Executive Overview

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 the toggle-ready network security platform NordLayer, the end-to-end encrypted credential manager NordPass.

- Founded in 2012

- 20 000+ business customers worldwide

- 2000+ employees

- Private

Product & Service Offerings

NordLayer

NordLayer offers reliable connection, protection, threat detection, and response for businesses needing strong network security. Built on NordVPN standards, NordLayer is a trusted cybersecurity platform that integrates easily with any network and technology stack, all with unmatched support. Helping organizations to adopt FWaaS, ZTNA, and SWG principles, NordLayer is focused on the Security Service Edge of cybersecurity services.

NordPass

NordPass is an end-to-end encrypted credential manager that lets teams store logins securely, eliminate sprawl, and control access from one place while helping businesses comply with the strictest global cybersecurity standards. Using robust data breach detection, NordPass reduces the timeline between breach and discovery, saving businesses millions in losses. Store corporate credentials, passwords, and secure notes in a centralized, encrypted location.
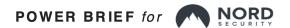
NordStellar

NordStellar is a threat exposure management platform that helps security teams monitor and protect an organization's assets in real-time. It provides 24/7 real-time visibility into external threats from the dark web and helps safeguard what matters most to your business: employees, clients, infrastructure, and brand. By combining data from different sources and gathering incident alerts in one place, the platform makes it easier for security teams to identify risks, respond effectively, and stay ahead of potential cyber threats.

Key Features & Differentiators

NordLayer

- Easy Start & Onboarding: 10-minute deployment, 24/7 support, and an intuitive interface ensure a highly efficient experience.

- Flexible Integration & Scaling: Supports all key OS versions, infrastructure, and applications, easily adapting to your existing tech stack and scaling users without stress.

- Affordable & Flexible Security: Top-notch security without breaking the bank, offering low minimum license requirements and three plans.

NordPass

- Highest Standard of Security: End-to-end encryption, zero-knowledge architecture, and certifications (ISO 27001, SOC 2 Type 2, HIPAA) ensure privacy.

- Boost Productivity & Value: Eliminates password reset time and offers 24/7 support, a simple interface, and advanced features at a competitive price.

- Future-Proof & Secure Authentication: Utilizes XChaCha20 encryption, machine learning autofill, and biometric 2FA for enhanced security.

NordStellar

- Proactive Threat Detection: Continuously monitors the deep & dark web with one of the largest data pools to identify emerging threats.

- Comprehensive Coverage & Visibility: Protects employees, customers, brand, and infrastructure with features like leaked data management and domain squatting detection.

- Compliance & Rapid Deployment: Simplifies compliance with regulations like DORA and ISO 27001, with fast setup and 24/7 monitoring.

Top Industries Served

- Other
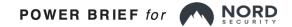
Ideal Customer Profile

NordLayer & NordPass:

- Size: SMB and SME organizations with NO MINIMUMS on customer size, generally:

- NordLayer: 10-200 employees (sweet spot); up to 500 users

- NordPass: 10-200 employees (sweet spot); unlimited number of users

- Well-suited for forward-thinking companies that want to boost cybersecurity for remote and/or hybrid users, and/or execute on cyber insurance requirements

Key characteristics:

- NordLayer: Legacy and SaaS-based infrastructure, multi-location organizations with remote and hybrid work setups, reliance on cloud and hybrid resources (AWS, Entra, Google Cloud), compliance seeking to reduce reliance on traditional VPN

- NordPass: high employee turnover rate, businesses handling sensitive data, compliance requirements, companies frustrated with existing password management solutions

- Decision-maker: Business owner/CEO, General Manager, Office Manager, IT Manager/Director, IT Administrator, Help Desk Manager, IT Security Manager/Director, IT Director, Compliance Officer, CISO, Network Administrator, Head of IT, Network Security Engineer
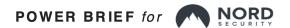
NordStellar:

- Size: Mid-to-Enterprise organizations with 200-2000 employees (sweet spot); up to 5000 employees

- 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:

    - 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

- Decision-maker: IT Security Manager, IT Director, Head of IT, CISO, Security Operations Center (SOC) Manager, Security Analyst, Incident Response Manager, It Security Director

Qualifying & Technical Questions

NordLayer:

1. How are you securing all endpoints today, especially remote workers and application endpoints?

2. Do you store any of the following data in a cloud? Clients' records, Financial information, Business and operational data, Transaction and payment date, Intellectual property or Employee personal data? How do you secure your cloud resources?

3. Are you applying security and routing policy in technology deployments, or by assigning the policies directly to the employee?

4. How are you restricting access to applications to the correct user groups? Utilizing a Zero Trust architecture for a software-defined perimeter yet?

5. 82% of companies allow BYOD (Bring Your Own Device) policy for employees with over half of those willing to say they have no way of securing those endpoints. What's your policy on BYOD and how are you securing it?

6. What other security tools are you currently using? To protect your network, your data, and enforcing credentials/password hygiene

7. What is the mixture of business-critical on-prem, cloud and SaaS applications?

8. Are you utilizing an Identity Management platform, such as Entra ID/G-Suite, Okta?

9. Do you seek solutions that could actively contribute to your company's compliance such as GDPR, HIPAA, ISO 27001, PCI-DSS, NIS2?

NordPass

1. How do you manage employee access to corporate IT resources?

2. Do you keep track of passwords for external unmanaged employee tools? How do you secure access to those tools?

3. When a new employee joins, how do you give them access to IT resources? 4. When an employee leaves the organization, how do you remove their access?

5. Do team members share logins? If so, how do you ensure shared login security?

6. Does your organization store/manage sensitive personal or client information?

7. How do you ensure password policy compliance?

8. Do you seek compliance with access control regulations such as PCI, SOC2, GDPR, UL, HIPAA, NERC CIP, ISO 27001, SSAE16?

9. Do you track website breaches where your employees log in, and how do you manage this risk?

NordStellar

1. Could you briefly describe how your organization currently manages and stores its data, particularly any data related to regulatory compliance or sensitive customer information?

2. Are you subject to any industry regulations? What are the biggest challenges your organization faces when it comes to meeting data residency and compliance requirements (like GDPR, CCPA, etc.)?

3. Do you need to audit user access?

4. How do you control access to sensitive data?

5. Are you planning any expansion soon? / Do you have any plans to expand into new geographic regions or offer new services that might require you to manage data in different locations?

6. How many remote users do you support?

Elevator Pitch

NordLayer: Securing your data, resources, and employees in today's cyber threat landscape is no easy task. But with NordLayer, you can turn the tables on these threats. NordLayer's stress-free, cutting-edge solutions simplify work and cybersecurity, protecting modern businesses' networks. With easy setup, seamless integration, and scalability, NordLayer provides comprehensive protection aligned with the and principles. Secure your access to the internet, streamline your network and resource management, and ensure compliance. Get peace of mind and embrace future-ready cybersecurity. Take action today for a safer tomorrow with NordLayer.

NordPass: Cybersecurity can be a significant challenge for organizations operating without dedicated IT. Verizon's 2024 Data Breach Investigations Report shows that 72% of breaches occur due to human errors, such as falling for scams or making mistakes with passwords. NordPass, an advanced and intuitive password manager developed by the team behind NordVPN, can significantly mitigate such risks without requiring extensive tech expertise from its users. Beyond streamlined password management, NordPass can help with regulatory compliance and offer insights into potential vulnerabilities throughout the organization. Experience the peace of mind that comes from protection tailored to the needs of your business