

HOW OUR MSP PARTNERS ARE DEPLOYING TIMUS SASE FOR THEIR CLIENTS

Timus SASE

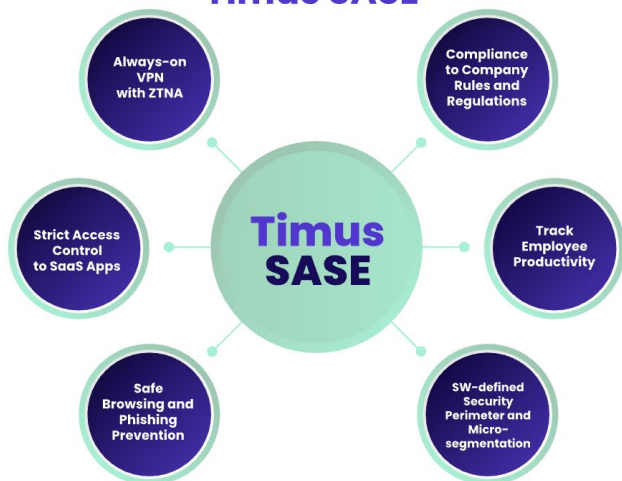
The Network Security Solution
for the Cloud Era

Deploy in 30 minutes or Less.



Timus SASE simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance. Through Timus SASE, MSPs can move from complex setups involving multiple tools into a single, unified solution that secures networks and protects their clients' employees, regardless of their location or device. Below are some examples of the Timus SASE deployment use cases by our partners.

Minimize Business Risks with Timus SASE



Replace VPNs with Timus SASE's always-on, secure connectivity to resources and enforce compliance

A lot of employees forgo using their VPNs as they are usually clunky, exposing the company to public wifi risks at coffee shops, airports, or conferences. Plus, VPN credentials are easily bought and sold in the dark web. When hackers access a corporate network via breached VPN credentials, they can access any part of the network laterally, which can be catastrophic when it comes to customer PII, financial data, IP, payroll info, and more.

Timus SASE replaces traditional VPNs with an **always-on VPN layered with ZTNA**. The contextual policy engine makes sure that the **identity of the user** is thoroughly verified before granting **granular** access to company resources.

Remote Desktop Protocol (RDP) Replacement

If clients are using RDP (Remote Desktop Protocol) to access files remotely, this can be replaced with Timus SASE, layering on ZTNA to verify all users thoroughly.



Enforce Compliance to Security for Employees Who Travel

Any employee who is traveling (MSP or their clients) should adopt a zero-trust approach to accessing the corporate network, company SaaS apps, or data remotely. Airports, conferences, and coffee shops are prime locations for hackers to steal credentials.

Always-on connectivity layered with ZTNA is a core part of the Timus solution and ensures that the employees can access the company network seamlessly and securely no matter where they are and which device they access it from.

Strict Access Control to SaaS Apps via Static IPs

Timus SASE provides a dedicated Static IP for each of its cloud gateways that are never shared between clients. This **Static IP can be allowlisted** in the SaaS apps for strict access control. For example, MSPs hide their own RMM, PSA, and documentation tools behind the Static IP so that no one without the Timus agent can access them.



Safe Browsing, and Phishing Prevention

Timus SASE comes with Secure Web Gateway integrated into the Cloud Firewall that protects users from malware, phishing attempts, malicious sites and downloads, including drop servers, drive by downloads, adware, command and control botnet hosts, and parked sites and domains, among others. Timus SWG also comes with **full SSL inspection** to decrypt and inspect the contents of the HTTPS traffic. The solution also allows for geolocation-block helping prevent fraud among other use cases.



Centralized Management via Single Pane of Glass

The intuitive, multi-tenant Timus Partner Portal offers MSPs a unified dashboard to manage and monitor all their client deployments centrally.

Layered Security Offering - We complement, not compete with other vendors

Timus fits perfectly into an MSP's cybersecurity bundle, allowing for a layered security offering that will usually include on-prem FWs, EPPs, SASE, and EDR while having a fixed monthly cost that they can add a margin onto. Timus SASE is integrated into many tools such as Key Identity Providers, **Connectwise PSA**, and leading EPPs for increased device posture check telemetry. We are vendor agnostic when it comes to the MFA tools, and on-prem Firewalls. Timus SASE also supports **SAML 2.0 for SSO** integration to streamline access.

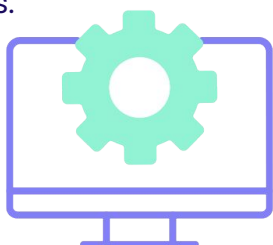


Control Client Networks Remotely

Timus can help set up and control a full network for employees who are not necessarily working in the same physical location. The Timus solution provides deep visibility to all employees and devices, it makes sure everyone can access only what they need without compromising on security. Timus can restrict access to certain cloud apps and websites if needed and all the traffic, user, and device logs show up in a single location for the administrator to review and report on.

Vendor Consolidation

Timus may help with simplifying the tech stack and consolidating vendors by offering multiple services in a single solution: VPN replacement, network-level malware and category filtering, SWG, URL-based web filtering, Dark Web Monitoring, Activity Tracking, Static Dedicated IP to allowlist apps, and Cloud-FW. Timus SASE also eliminates the need to pay for paid MFA as it works well with tools like Google Authenticator and others.



Replace Desktop as a Service

With Timus, you might be able to replace existing tools such as Azure VDI and Citrix.



Device Management, and Infected Device Isolation via Device Posture Check (DPC) and Dynamic Tagging

Timus Connect agent is integrated into leading EPPs like Sentinel One, BitDefender, MS Defender and Heimdal with more on the way for enhanced DPC. In addition to policy enforcement for network access, EPP integrations together with dynamic tagging capabilities allow for device isolation of infected devices in the network.

Productivity Tracker

With remote/hybrid working environments, employers might be worried about the productivity of their employees. With Timus giving deep, and continuous visibility into a client's network, MSPs can utilize the Productivity Tracker feature to create custom trend reports and dashboards on the productivity of the company, its teams and users across app usage, and accessed URLs.



Compliance & Cyber Insurance Needs

Timus makes it easier for clients to fulfill requirements for added security, activity logging, and reporting for compliance standards such as HIPAA, FINRA, SOC2, CMMC, ISO 27001 and meets the requirements of cybersecurity insurance. Timus itself is SOC 2 Type 2 and ISO 27001 compliant.

Integration API

Timus SASE comes with an API that MSPs can use to integrate into their workflows. For example, an MSP integrated the API with their workflow, allowing a user also getting kicked out of any Timus Connect connection if they're deleted from internal systems. MSPs love working with Timus to automate flows to the extent possible and gain operational efficiencies.



MSP Partner | Case Study

One of our MSP Partners deployed Timus SASE for a client that does Software Development. They allowlisted the PaaS tool used by the coders behind the Timus static private IP so that coders could develop safely once they accessed the PaaS tool via the Timus Connect agent. This ensured that no one could access the PaaS tool without getting zero-trust verified by Timus first.



Automated Reporting

Timus allows for automated reporting on many network activities that the MSPs can utilize to update their clients about what's going on in the network.

Competitive Advantage

Are you looking to become the Trusted Advisor for your clients? In the current risk economy, when it's not a matter of if but when for a lot of clients getting breached, you can have an award winning zero-trust network security vendor in your tech stack, giving you an advantage in the market. The ease with which you can get started on Timus will give you more time to scale your business.

