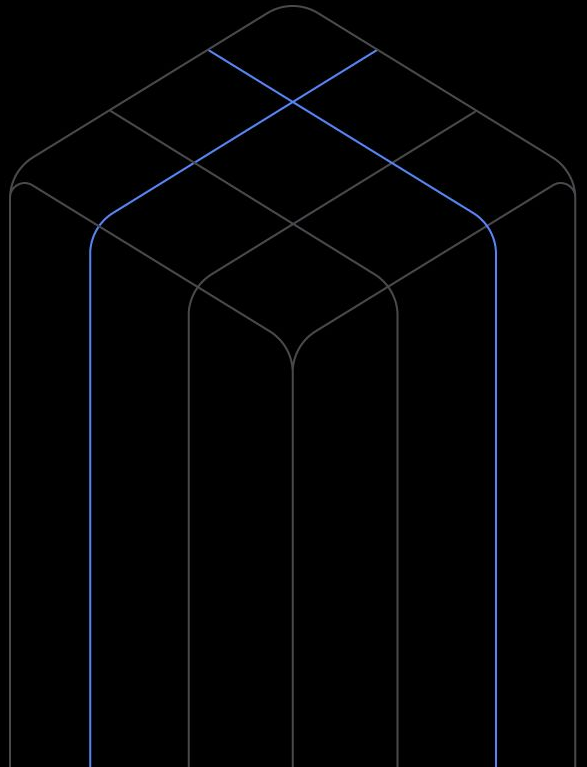
NORD SECURITY
Business Suite — NordPass — NordLayer — NordStellar

THE CREATORS OF NordVPN

Cybersecurity in the context of **Artificial intelligence**



Andrius Buinovskis, Head of Product @ Nord Security

2012

Co-founders Tom Okman and Eimantas Sabaliauskas launched the first version of NordVPN for Windows

2013

NordVPN

The NordVPN app went live

2014

Exponential growth - surpassed 10K users and rolled out 24/7 support

2016

Donated our first emergency VPN accounts

2019

Launched three additional cybersecurity products

- NordPass
- NordLayer
- NordLocker

2020

Introduced NordLynx protocol for superior speed

2022 $1.6B

Achieved Unicorn status. In our first-ever funding round of $100M, we reached a total valuation of $1.6B

2023 $3B

Raised a second investment round $100M and doubled total valuation to $3B

2024

Introduced three new products:

- NordStellar
- Saily
- NordProtect

2026

Introduced business browser

- NordLayer Browser

NORD SECURITY
Business Suite

Your security challenges, solved

NordStellar

Threat exposure management platform that enables you to detect and respond to cyber threats targeting your company before they escalate

NordPass

End-to-end encrypted password manager that ensures the finest standards of privacy and security for business

NordLayer

Network security, threat detection, and response platform that integrates seamlessly with any technology stack and comes with unmatched support

1. Your organization starts using **NordStellar** for threat intelligence to detect leaked employee, consumer & partner data, cybersquatting, external vulnerabilities, and data exposure.

2. To mitigate leaked data, your company adopts **NordPass** for secured credentials, unmanaged access, shared accounts, and shadow IT management.

3. Next, your organization implements **NordLayer** to restrict the attack surface by allowing access to your resources only from a dedicated IP, improving network access control and endpoint security.

4. Your company continues using **NordStellar** for 24/7 monitoring.

NORD SECURITY
Business Suite — NordPass — NordLayer — NordStellar

THE CREATORS OF NordVPN

User-first cybersecurity suite
Created for security, designed for productivity

One of the world's **leading cybersecurity** solutions providers

20,000+
businesses protected

10+ years
in the market

$3B
valuation – the official Unicorn

WHAT HAPPENED

We moved from installed software to SaaS.	→	Attackers don’t always "hack in". They log in.
Shadow IT transformation.	→	Good people are trying to do their jobs faster.
Supercharged social engineering.	→	The easiest way into a company is by hacking trust.
	↗	**Shadow AI** has emerged.

WHAT'S HAPPENING

Highly skilled hackers still exist...

...and they are building toolkits,
platforms, and "cyber crime services".

Cybercrime became a **business.**

Then

High skill,
low volume
attacks.

Now

Low skill,
massive volume
attacks.

Not because you’re special.

But because you’re reachable.

Phishing

"Your Microsoft session has expired. Please login again."

Fake websites

Pixel-perfect clone of your real login portal: Microsoft 365, Google; Okta; internal SSO

Domain spoofing

- micrsoft.com (missing o)
- micosoft.com (missing r)
- microsfot.com (f <> o)
- microsofft.com (double f)
- rnicrosoft.com (👀?)

Deepfake voice

"I'm in a meeting. I need this transfer done urgently. Don't delay."

Deepfake video

...this one scares me as well.

ATTACKER'S GOALS

Get paid

Get data for selling, use data for blackmail, or engage in other manipulation tactics to get paid.

Business cloning

Capture revenue by fast-tracking plans, products, and features already validated for profitability.

The hard part:

PEOPLE

Usually people imagine an insider threat as

- a malicious employee
- someone stealing data
- someone sabotaging systems

But in reality, the biggest insider threat is

unintentional.

Especially when working with **AI tools.**

Prompt paste

Employees paste source code, client lists, unreleased financials.

Training contamination

Training or fine-tuning models without privacy guarantees can cause memorization.

Retrieval of misconfiguration

RAG systems that draw from broad indexes can surface documents beyond least-privilege, exposing content to users who shouldn't have access.

Generative code/tools

AI-generated commits may inadvertently embed secrets (API keys, tokens).

Model output

Auto-generated reports, images, and prompts can contain sensitive information.

SHADOW AI

It’s not just hackers breaking or loging in...

...misuse of **AI** causes us to hand out data.

PREVENTION

The easy* part:

TECHNOLOGY

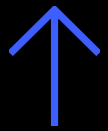
* - compared to educating employees and raising awareness

The risk is **never zero**...

The goal

reduce
likelihood

reduce
impact



recover
faster

Centralized, policy-enforced AI access

Securing user access to the internet by enforcing policies, filtering malicious content.

Automatic redaction and secret scanning

Strip PII/keys from prompts/uploads; block sensitive categories via classifiers.

Private/isolated AI for sensitive work

VPC/on-prem models, data residency, and vendor no-training guarantees.

RULE #1

Forget the mindset that everyone can access everything...

...start with **zero trust**, grant what's necessary.

Data minimization and segmentation

Least-privilege access, scoped context, isolated vector stores per team/tenant.

Short retention and strong encryption

Time-bounded logs/caches with KMS-managed keys and separate encryption domains.

Output and retrieval controls

Watermark/fingerprint outputs; ACL-aware RAG to limit unauthorized resurfacing.

Segmentation & ZTNA

- least privilege access
- role-based permissions
- separating systems
- separating environments
- limiting what an account can reach

Continuously verifying whether a specific user, using a particular device in the given context, can access specific resources.

This is how modern organizations can survive incidents

Readiness & Backups

Personnel are prepared for disruption, and there are regularly tested backups.

Response & Recovery

Guides for coordinated actions to contain incidents and rapidly restore or hot-swap to safe modes.

Testing & Improvement

Validates recovery capabilities through drills and testing.

Let’s wrap it up!

NOW

AI and **Shadow AI** is emerging faster than we could ever expect.

Massive scale, automation, SaaS everywhere.

RECIPE

- Awareness
- Insider threat mitigation
- Accepting that the risk is never zero
- Designing IT infrastructure so incidents don’t become disasters

It is everyone’s responsibility to

1. Help IT with the "easy" part
2. Take ownership of the "hard" part

NORD SECURITY
Business Suite

We can help with "easy" part

NordStellar

Threat exposure management platform that enables you to detect and respond to cyber threats targeting your company before they escalate

NordPass

End-to-end encrypted password manager that ensures the finest standards of privacy and security for business

NordLayer

Network security, threat detection, and response platform that integrates seamlessly with any technology stack and comes with unmatched support

1. Your organization starts using **NordStellar** for threat intelligence to detect leaked employee, consumer & partner data, cybersquatting, external vulnerabilities, and data exposure.

2. To mitigate leaked data, your company adopts **NordPass** for secured credentials, unmanaged access, shared accounts, and shadow IT management.

3. Next, your organization implements **NordLayer** to restrict the attack surface by allowing access to your resources only from a dedicated IP, improving network access control and endpoint security.

4. Your company continues using **NordStellar** for 24/7 monitoring.