timus
ZERO TRUST NETWORK PROTECTION

ITSNYC
INTEGRATED TECHNOLOGY SYSTEMS

CASE STUDY

ELIMINATING NETWORK **SECURITY VULNERABILITIES from MOBILE USERS**: ITSNYC'S JOURNEY WITH TIMUS SASE

Case Overview

ITSNYC had a client with a mixed IT infrastructure of physical offices, cloud resources in Microsoft Azure, and a mobile sales and support team using various devices. Their client was facing significant security challenges, especially with the exposure of a publicly accessible website and inadequate control over mobile access to corporate resources. After years of dealing with security vulnerabilities and growing frustration with VPN solutions, ITSNYC decided to deploy Timus SASE to address these concerns.

Main Challenge: Secure mobile access to their client's resources over a hybrid environment

Before

- Lack of Secure Access
- İnefficient VPN Solutions
- Frequent Support Tickets

Today

- Enhanced Network Security
- Scalable and Easy-to-Manage Secure Access
- Substantial Reduction in Tickets

Streamlined Security for Mobiles and Remote Users

30%

Decrease in Number of Support Tickets

Increased Client Satisfaction

Challenges and Solution

The main challenge this client faced involved securing an application server in Microsoft Azure, which included a publicly accessible website without Multi-Factor Authentication (MFA). Despite requiring credentials, the site was vulnerable to numerous brute force login attempts with invalid credentials, posing significant security risks. This vulnerability persisted for over ***five years*** and was frequently flagged in penetration tests and security audits.

Although alternatives like OpenVPN were considered, they were inconvenient and hard to manage due to frequent certificate updates, making them unsuitable for mobile access and scalable deployment. Around ***50% of the users*** from the client required consistent access to the application, which complicated the adoption of stringent security measures.

> *The flexibility of having a smaller, more personal company was key for us, we had the opportunity to have direct involvement with assistance in deployment.*
>
> **Jay Edlin**
>
> **Director of Technology, Integrated Technology Systems**

Timus stood out to Integrated Technology Systems due to its **personalized approach**. They had direct involvement from the CTO and access to high-quality support during the deployment. Furthermore, Timus SASE was easy to deploy via Microsoft Intune and allowed for **scalability**.

ITSNYC deployed Timus Networks across the client's infrastructure, including both laptops and mobile devices. The Timus solution helped close vulnerabilities by protecting the application server and eliminating the need for site-to-site VPNs and the unreliable Sophos SSL VPN client. Key features that stood out:

- **Zero Trust Architecture:** Timus ensured secure access to Azure resources without the need for a public-facing application.
- **Simplified Mobile Access:** Timus replaced the buggy Sophos SSL VPN with a more reliable solution, securing access for mobile users without compromising convenience.
- **Supportive Partnership:** ITSNYC valued Timus' hands-on support, including direct engagement from the CTO, which helped smooth over any deployment issues.

Outcome and Results

Enhanced Security Posture: Timus' security features, such as MFA and integration with single sign-on, closed critical security gaps giving the client peace of mind and reducing exposure to data breaches.

Streamlined Remote Access: Timus simplified remote access with a scalable and user-friendly solution allowing for continuous workflow and improved end-user experience for the client.

Decreased Support Tickets: There was an immediate reduction in support tickets related to VPN connectivity issues. This saved the client time and minimized maintenance costs.

SImple Per-User Pricing: ITSNYC valued Timus for its simple per-user pricing, ease of deployment, and ease of use. This resulted in improved scalability as well.

> ***The most impactful change is that we're finally able to stop those attacks... and ensure their data is secure.***
>
> **Jay Edlin**
>
> **Director of Technology, Integrated Technology Systems**

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
INTEGRATED TECHNOLOGY SYSTEMS

Integrated Technology Systems is a complete IT solution provider that has been in business since 1994. Having the "right" technology in place improves a company's overall efficiencies and marketplace performance. Employees are more productive, internal and external project collaboration is easier, and communication is enhanced with current technological tools.

Choosing the best technology for your work environment can be difficult since it is constantly evolving. A well-designed network infrastructure is secure and is scalable. The design of the network can mean the difference between being operational and being put out of business due to malware, ransomware, or some other kind of cyber security issue.

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.

ZERO TRUST NETWORK PROTECTION

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.