timus

Feature Overview and Use Cases for MSPs & Their Clients

FEATURE OVERVIEW

Timus Networks

The Network Security Platform for the Cloud Era

Companies struggle to meet the network security demands of the cloud era; balancing easier remote access with stricter cybersecurity requirements.

Existing solutions like VPNs and hardware-based firewalls don't cut it. VPNs are vulnerable to phishing and credential theft and hardware-based firewalls weren't built for remote work and data living in the cloud.

Timus Networks helps companies orchestrate secure access regardless of location and device while protecting the network against cyberattacks.

With Timus, employees can stay productive and protected, no matter where they work from.

Timus is the only MSP-focused network security platform combining secure, zero-trust network access with an intelligent cloud firewall that adapts to user risk profiles and blocks threats in real time.

Built by firewall experts with decades of cybersecurity experience and praised by customers and industry thought leaders, Timus is the answer to the network security needs of the cloud era.

Secure Remote Access with Intelligent Network Protection

Protect your network with cutting-edge technology, while making sure employees have secure access to data and applications to stay productive, regardless of their location.

Zero Trust Network Access: Timus uses a zero trust approach to all network access requests with least privilege principle:

- Zero Trust Network Access Policies can verify user & system administrator identities based on their behaviors and context
- Timus has one of the richest zero-trust verification checklists in the market to verify the identities including impossible travel, and email breaches on dark web
- Multi-factor authentication can be enforced adaptively based on behaviors and risk level
- Notifications can be sent to the administrators and users on suspicious sign-in attempts
- Sign-in activities are logged in detail and are shown on the world map to visually see any suspicious activity

Replace VPNs with Timus Connect Agent: Super lightweight, OS-agnostic & always-on agent available for iOS, Android, Windows, and Mac. Replaces the need for any VPN. The user does not need to make any configurations as settings and updates are automatically downloaded from the server. Can use either Wireguard or OpenVPN.

Adaptive Cloud Firewall: Dynamic user-centric cloud firewall that follows users in real time.

- Layer-3 & layer-7 stateful firewall
- Rules follow users and devices an all gateways
- Create rules based on source, destination, service, device, and time of day or week
- Port forwarding
- IPSec tunnels to 3rd party firewalls and routers
- Detailed network traffic logs

Adaptive MFA: Timus doesn't stop at two-step verification. When threat levels go up, Timus adapts and presents additional verification steps.

Private Dedicated Gateway: Providing a private dedicated gateway with a static IP address to each client's traffic increases security, bandwidth, and speed.

Static IP: Gives the MSPs and their clients the ability to allowlist cloud apps and services behind a static, private IP.

Micro-segmentation: Create micro-segments with granular and specific permission sets down to individual users or devices. This allows sensitive resources to have a high level of security.

Port-forwarding and NAT: Benefit from static, source, and destination-based port forwarding, as well as Network address translation (NAT).

Secure Web Gateway: Protect employee web usage with category filtering and network level malware protection that prevent access to unwanted and unsafe sites

- advanced web filter with SSL inspection
- write rules for web categories, keywords and specific websites
- Web categories and blocking pages can be customized
- 30 predefined web categories with frequent website list updates
- Detailed web access logs at user level

Safe Browsing: Protect users from malware, phishing, and malicious sites from wherever they may encounter it (any device, application, protocol or port):

- Malicious software including drop servers and compromised websites, including drive by downloads and adware
- Fraudulent phishing websites that aim to trick users into handing over personal or financial information
- Command and Control botnet hosts
- Sites which serve files or host applications that force the web browser to mine cryptocurrency
- Parked sites & domains that may no longer be controlled by the original owner

Dark Web Monitoring: All user and system administrator email addresses are checked in the dark web to see if they have been part of a breach or disclosure.

- Ability to use in zero trust sign-in policies to challenge the sign-in to the Timus network with MFA
- Emails are checked on the dark web every 12 hours for all accounts. When a breached email is detected, a warning sign is present next to the names, and details of the breach can be seen by clicking that sign.
- Further alerts and notifications are nearterm roadmap items

Device Posture Check (coming soon) Timus continuously checks the security posture of the devices and will let you enforce policies depending on their posture. Checks will be performed through Timus Connect agent, as well as the endpoint protection products like Windows Defender, SentinelOne, and Bitdefender.

Productivity/Activity Tracker: Do a deep dive on activity by identity, including most used apps and overall usage. Ability to do custom productivity reports coming soon.

Centralized Client Administration

Timus was built to make it easy for MSPs to deploy, onboard, and manage multiple clients from a single pane of glass.

Multi-Tenant MSP Partner Portal: Easily deploy, manage, and monitor all your clients from a single pane of glass centrally.

User-friendly admin UI: From rule creation, automation, and firewall policies, Timus was built to be intuitive, fast, and easy to use, even for non-experts.

Access logs: Monitor and export access logs by users and devices.

Threat analytics: See suspected threats and malicious activity in the admin console.

Automated reporting: Set up filtered views of activity and get automatic reports on a schedule of your choice.

Slack and Telegram notifications: Timus integrates with Slack and Telegram, allowing for instant notifications for critical events

User login data: User login information can be exported to Google Sheets for analysis and time-tracking purposes.

User Management: User accounts can be created locally, or through identity, like Microsoft Active Directory, Microsoft Entra ID (Azure AD), Okta, and Google Workspace..

Audit-records: Admins can pull detailed records and traffic information for auditing or investigation purposes.

HOW OUR MSP PARTNERS ARE DEPLOYING TIMUS FOR THEIR CLIENTS

Timus Networks

The Network Security Platform for the Cloud Era

Timus offers a 100% cloud-based zero trust network security solution for MSPs and their clients. In addition to some obvious use cases such as utilizing Timus to replace traditional VPNs with a solid zero-trust secure remote access, MSPs are finding ways to get the most out of the Timus Solution. MSPs especially love that the available use cases are accessible through not only a single vendor, but via a single product, the Timus Solution.

Replacing VPNs with Timus

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 replaces VPNs with a solid zero-trust secure remote access in which not only the credentials are verified but also the identity of the user (via a powerful contextual policy engine at the dedicated Timus gateway)

MSP Partner | Case Study

One of our MSP Partners deployed Timus 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 Gateway. This ensured that no one could access the PaaS tool without getting zero-trust verified by Timus first.

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

Timus fits perfectly into an MSP's cybersecurity bundle, allowing for a layered security offering that includes on-prem FW, EPP, SASE, EDR while having a fixed monthly cost that they can add a margin onto.

Control Client Network 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 visibility to all employees and devices, it makes sure everyone can access 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, DNS filtering, Dark Web Monitoring, Activity Tracking, Static Dedicated IP to allowlist apps, Cloud-FW.

Replace Desktop as a Service
With Timus, you might be able to replace existing tools such as Azure VDI and Citrix

RDP Replacement
If clients are using RDP (Remote Desktop Protocol) to access files remotely, this can be replaced with Timus that is highly secure, easy to deploy and manage.

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

Static IPs and Secure Web Gateways
Timus provides a Secure Web Gateway for custom category filtering along with an adaptive cloud firewall that protects data and apps while allowing employees to access data from a single, static IP address.

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.

Productivity Tracking
With remote/hybrid working environments, employers might be worried about the productivity of their employees. With Timus giving deep visibility into a client's network, MSPs can utilize the Productivity tracking feature to create custom reports on the productivity of endpoints (customizable definition of "productivity").

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.

Questions?

If you have questions about Timus features and capabilities, please reach out to our team at **business@timusnetworks.com**

timus

timusnetworks.com

About Timus

The Network Security Platform for the Cloud Era.

Companies struggle to meet the network security demands of the cloud era; balancing easier remote access with stricter cybersecurity requirements.

Timus Networks helps companies orchestrate secure access regardless of location and device while protecting the network against cyberattacks.

Timus is the only MSP-focused network security platform combining secure, zero-trust network access with an intelligent cloud firewall that adapts to user risk profiles and blocks threats in real time.

Built by firewall experts with decades of cybersecurity experience and praised by customers and industry thought leaders, Timus is the answer to the network security needs of the cloud era.