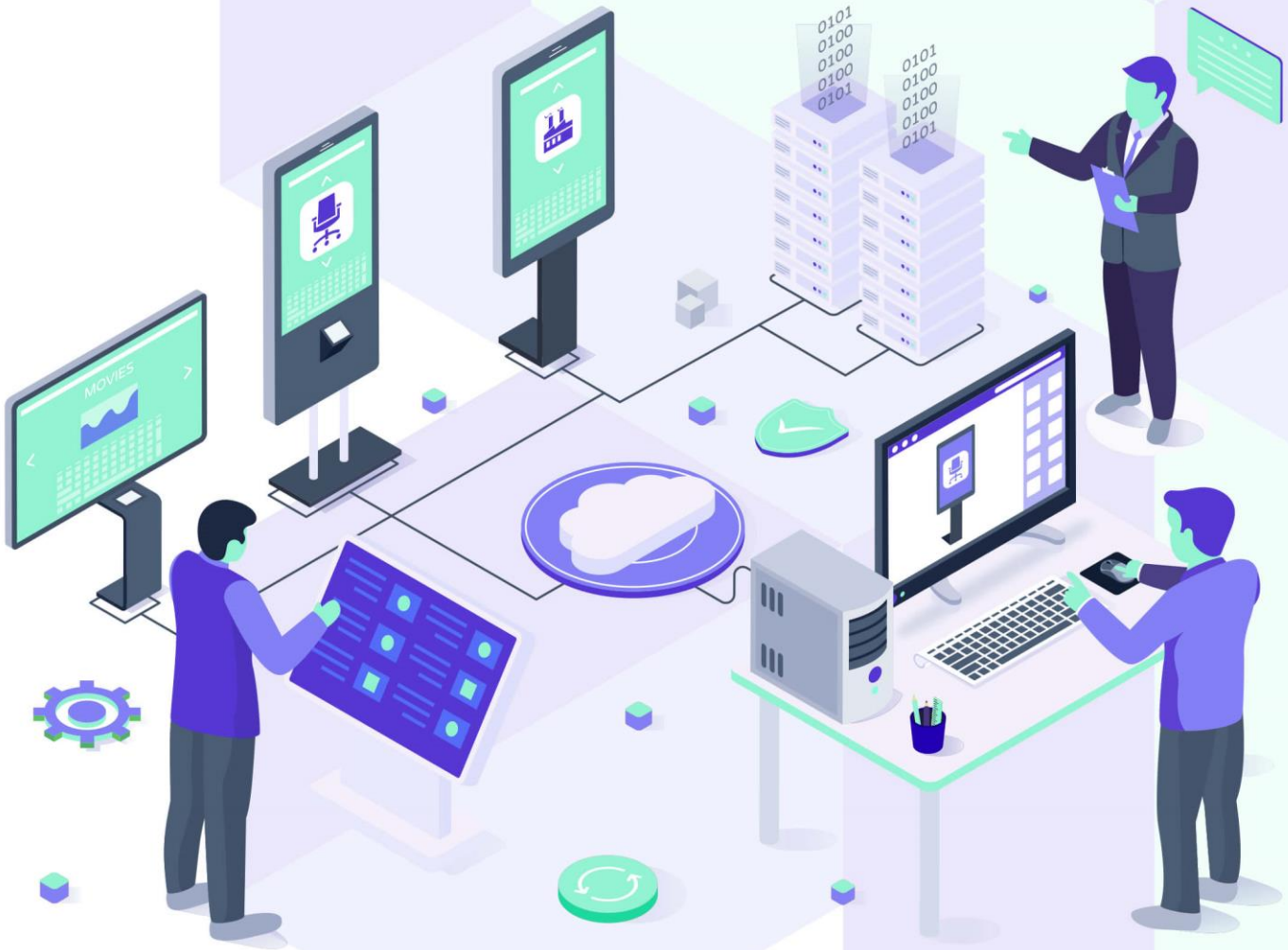
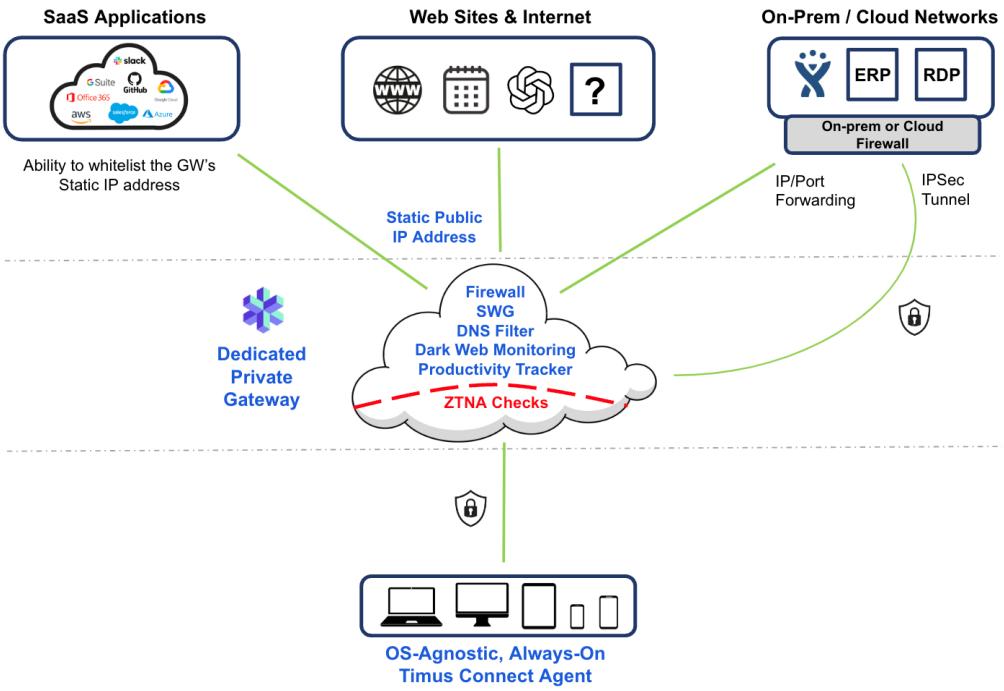
timus

# Technical FAQ



## Q. How does the high-level Timus architecture for a Client look like?




## Q. How does Timus help us against ransomware & phishing attacks?

Timus uses zero-trust secure remote access and least privilege principles before granting any access to the network and data to protect against hackers, criminals, and ransomware. Additionally, Timus uses a best-of-breed DNS filter (at the network level) protecting users from zero-day threats and malicious sites from wherever they may encounter it (any device, application, protocol or port). A user is protected against all of the below:

- 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
- Domains which have been registered in the last 30 days and in the last 24 hours

- Parked sites & domains that may no longer be controlled by the original owner

**Q. What intelligence services are utilized by Timus for better protection?**
Timus uses best-in-class intelligence services for better protection. Intelligence data is used in firewall rules, ZTNA policies and logs. Some examples include:

- IP address intelligence for users' public IP addresses to see if they are part of abusive activities, a proxy or TOR network, a botnet, etc.
- Geo-location intelligence for users' location
- Malware, ransomware, phishing and many other suspicious domains
- Dark web monitoring for users' and administrators' email addresses daily to see if they are breached

**Q. How does Timus ZTNA improve security?**
The Timus solution is superior to traditional VPNs for secure remote access. User verification is hardened with behavioral and contextual analysis. Multi-factor authentication (MFA) can be deployed adaptively (ie. when signing in from a new device, new country, etc), improving user experience. Timus ZTNA can work with another IAM solution or standalone. Timus has one of the richest behavioral checks in the industry for Zero Trust Verification.

**Q. What is the maximum number of firewall rules we can create on your platform?**
There is no limit on the number of firewall rules that can be created.

**Q. How many site-to-site tunnels can we create?**

The number of gateways that you can create are dependent on your Timus plan, but the number of tunnels associated with the gateways are **unlimited**. You can build tunnels to as many sites as needed.

**Q. Does Timus provide shared or dedicated gateways?**
Timus provides dedicated gateways with static IP addresses. An MSP can whitelist the Static IP in SaaS applications for controlled access and security.

**Q. Is there a limit on the amount of traffic passing through Timus gateway?**
No, traffic passing through the gateway is not limited.

**Q. Is there a limit on the bandwidth of traffic passing through Timus gateway?**
Bandwidth through the gateway depends on your Timus plan. There are 500 mbps and 1000 mbps options.

**Q. Can we create custom web categories and use them in firewall rules?**
Yes. Timus has 30 pre-defined web categories with frequent website list updates that can be used in firewall rules to allow/deny access. You can also create custom categories with your own website lists and keywords. Timus also provides detailed web access logs at the user level.

**Q. How long do you retain logs?**
Depending on the pricing plan, we will retain logs for either 15 or 30 days.

**Q. Do we still need to have an EDR solution if we use the Timus platform?**
While Timus provides a suite of security services attached to our gateways, our domain is primarily in network security, with a very light-weight, OS agnostic agent installed on the device. Timus recommends that you maintain endpoint security in your stack in unison with our network security to provide a holistic protection of your customers' devices and resources.

**Q. How do we download Timus Connect agent?**
Download links to Timus Connect application are available in the following places:

- Inside Timus management portal manage.timusnetworks.com, Manager->Settings->Downloads page. Admins can access here.
- Inside my.timusnetworks.com user portal Downloads page. Users can access here with their Timus credentials
- Inside Timus Networks web site timusnetworks.com, Resources page Documents & Downloads section.

**Q. Which tunneling protocols are supported by the Timus Connect agent?**

WireGuard and OpenVPN tunneling protocols are supported.

**Q. How does split tunneling work?**
The tunnel for secure connections can be configured to pass all user traffic, or just part of it, through the tunnel. Split tunnel configurations can be created in the Manager->Settings-Tunnel Configuration page. Default configuration is all traffic passes through the tunnel. Timus Connect agent gets the tunnel configuration valid for the user and context, and passes traffic through the tunnel accordingly. This feature is currently available only for Windows and macOS releases of the Timus Connect app.

**Q. Can we manage Timus Connect agent settings centrally?**
Yes. Agent profiles can be created in Timus Manager. Settings can be configured as only the admin can edit, or users can edit as well.

**Q. How is the Timus Connect app updated?**
When a new update is available, the Timus Connect application will automatically notify you that there is an update, along with a button to start the update wizard.

**Q. I have to periodically send out reports to my CTO regarding network traffic and utilization. Can I use your platform for this?**
We allow organizations to send out automated reports on a scheduled basis. These reports can be shared to whomever is required to view this information. All you need to do is provide their email address and the reports will automatically be sent out at a time of your choice.

**Q. I work with healthcare providers and credit card companies. Are you HIPAA or PCI DSS compliant?**
We are **SOC 2 Type 2** and **ISO 27001** compliant today, but, because we are not storing patient or consumer data, we do not need to be compliant as such. However, our platform can be used to enable compliance for our customers with our granular access and zero-trust controls.

**Q. How many users are supported comfortably on your platform?**
We can support about 100 users per gateway, depending on the traffic of the users. Of course, adding more than one gateway will optimize the experience and allow for more users. This will also further facilitate remote work as more gateways in more regions will minimize latency and increase available bandwidth.

**Q. How can we reduce latency and have redundancy for gateway connections?**
To reduce latency, you should have gateways close to your users as much as possible. Thus select the datacenter region accordingly while creating a site in Timus Manager.
You can have multiple gateways for redundancy. Users can be allowed to access all or some of the sites. Timus Connect agent can be configured to connect to the gateway that has the fastest round-trip time, which means the fastest gateway connection to the user.

**Q. How are ZTNA policies prioritized?**
Only one policy will be valid for each sign-in attempt, and that will be the most specific policy with respect to the source items selected.

Policies within Timus' Zero Trust Network Access (ZTNA) security framework are automatically prioritized from specific to general. More specific policies take precedence over general policies. The most specific policy with respect to the source items has the highest priority.
For example, if there is a specific policy that denies access to a specific user and a general policy that allows access to all users, the specific policy will take precedence, and the specific user will be denied access.

**Q. I only want to be alerted of mission-critical sign-ins. How can I limit what is blowing up my inbox?**
When creating a user sign-in policy, select the Alerts and Notifications tab and select Notifications. You can select a higher severity for notifications, so that you are only notified when something our system has determined to be high-risk has occurred.

**Q. Which MFA methods are supported?**

- MFA with an authenticator app like Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile.
- MFA with email. A one-time code is sent to the user's email address.

**Q. How do we set MFA policies for users or administrators?**

MFA policies are set within ZTNA policies, both for users and admins. MFA can be configured adaptively based on certain behaviors like new devices, new country, etc. If no behavior is selected, MFA is applied to all sign-in attempts.

**Q. I want to create a global rule to block all users from accessing certain websites. What should be selected as the source?**

Our dynamic firewall can be used in a couple of ways to create global rules.

1. The source can be set to IP: Wireguard Client Subnet or IP: OpenVPN Client Subnet
2. A **team** can be created that includes all users within Timus and it can be used as the source.

**Q. If I am using my identity provider to sync users into Timus, will new users created within Timus also backwards sync into my IdP?**

Identity integrations use your chosen IdP as a single source of truth. For this reason, two-way syncing can become messy, especially if more than one IdP is added to the SDN. If you need to add a new user into your IdP, it is required that the user be added from the IdP. From there, the user will be synced to Timus.

**Q. I have several on-prem file shares and web servers that I need to have access to. Can I use your platform to enable remote access to them?**

By utilizing the firewall functionality with IPSec site-to-site tunneling to on-prem environments, you can enable granular remote access to your resources by connecting the edges of the two networks and forwarding RDP or SSH traffic to the relevant devices.

**Q. Are there any integrations available?**

User synchronization & SSO

- Active Directory

- Microsoft Entra ID(Azure AD)
- Google Workspace
- Okta

Communications

- Slack
- Telegram
- Google Sheets

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.