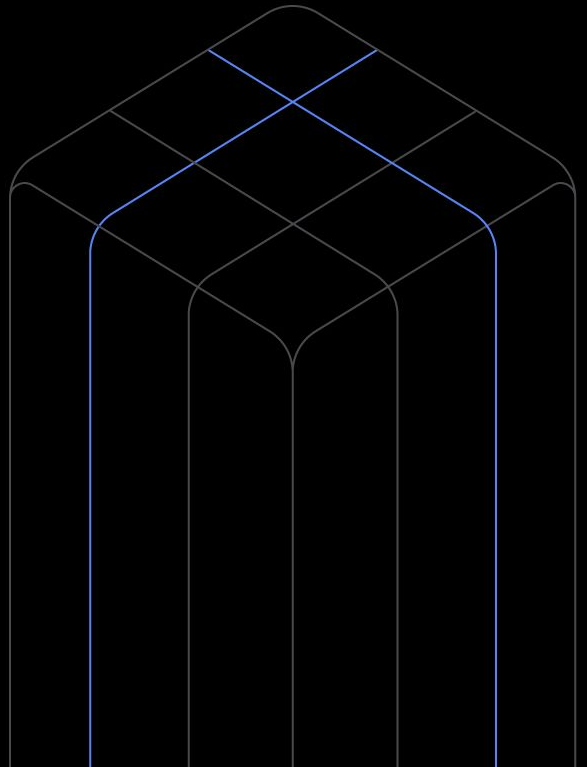
NORD SECURITY
Business Suite — NordPass — NordLayer — NordStellar

THE CREATORS OF NordVPN

Cybersecurity: **Then, Now, Why & How**



Andrius Buinovskis, Head of Product @ Nord Security

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

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

One more product in portfolio

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.

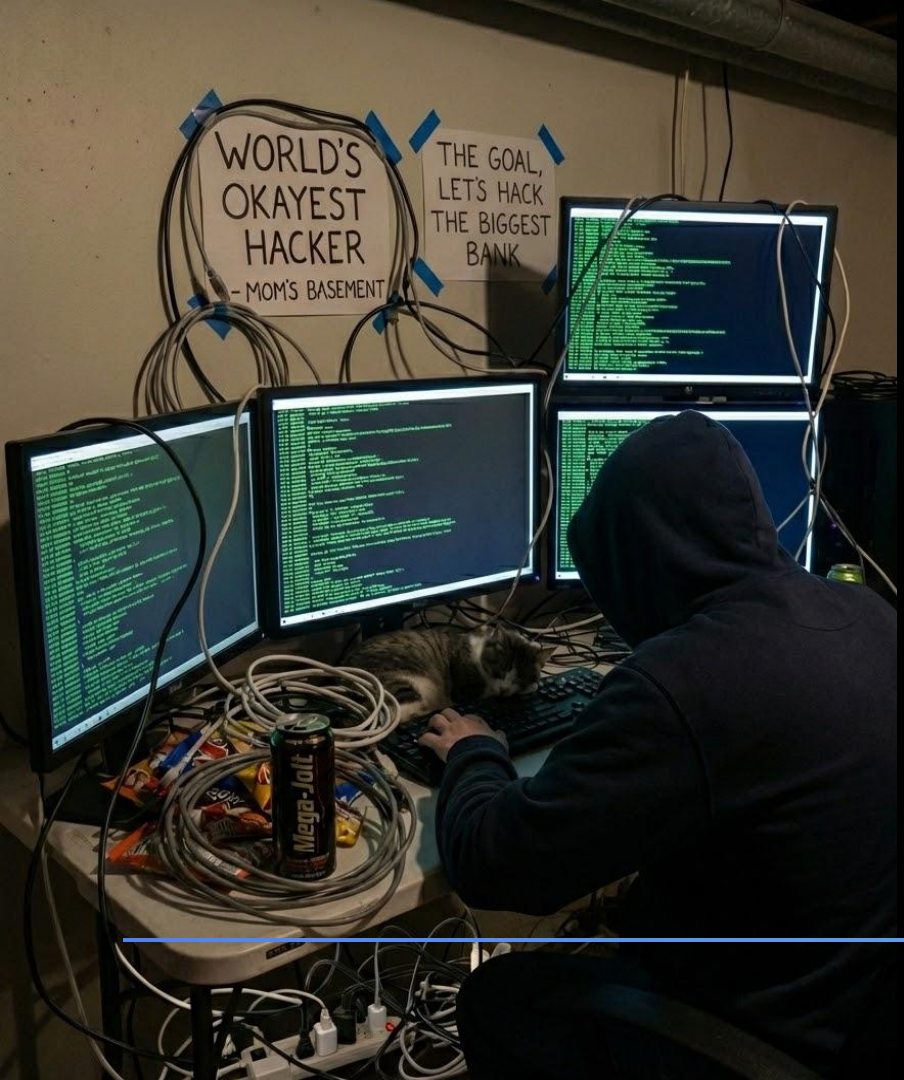
3. Next, your organization implements **NordLayer** to restrict the attack surface by allowing access to your resources only from a dedicated IP, improving network access control and endpoint security.

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

THEN

The world was already interconnected...

...yet interconnection was growing at the speed of light



Hackers

Back then, cyberattacks required strong technical skills, time, patience, and usually a **specific target**

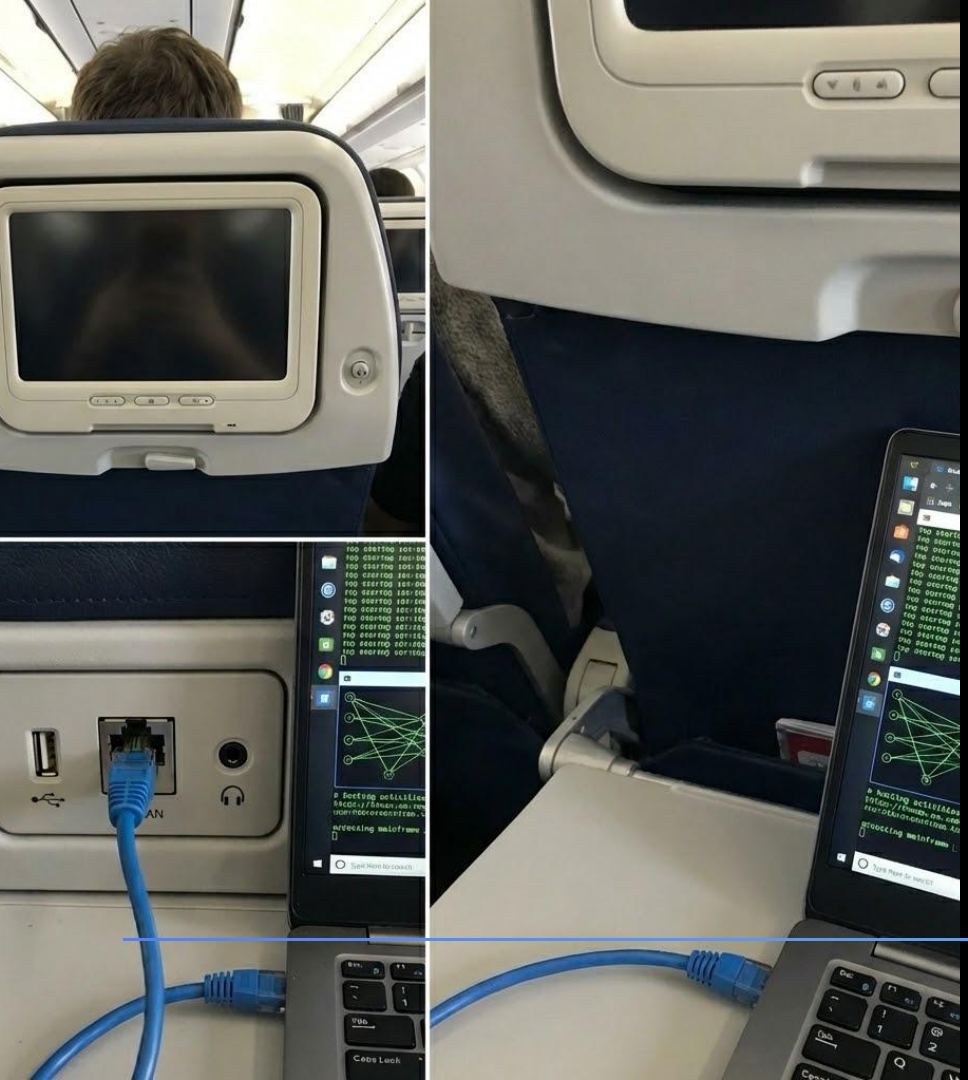
Opportunists

Back then, they were more like script-kiddies downloading tools they didn’t fully understand, running generic and limited-scale attacks

Is a closed system a myth?

Closed system?

Charlie Miller and Chris Valasek demonstrated they could remotely access a Jeep Cherokee's internal systems



Closed system?

Chris Roberts case, where he claimed he could access aircraft systems through the in-flight entertainment network.

NOW

Hoodie hackers still exist...

...but 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.

Now, anyone can become a victim

Not because you’re special.

But because you’re reachable.

WHY

The world has changed...

...the mindset around cyber defence should change as well

WHY

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.

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

Invoice fraud

"We changed our entity name. Use this new bank account."

Domain spoofing

- micrsoft.com (missing o)
- micosoft.com (missing r)
- microsfot.com (transposed f and 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

Accept the truth...

The hard part:

PEOPLE

Awareness is **everyone's** job

- slow down when it's urgent
- verify when it's emotional
- double confirm when money is involved
- don't trust links blindly
- question anything that feels slightly off

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.

Any of us
can become one.

Cybersecurity is not about:
"click the wrong link → you get fired."

One incident can cause
the **business closing**

HOW

The easy* part:

TECHNOLOGY

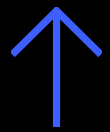
* - compared to educating employees and raising awareness

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

The goal

reduce **likelihood**

reduce
impact



recover
faster

Secure Web Gateway (SWG)

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

Threat Exposure Management

Dark web monitoring and attack surface management

Detection and Response

Data correlation, detection and coordinated response across endpoints, network, cloud, email, and identity domains

Segmentation or 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

Testing & Improvement

Validates recovery capabilities through drills and testing

Let’s wrap it up!

NOW

Massive scale, automation, SaaS everywhere, opportunists everywhere.

RECIPE

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

It is our all 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.