KNOVATION
SOLUTIONS

Secure Anywhere

Closing the posture-to-access gap, for every device, everywhere

You've invested in device management, firewalls, and cloud platforms. But most of that investment leaves one critical gap completely unprotected: the disconnect between device compliance and network access.

Managed devices connecting through unmanaged VPNs. Posture checks that don't govern access. Legacy tunnels that authenticate once and trust forever. These are the vectors attackers use to move from a compromised endpoint to corporate resources.

Secure Anywhere delivered by Knovation Solutions closes that gap.

Business challenge

Your devices are managed, but access isn't tied to compliance.

Your environment probably looks like this:

- Devices are enrolled in an MDM
- Firewalls are in place at the perimeter
- MFA is deployed for cloud applications

Yet network access is still governed by a VPN that:

- Doesn't know or care about device posture
- Authenticates once at connect time and trusts the session indefinitely
- Gives full-network access when per-app would suffice
- Runs through infrastructure that your team must deploy, patch, and scale
- Treats mobile and desktop as two separate problems

This creates a posture-to-access gap. Your endpoint management knows a device is compromised. Your network doesn't act on it. Attackers don't need to break through the firewall. They gain entry on a trusted connection from a compromised device.

Key capabilities

Secure Anywhere is an endpoint security architecture built on two vendor stacks: **Ivanti** for endpoint management, secure access and mobile threat defence, **WatchGuard** for identity, DNS protection, endpoint protection, and automated response. Every device, mobile and desktop, is covered without vendor sprawl.

Category	Without Secure Anywhere	With Secure Anywhere 2.0
Device-to-access link	None, VPN ignores posture	Continuous, posture governs access in real time
Mobile secure access	Separate VPN app, separate vendor	Embedded in the MDM client, no separate app
Mobile threat defence	Separate MTD product, separate console	Embedded in the Ivanti client, managed in one place
Desktop secure access	On-prem VPN appliance	Cloud-managed ZTNA with lightweight gateway VM
Endpoint protection	Separate AV/EDR vendor	WatchGuard EPDR with zero-trust process classification
Vendor count	5+ (MDM + VPN + AV + DNS + MFA)	2 stacks (Ivanti + WatchGuard)
IT management overhead	Multiple consoles, manual response	Two dashboards, automated response

Business benefits

One architecture. Six outcomes that matter to your board.

1. **Posture-driven secure access across every device**

   Every device, every connection, governed by compliance in real time.

   Legacy VPN is the weakest link in most security architectures. It authenticates once and trusts forever. Secure Anywhere 2.0 replaces that assumption: access is continuously evaluated against device posture. If a device becomes compromised mid-session, access is revoked automatically, without waiting for your team to act.

2. **Desktop and mobile endpoint protection**

   Active threat protection across your entire device fleet.

   Managed devices without active endpoint protection are compliance risks and breach liabilities. WatchGuard EPDR protects every desktop. Ivanti Mobile Threat Defence protects every mobile device embedded in the Ivanti client and managed from the same console as MDM. No gaps. No separate vendors. One view of your entire endpoint estate.

3. Identity and DNS protection everywhere

Stop credential theft and phishing before they reach your network.

Identity controls who accesses what, regardless of network location. DNS protection blocks threats at the earliest possible interception point, before malicious connections are established. Both work independently of VPN, so your protection travels with your people.

4. Detection and automated response

Correlated detection across the WatchGuard stack, with automated response.

Most mid-market security stacks detect threats in silos and respond manually. By the time a human acts, the damage is done. WatchGuard ThreatSync correlates signals from EPDR, Authpoint and DNSWatch and responds automatically, isolating compromised endpoints, revoking sessions and blocking malicious domains. For teams that need full analyst coverage, WatchGuard Total MDR extends ThreatSync with 24x7 oversight.

5. Regulatory and compliance alignment

Auditable, continuous, demonstrable – not periodic and approximate.

Secure Anywhere is built to support the frameworks your board and auditors require:

Framework	How Secure Anywhere 2.0 supports it
POPIA	Demonstrable access controls; personal traffic never touches corporate infrastructure
JS2 FSP (Joint Standard 2 of 2024)	Continuous device posture, per-app access governance, audit ready for regulated financial services
ISO27001	Endpoint security governance, configuration control, continuous posture evaluation
NIST CSF 2.0	Protect, Detect and Respond functions covered end-to-end across endpoint, identity and DNS

Compliance is no longer a periodic assessment exercise. It is a continuous, auditable state, with the evidence to prove it.

6. **Vendor consolidation and cost reduction**

   From five vendors to two – without reducing coverage.

   If you are currently running MDM, a separate VPN, a separate AV, separate DNS protection and separate MFA, you are paying the integration tax every day: in licensing overlap, management overhead, and the time your team spends context-switching between consoles.

   Secure Anywhere consolidates that into two stacks. Two dashboards. Automated response. One partner who knows your environment inside out.

Summary

This is not a rip-and-replace of every security tool in the environment. It's a purpose-built architecture that closes the specific gap legacy VPN and disconnected point solutions leave open: the gap between what your endpoint management knows and what your network acts on.

- One architecture covering mobile and desktop
- Posture-to-access enforcement in real time
- Compliance evidence that's continuous, not periodic
- Vendor consolidation from five tools to two stacks
- Delivered by a single partner who shares accountability for the outcome

Let's talk about closing the gap in your environment.
Reach out to the Knovation Solutions team to discuss your architecture.

Knovation Solutions:

Website: www.knovation.co.za

Call: +27 83 326 1198

Email: info@knovation.co.za


KNOVATION
SOLUTIONS