NordLayer®

Transforming remote access with multi-layered security

NordLayer is an adaptive network access security solution for modern businesses — fromthe world's most trusted cybersecurity brand, Nord Security.

We 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.

Quick and easy to integrate with existing infrastructure, hardware-free, and designed with ease of scale in mind, NordLayer meets the varying growth pace and ad-hoc cybersecurity requirements of agile businesses and distributed workforces today.

NordLayer makes it easy for businesses to:

Start

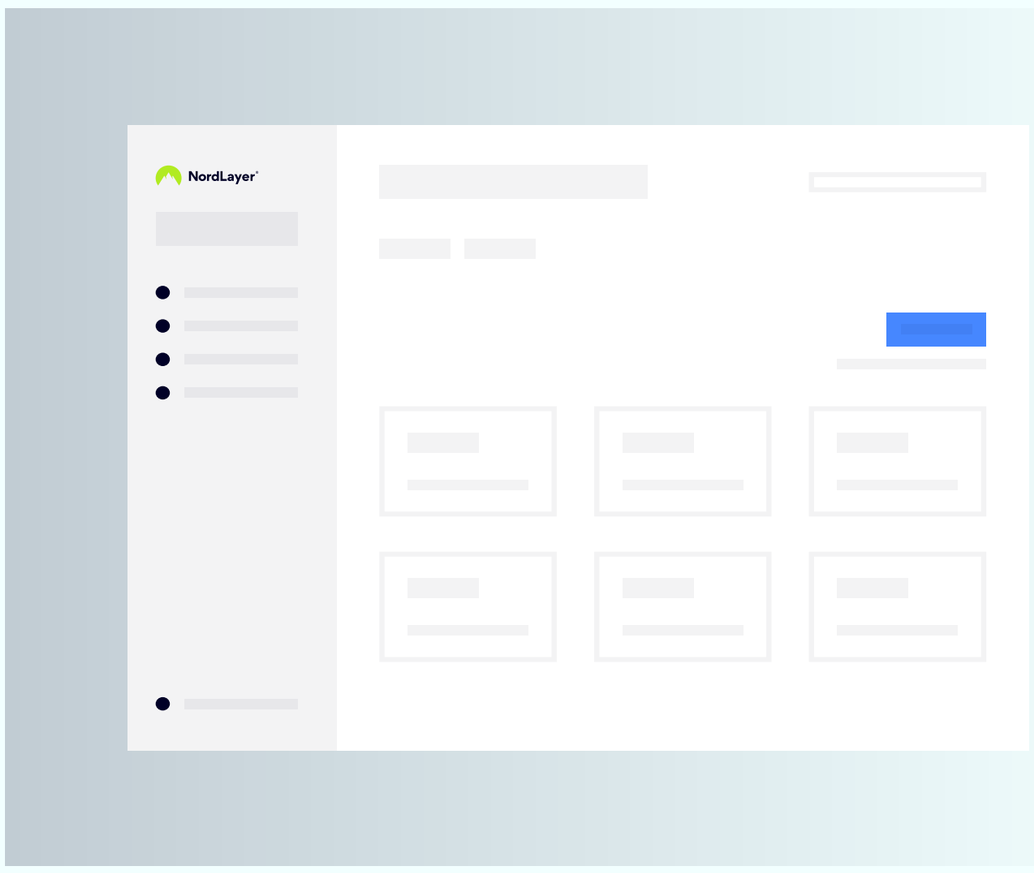
We provide the foundation for network access security for businesses of any size — offering a low barrier to entry with robust capabilities & performance

Combine

We understand that one size doesn't fit all businesses — we offer adaptive security solutions that integrate with a multitude of operating systems and cloud apps

Scale

We provide the perfect platform for sustainable and unpredictable growth



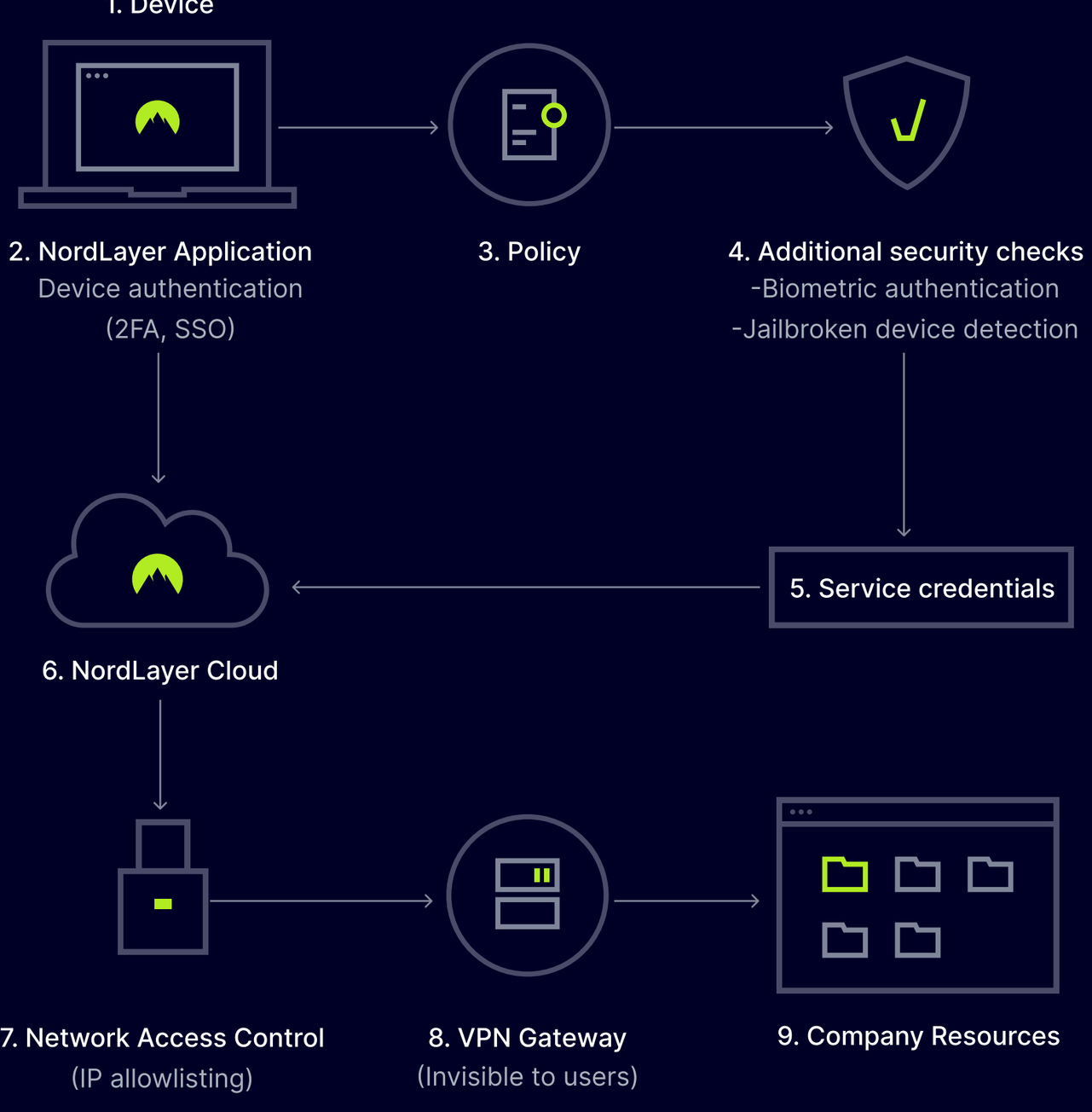
One of our core offerings is an advanced VPN that's been designed specifically with businesses in mind, and provides a number of benefits that differentiate it from a personal VPN.

Business VPN

When do you need it?

Business VPNs enable employees working remotely to securely access a company's resources. It also allows organization leaders to control user access to certain information and even monitor their service activities from a centralized control panel.

How does NordLayer work?



Device

Use a secure authentication method to log on to your device.

Application

Use secure logins to access the NordLayer app and set up multi-factor authentication (2FA, SSO).

Policy

Build teams for network segmentation, assign user permissions and create gateways based on employee trust level.

Further measures can be enabled at this stage such as Biometrics, for additional verification. NordLayer will also detect jailbroken / rooted iOS devices on the network.

NordLayer Cloud

Connect to work applications via a NordLayer secure tunnel, encrypting activity from those outside of the network perimeter.

Network Access Control

IP allowlisting enables admins to set specific user permissions so users can only access the resources relevant to their job role.

VPN Gateway

Network segmentation is ensured with users assigned to specific gateways — each with unique team access permissions.

Complete Network Security

Access permissions are granulated by IP address — based only on what the user needs to do their job and nothing more.

Benefits of a business VPN

Here's a closer look at some of the business VPN use-cases and benefits to companies:

Enable remote access

Nobody expected remote work to become a new norm almost overnight. The possibility to work from homes, cafes, co-working spaces, and hotel rooms in various destinations has allowed us to have more freedom and flexibility. For many of us, remote work proved to be pleasurable and productive. But it brought along new challenges, including increased risks of cyber-attacks. For example, your employee, working from a cafe, may expose your company's data to bad actors simply by connecting to a corporate network via public Wi-fi.

Business VPNs enable remote access by creating an encrypted data tunnel between a remote worker's device and the company's network, leaving no chance for a hacker to decipher the data — even if they are lucky enough to steal it. That way, remote workers can securely access their company's intranet, emails, applications, and other multi-cloud resources from anywhere in the world.

Avoid data breaches

Data breaches can be devastating to both small and large companies. They not only result in financial losses but may seriously damage a company's reputation and even put it out of business completely. 44% of customers would stop buying from a company that fell victim to a cybercrime. Last year, data breaches cost companies an average of 3.86 million dollars, 40% of it due to lost business.

You can protect your company by using a strong password management tool and setting permissions that allow users to access certain data and apps, rather than the entire network. A business VPN enables you to manage employee's devices centrally. If you are looking for specific functionalities, NordLayer can provide you with custom solutions.

Manage member access

Some business VPNs provide the possibility to buy dedicated servers with static IP addresses assigned solely for your use. NordLayer does this to ensure flexibility, security, and access control. It allows an organization's admins to create various teams and gateways as well as assign specific servers to specific users. Allow-listing IP addresses helps to filter unauthorized access and segment network access. This means that certain teams can only access the specific resources that they need to do their job.

Access home content from anywhere

Some regions have internet restrictions and can cut you off from accessing tools and services needed for work. Fortunately, a VPN has the power to unblock the content regardless of your location.

So, next time you go abroad on a business trip, use a business VPN to bypass geographical restrictions. By connecting to a VPN server closer to your home country, you can make it appear as if you are in an unrestricted area and regain access to all needed documents, databases, and services.

Advanced secure remote access solutions

Some providers, such as NordLayer, offer much more than just secure access to a company's internal network. Our advanced secure remote access solutions include secure internet browsing, DNS filtering, malware protection, access to private networks/apps, and more. As an alternative to traditional VPN, we provide a cloud-based VPN that doesn't require infrastructure on a user's endpoint and can be deployed in just a matter of minutes.

Personal VPN

When do you need it?

A personal, or consumer VPN is a service designed for securing your own devices and online activity outside of work. One in four internet users have utilized a VPN at least once. Common reasons to use a personal VPN are mostly to protect data online, enjoy more privacy, and access global content.

Here's a detailed rundown of the main reasons to have your own VPN service for personal use:

Safely connect to public Wi-fi

Every café, airport, and shopping mall offers public Wi-fi but connecting to it might be risky. That's because cyber-criminals may be peeping at your internet traffic intending to empty your bank accounts, steal your login details, or even identity.

When you enable VPN on your laptop, smartphone, or tablet, your internet traffic is encrypted, making it inaccessible to criminals or anyone else. The encryption provided by VPN helps secure your online activities, from sending emails to checking your account balance and shopping.

Unlock content

Some content is only available in specific regions. For example, you may realize that your favorite social media, gaming platform, or news site is not available in the country you've traveled to. To avoid such disappointments, you can click on a VPN server close to your home and enjoy the content as if you've never left. That's because the sites you want to access will see the IP address of the server you're connected to, and not your real one.
And who doesn't love a good deal? As an extra bonus, a VPN can help you save money on things like plane tickets, hotel rooms, and car rentals. Often, the prices increase because the website knows you have checked their product before. Next time you're buying something online, try connecting to various server locations to find the best deal.

Browse privately

Every time you go online, your internet service provider (ISP) ensures you have an internet connection. As all your web traffic goes through their servers, the ISP can see everything you do online, and share this information with advertisers, corporations, and governments. A secure VPN prevents your ISP from tracking your online moves so you can browse the internet privately.

NordLayer® Business VPN **vs** NordVPN® Personal VPN

As already mentioned, one of NordLayer's key offerings is a VPN specifically designed for business use. The table below highlights the key differences between the two types of VPN as well as the benefits for companies using NordLayer over a personal VPN.

NordLayer Business VPN	NordVPN Personal VPN
Business use	**Personal use**
Protects your company's network and enables workers to safely access the company's resources while working remotely. Secures all internet traffic with powerful encryption. Provides next- generation VPN solutions.	Creates an encrypted tunnel for online traffic so nobody can get their hands on your internet data. Provides peace of mind when using public Wi-fi and keeps your browsing history private.
Centralized billing	**Individual subscription**
Centralized billing means you won't have to arrange a payment every time a new user joins – it will be done automatically.	Each customer pays for their own user license.

Multiple users

Covers the needs of an entire organization. All employees can get access to a VPN and securely reach their company's resources, from any location. Every user can secure up to 6 devices. Licenses, dedicated servers, and company gateways can be added as the organization grows.

A single user

Designed for an individual user. Can secure up to 6 devices at the same time, on all major operating systems.

Users are managed centrally

The owner of the organization creates an account and invites their colleagues to join. Via the Control Panel, he/she adds more members, assigns them rights, and creates teams.

Core and Premium plan holders are able to set up private gateways and dedicated servers. They can see which gateways and devices the members are using and audit all Control Panel actions made by them and other admins.

Settings such as biometric authentification, SSO and 2FA can also be enforced and implemented centrally — so that layers of protection are mandatory for staff.

Personal use

You have complete control over your account.

Dedicated server option

You can purchase dedicated servers with static private IP addresses, allow-list the IPs, and create gateways for convenient access control. A dedicated server ensures a more stable performance because it's not shared with any other organization.

Dedicated IP option

You may use a shared IP or purchase a dedicated IP solely for your use. A dedicated IP is less likely to be excluded from certain websites, enables you to avoid CAPTCHAs, and makes online payments easy.

Two-factor authentication and Single Sign-On

A team member can use their existing credentials to log in to the app with Azure AD, Google, and Okta.

Two-factor authentication is also available and can be enforced for the whole organization.

Two-factor authentication

You can protect your account with an extra layer of security by setting up 2FA.

As you can see, you need a personal VPN to protect your data online, have more privacy, and access global content. But using a personal VPN won't cover the complex needs of an organization and won't provide you with benefits such as scalable user license management, Single Sign-On, and centralized settings or billing.