timus
ZERO TRUST NETWORK PROTECTION

IT First Responder

CASE STUDY

IT First Responder Secures **Remote Access** and **Streamlines Operations** with Timus SASE

Case Overview

ITFR, a Timus MSP partner in Australia, needed a secure, flexible alternative to legacy VPNs for managing remote access to terminal servers. They chose Timus Networks' SASE solution, which provided Zero Trust security, multi-factor authentication, and seamless remote access via point-to-point and IPsec tunneling. The deployment was fast and efficient, enhancing security and reducing complexity for ITFR's clients, resulting in greater flexibility, business growth, and client satisfaction.

Main Challenge: To securely manage remote access to terminal server environments

Before

- Struggled with Secure Remote Access
- Complex and Complicated Configurations
- Difficulty Integrating MFA

Today

- Implemented ZTNA
- Simplified Deployment
- Seamlessly Integrated MFA

Seamless Transition to Cloud-Native Timus SASE

Improved Security Posture and Compliance

Cost savings, Timus MFA, less complex solution, no RDS GW required.

Challenges and Solution

Before adopting Timus, ITFR's clients struggled to implement secure remote access for their terminal servers. The primary requirement was to ensure multi-factor authentication (MFA) and provide access in a way that minimized the need for additional servers or complex configurations. Traditional solutions, like Microsoft Remote Desktop Gateway, demanded extra servers in a DMZ, increasing complexity and security risks.

The most significant pain point was the need for a solution that could deliver secure, streamlined access while seamlessly integrating MFA without extensive configuration. Clients were also burdened with managing legacy VPN solutions that required additional third-party MFA tools like Duo, further complicating secure access to terminal servers.

Timus just works. The user-level licensing is a huge win for us, allowing multi-device access without extra cost, and the gateway is both fast and affordable. I use it daily from New Zealand to Australia without any issues—it's become my go-to solution for secure, seamless access.

Barry Trotman

Director Security Services, IT First Responder

ITFR evaluated various options before selecting Timus Networks as the solution provider. With Timus, ITFR could fulfill its client requirements by providing secure, efficient remote access without the overhead of additional servers and third-party software. ITFR implemented two distinct solutions for its customers:

- **Point-to-point connections:** For smaller customers who needed secure desktop access via VPN.
- **IPsec tunneling:** For larger, mixed environments requiring more robust security features and access controls.

Timus offered ITFR a Zero Trust-based solution that combined secure tunneling with the benefits of two-factor authentication (2FA), firewall management, and antivirus protection. This comprehensive solution ensured that users accessing the terminal server environments were properly authenticated and secured through Timus's Secure Access Service Edge (SASE) capabilities.

ITFR found several features that distinguished Timus from the competition including:

1. **Micro-segmentation:** Timus enabled ITFR to granularly control what users could access within the network, ensuring that only authorized users could reach sensitive areas of the infrastructure.

2. **Posture management:** Timus conducted posture checks on connecting devices, guaranteeing that each device met security standards before granting access.

3. **Ease of deployment:** Timus's solution required less configuration and skill level to deploy compared to enterprise-focused products like Microsoft or Cloudflare.

4. **User-level licensing:** ITFR appreciated the user-level licensing model, which allowed for multi-device access without extra costs, proving highly beneficial for their clients.

What I love about Timus is how easy it is to use and scale. It's everything we need for secure remote access.

Barry Trotman

Director Security Services, IT First Responder

The deployment of Timus across ITFR's client base was smooth and efficient. For smaller clients, ITFR deployed Timus to provide secure, point-to-point desktop access, allowing employees to easily connect to their office networks via VPN.

For larger clients with more complex needs, ITFR set up secure IPsec tunnels, enabling secure, managed access from remote locations to terminal servers. Timus's firewall and authentication capabilities ensured that only authorized users with secure devices could access the network.

The entire process was seamless, requiring minimal configuration from the clients' end. ITFR's support teams handled any minor issues that arose during onboarding, and post-deployment, there was minimal demand on the help desk.

Outcome and Results

The switch to Timus Networks significantly improved ITFR's operations and those of its clients. ITFR's clients now enjoyed:

- **Enhanced security:** Timus provided Zero Trust security and MFA, which were crucial requirements for clients accessing terminal server environments remotely.
- **Seamless user experience:** Users could connect securely without complex configuration or technical issues, reducing the load on ITFR's help desk.
- **Increased flexibility:** Clients could now seamlessly support remote work, allowing users to access private infrastructure securely from any location.
- **Added value:** Beyond secure access, Timus's solution provided added value through features like web category filtering and antivirus protection, making it a comprehensive security solution.

ITFR continues to use Timus as its primary remote access solution. With Timus's low latency and reliable performance, ITFR has been able to deliver high-quality secure access for users based in different regions. The relationship between ITFR and Timus remains strong, with ITFR relying on Timus's ongoing support and feature updates to meet evolving client needs.

The success of this deployment has positioned Timus as a trusted partner for ITFR, and ITFR plans to continue expanding the use of Timus across its client base.

Connectivity and Security in One

Always-On Secure Access, ZTNA, Safe Browsing, Dark Web Monitoring and more under a single SKU for layered security.

Easy to Deploy and Manage

100% cloud-based SASE solution. No hardware. No maintenance. Deploy in less than 30 minutes.

Built on Zero Trust

Timus SASE users connect through private, never shared cloud-hosted gateways. Protect employees, wherever they work from.

ABOUT
IT First Responder

CASE STUDY

IT First Responder

Based in Sydney, IT First Responder is your go-to team for cybersecurity and tech incident response. We're committed to a smooth, frustration-free experience. No cookie-cutter scripts or robotic responses—just real people solving real problems, keeping your tech secure while you focus on your business.

Because risk reduction and peace of mind are what we're all about. **That's the IT First Responder difference.**

ABOUT
TIMUS NETWORKS

Timus Networks simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Our premier product, Timus SASE, transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE is purpose-built for the MSP/MSSP Channel. It offers simplicity and rapid deployment, with installation in under 30 minutes.

Timus and the Timus Networks logo are trademarks of Timus Networks, Inc., in the United States, other countries, or both. The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on Timus Networks' current product plans and strategy, which are subject to change by Timus Networks without notice. Timus Networks shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or similar materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from Timus Networks or its channel partners or licensors, or altering the terms and conditions of the applicable agreement governing access to the Timus Platform or related products and services.

timus

ZERO TRUST NETWORK PROTECTION

timusnetworks.com