

| IDEX Biometrics ASA

# IDEX

## Business update

Oslo

April 2026



# IDEX is restructured, refocused and re-rated

1. New management team
  - CEO holding approx. 30% (directly and indirectly)
2. Transformed the business from component supplier to product company
  - Launch world-class Access products (Physical (doors) and Logical (PC's))
  - Compliant with customers existing security infrastructure (Microsoft Entra, HID, Mifare DESfire)
3. Streamlined operations and reduced OpEx to \$1.5M - \$1.7M Q1 2026 (vs \$4.6M avg Q 2024)

*The only thing that is left is the name and IP*

*"The main reason behind my investment was that I believed that AI would soon be able to tear down the worlds old security architecture, and that I saw that the building blocks (IP) in IDEX could be put together in a way that would respond to this threat in a unique way (!)" - CEO, Anders Storbråten*

## NEW MANAGEMENT

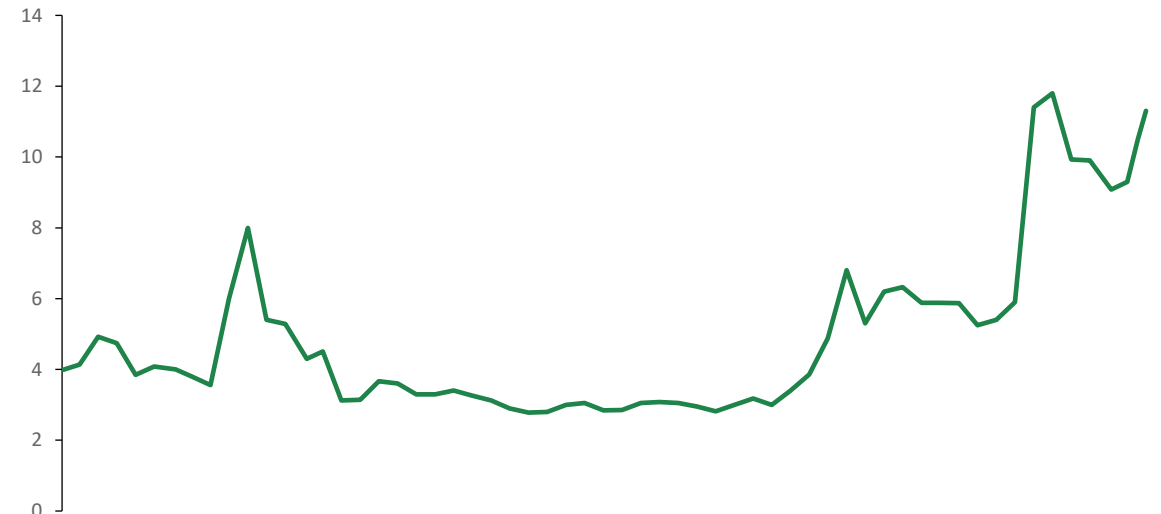
11 Mar 2025 – 21 Apr 2026

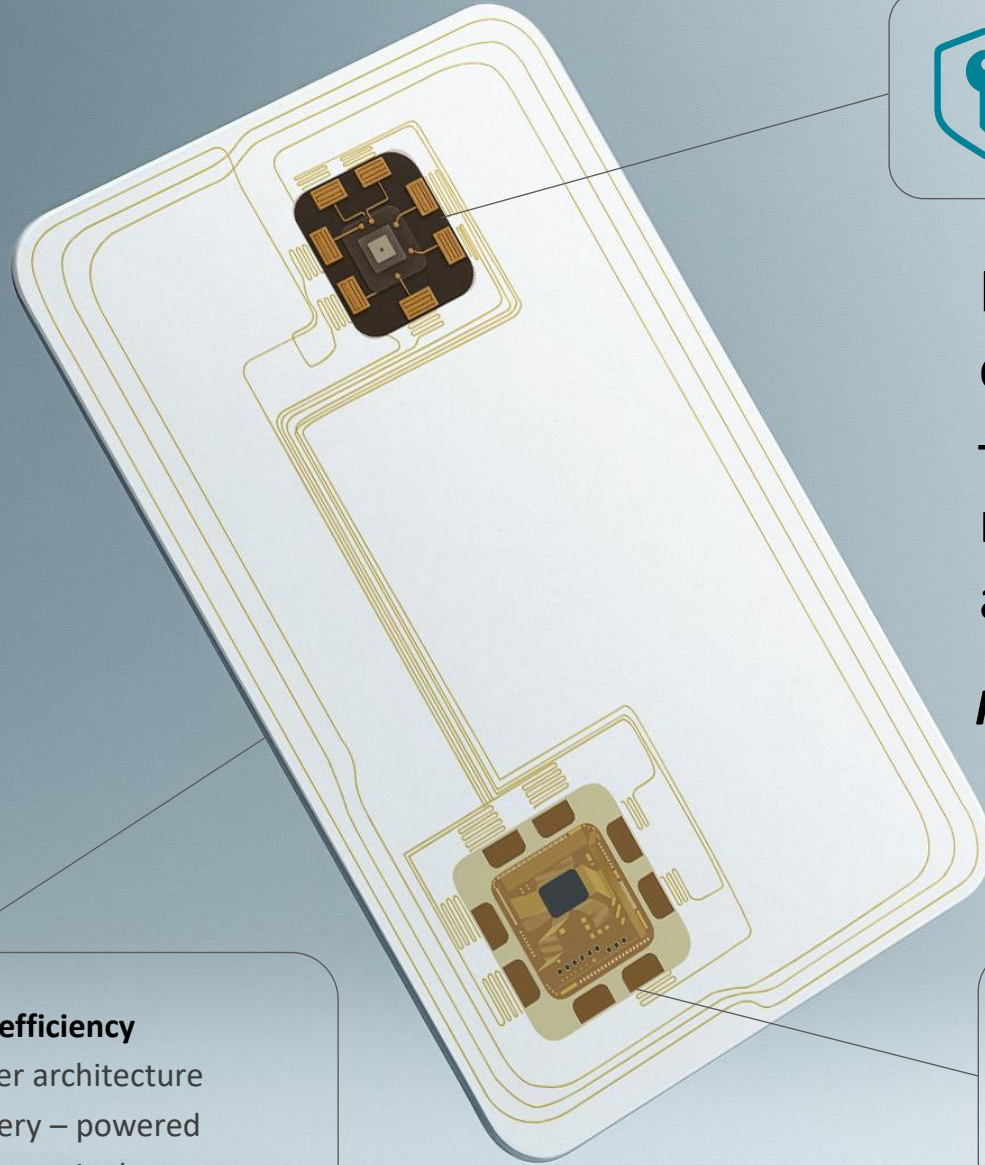
# +183%

NOK 3.99 → NOK 11.30

NOK 1.00 → NOK 11.30 (for investors participating in the convertible loan in Mar'25)

Share price (NOK)





### Secure element

Access keys are encrypted and stored offline – no cloud.

IDEX keeps you secure and compliant pre and post 7 April 2026 – it's easy to use, **without** the requirement of large IT budgets, and is fast to deploy

*Identity-bound access built for the AI era*



### World class power efficiency

Advanced low-power architecture runs without a battery – powered by NFC readers and terminals.



### Fingerprint sensor

Built-in liveness detection prevents spoofing and fake fingerprints. Certified by Visa, Mastercard FIDO

## The problem today: Fragmented, cumbersome and vulnerable

Mobile authenticators can be phished. Hardware keys can be shared. None verify your identity.

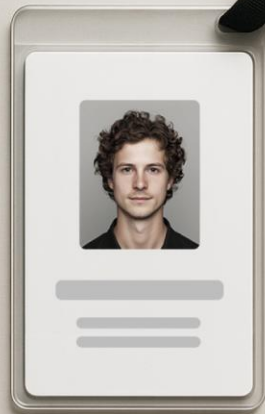
### Hardware key

Login to office computers and accounts.



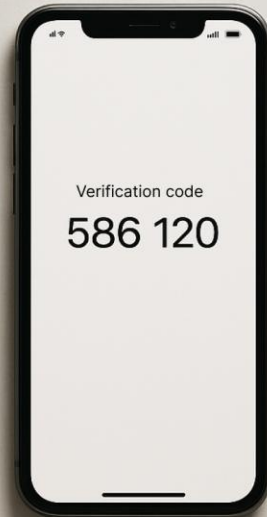
### Key fob

For building and room access.



### ID card

For identification and physical access.



### Mobile authenticator

SMS or OTP-based 2FA for digital services.

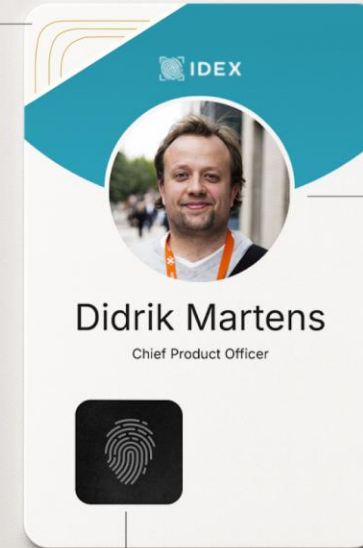
## The solution: One card. True identity

Get digital login, door entry, and ID – all in one.

No cloud. No app. No attack surface

### Contactless power

The reader wirelessly powers the card – no battery needed.



### ID card

Serves as your employee ID and access card in one.

### Fingerprint sensor

Biometric authentication certified by Visa, Mastercard and FIDO.

# The cost of data breaches can be substantial...

MoneyWatch

## UnitedHealth data breach caused by lack of multifactor authentication, CEO says

By [Kristopher J. Brooks](#)

Updated on: May 1, 2024 / 8:11 PM EDT / CBS News

Add CBS News on Google

The breach has already cost UnitedHealth Group nearly \$900 million, company officials said in reporting first-quarter earnings last week, not including ransom paid.

## Cyber-attack on Hydro

Hydro is in dialog with relevant Norwegian and international authorities, including Norway's National Investigation Service (Kripos) and the Norwegian National Security Authority (NSM). Hydro has estimated the total cost to be around 800 MNOK. The company has a robust cyber insurance in place with recognized insurers.

DNV CYBER

Hydro highlights the vulnerabilities in our interconnected world and the need for strong Identity and Access Management (IAM) protocols. This incident, involving the LockerGoga

## JLR hack is costliest cyber attack in UK history, say analysts

22 October 2025

The cyber attack on Jaguar Land Rover (JLR) will cost an estimated £1.9bn and be the most economically damaging cyber event in UK history, according to researchers.

## The data attack against Tomra cost 200 million kroner

20.11.2023 - 04:55

The costs following the computer attack against Tomra this summer were NOK 80 million higher than previously estimated, reports [NRK](#).

BBBC

## Co-op says cyber-attack cost it £206m in lost sales

25 September 2025

## ISS World hack leaves thousands of employees offline

20 February 2020

[Joe Tidy & David Molloy](#)  
BBC News

Projected annual cost cybercrime \$10T, 6+bn attacks annually, Average cost of breach (EU \$4.4M), 60% of SMEs that suffers a major out of business within 6 months (Source: Angelo Cosoli, SUPSI – Swiss Cyber AI 2026 Lugano 14 April 2026)

# ...as seen in recent weeks with high profile attacks in Norway...

16 April 2026

TELEKOM

## Nkom med nytt Telia-tilsyn: Kunder kunne spores når man ringte dem

Nasjonal kommunikasjonsmyndighet (Nkom) vil åpne tilsyn med Telia etter varsel om et alvorlig sikkerhetsavvik, opplyser myndigheten på sine nettsider.



24 March 2026

1. april 15:00 NTB



Treningskjeden Sats bekrefter at selskapet har vært utsatt for et datainnbrudd. Foto: Håkon Mosvold Larsen / NTB

Del

Treningskjeden Sats bekrefter onsdag at de har vært utsatt for et datainnbrudd og at flere medlemmer har fått personopplysninger lekket.

Selskapet identifiserte uautorisert tilgang til deler av sitt IT-miljø allerede 24. mars, skriver [E24](#).

13 February 2026

## Stjålne data fra Telia lagt ut på det mørke nettet

En hackergruppe har publisert flere hundre tusen filer som de hevder kommer fra Telia Norge.



Julie Helene Günther  
Journalist

+ 4 til

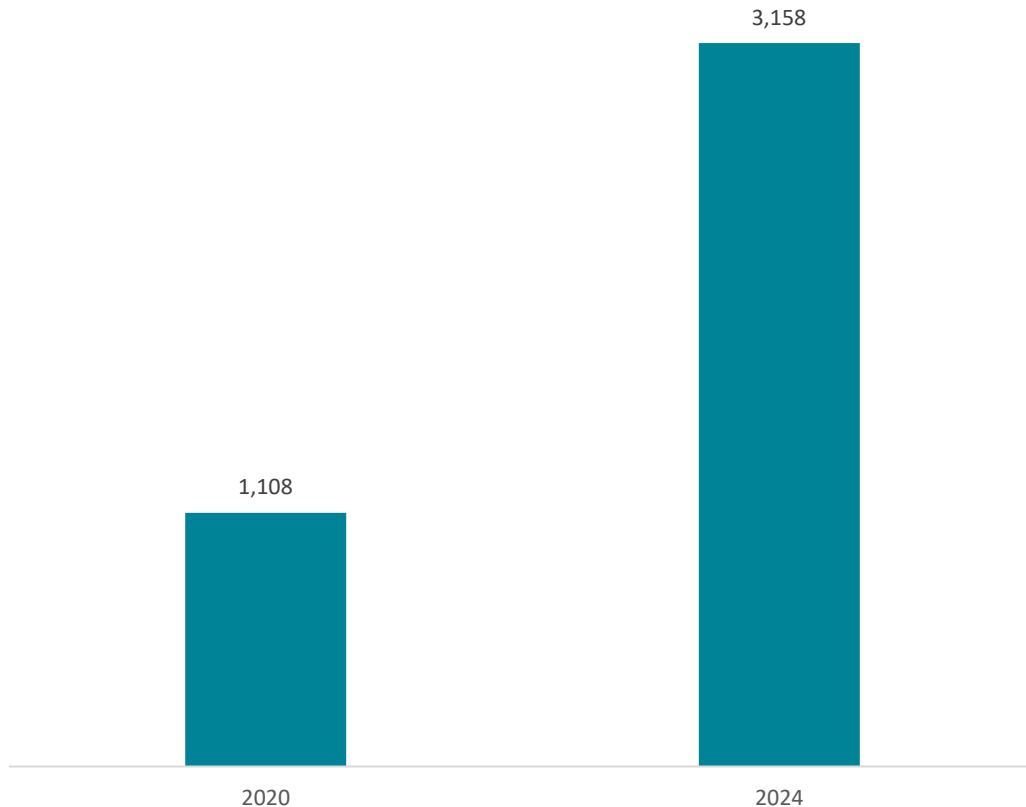
Publisert 13. feb. kl. 13:12  
Oppdatert 16. feb. kl. 15:20

HACKERÅNGREP: Telia Norge er utsatt for et datainnbrudd. Informasjon hentet fra selskapet er lagt ut på det mørke nettet.

# ...and the risk is increasing

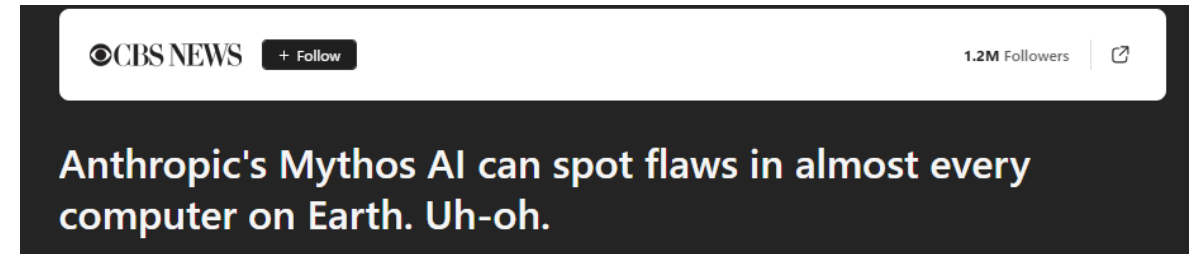
Data breaches have tripled – and AI will accelerate the trend

Data breaches in the US



Source: Identity Theft Resource Center (ITRC)

Anthropic's Mythos: "The storm isn't coming – the storm is here"

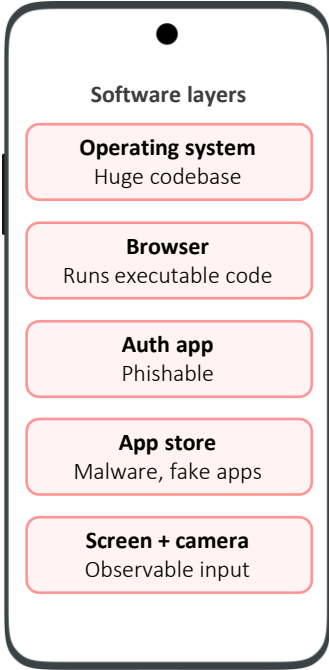


- **Anthropic refused to launch Mythos publicly (April 2026)** – Access limited to 40 select companies including Amazon, Apple and Microsoft ("Project Glasswing")
- **Software-based security can't keep up** – Mythos finds vulnerabilities faster than they can be patched
- **IDEX is immune** – Biometric verification happens offline, on the card. No network, no attack surface.

# Mobile phones easily hackable, IDEX Biometric Card is air-gapped

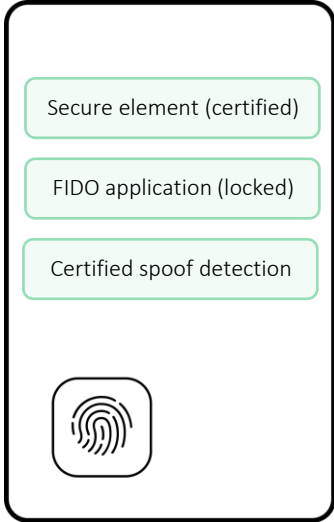
## Mobile phone

**Always online** – can be attacked remotely.  
Many layers of software exposed to the internet.



## IDEX Biometric Card

**Always offline** – not reachable over any network.  
Software is locked down at manufacturing.



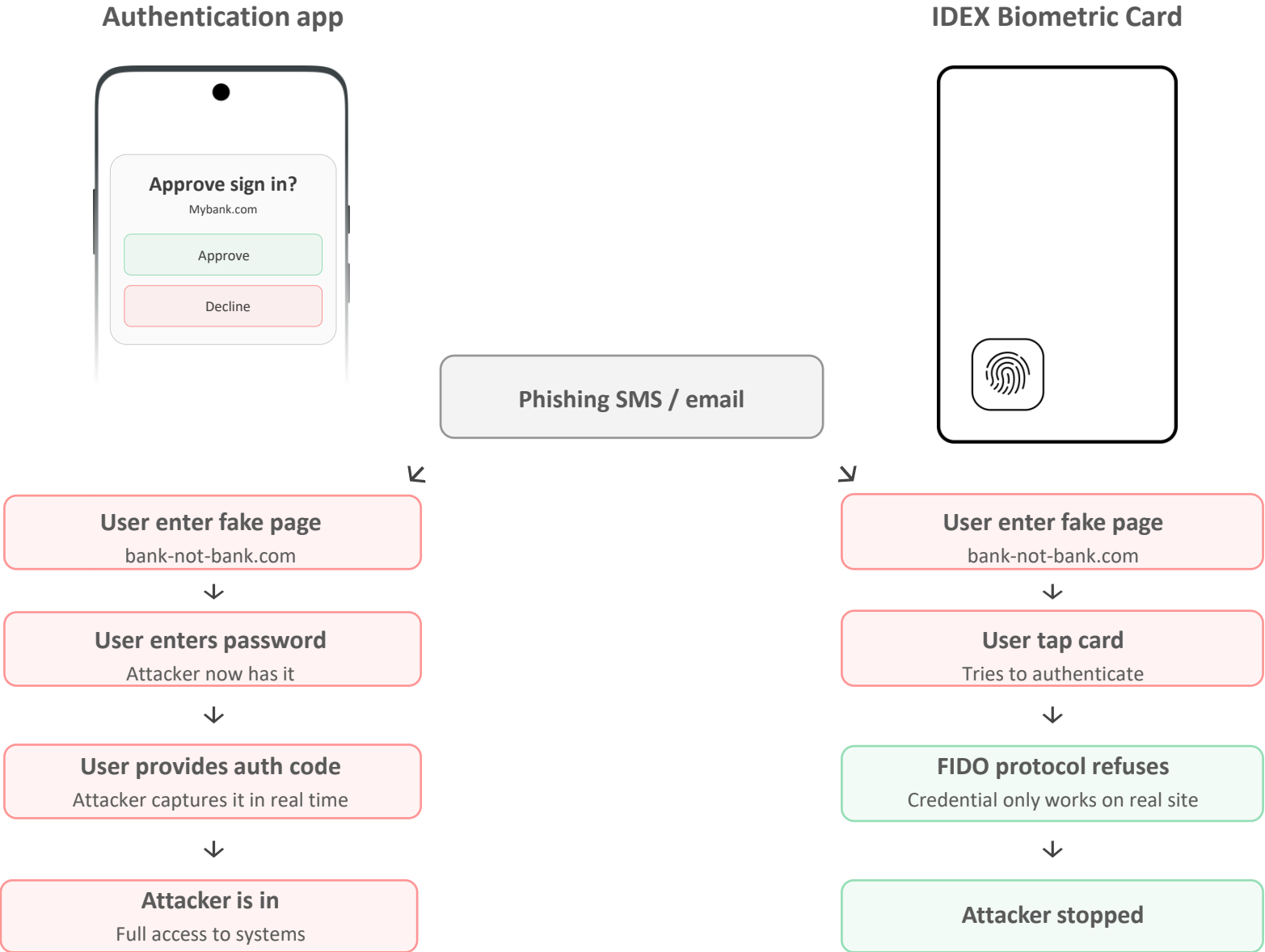
**Before AI tools like Mythos**  
Bugs found slowly, by skilled hackers.  
Organisations had time to patch.



**After Mythos**  
AI finds critical bugs across all software layers.  
Near-instant mass exploitation via the internet.

**After Mythos**  
Air-gapped: not reachable remotely.  
Software is locked down at manufacturing.

# IDEX is safer than the “safest” solutions



# Our current technology is unique and will take years to replicate



## Technology

- **Sub-250ms verification** – On-card fingerprint matching, faster than unprotected access
- **No charging** – Draws power from reader and is off-grid when not in use
- **Built-in liveness detection** – Prevents spoofing and fake fingerprints
- **Secure element architecture** – Keys encrypted and stored offline, no cloud
- **Technology agnostic** – Works within existing standards and infrastructure

## Certifications & Compliance




- **FIDO2 certified (February 2026)** – Phishing-resistant authentication, key deployment blocker removed
- **Visa & Mastercard certified** fingerprint sensor
- **Microsoft Entra passkey approved** – Ready for enterprise identity ecosystems
- **India RBI approval** for biometric payments
- **Regulatory compliant** – Designed for NIS2, DORA & GDPR requirements

## Ecosystem Compatibility

- **HID & NXP compatible** – Slots into readers enterprises already have
- **MiFare DESFire EV3 support** – Industry-standard secure access
- **No rip-and-replace** – Adoption at scale, not pilots that never deploy

# IDEX solution is also cheaper than today's solutions

## Typical IAM stack

	Standard access card	~\$10
	Biometric FIDO2 hardware key including spare keys	~\$140
	Password-related time loss Sources: Forrester and SSB	Yearly ~\$650
Cost per employee	\$650 annually + \$150 in credentials	

Excluding cost of a data breach  
Excluding cost of mobile device management and authenticator solutions

## IDEX



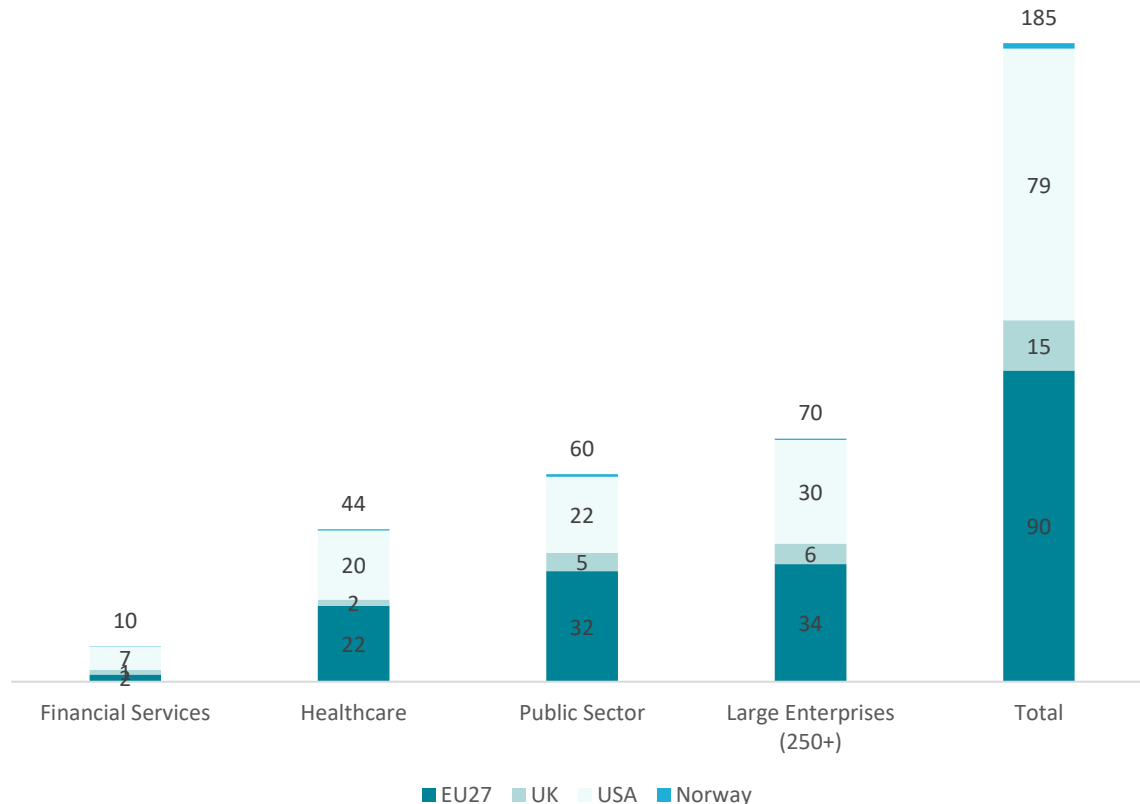
Payback period in weeks\*

\* Payback based on replacing \$650/year in password-related costs with a one-time card cost and an annual subscription.

# TAM in the western security-focused world is almost 200m units, but our potential goes way beyond this

185m employees in Europe and the US where security really matters

Employees by sector and country



- **Regulatory tailwind accelerating** – NIS2 deadline passed Oct 2024; enterprises now face fines up to EUR 10m or 2% of turnover for non-compliance
- **Every badged employee is a potential unit** – Unlike software licenses, biometric access cards scale 1:1 with headcount
- **Infrastructure-ready** – IDEX works with readers enterprises already have (HID, NXP)
- **Significant potential beyond regulated and core sectors:**
  - **Already in pilot** with a commercial real estate company
  - **Logistics & Warehousing** – high-value inventory, contractor access
  - **Critical manufacturing (NIS2-covered)** – IP protection, restricted areas
  - **Utilities & Energy (NIS2-covered)** – Critical infrastructure
  - **Data centers** – Tier-1 physical security requirement
- **High repetitive sales** from recurring (BaaS) and replacement cycles (employee turnover and lost cards)

# Product and commercial traction

## Recent commercial highlights

- **USD 1.75m order from ID Centric placed in March (initial delivery for starting in Q2-Q4 2026) together with a commitment to invest NOK 90m. Ambition for 10 million by YE27**
- **Several customer pilots live or in final planning stage**
  - **Customer pilot** - Signed leading Norwegian government agency for IDEX Access card (Q1)
  - **Customer pilot** - Signed leading Norwegian real estate company
  - Close to sign several customers including leading Cyber security reseller and leading smartcard distributor

## Product

- **Only biometric card integrated with HID, NXP (Mifare Desfire) and FIDO2**
  - HID - Works on 90% of HID door readers (including SEOS) – HID is selling 1bn access cards annually
  - Partnership with NXP (Mifare Desfire) – largest market share for physical access
- **FIDO2 certified February 2026**

## Events participation

Trustech Paris December 25, Swiss Cyber AI Lugano 14 April 26, Sikkerhetskonferansen Oslo 21 April 26, Totalforsvarets cyber sikkerhetskonferanse Lillehammer 6-7 May 26, Oslo Tech Show Lillestrøm 6-7 May 26, Identity Week 9-10 June 26 Amsterdam, Money 20/20 2-4 June 26 Amsterdam

# Post-Mythos: Two questions enterprises must answer now

April 2026 – Anthropic warns of 6-month window to secure compliant authentication

## QUESTION 1: The threat

Can we identify, source and deploy compliant security in 6 months?

Most: no

## QUESTION 2: The solution

IS IDEX compliant, secure, affordable, deployable, and available?

Compliant

Secure

Affordable

Plug & play

In stock



Can enterprises say no to IDEX?

3M sensors in stock

# *APPENDIX*

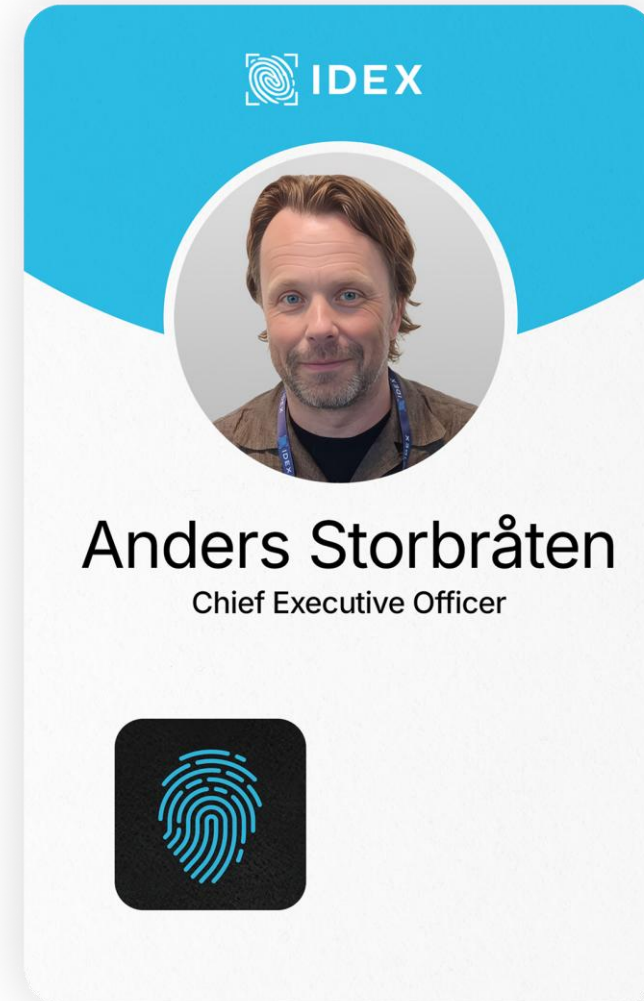
---

“

ANTHROPIC

*Mythos – we have been  
expecting you, what took  
you so long?*

– Anders Storbråten, CEO, IDEX



Anthropic has just announced a new AI model that autonomously finds and exploits critical vulnerabilities in every major operating system and browser

---

**Claude Mythos announcement**

April 7, 2026

# Claude Mythos announcement

April 7, 2026

*"The old ways of hardening systems are no longer sufficient."*

Anthony Grieco, SVP & CSTO, Cisco

*"What once took months now happens in minutes with AI."*

Elia Zaitsev, CTO, CrowdStrike

**1000+**

critical zero-day bugs identified

**27**

year old major vulnerability found

**100%**

of major OS and browsers affected

# Software-only security is not enough

Compliance frameworks like DORA and NIS2 were designed for a world where attacks required high expertise and time. AI has fundamentally changed that assumption.

## *The old assumption*

- Attacks require months and rare expertise
- Software patches keep pace with threats
- Passwords + OTP meet compliance

## *The new reality*

- AI finds and exploits vulnerabilities in hours
- Patch cycles can't match AI-speed discovery
- Defence starts where software ends – at the hardware layer

14 April 2026

We are just back from Swiss Cyber AI 2026 in Lugano, and the message was clear.

## Cybersecurity over time

- 1980s - 1990s: the Perimeter Era

- Late 1990s - early 2000s: The Connectivity Explosion

Question from the stage at Swiss Cyber AI 2026

Have we solved the new identity problem raised by AI?

**Nobody raised their hands**

- Mid 2010s - 2020: The Cloud & Zero Trust Shift
- 2020 - Present: AI, Autonomous Systems and Compliance

- What's next ? ...

“

*Now is the time to modernise cybersecurity stacks everywhere.*

Lee Klarich

Chief Product & Technology Officer, Palo Alto Networks

---

On the launch of Anthropic's Project Glasswing, April 7 2026

IDEX Biometric Access Card

**You need to be offline,  
to be safe online**



# Works with existing infrastructure

Supports MIFARE DESFire and FIDO2 – the leading open standards for physical and digital access.

Compatible with over 90% of HID readers.

## Physical access



## Digital access (FIDO2)



| Fingerprint enrolment

Self-service enrolment via mobile or centralised enrolment, for enterprise security and audit trails.

