



## Why do you need NordLayer?

NordLayer is a flexible network access security solution designed for modern businesses. Built by cybersecurity leader Nord Security, it addresses the scaling and integration challenges organizations face when implementing secure remote access.



NordLayer offers a comprehensive approach to cybersecurity that is both simple to implement and scalable. Our solution focuses on three key areas:

**Internet Access Security** protects employees from online threats by securing public Wi-Fi connections, enabling access to geo-restricted content, and masking IP addresses for enhanced privacy.

**Network and Resource Access Management** provides granular control over company resources, allowing for network segmentation and facilitating secure remote access to devices, networks, and cloud platforms.

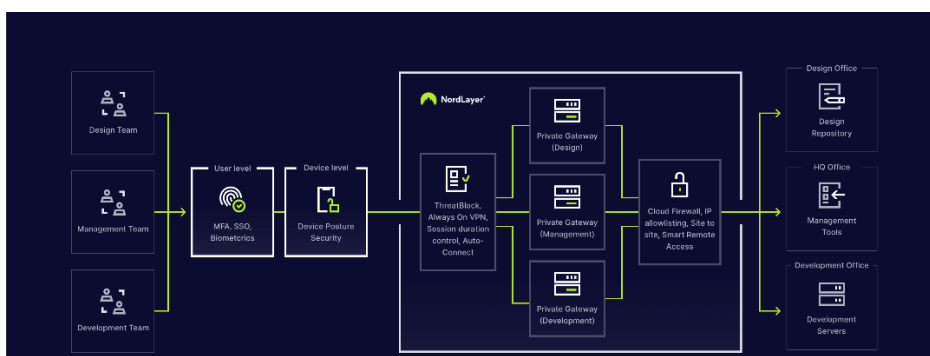
**Compliance** support helps organizations meet regulatory requirements through visibility into network activity, user behavior, robust identity and access management, and encrypted data transmission.

## How does it work?

NordLayer uses strong authentication, including multi-factor verification, to protect access to company network. By segmenting networks and assigning specific permissions based on roles, NordLayer ensures that only authorized users can access necessary resources. Additional security measures like biometrics and device checks further strengthen protection.

Once authenticated, users access company applications through NordLayer's secure tunnel, which encrypts all network traffic. The platform's granular control over user permissions and network segmentation maintains strict security while enabling seamless employee productivity.

Essentially, NordLayer combines robust authentication, granular access control, and encryption to protect company data and provide secure access for employees.





### **Secure access to the NordLayer application**

Once you've safely logged on to your device, secure logins must be used to gain access at the application level. NordLayer's multi-factor authentication features like 2FA and Single-Sign-On (SSO), enable the first layer of secure protection for users when using the service:

- **Strengthen security** — Having a second identification level drastically reduces the risk of malicious users gaining access to your devices or sensitive information.
- **Keep remote workers safe** — Multi-factor authentication allows employees to access company resources from any device with complete safety, whatever their location.
- **Limit unnecessary admin** — Responsibility of password management is removed from IT admins with users able to do this themselves.

### **Implement team and user policies**

Using NordLayer, you can build teams for [network segmentation](#), assign user permissions, and create gateways based on employee trust level.

- **Increase access limitations** — Creating team gateways allows users to only access specific network resources they need to fulfil their roles and nothing more.
- **Improve visibility** — NordLayer gives you full insight into who and what is accessing which areas of the company network.
- **Implement Biometrics at this point for additional security** — fingerprint or face ID verification. NordLayer can also detect jailbroken or rogue iOS devices.



### **Hide data and manage user activity**

Connect to company applications, resources and data via a NordLayer secure tunnel. The tunnel works to encrypt transferred data and network activity from any unknown and untrusted users.

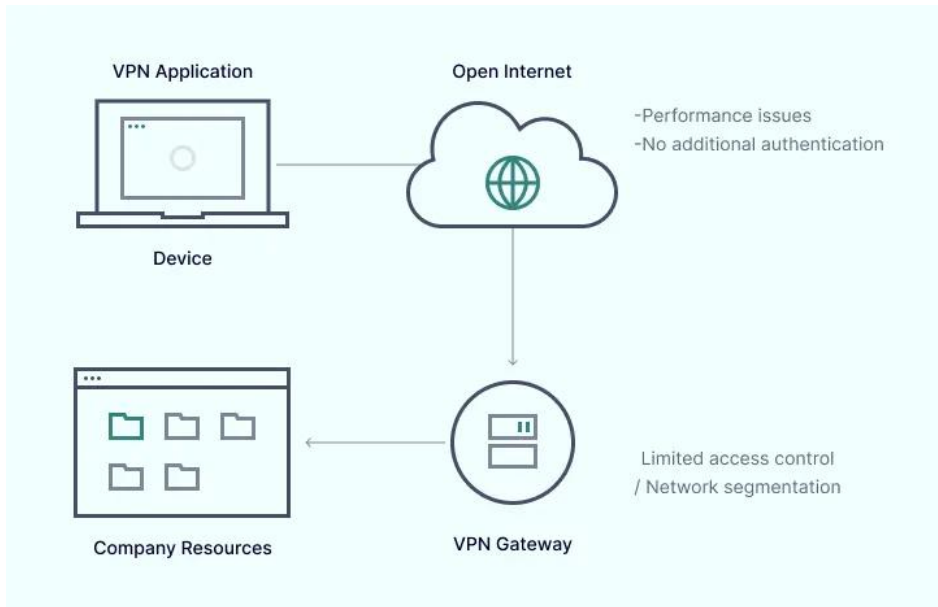
- **Hide activity** — Through NordLayer’s military grade encryption, all activity on the network remains invisible to users outside of the network perimeter.
- **Protect transferred data packages** — With all data and activity hidden, the likelihood of data being intercepted or leaked is significantly reduced.

### **Gain complete access control**

Network segmentation is ensured with users assigned to specific gateways — each with unique team access permissions. Using NordLayer’s IP allowlisting also enables admins to set specific user permissions so users can only access the resources relevant to their job role.

- **Permission-based access** — Set user permissions based on employee trust level, to make sure their permissions stretch to what they need to access to fulfil their work.
- **Trusted users only** — Create a bespoke allow list with trusted user IP addresses to granulate access permissions and segment areas of your network.

## Without NordLayer



Many legacy solutions handling the needs of a business network may now be unfit for purpose by today's [cybersecurity](#) standards — often having limited capability and running at suboptimal performance. Without the protection and adaptability that NordLayer provides, your company could unknowingly be leaving the network underperforming, and your data and resources vulnerable to exposure.

- **Lower speed & reliability** — A personal VPN utilizes a single tunnel to handle all user traffic. For businesses using this service for all employees, performance issues will occur including reduced speed and increased latency.
- **Increased visibility** — Legacy VPN gateways are public. Therefore, they have a higher risk of being exposed to malicious attacks. Businesses can mitigate this risk with a more advanced network access solution, which hides dedicated gateways from outside users.
- **Difficult to scale & maintain** — Modern network access solutions like NordLayer are quick to install and manage. Without features like a centralized Control Panel, and easy license transferability, managing and scaling users across the business becomes an unnecessary obstacle to overcome.

Combining layers of protection into one easy-to-use solution - NordLayer - provides businesses with all of the tools to achieve complete network security. Built on [Zero Trust principles](#), NordLayer security solutions help organizations of all sizes to fulfill scaling and integration challenges when building a modern [secure remote access solution](#), within an ever-evolving [SASE framework](#).