NORD SECURITY
Business Suite

Partner Sales Playbook

Welcome to your journey with Nord Security

This essential guide, packed with tools and insights, is designed to help you sell our cybersecurity solutions effectively.

Your navigation map:

1. Cybersecurity market overview
2. Nord Security Business Suite
3. Use cases
4. Ideal Customer Profile (ICP)
5. Industry talking points to start conversations
6. How to spot the right customers
7. Winning statements in the market
8. Handling objections
9. Client testimonials

① Cybersecurity market overview

Here's a quick glance at the key trends and financial impacts of cyber-attacks in 2024. These numbers highlight the critical challenges in today's cybersecurity landscape.

$ 4.88M

The global average cost of a data breach in 2024

$ 5.2M

The average cost of a ransomware attack

1 billion

Records stolen globally

46%

Breaches involving customer data

292 days

Time to detect and contain breaches with stolen credentials

68%

Data breaches caused by human error (e.g., phishing)

65%

Manufacturing companies hit by ransomware in 2024

Sources: IBM report 2024; Verizon report, Sophos

② Nord Security Business Suite

User-first cybersecurity suite

Created for security, designed for productivity

20,000+	**10+**	**$3B**
businesses protected worldwide	years in the market	valuation - the official Unicorn

Nord Security is one of the world's leading cybersecurity solutions providers. Designed to meet the needs of a digital workforce, the Nord Security business suite brings together:

NordLayer®

A toggle-ready network security platform with Zero Trust access and real-time threat detection so customers can protect hybrid teams and keep attackers out.

NordPass®

An end-to-end encrypted credential manager that lets teams store logins securely, eliminate sprawl, and control access from one place.

NordStellar®

A threat exposure management platform that helps detect leaked credentials and vulnerabilities and stop breaches before they happen.

How Nord Security products work together for comprehensive business security

Step 1

NordStellar®

for threat intelligence

NordStellar detects:

- Leaked business data
- Cybersquatting
- External vulnerabilities
- Data exposure

Step 2

NordPass®

as a credential manager

NordPass secures:

- Credentials
- Unmanaged access
- Shared accounts
- Shadow IT management

Step 3

NordLayer®

for network access control and endpoint security

NordLayer:

- Allows access to your resources only from a dedicated IP
- Improves network and endpoint security

Step 4 24/7 threat **NordStellar** monitoring

3 Use cases

Learn how three products solve four common SMB challenges, so you can match the right solution to each client's needs.

Protect remote and hybrid teams

Use case by product

NordLayer®

Employees connect via unsecured networks (public Wi-Fi / Home networks)

NordPass®

As teams grow, access control must scale with clear policies and role-based permissions

NordStellar®

A growing digital footprint introduces new domains and assets that must be monitored for threats

Problem

Employees using public Wi-Fi or home networks risk exposing sensitive data to hackers

Solutions

NordLayer®

Enables secure remote access across global sites with flexible server options and site-to-site connectivity

NordPass®

Manages all company credentials centrally and applies policies by the team after deleting the employee's account

NordStellar®

Monitors the expanding attack surface for any threats or vulnerabilities that could harm the business

Support compliance efforts

Use case by product

NordLayer®

Sensitive systems need secure access controls like IP Allowlisting and 2FA

NordPass®

Businesses must enforce password policies to meet standards

NordStellar®

Vendors and third parties introduce supply chain risks that must be monitored

Problem

Businesses must meet strict compliance standards for access, credentials, and third-party risk

Solutions

NordLayer®

Provides Dedicated IPs and 2FA to secure access and support compliance

NordPass®

Enforces password policies by role using the Password Health tool

NordStellar®

Monitors the dark web to detect exposed partner or vendor data before it becomes a breach

Control unmanaged devices and accounts

Use case by product

NordLayer®

Unmanaged devices need secure access to cloud-based company resources

NordPass®

Cloud apps are accessed by temps or freelancers with reused or untracked credentials

NordStellar®

BYOD and personal accounts increase the risk of infected devices and data leaks

Problem

BYOD and temp hires create gaps in access control and device security

Solutions

NordLayer®

Applies endpoint protection, device visibility, and traffic filtering to secure unmanaged devices

NordPass®

Tracks all credentials under the private account and retains all data, even after offboarding

NordStellar®

Monitors the dark web for malware-infected devices and leaked credentials

Secure customer access at scale

Use case by product

NordLayer®

Businesses expanding across locations need flexible, cloud-ready access to internal systems

NordPass®

As teams grow, access control must scale with clear policies and role-based permissions

NordStellar®

A growing digital footprint introduces new domains and assets that must be monitored for threats

Problem

The company is scaling horizontally, or merging, creating branches, divisions and complex access needs that increase digital risk

Solutions

NordLayer®

Enables secure remote access across global sites with flexible server options and site-to-site connectivity

NordPass®

Manages all company credentials centrally and applies policies by the team after deleting the employee's account

NordStellar®

Monitors the expanding attack surface for any threats or vulnerabilities that could harm the business

4 Ideal Customer Profile (ICP)

ICP is your shortcut to selling our security services more effectively. It helps you focus on businesses that need protection and are ready to buy. Spend **less time chasing, more time closing.**

Business Suite ICP

Company size

NordLayer® **NordPass®**

Small-to-Medium Business (SMB)

10-200 employees (sweet spot)

NordStellar®

Mid-to-Enterprise

200-2000 employees (sweet spot)

Business verticals

Broad range, including:

- Finance
- Healthcare
- Education
- Legal
- Engineering & Manufacturing
- Government

Key pain points

- Rising cyber threats
- Remote work security
- Data security and compliance
- Security expertise gap

Tech stack

Remote Desktop Protocol (RDP)

Office 365

Google Workspace

slack

Product-specific ICP additions	NordLayer®
Core use case	Secure Access & Zero Trust Networking
Well-suited for clients	• Requiring secure remote access, implementing Zero Trust Network Access (ZTNA) principles, and managing complex network access controls • With a significant mobile or remote workforce and distributed infrastructure
Key characteristics and indicators	• Legacy and SaaS-based infrastructure • Multi-location organizations with remote and hybrid work setups • Reliance on cloud and hybrid resources (AWS, Azure, Google Cloud) • Need for granular access control based on user identity and device posture • Existing IP allowlisting practices • Compliance-driven companies seeking to reduce reliance on traditional VPN • Suitable for EN speakers, as the SMP is available in English only

Product-specific ICP additions

NordPass

Core use case	Business Password Manager
Well-suited for clients	• Prioritizing password security and simplifying password management for all employees • Handling sensitive data, facing stringent compliance requirements, and looking for a user-friendly yet robust solution
Key characteristics and indicators	• High employee turnover rate • Businesses handling highly sensitive data (e.g., financial information, healthcare records) • Compliance requirements (e.g., GDPR, HIPAA, PCI DSS) • Organizations seeking to improve password hygiene and reduce the risk of data breaches • Companies frustrated with existing password management solutions • Marketing materials and MSP Admin guide are available in EN, DE, NL, FR, IT, and ES. The MSP Admin panel is available in English (EN)

Product-specific ICP additions

NordStellar

Core use case	Managed Detection & Response (MDR)
Well-suited for clients	• In need of advanced threat detection and response capabilities, regardless of whether they have internal IT security teams or not • Facing sophisticated cyber attacks, requiring 24/7 security monitoring, and needing expertise to manage complex security incidents
Key characteristics and indicators	• Dedicated IT security teams with in-house expertise or without any IT team within the client's company • Proactive approach to threat hunting and incident response • Significant IT security budget • Focus on regulatory compliance and data protection • Complex IT infrastructure with multiple layers of security • Concerned about advanced persistent threats (APTs) and targeted attacks

5 Industry-specific talking points

Focus on what matters most to each industry. These key talking points help you show how our solutions solve their unique challenges and drive success.

Healthcare

Ransomware is a growing threat

It hit 67% of healthcare organizations in 2024.

HIPAA compliance is complex and costly

The average healthcare data breach costs $9.8 mln.

Remote access and third parties add risks

These two factors caused 48% of 2024 healthcare breaches.

Finance

Phishing remains a primary attack vector

90% of data breaches involve phishing.

Compliance with evolving regulations

Companies need to follow regulations like NIST, HIPAA, and NIS2.

Ransomware attacks

65% of financial institutions faced ransomware attacks.

Legal

Ensuring data protection and compliance

Legal firms must meet regulations, such as HIPAA and CCPA, to avoid fines.

Protecting access to sensitive data

29% of legal firms had a breach. Secure access needs strict identity verification.

Complex supply chains

66% of legal sector breaches stem from third parties.

Engineering & manufacturing

Production lines are disrupted by ransomware

Ransomware can stop production lines in minutes, causing major losses.

Design files and blueprints are at risk

Leaked CAD files or specs can hurt a company's reputation and edge.

Vendor connections can bring risks to your factory

Supplier or partner breaches can impact you, and robust access controls are essential.

Education

Cyber-attacks are disrupting learning

66% of schools faced ransomware in 2024.

Backups alone aren’t enough

71% of schools had backups attacked, and many lost them.

Recovering from an attack is expensive

Cyber-attacks drain IT budgets and slow down operations.

Sources: Sophos report, ENISA report, Verizon report, IBM Cost of a Data Breach Report 2024, Censinet

6 How to spot the right customer

Spot high-value leads quickly and connect them with the right products. Here are the qualifying questions based on key problems Nord Security Business Suite could solve:

Problem	Questions	Keywords to watch out for	Product
Unsecured networks / remote access	How often do employees work off-site?	#Remote access	
	Do you worry about employees using public Wi-Fi?	#Unsecured networks	
	What protects data when employees are remote?	#Remote login security	
Compliance	Are you subject to any industry regulations?	#Compliance	+ +
	Do you need to audit user access?	#Auditing	+
	How do you control access to sensitive data?	#Access control, #Access segmentation	+ +
BYOD / personal devices / Contractors	Do employees use personal devices for work?	#BYOD, #Personal devices	+
	Is remote work common for temporary staff?	#Working from home, #A hybrid workplace	
	How do you secure contractor access?	#External contractors	
Scaling / Expansion	Are you planning any expansion soon?	#Scaling, #Expansion	+
	Are you migrating to the cloud?	#Migration to the cloud	
	How many remote users do you support?	#Remote users, #Global	+
Password security	Do you have a password policy in place?	#Policies	
	What prevents compromised credentials?	#Cyber threat monitoring	
	Do employees reuse passwords?	#Password protection	

7 Winning statements in the market

What to say when your prospects mention competitors:

NordLayer®

- Built by the NordVPN experts, it is a cloud-first network security platform for modern businesses
- Offers the fastest VPN with NordLynx, Cloud LAN, and Browser Extension for secure access
- Offers lag-free connectivity up to 1 Gbps with high-performance VPN servers
- Combines ZTNA, SWG, and FWaaS into a single, cloud-native SSE solution
- Seamlessly integrates with Google Workspace, Okta, Entra ID, JumpCloud, and OneLogin
- Includes a 14-day free Trial for every client
- Backed by 24/7 technical and strategic support whenever you need it

NordPass®

- Features a user-friendly interface built for fast onboarding and rapid adoption
- Provides a Data Breach Scanner that alerts clients and users to exposed credentials in real-time
- Offers transparent pricing with no hidden fees or complex tiers
- Seamlessly integrates with IAM providers like Entra ID, MS ADFS, Okta, and Google Workspace
- Built on XChaCha20, an advanced encryption algorithm
- Fast, seamless deployment means getting customers protected in minutes, not weeks
- Includes a 14-day free Trial for every client
- Backed by 24/7 technical and strategic support whenever you need it

NordStellar®

- Protects employee, customer, brand, and infrastructure with real-time threat intelligence
- Provides insights from one of the largest deep and dark web data pools, including data breaches, malware infections (infostealers), and credential lists from forums, ransomware blogs, Telegram and marketplaces
- Helps organisations meet regulatory requirements like DORA, NIS2, SOC 2, and ISO 27001
- Speeds up breach detection with 24/7 automated monitoring, enabling MSPs to act fast
- Aligns detection and reporting with real-world use cases for faster decision making
- Provides proven threat intelligence built by Nord Security, the creators of NordVPN
- Gives real visibility with complete context and details behind the incident, not just a notification
- 100+ million consumers protected with NordStellar ATO solution

8 Handling objections

How to turn your customers' doubts and concerns into dealbreakers

Objection	Handling
"Too small to care" / We are too small"	• Over 50% of breaches now affect SMBs • 60% of SMBs go out of business within 6 months of a major cyberattack • SMBs are prime targets for cyber attacks because they often lack the security infrastructure of larger enterprises
"My IT provider has it covered" / "We have antivirus software"	• Over 80% of breaches in 2024 involved threats that traditional antivirus alone couldn't stop, like ransomware or phishing attacks (source: IBM report 2024) • 43% of cyberattacks target small and medium businesses that rely solely on basic antivirus protections, making them prime victims
"Too expensive"	• The global average cost of a data breach in 2024 is $4.88 million • Spending money on security tools and staff costs much less than paying to recover from an attack
"We use strong passwords. We are fine"	• 81% of breaches in 2024 involved compromised or stolen credentials (not just weak passwords, but phishing or password reuse) • Even the strongest passwords can be bypassed without multi-factor authentication (MFA). Companies using MFA reduce breach costs by up to $1.5 million

Sources: Sophos report, ENISA report, Verizon report, IBM Cost of a Data Breach Report 2024, Censinet

9 Client testimonials

Use real-world examples to win trust and prove our products work.

NordLayer®

“With NordLayer, you don’t have to care how fast your team scales. No extra network security technical integrations are required when a company expands.”

whatagraph - A data analytics company

Read more

NordPass®

“And at the end of the day, thanks to NordPass, I forget about passwords and don’t remember them because they are too complex, so how can anyone else know them?”

esken - A media & entertainment company

Read more

NordStellar®

“Cyber threats today are relentless, and many solutions simply don’t go far enough. But NordStellar stands out. NordStellar’s dark web monitoring, instant alerts, and advanced threat detection go beyond the basics, equipping businesses with tools they genuinely need to stay ahead.”

cybernews® - An independent media outlet

Support channels

For product documentation and guides, explore:

NordPass Help Center

NordLayer Help Center

NordStellar Documentation

Need a hand?

Your Partner Success Manager is always here to support and guide you or email us via partners@nordsecurity.com