weren't designed for organisations at your scale to operate. Traditional managed service providers offer basic monitoring without real detection capability. Zero Trust remains an aspiration, not a reality.

This gap isn't just technical. It's operational.

Enterprise security frameworks assume you have security analysts to operate SIEM platforms, tune correlation rules, and investigate alerts. Mid-market organisations don't have these resources. You need security visibility that comes with operational capability, not platforms requiring expertise you can't afford to hire.

Zero Trust Detection & Response (ZDR)

Not just software. Security-as-an-outcome.

We built ZDR to close the gap between what mid-market organisations need and what they can actually operate.

Built on Zscaler's Zero Trust Exchange platform. Monitored 24/7 by The Instillery's Security Operations Centre (SOC) team. Managed by Zscaler Aces-certified engineers.

Accessible

Enterprise-grade Zero Trust at mid-market economics

Per-user monthly pricing designed for 50-300 user organisations. No massive upfront investment. Deployable at your scale without capital commitments that don't make sense for your business.

Operational

We handle security operations. You handle business decisions

24/7 SOC monitoring and response built in. Zscaler Aces engineers manage platform deployment, policy tuning, and continuous optimisation. It actually gets run properly, not just licensed and forgotten.

Effective

Complete visibility with inline threat blocking

Real-time threat detection across endpoints, identity, and network layers. Inline blocking where attackers operate. Security that improves over time, catching threats that single-layer approaches miss.

What makes ZDR different?

Traditional vendors sell licenses. Other managed service providers resell those licenses with basic monitoring. Neither delivers operational security.

Zscaler Aces Expertise

Elite Partner Status. Exceptional Outcomes.

Zscaler Aces represents a tiny fraction of Zscaler's global partner ecosystem. Reserved for "the best of the best", elite professionals who've demonstrated exceptional technical expertise in Zero Trust Exchange architecture.

We deliver outcomes: Threats detected and blocked in real-time. 24/7 expert response. Continuous platform optimisation. Measurable security improvement.

About Virtual IT Group & The Instillery

Virtual IT Group and The Instillery deliver managed IT and cybersecurity services across Australia and New Zealand. As Zscaler Aces-certified partners, we represent the elite tier of Zscaler's technical partner community, bringing exceptional Zero Trust expertise to organisations that need enterprise-grade security at mid-market economics.

CONTACT

1300 144 984
vitgsales@vitg.com.au

HEAD OFFICE

Level 7, 122 Arthur Street,
North Sydney, NSW 2060

www.vitg.com.au
www.theinstillery.com