PROMON

2024 Case material

CBS Finance Competition

CBS FINANCE COMPETITION

Dear participants,

I am pleased to announce that Promon will be the focus of this year's Copenhagen Business School Finance Competition. As a leader in proactive mobile app security, we aim to enhance digital safety in an ever-evolving technological landscape. The rapid pace of change, driven by technological advancements, offers tremendous growth potential but also introduces new challenges. Promon strategically adapts to these changes to strengthen security measures.

In a world with over 7 billion smartphones and billions of mobile applications, the risk of threats is omnipresent. While seamless access to essential services has improved user convenience, it has also heightened the exposure to cyber threats. Promon plays a vital role in creating a secure environment where convenience and safety coexist.

The growing awareness of data compromises has heightened the societal demand for enhanced protection. Users impacted by data breaches underscore the need for robust security measures, making app security support increasingly essential.

Our mission at Promon is straightforward: to sustain our expansion and reinforce our critical role. Fueled by innovation and a commitment to global prominence, our success depends on collaborative partnerships with stakeholders – owners, employees, and clients. It is crucial for you, as participants, to consider the future potential of Promon within the various exit opportunities presented in this case.

Your involvement is integral to shaping the future performance and ownership structure of Promon. I look forward to the unique perspectives and insights you will bring forth in your case solutions. May this competition serve as a platform for valuable learnings and insights that will contribute to your future endeavors.

In conclusion, embrace the challenges this case presents, and let your analytical prowess shine. Now, let's get to work!

Sincerely,

Andreas Thome
Executive Chair & CEO

PROMON

Table of Content

PROMON

A paradigm shift in digital security

The next paradigm shift in digital security is already here. The mobile application market is growing at an unprecedented rate, and many enterprises now generate a substantial portion of their revenue from digital services. Across the board, adopting a "mobile/app first" strategy has become pivotal, and an average of 100,000 new Android/iOS apps are launched each month. This is ushering in a new paradigm in digital security –with apps, APIs, and other communication protocols as the primary battleground.

In the 2000s, digital security was all about networks and by the 2010s, focus shifted to end-point security. The new field in the 2020s is app security. Today, most people have dozens of apps installed on their smartphones, from travel apps, banking services, and games to preinstalled apps that they were unaware existed. While this has provided convenience like never before, it has also opened new digital surfaces that malicious actors and cybercriminals can attack. Currently, more than 50% of the world's banking, trading, and payment apps with more than 5 million downloads are susceptible to repackaging attacks from malicious hackers. This allows the hacker to enter the app on your phone and re-engineer it to do something different the next time you open it, such as transfer money to another bank account or share your personal data.

It is not just the end-user who suffers from attacks or data breaches. Under GDPR (General Data Protection Regulation), companies that collect personal data from European citizens must self-report all significant breaches within 72 hours, and each GDPR violation risks a fine of up to 4% of an organization's annual worldwide turnover, or €20 million, whichever is larger. More importantly, data breaches damage a company's reputation, which can have a negative impact on the company's growth, customer retention, and brand equity. The solution is to use added digital security to protect the app against attacks. However, many companies face an uncomfortable trade-off between app performance and digital security.

As applications become more complex and interrelated, a growing awareness of dataflows between different applications, organizations, and devices is needed. Digital security considerations are expanding to include APIs (Application Programming Interfaces), identity governance around apps, and IoT (Internet of Things) devices, which are increasingly deployed to administer and control critical assets and infrastructure. The digital security field is continuously evolving and is increasingly appearing on the C-level decision-making agenda. The importance of Digital Identity and API security will only grow over the coming years, as the prevalence of API-led malware attacks is accelerating rapidly, and modern enterprises are becoming more digitalized and interconnected. Malicious actors are becoming increasingly sophisticated; however, the digital security industry is catching up.

Introduction to GRO Capital

PROMON

GRO Capital x Promon

GRO is a prominent B2B software-focused Private Equity fund with offices in Copenhagen, London, and Oslo. GRO focuses on investing in business-critical software companies and has a solid growth momentum in Northern Europe. With assets under management (AUM) exceeding EUR 1 billion, GRO boasts a remarkable track record of partnering with firms on transformative journeys through active value creation. This is accomplished by providing capital and close strategic support through the operating team and the investment team in conjunction on topics such as building an efficient go-to-market motion, expanding internationally, achieving product excellence, or pursuing acquisitions - all with the overarching ambition of creating category leaders in B2B software.

GRO takes a thematic approach to investing by addressing fundamental societal challenges within four key areas:

i. Unlocking resource efficiency
ii. Improving safety in the digital world
iii. Energy transformation & sustainability
iv. Enabling the digital transformation

Reflecting GRO's digital safety thematic, GRO recognized a compelling investment case in Promon when investing in the company in 2021 out of their Fund III. Promon is a Norwegian software as a service (SaaS) company that specializes in application security software. The company was founded in 2006 by Tom Lysemose, who identified a pressing need for enhanced protection for mobile applications while studying for his Ph.D. With major customers in a diverse set of verticals such as banking, government service, healthcare, streaming, payments, and gaming, Promon's core SHIELD technology protects more than a billion app users today.

To GRO, Promon stood out positively on several key areas. Most importantly, Promon's unique approach to mobile application security leveraging highly defensible and differentiated technology based on years of academic research poised the company to remain one of few globally recognized players which effectively could help safeguard application users and companies globally against the rapidly evolving threat landscape of tomorrow. By applying the right strategic levers during its ownership, GRO recognized a strong value creation journey ahead. This included (i) expanding Promon's geographical presence with particular focus on the US and APAC, (ii) penetrating established and growing into new verticals, (iii) and focusing on continuous product investments to sustain leadership within application security and potential product adjacencies.

GRO finalized the investment in Promon in 2021 in a consortium led by GRO with both strategic and financial actors including Queensland Investment Company (QIC), Kirk Kapital, and Trifork (referred to as 'GRO consortium').

Exit considerations

PROMON

Strong market interest

After two years of ownership, the GRO consortium has received significant interest from various US and European entities, each highly intrigued by Promon's strong product, value proposition and market leading position. Among these, GRO is focusing on two specific proposals:

The Financial Sponsor: This top-tier sponsor is known for its transformative impact and substantial capital resources. With a track record of identifying and nurturing technology sector successes, they recognize Promon's product strength and unique positioning. They see acquiring Promon as a valuable addition to their portfolio, promising robust returns.

The Strategic Player: This bidder is a key player in the broader data security landscape and recognizes the major value-adding potential of combining Promon's innovative technology with their extensive customer network. They envision creating a comprehensive, integrated solution for advanced data and application security, creating a "one-stop-shop" for high-risk verticals. Their expertise in scaling similar technologies and their technical know-how could enhance Promon's existing capabilities, combined creating a powerhouse in the industry.

Two bids with varying nature

As GRO's potential advisor, you are invited to consider the following alternative scenarios for GRO's investment in Promon. You must consider the two unsolicited indicative bids along with the option to decline both offers and keep the investment in Promon for an extended period:

1. The Financial Sponsor offers to acquire 75% of the shares in Promon AS for a consideration of NOK 1,362m with a corresponding enterprise value of NOK ~1770m (10.0x ARR). This would result in GRO keeping a minority share, with a rollover to Fund IV.
    - All acquired shares are to be taken out of total shareholdings, given that GRO has drag-along rights.
    - The unsolicited offer hinges on the stipulated minority rights outlined below:
        - Right to appoint one board member
        - Consent rights on issuance of new securities, material acquisitions, and CEO changes
        - Access to customary information packages including annual report and monthly reports
2. The Strategic Player offers to acquire 100% of the shares in Promon AS for a consideration of NOK 2,170m with a corresponding Enterprise value of NOK 2,124m (12.0x ARR).
3. GRO declines both offers and keeps their current holding in Promon with a planned exit in 2026.

Case criteria

PROMON

Your role as an advisor

GRO hereby requests you to act as an advisor in the bidding process in the prospective divestment of Promon AS. Your presentation should encompass insights on the following topics, structured in a manner that aligns with your expertise and judgement:

Commercial considerations

- A commercial strategy until 2026, including:
    - Thoughts on key geographic markets
    - Thoughts on sales channels and the relative importance of each
    - Thoughts on how to increase annualized revenue per account (ARPA) from upselling
    - The impact on key SaaS metrics
- How to leverage the development roadmap to enhance organic top-line growth
- Description of relevant risks related to the commercial strategy and possible mitigation strategies

Equity story and exit considerations

- The advisor's view on Promon as an investment case, including in-depth analysis of the investment attractions of the company
- Your view on whether GRO should divest, either fully or partially, or if they should retain their current holding and divest in 2026
    - This should include your assessment of the pros and cons of choosing a partial divestment to the Financial Sponsor, a full divestment to the Strategic Player or no divestment at all

Valuation and financial considerations

- A valuation of Promon AS based on suitable methodologies, including:
    - Your view on the current standing offers and whether they represent a fair valuation of Promon AS. This should include your estimation on the current fair market value of Promon AS and the underlying assumptions

Governance and legal considerations

- The advisor's view on the key success factors and potential challenges for the suggested exit option, including:
    - A feasible timeline detailing key processes and milestones
    - Overview of legal considerations related to the exit
    - Considerations on what minority rights GRO should ask for in the case of a partial divestment

Case criteria

PROMON

Case assessment

The assessment of proposals will be conducted in accordance with the following five criteria, each assigned indicative weights. It is important you adhere to the deliverables and deadlines as outlined below.

Weightings

1. Commercial considerations (20%)
2. Valuation and financial considerations (25%)
3. Equity story and exit considerations (20%)
4. Governance and legal considerations (20%)
5. Quality of the solution (15%)
    - Visual representation of the solution
    - A clear, convincing, and well thought-out storyline

Deliverables

- Slide deck presenting your recommendations and supporting analyses
- Maximum 15 slides (excl. agenda, dividers etc.) and 15 pages of appendices
- Memo of maximum 1 A4 page, summarizing your answer, supporting arguments, and key observations

Timetable for delivery

Step	Dealine
Delivery of tender material (case launch)	April 13th, 2024, 12:00
Delivery of proposal	April 14th, 2024, 23:59
Indication of the bidders chosen to proceed to the semi-finals (9 teams)	April 15th, 2024, 23:59
Semi-final presentations	April 18th, 2024, 09:00
Indication of the bidders that have been chosen to proceed to the grand final (3 teams)	April 18th, 2024, 12:00
Grand final	April 18th, 2024, 17:00
Appointment of advisors (Selection of the winning team)	April 18th, 2024, 20:45

Glossary

PROMON

Commercial & financial terms	Description
ARPA	ARPA, or Average Revenue Per Account, is a metric used by businesses, particularly in the subscription and telecommunications sectors, to measure the revenue generated per account or user over a specific period. It helps companies understand the value each customer brings and can be used to track growth and profitability trends.
ARR	ARR, or Annualized Recurring Revenue, is a metric used primarily by subscription-based businesses to measure the predictable and recurring revenue components of their business on an annual basis. It excludes one-time payments and focuses on the revenue that the business can expect to receive every year from its subscribers or customers.
Cash EBITDA	Cash EBITDA" is a financial measure that reflects a company's earnings before interest, taxes, depreciation, and amortization, while factoring in changes in working capital and excluding non-cash items. It provides a clear picture of the cash generated by a company's core operations, excluding non-operational expenses, and is useful for assessing its ability to generate cash.
GRR	Gross Revenue Retention (GRR) is a financial metric for subscription-based businesses, measuring the percentage of revenue retained from existing customers over a period, excluding upsells or new customer revenue. It reflects the company's success in maintaining its revenue base, considering only cancellations or downgrades. GRR is used to evaluating customer satisfaction and revenue stability.
NRR	Net Revenue Retention (NRR) is a financial metric for subscription-based businesses, measuring the percentage of revenue retained from existing customers over time, including upsells, cross-sells, and downgrades, but excluding new customer revenue. It captures the company's ability to grow revenue from its current customer base, after accounting for potential losses. NRR differs from GRR in that it includes revenue gains from upsells and cross-sells within the existing customer base.
Land ARPA	Average Revenue Per Account at point of signing
The Rule of 40	The Rule of 40 is a benchmark for tech and SaaS companies, suggesting their combined growth rate and profit margin (Cash EBITDA) should be at least 40%. It serves as a quick measure to assess a company's balance between growth and profitability.

Developer terms	Description
API	API, or Application Programming Interface, is a set of rules and protocols that allows different software applications to communicate with each other. It acts as a bridge, enabling developers to access specific features or data from a service or application without having to know the details of how the entire system works.
IoT	IoT, or Internet of Things, refers to the interconnected nature of devices and systems that communicate with each other over the internet. These can range from everyday household items like refrigerators and thermostats to industrial tools. By embedding sensors and software in physical objects, IoT allows these objects to collect, exchange, and act on data, often without human intervention, leading to smarter, more efficient systems and processes.
SDK	SDK, or Software Development Kit, is a collection of software tools, libraries, documentation, and sometimes sample code that developers use to create applications for specific platforms or frameworks. An SDK provides a standardized set of development tools, enabling developers to produce software that can run on the intended platform or integrate with a particular service without having to start from scratch.

Glossary

PROMON

Developer terms	Description
Source Code	Source code refers to the human-readable instructions and statements written by programmers in high-level programming languages. This code represents the backbone of software applications, defining their functionalities and behaviors. Before an application can run on a computer, the source code is typically compiled or interpreted into machine code, making it understandable for the computer's hardware to execute.
Tokens	Tokens, within the context of digital security, are unique pieces of data or symbols that authenticate and verify user identity. Generated after successful login, these tokens enable users to access systems or perform actions without repeatedly entering credentials, thereby streamlining authentication processes and enhancing security by reducing the exposure of sensitive information.

Mobile security terms	Description
Blacklisting	Blacklisting is the process of identifying and blocking specific items, such as IP addresses, websites, software, or users, from accessing a particular system or network based on predefined criteria. In the context of cybersecurity, blacklisting helps protect systems by preventing known malicious or undesired entities from gaining access or causing harm.
Code hook	Code hooks are programming constructs that allow developers to insert or "hook" custom code into an existing system, application, or process without altering the original source code. These hooks act as specific interception points, enabling the execution of the custom code either before, after, or in place of the original functionality. Code hooks are widely used for various purposes, such as modifying behavior, monitoring events, or integrating with third-party systems, without having to rebuild or significantly change the primary software.
Malware	Malware, short for "malicious software," refers to any software specifically designed to harm, exploit, or perform unauthorized actions on a computer system, network, or user device. This encompasses a range of malicious entities such as viruses, worms, trojan horses, ransomware, and spyware, with the primary intent being data theft, system damage, or the creation of backdoor access points.
Obfuscation	Obfuscation refers to the deliberate act of making something unclear or difficult to understand. In the context of software development, obfuscation is often used to transform source code or data into a format that is hard to read and comprehend, primarily to protect the code from unauthorized access, theft, or tampering, while still retaining its original functionality.
Root & jailbreaking	Rooting: Specifically for Android devices, rooting provides users with "root" access to the Android operating system, allowing them to modify system files, remove pre-installed apps, and install specialized tools that require deeper system access. Jailbreaking: This term is primarily used for Apple's iOS devices. Jailbreaking lets users bypass Apple's strict ecosystem to install unofficial apps, themes, and extensions that are not available through the official App Store.
Whitelisting	Whitelisting is the practice of explicitly allowing certain identified items, such as IP addresses, websites, software, or users, to access a specific system or network. Contrary to blacklisting, where everything is allowed except what's specifically denied, whitelisting operates on the principle that everything is denied except what's specifically approved, making it a more restrictive security approach.

PROMON

Introduction to Promon

Creating a global category leader for mobile application security

November/2016

Forbes

Security firm sees Tesla risk from smartphone hackers targeting owner app

November/2022

TechCrunch

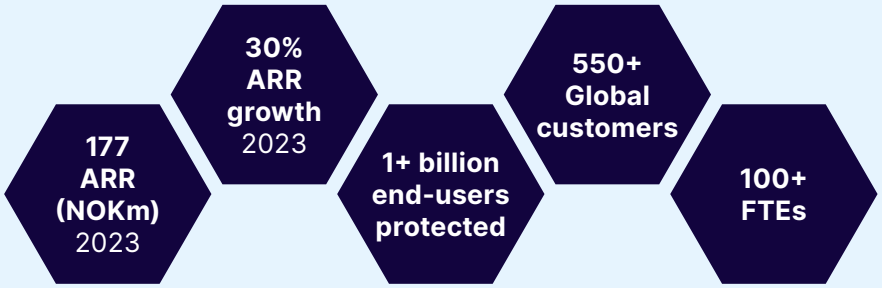
Aiphone door entry systems can be “easily“ bypassed thanks to NFC bug

December/2019

BBC

Android ‘spoofing‘ bug helps targets bank account

Key KPIs



Highlighted customers of select verticals[1]

Banking

HSBC · Deutsche Bank · citi · Santander

Payments and other finance

stc pay · albo · ZaloPay

IT Services and IT software vendors

accenture · Aurea · LUXTRUST Enabling a digital world · salesforce

Public sector

Agency for Digitisation, Ministry of Finance

Gaming

SUPERCELL

Other

NETFLIX · MERALCO · sky

Note: 1) List of verticals and customers within verticals are not exhaustive

Promon's history

PROMON

A look back

In 2006, Promon was founded with a mission to transform the mobile app security and digital trust industry. At the time, mobile app security was in its early stages, characterized by limited attention to app protection and significant security vulnerabilities. Promon set out to address these vulnerabilities and reshape the landscape of mobile app security through their core product, the SHIELD™ platform.

SHIELD™ is an advanced security platform designed to protect apps on various mobile devices. It focuses on preventing attacks both when the app is running and when it's inactive, a step beyond the normal protection that competitors provide.

Promon quickly gained recognition by proving the ease of hacking into reputable systems, underlining the need for improved mobile app security. Their ability to hack into e.g., a Tesla or into the White House's intercom provider underlines the necessity of continuous improvements of application and IoT security, even for the most secure institutions of the world.

Timeline

2006
Promon founded by Tom Lysemose to combat rising threat levels towards mobile applications

2021
Promon announces partnership with F5 to simplify mobile SDK integration[1]

2021
Promon receives strategic investment from GRO, QIC, Kirk Kapital and Trifork (the GRO consortium)

2023
Promon launches their state-of-the-art Jigsaw code obfuscation technology

Note: 1) F5 is the industry's leading multi-cloud application security and delivery company

Taking Promon further

Executing on strategic objectives

Promon is, and strives to remain, a product-first company, becoming the category leader in app-shielding. As Executive Chair & CEO Andreas Thome states, the company must be top of mind in Silicon Valley when data protection is considered.

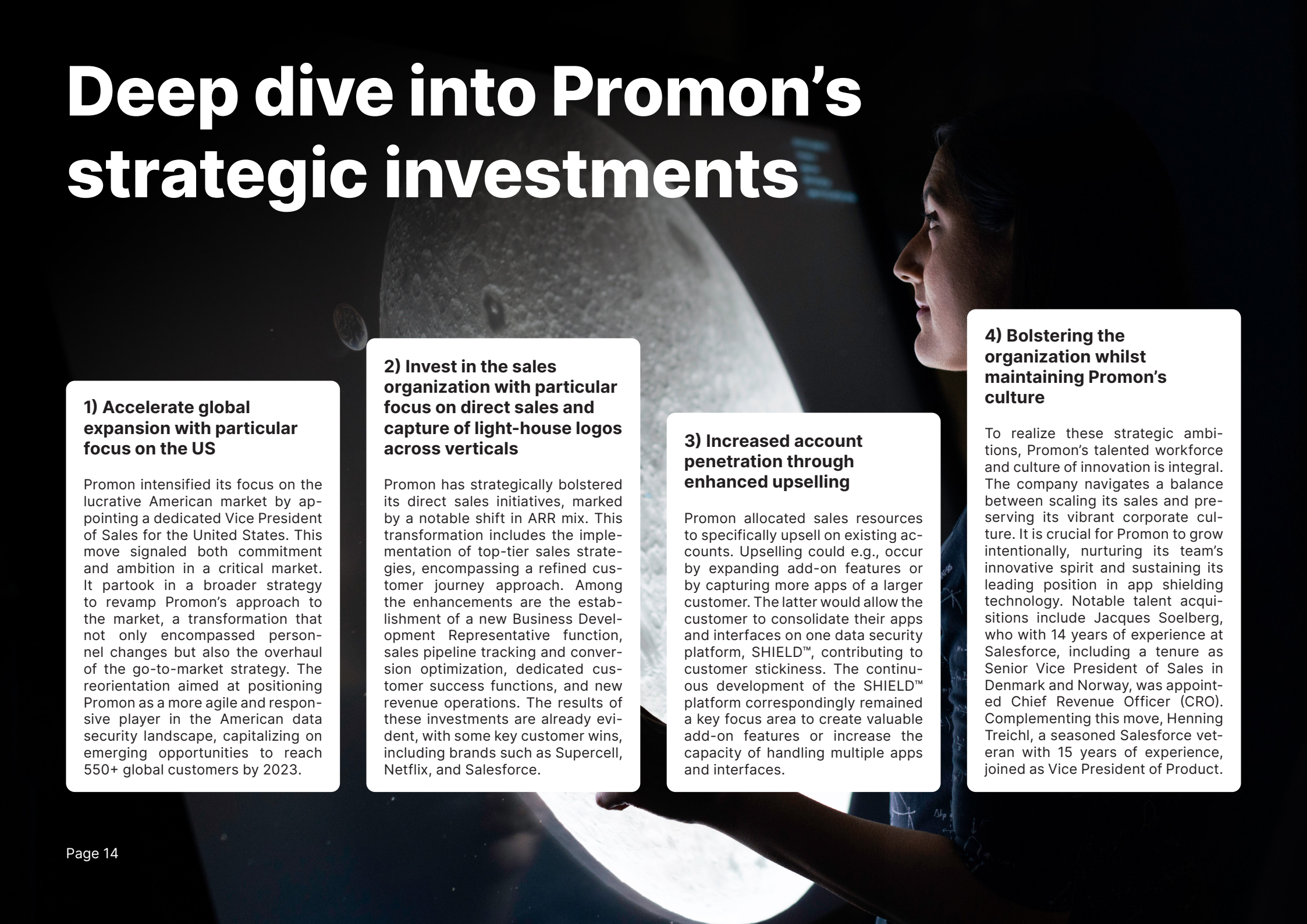
This should be accomplished by leveraging the strong Promon SHIELD™ platform and building standardized solutions for different verticals on top of the advanced platform. Thus, Promon aims to avoid becoming a consultancy tailoring solutions to key accounts.

Executing on strategic investments

The GRO Consortium's acquisition of Promon marked a major shift, with a renewed focus on new strategic goals requiring significant investments. Recognizing the strength of the SHIELD™ offering, GRO strategically focused on increasing the company's ARR by targeting four main areas:

i) Accelerate global expansion with particular focus on the US
ii) Invest in the sales organization with particular focus on direct sales and capture of light-house logos across verticals
ii) Increased account penetration through enhanced upselling
iii) Bolstering the organization whilst maintaining Promon's culture

Deep dive into Promon's strategic investments



1) Accelerate global expansion with particular focus on the US

Promon intensified its focus on the lucrative American market by appointing a dedicated Vice President of Sales for the United States. This move signaled both commitment and ambition in a critical market. It partook in a broader strategy to revamp Promon's approach to the market, a transformation that not only encompassed personnel changes but also the overhaul of the go-to-market strategy. The reorientation aimed at positioning Promon as a more agile and responsive player in the American data security landscape, capitalizing on emerging opportunities to reach 550+ global customers by 2023.

2) Invest in the sales organization with particular focus on direct sales and capture of light-house logos across verticals

Promon has strategically bolstered its direct sales initiatives, marked by a notable shift in ARR mix. This transformation includes the implementation of top-tier sales strategies, encompassing a refined customer journey approach. Among the enhancements are the establishment of a new Business Development Representative function, sales pipeline tracking and conversion optimization, dedicated customer success functions, and new revenue operations. The results of these investments are already evident, with some key customer wins, including brands such as Supercell, Netflix, and Salesforce.

3) Increased account penetration through enhanced upselling

Promon allocated sales resources to specifically upsell on existing accounts. Upselling could e.g., occur by expanding add-on features or by capturing more apps of a larger customer. The latter would allow the customer to consolidate their apps and interfaces on one data security platform, SHIELD™, contributing to customer stickiness. The continuous development of the SHIELD™ platform correspondingly remained a key focus area to create valuable add-on features or increase the capacity of handling multiple apps and interfaces.

4) Bolstering the organization whilst maintaining Promon's culture

To realize these strategic ambitions, Promon's talented workforce and culture of innovation is integral. The company navigates a balance between scaling its sales and preserving its vibrant corporate culture. It is crucial for Promon to grow intentionally, nurturing its team's innovative spirit and sustaining its leading position in app shielding technology. Notable talent acquisitions include Jacques Soelberg, who with 14 years of experience at Salesforce, including a tenure as Senior Vice President of Sales in Denmark and Norway, was appointed Chief Revenue Officer (CRO). Complementing this move, Henning Treichl, a seasoned Salesforce veteran with 15 years of experience, joined as Vice President of Product.

Organizational overview

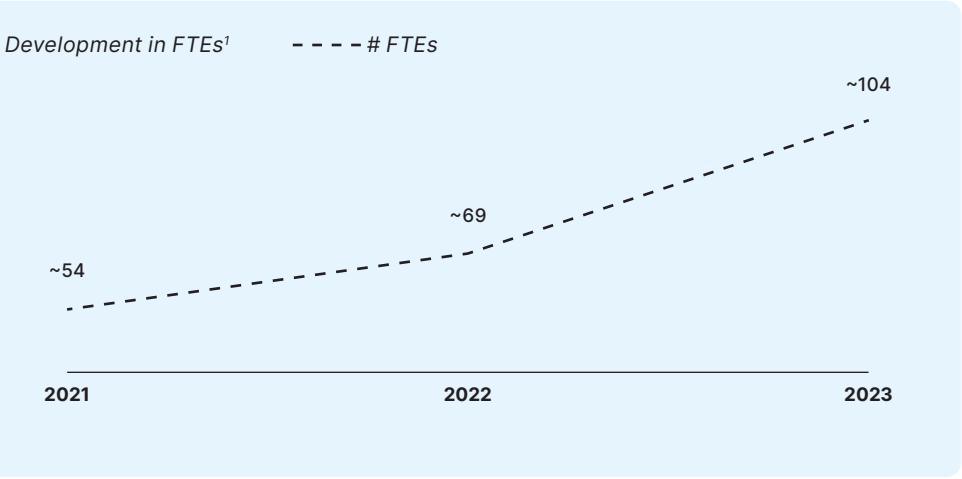
PROMON

Promon's strategic growth and cultivated culture

With over 100 employees spanning across 15 countries, Promon has experienced significant growth over the past 2-3 years. Despite its expansion, the organization maintains a healthy dynamic, characterized by high engagement levels, low turnover rates, and minimal sick leave.

Recognizing the importance of continual improvement and development, Promon has made substantial investments to bolster its capabilities and drive strategic objectives forward. Central to the realization of these ambitions is Promon's talented workforce and culture of innovation.

The company adeptly navigates the delicate balance between scaling its sales operations and preserving its vibrant corporate culture. This holistic approach ensures that Promon's growth fosters a culture where creativity and market leadership seamlessly intertwine.



Promon's management team

Andreas Thome
Executive chair & CEO

Experience: Former CEO of Play Magnus Group and Former COO of Opera

Jacques Soelberg
Chief Revenue Officer

Experience: Former SVP of sales at Salesforce for Denmark and Norway

Tom Lysemose
Chief Technology Officer

Experience: Founder and CTO of Promon

Jan Vidar Krey
Chief Development Officer

Experience: Team manager and lead developer at Opera Software

Ane Nysveen Hellum
Chief People Officer

Experience: Senior HR Advisor at KMPG and HR Recruitment Business Partner at Nets Group

Amelie Dunder
Chief Financial Officer

Experience: Senior Auditor at Deloitte, Risk Manager at Niam AB, and Financial Controller at Gresvig AS

Management experience

Deloitte. nets PLAY MAGNUS GROUP OF COMPANIES

cisco KPMG Opera salesforce

Note: 1) See financials for a detailed overview of FTEs per function

PROMON

Promon SHIELD™ and Mobile Application Security

An introduction to mobile application security

PROMON

What is mobile application security?

When an app is downloaded onto a device, the app—and by extension, its developers— is granted access to a section of the phone or tablet that lies beyond the built-in antivirus and API protection. This exposed area offers potential attackers a tempting gateway to the device and its stored data and ongoing activities. Threats can stem from legitimate apps with inadequate defenses against external dangers or from illegitimate apps that exploit this vulnerability to gain unauthorized access. The consequences can be severe, as hackers may gain access to a phone's entire operating system through an infiltrated app. This can lead to hackers extracting passwords, personal information, or create overlays to continuously monitor activity on the mobile device, with the user being oblivious to this occurring. The impact on businesses is significant with accumulated losses to online payment fraud estimated at more than $200 billion between 2020-2024 for key industries. Promon addresses this frequently overlooked middle-layer of data protection with the SHIELD™ security platform, and active deep protection technology.

Source: Promon website

The three layers of mobile security

1

Antivirus protection

Antivirus layers in mobile devices consist of real-time scanning mechanisms that actively monitor and analyze app behavior, files, and web traffic to detect and neutralize malicious activities. They also include system optimization tools and privacy measures to enhance device performance and protect user data from unauthorized access.

PROMON

2

App protection

The app protection layer extends beyond the standard antivirus and API protections built into most mobile devices. It is an unprotected part of the device's environment, particularly susceptible to security breaches from under-protected or malicious apps. Often overlooked, this layer is where Promon specializes in delivering leading security solutions.

3

API protection

API protection in mobile devices involves securing the communication between mobile applications and the external integrations / servers to prevent unauthorized access and breaches. This includes implementing measures such as authentication, encryption, and API rate limiting to safeguard sensitive information and ensure data integrity.

Promon SHIELD™

PROMON

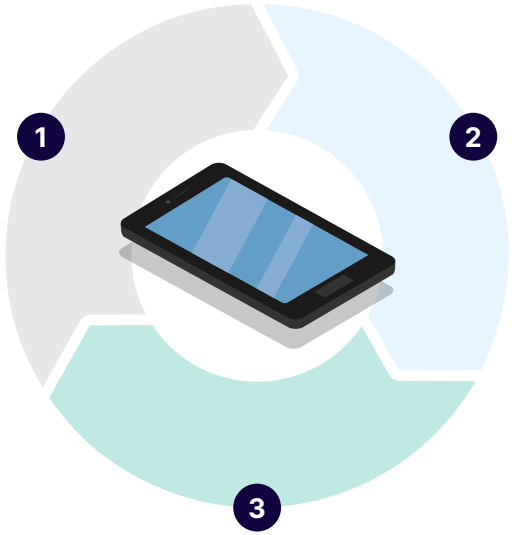
Promon SHIELD™ is the company's platform for building in-app security parameters. While many security solutions focus on protecting apps from external threats, SHIELD™ specializes in i) defending against attacks while users are active on the app (runtime attacks) and, ii) when users are not active on their app (rest periods). Many traditional mobile security solutions focus on perimeter defenses like ensuring only authorized apps are downloaded. However, once an attacker gets past these defenses, and the app is running, the application often becomes vulnerable without proper runtime protection.

SHIELD™ aims to protect the most common types of mobile devices, such as Apple, Android, Desktop and IoT devices.

Many legacy mobile app security solutions work through blacklisting. This is a reactive approach, where known threats are blocked, while all other signals, either known or unknown, can pass through the security parameters. The drawback to this approach is the potential for malware to enter the apps protected environment if it has not been blacklisted. SHIELD™ uses the opposite approach, utilizing a method known as whitelisting. Whitelisting only allows specific preapproved entities access to the app, whether they be API endpoints, IP addresses or other software applications. All other entities are either blocked from the app or flagged for subsequent review.

SHIELD™ continuously checks for malicious signals, either while the app is at rest or during runtime. When an event or signal is detected, the appropriate response can then be defined by the customer. This includes everything from providing notifications to the developers or users, to shutting down the app, preventing a security breach.

SHIELD™: An end-to-end mobile app security platform



1

Protect

Protect against:
- Reverse engineering
- App modification and spoofing
- Security control tampering

2

Detect

Monitor and detect:
- App runtime behavior
- Insecure environment execution
- Overlay attacks, debuggers, and emulators

3

React

Modify app behavior in real-time by:
- Blocking execution of injected code
- Notifying security admins
- Terminating infected apps

SHIELD™ security layers

PROMON

Device protection

When a device is compromised, the user or hacker is allowed to access subsystems of the mobile device. This is known as rooting/jailbreaking. It allows the hacker to gain additional capabilities and to deactivate crucial security mechanisms. Promon has several mechanisms to detect root/jailbreaks and notify administrators or launch direct countermeasures.

Malware protection

Malware is malicious software designed to give unauthorized access to operating systems, with the aim of stealing data, compromising the device, or creating backdoors. Malware can be installed by malicious droppers, which are apps that either have or pretend to have the functionality of popular apps and are installed via official app stores. Once downloaded onto the unprotected environment, they can access the user interface (UI) of other apps introducing screen readers to e.g., read confidential information or access codes. SHIELD™ can detect whether malicious screen readers are active and block them from accessing the protected app, while hindering screenshots or mirroring.

Reverse engineering

Reverse engineering implies dissembling and analyzing an application with the purpose of extracting information such as passcodes or tokens. Attackers will usually try to reverse engineer an app with the purpose of understanding its weaknesses, stealing sensitive information or valuable parts of the app. Promon counters this through its obfuscation technology, making the source code inherently difficult to analyze, while constantly monitoring the app's runtime behavior for anomalies.

App repackaging

App repackaging involves attackers accessing the source code of a popular app, modifying the code to install malware upon download, and then redistributing it. The new app, visually identical to the original app, is however infected with malicious code potentially compromising the security of the device. Integrating SHIELD™ into the app's source code creates a strong binding that makes dismantling security features extremely difficult for hackers, while obfuscation through Promon's Jigsaw technology makes it extremely difficult to introduce malicious coding into the app.

Code injection

Attackers can discreetly inject code into an app to gain control of it. The code can then be used to read encrypted information, bypass security measures, or intercept user inputs. SHIELD™ can detect code injection and block them before they become a security breach.

Data/asset protection

As users increasingly use mobile devices to store sensitive data through banking apps, social security cards, drivers' licenses etc., the threat of attacks increases and correspondingly does the requirement for protection. The data or assets we store may be compromised due to inadequate encryption, insecure data storage, insufficiently protected API-linkages, and a lack of proper authentication allowing unauthorized users access to certain data. Promon counteracts these threats by storing app secrets through tokens, API keys, and personally identifiable information, stored locally and encrypted. The encryption key is not stored locally on the device for attackers to find and use but is dynamically generated such that it cannot be used to decrypt sensitive information.

Next generation protection

One of Promon's cornerstones for data protection is their obfuscation technology. Obfuscation works by randomly scrambling the source code of an application, making it very difficult to read for attackers. In short, obfuscation is a way of encrypting the underlying code of an app. This technique is valuable in protecting against attacks where the source code is either copied and its IP stolen, is injected with malicious lines of code, is reversed engineered, or to prevent the theft of sensitive information written into the source code.

Historically, obfuscation has worked using a static rule-based system. This can be compared to a lock with a single key: if you have the correct key, you can open the lock. While this has worked well previously as security providers were able to safely store the encryption key such that the obfuscated code could not be reassembled into the original form, the advances in AI has led to great vulnerabilities as the AI is able to analyze the patterns in the scrambled source code and thus reverse engineer the encryption key, leading to a serious security breach.

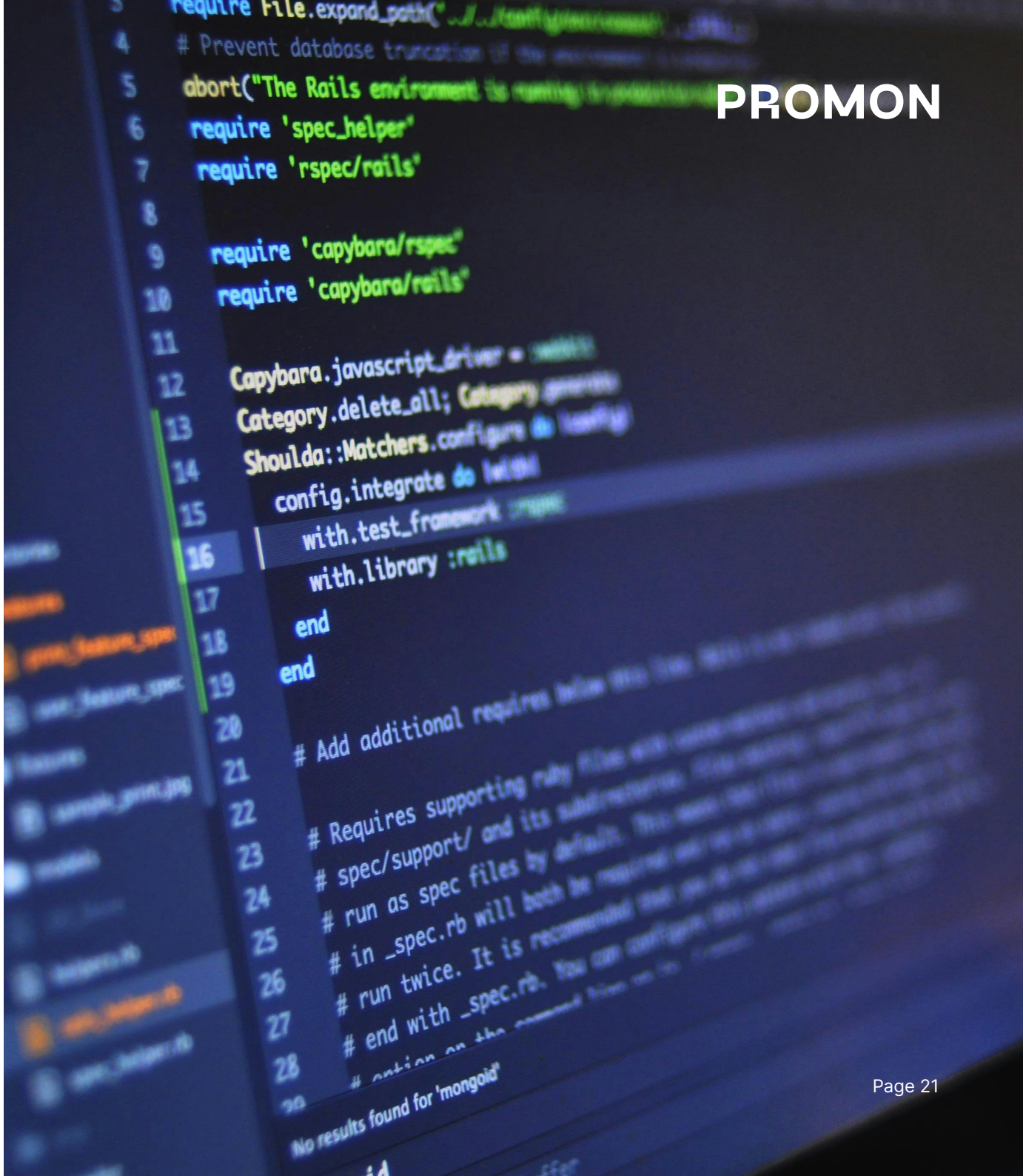
Promon's patent-pending Jigsaw obfuscation technology works as a major differentiator in this aspect, as it is prepared to incorporate dynamic obfuscation of the source code with low code/high user friendliness. Dynamic obfuscation is a technique in which code is obfuscated in real-time while the application is running. This means that even if an attacker manages to decipher a portion of the obfuscated code at one point in time, that deciphered code might be obfuscated differently moments later, rendering the attacker's insights obsolete. This advanced feature will help significantly enhance the levels of security provided by the SHIELD™ platform.

Promon Integrator

Working with customers to incorporate SHIELD leads to a reoccurring question: how to securely add the program to the source code. Usually, this task is complex and time-consuming, often causing issues like incompatibility with existing code, increased complexity, or worsened app performance. Additionally, developers typically prefer to focus on creating new features and improving user experience, rather than on security enhancements.

To address this, Promon developed the Integrator Tool. The technology is offered as a Software Development Kit (SDK), a 'toolbox' for programmers that automatically integrates SHIELD™ into the source code, reducing what could be a lengthy task to minutes. This saves developers time while allowing them to concentrate on enhancing or developing new core features. This technology is a major differentiator for Promon over its competitors and a key supporting tool for the SHIELD™ platform. Integrator has also been leveraged to gain access to attractive partnerships.

While Integrator primarily serves as a support tool, there's been discussion about its potential as a standalone product.



What is next for Promon?

PROMON

Unlocking greater value for customer verticals

Promon is actively enhancing its security features to maintain its position as a leader in mobile application protection. This involves staying ahead of both competitive developments and evolving cybersecurity threats. In parallel, Promon is innovating to provide more customized solutions for diverse verticals, such as banking, payment processing, gaming, streaming, and healthcare. While all prioritizes effective data protection, each industry also has unique security needs; for instance, government and healthcare sectors are expected to safeguard highly personal information, while gaming companies focus on safeguarding in-game elements like tokens and to prevent cheating.

To address these varied requirements, Promon prioritizes introducing industry-specific data protection packages. These standardized solutions will better align with the distinct needs of each industry. The technical groundwork for this customization has been laid through enhancements to the SHIELD platform, which now boasts greater flexibility. This effectively allows Promon to activate or deactivate specific features or lines of code based on client needs. Additionally, it paves the way for the potential introduction of a 'light' version of the SHIELD platform, expanding Promon's reach to smaller businesses.

While the development of these customized vertical solutions is nearly complete, critical decisions remain. These include determining the appropriate mix of protection features for each industry and establishing a pricing strategy that reflects the value delivered to each vertical.

What is next for Promon?

Promon Insights

Promon's extensive customer base grants it access to a wealth of global data on cybersecurity threats. This allows the company to leverage advanced analytics for identifying varying patterns and trends in malicious attacks. Exploring this capability, Promon is considering the creation of an additional service: providing clients with detailed threat assessments and insights.

This new service would enable clients to better understand the specific security risks their applications face. By offering timely and informed threat analysis, Promon can help clients anticipate and prepare for potential security challenges, thereby enhancing clients' data integrity. Moreover, these reports could include practical and actionable recommendations on how to better fortify their apps. A key feature of 'actionable insights' would be implementation of security enhancing code, without necessitating updates, streamlining the process for enhancing app security, while making usage easier and safer for the end-user. This add-on service could be a valuable extension to Promon's existing offerings.

Other considerations

In addition, the adaptability of the SHIELD platform itself opens numerous opportunities for market expansion. This could involve branching out to new device types or into related security domains, such as integration with various IoT applications. While these possibilities are tempting, it is imperative for Promon to balance the opportunities with the ability to maintain its scalability and not compromise its established strengths in protecting mobile applications.

PROMON

Go-To-Market

Promon Go-To-Market strategy

PROMON

Pricing

Promon employs a SaaS business model centered around its SHIELD™ security platform, and its pricing strategy is tiered along app-usage as well as the depth of security requirements of the clients. For applications with more than 2 million annual users, Promon offers customized pricing. In contrast, for smaller customers, a standardized tier-based pricing system is employed, determined by the annual number of users on all applications associated with the specific account.

The final pricing is influenced primarily by two factors: firstly, the total number of users and applications protected by SHIELD™, and secondly, the quantity of additional modules purchased. These modules represent value-adding features, such as enhanced IP protection, improving the base protection. Additionally, for every application a customer opts to secure with SHIELD™, Promon charges a one-time fee.

While the existing pricing model has been effective, Promon and GRO are exploring ways to refine it further, aiming to maximize value for their customers. This focuses on three main considerations: firstly, implementing pricing based on active users instead of total users to more closely align with the value delivered to customers; secondly, customizing offerings and pricing for specific industry verticals to address the diverse needs of various customer segments; and thirdly, adjusting pricing according to regional markets, acknowledging the variations in willingness to pay across different geographies.

Promon Go-To-Market strategy

PROMON

Sales channels

Promon markets SHIELD™ using two primary channels: direct and indirect/ partner sales. Historically, partner sales constituted most sales volumes. Major partners include OneSpan, Lookout, and F5, where SHIELD™ is often integrated into the partner's existing solutions as a white-labelled product, complementing their offerings. Such relationships would be considered OEM agreements. The key benefit of the OEM partnerships is their ability to tap into extensive new customer bases while maintaining low customer acquisition costs (CAC). Additionally, integrating SHIELD™ into broader security systems enhances the overall value proposition to end users.

The partner channel pricing structure is dependent on the level of commitment each partner is willing to make to Promon. The greater the commitment, the lower price the partner can offer its customers, and the greater the number of dedicated resources the partner will receive from Promon.

Effect of strategic investments

Direct sales have played an increasingly important role since the GRO consortium's entry into Promon, as investments into the company's own sales force were greatly increased. The direct channel was prioritized for two key strategic reasons: firstly, it allows for enhanced control over the sales process, and secondly, it enables direct engagement with progressively larger accounts. The investments have so-far proven effective, with the share of ARR coming from Direct channels being up from 41.7% in 2021 to 58.3% in 2023.

Selected OEM partners

F5 is a provider of application delivery and security solutions. Their product portfolio includes application delivery controllers, load balancers, web application firewalls, and DDoS protection services.

Lookout provides cutting-edge mobile cybersecurity solutions since 2007. Their product offerings include mobile endpoint security solutions, app security, threat intelligence services, and mobile risk management tools.

OneSpan is a provider of digital identity and anti-fraud solutions. Their product offerings include digital signature solutions, authentication tools, mobile security, and transaction security solutions.

"The greater the commitment, the lower price the partner can offer its customers ..."

PROMON

Upselling to key accounts

Upselling through trust

Promon’s Land & Expand strategy focuses on upselling add-on services and expanding coverage for accounts once the technology is proven to the customer. Customers, typically conservative and risk-averse, find this approach appealing as it allows them to verify the viability and security of the technology before scaling their commitment. Key to Promon’s business model is therefore to incorporate the flexibility to scale either through upselling add-on services or expanding the scope of applications that SHIELD protects for the account or in many cases a combination of both.

Direct channels

‘Land & Expand’ aligns well with the conservative and risk-averse nature of most customers, initiating the relationship with a foundational level of SHIELD protection on an application. This cautious first step allows customers to assess the effectiveness and reliability of the technology in a controlled environment. Following the validation of Promon’s solution, there is potential to escalate the security measures across a broader spectrum of the customer’s applications, coupled with the introduction of additional specialized services. This careful expansion strategy has a track record of increasing Promon’s ARPA by 15-20% annually.

Partner channels

The partner strategy begins by building a foundation of trust, showcasing the capabilities of SHIELD. From there, the aim is to strengthen these relationships by aligning with the OEM partners’ Go-To-Market strategies, thereby increasing mutual commitments. This approach has fostered significant partnerships, for example with OneSpan. In this collaboration, SHIELD has become an integral component of OneSpan’s extensive security solutions, offered as a white-labelled product, creating mutual benefits such as improved product offering and access to a larger customer base.

Taking the strategy further

Promon’s Land & Expand strategy has successfully grown the company’s ARR. However, it is believed that greater value can be extracted from an even more focused execution. This hypothesis is supported by the strategic expansion of the sales force and customer success teams, intensifying resource dedication to existing accounts. It is believed that greater allocation of resources towards existing accounts combined with the future roadmap will enable the company to provide more tailored solutions and in turn drive continuous growth in ARPA.

PROMON

Market and Competitors

Market context and dynamics

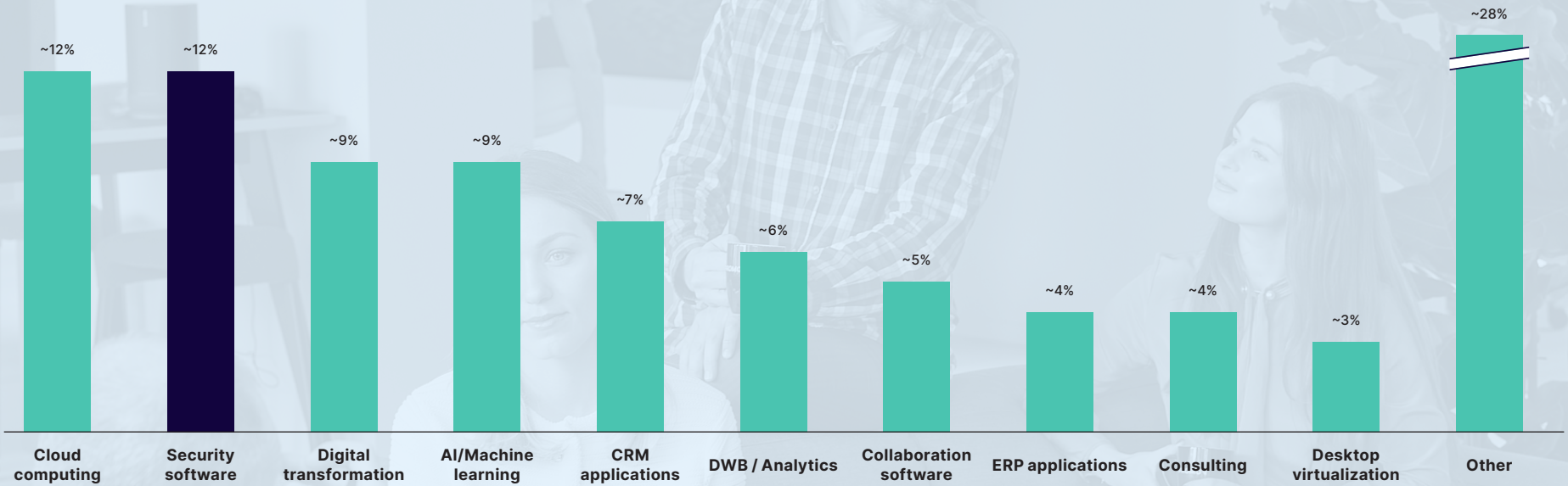
PROMON

Growing awareness of mobile security in the C-suite

With an ever increasingly digital world, security breaches continue to be a threat for consumers and enterprises, creating an urgent threat that companies need to deal with. Out of the overall number of security breaches, 30% are web and application breaches, with the average breach costing $8 million.[1] This percentage could increase as the number of new vulnerabilities found in mobile applications has increased by 300% since 2017.[2] As such, IT security, remains a top agenda for C-suite members and is among the top-ranking CIO IT investment priorities.[3]

CIO Top investment priorities

Projects, with largest spend increases for 2022 (% 0f respondents, n = 100)



Source: 1) Markets and Markets; 2) Build Mobile Security; 3) Morgan Stanley Research

Key market drivers

PROMON

Growing number of connected devices

Today's hyper-connected business environment boosts the rapid development of digital solutions, and associated services leading to an expansive IoT ecosystem. The surge in IoT adoption is reshaping the business landscape, with companies leveraging IoT technologies to gather, analyze, and act upon vast amounts of real-time data. As this ecosystem expands, so does the attack surface for potential cyber threats. This requires new and innovative ways to protect organizations' critical infrastructure against data risks and ransomware.

With Covid came the proliferation of remote work. This decentralization of the workforce, with employees operating beyond secure office networks, has become a focal point for cyber threats. These often less-secure working environments have presented an expanded attack surface for malicious actors seeking to exploit vulnerabilities in remote access points, unsecured home networks, and personal devices used for work. This is further exacerbated by the adoption of the Bring Your Own Device (BYOD) in which freelancers and employees are allowed to use personal electronic devices at work. From 2017 to 2023, the number of freelancers in the US grew with a CAGR of 4.2%. This trend presents challenges, such as unauthorized data access, data loss, and malware assaults.

Enterprise mobility

Increase in mobile apps

Every month over 100,000 new Android/IOS apps are released. Many of these apps, particularly those designed for consumer use, often necessitate access to sensitive information, ranging from personal details to financial data. This issue becomes particularly critical given the habits of the average user, who typically has more than 80 apps installed on their mobile device. Each of these apps represents a potential entry point for cyber threats, especially considering that 60% of applications with over 5 million downloads reportedly include some form of security flaw. Consumer-facing apps that deal with sensitive information become prime targets for cybercriminals seeking to exploit vulnerabilities for financial gain or unauthorized access to personal data.

Ensuring robust mobile app security is paramount for maintaining a company's reputation. Security breaches can inflict severe damage, diminishing customer trust in a business handling their data. The aftermath of a security incident often leads to lost customers and revenue, as news of compromised user data spreads rapidly, eroding confidence both in the app and the organization behind it. With increasing focus on mobile application security, an increased number of companies have heightened their focus on implementing sufficient security parameters.

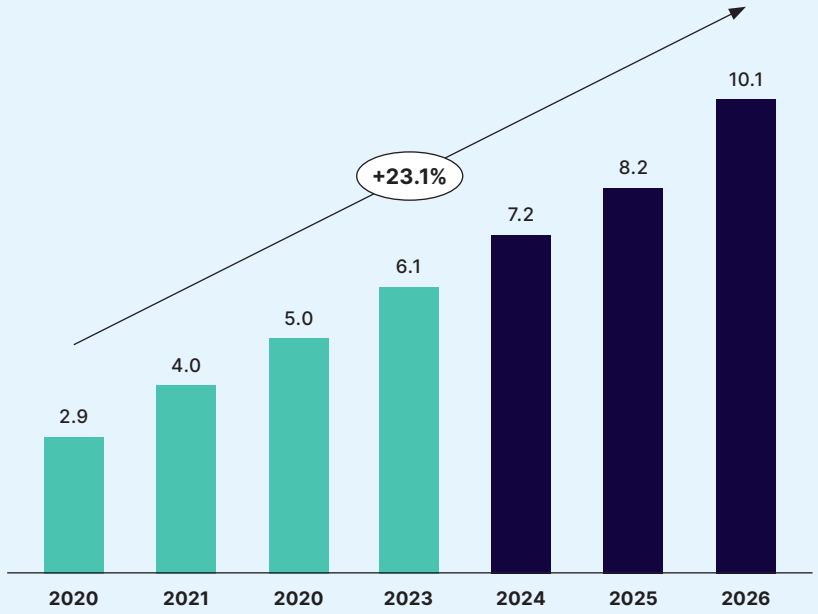
Reputation

Market size

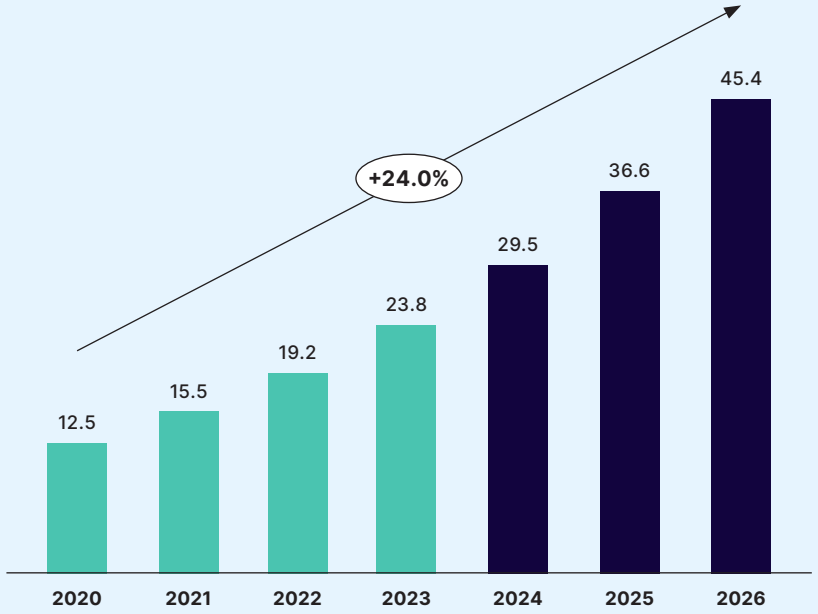
PROMON

Within the next couple of years, the global app security market is expected to grow with a **CAGR of 23.1%**, reaching a total size of **10.1 billion dollars** in 2026.

Global app security market, billion dollars



Global IoT security market, billion dollars

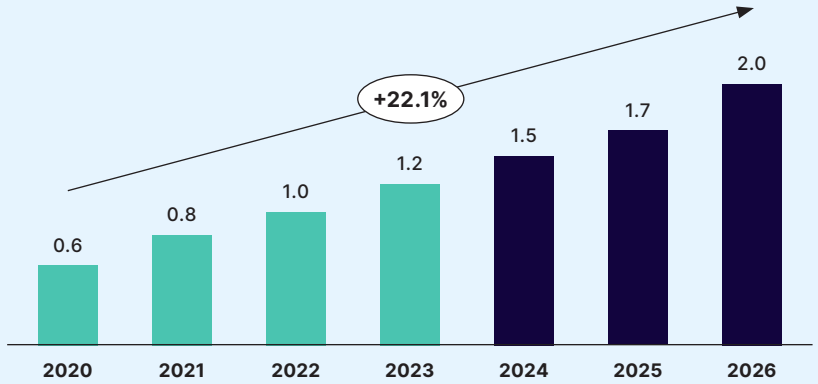


Source: Gartner

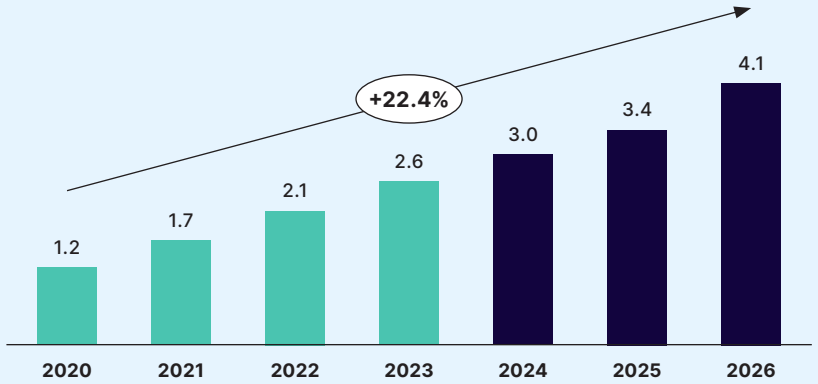
Geographic market split

PROMON

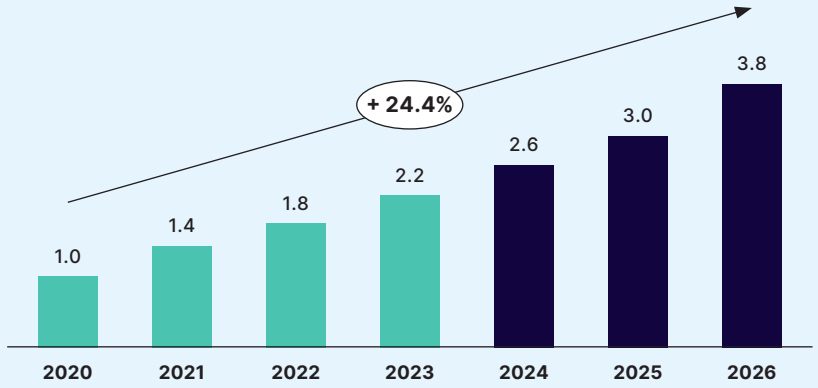
EMEA app security market, billion dollars



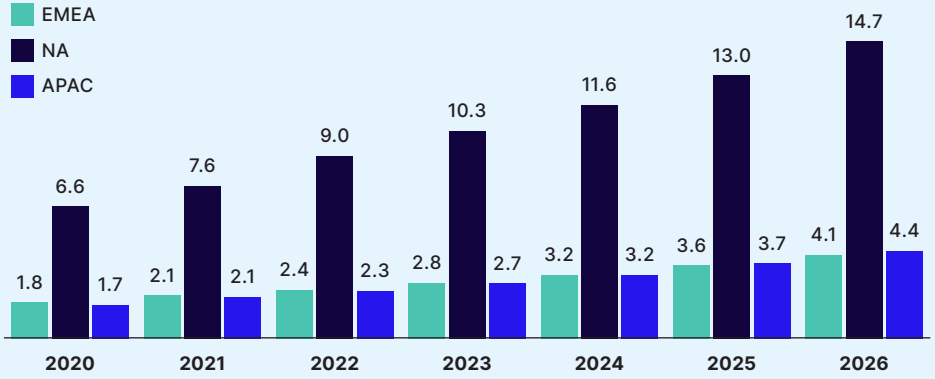
North America app security market, billion dollars



APAC app security market size, billion dollars



Application security spend per employee, dollars



Source: Statista and case writers' own analysis

Main competitors

PROMON

Competitor landscape

Promon differentiates itself from its main competitors through its innovative security solutions and unique integration capabilities, notably via the Integrator tool. This combination of innovation and practical integration offers a distinct advantage in the market. Positioned as a next generation app security vendor, Promon encounters competition from established legacy app security vendors, with the largest four being Digital.ai, Guard Square, Appdome, and Zimperium. The comparison of the five companies' capacity for service offerings clearly showcases Promon's leading position.

	Next Generation App Security	Legacy Mobile App Security Vendors			
	PROMON	digital.ai	GUARDSQUARE Mobile application protection	appdome	ZIMPERIUM
Runtime protection	●	◔	◔	◔	◑
Integration & Deployment Speed	●	◔	◔	◕	◔
Configuration	●	◔	◔	◔	◔
Effect on End-user Experience	●	◑	◑	◔	◑
Security Level	●	◕	◑	◔	◔
Self-contained Autonomous Security Assessment	●	◔	◔	◔	◔
At rest protection	◕	●	●	◔	●

Competitor deep-dives

PROMON

digital.ai

900+ FTEs

Digital.ai is a major player in the app shielding sector, specializing in mobile and web application security. Their extensive product line-up includes security software, assessments, and intelligence tools, offering valuable insights and enhanced functionalities. Compared to Promon, Digital.ai is more entrenched in run-time protection and closely matches Promon in overall security capability. In the US market, Digital.ai serves as Promon's primary competitor. Their diverse portfolio allows them to leverage cross-selling opportunities, expanding their client base across various channels. With a strong presence among the top US and European banks, US airlines, and top ten largest gaming companies, Digital.ai boasts significant brand recognition

GUARDSQUARE

Mobile application protection

150+ FTEs

Guard Square provides mobile app security with multiple layers of protection, helping companies across industries, ranging from financial services to e-commerce, gaming, and media, in assessing and identifying security weaknesses and optimizing their security. They support developers in the development phase via vulnerability assessments, enabling developers to identify security gaps and make early improvements before external penetration testing. Once the app is developed and protected, Guard Square offers continuous security support and monitoring and provides feedback on the protection's coverage and efficacy. Like Digital.ai, Guard Square is more established in run time protection than Promon.

appdome

150+ FTEs

Appdome stands out from the other three competitors in terms of their capabilities in integration and deployment speed, closely following Promon on this parameter. Appdome has a good depth and breadth to their security solutions, i.e., customization abilities alongside a largely automated product implementation. For example, Appdome's automation platform enables developers to fully implement their choice of over 150 different mobile app security features into any iOS and Android app instantly. However, they are clearly behind on the other parameters, resulting in the lowest security level of the five companies.

ZIMPERIUM

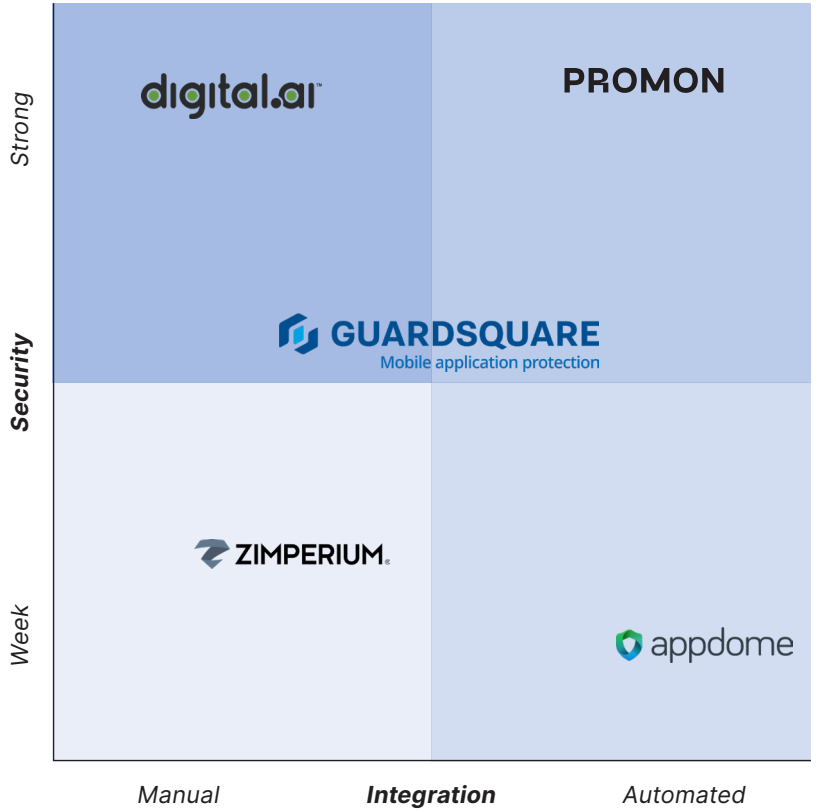
200+ FTEs

Zimperium specializes in a range of security solutions for mobile apps, encompassing security assessments, protection through obfuscation and anti-tampering, as well as a unified platform that allows for centralized management of app security. Like Guard Square, they support developers in the development phase via vulnerability assessments and continue their support later, especially via runtime protection. Like Promon, Zimperium's mobile security offering and platform supports differentiated protection packages to different verticals. However, this is a largely manual process making it a more resource-intensive process of selling each unit.

Competitor matrix

PROMON

The five companies are all trying to seize the opportunity of filling the demand for enhancing app security and safeguarding user activities on apps. While the competitors encompass respective advantages, **Promon excels in easy integration and deployment speed.** Furthermore, the unique obfuscation engine, Jigsaw technology, runtime and rest protection and the Integrator Tools make for a substantial competitive advantage.



PROMON

Financial Performance

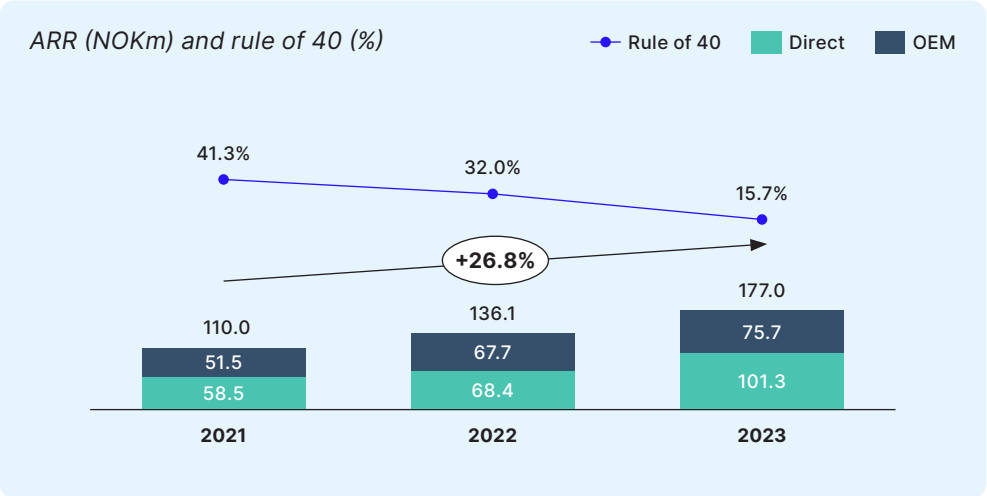
SaaS performance metrics and ARR

PROMON

The following section pertains to the consolidated financial statements of Promon and its subsidiary companies.

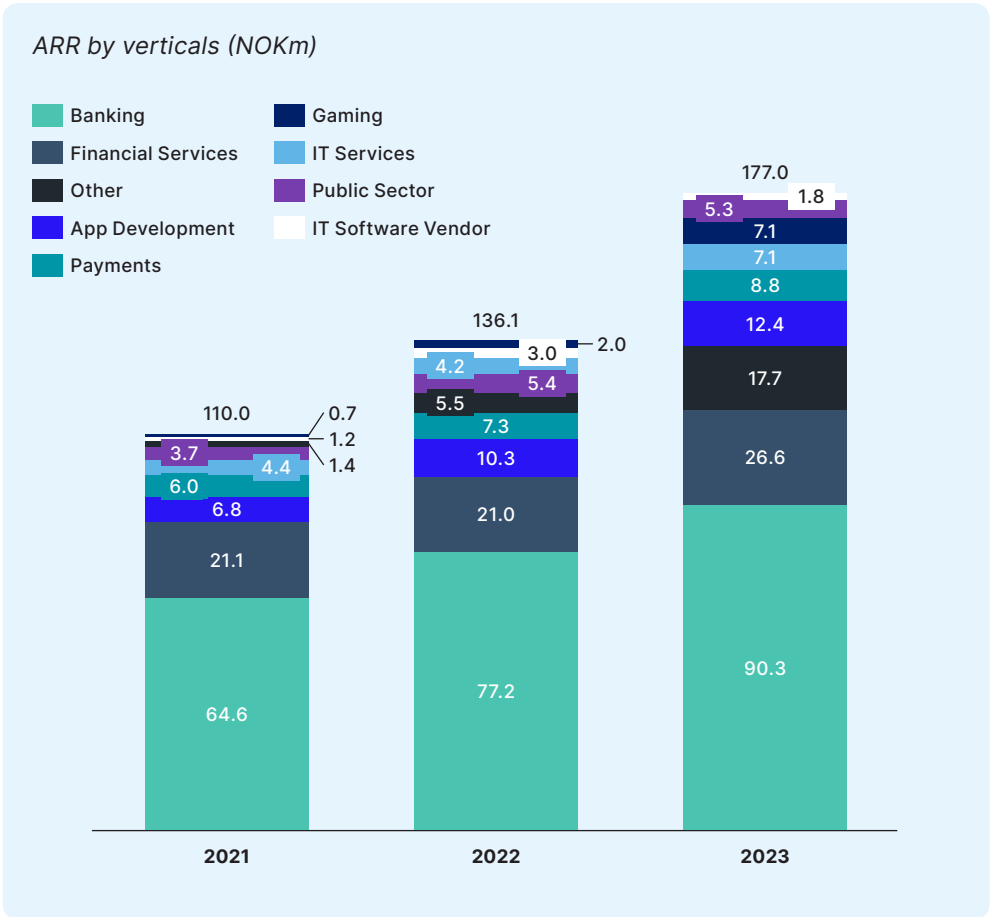
Promon has experienced a substantial surge in ARR since 2021, witnessing a growth from NOK 110m to NOK 177m by 2023. This expansion is attributed to the segmentation of ARR into two primary channels: direct and partner. Historically, the distribution between these channels has been relatively balanced. However, there is a notable shift towards the direct channel, making up 57.2% of the total ARR in 2023, with the shift towards direct channel expected to continue. Focus on ARR growth and a shift towards direct, has meant that margins have decreased as large investments in S&M have been made. This can be observed in both the decreasing rule of 40 and cash EBITDA margin. Thus, GRO and Promon have deliberately prioritized the expansion of their S&M division, accepting current lower margins. Going forward, for 2025-2026, management expects ARR growth in the range of 35-40%, with a cash EBITDA margin of 0% or above.

Management expects that the ARPA of existing customers will be NOK 540k while ARPA for new customers will be NOK 470k. Further, management assumes that customer acquisition costs (CAC) will be NOK 1m while the Customer Lifetime Value (LTV) will be NOK 11m.



ARR by vertical

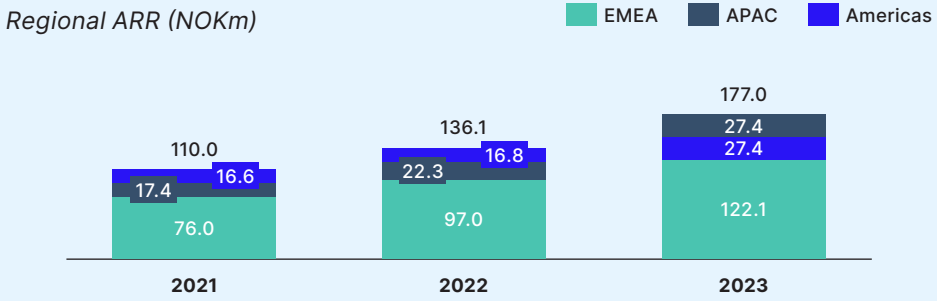
Examining ARR by vertical, the Banking and Financial Services sector previously dominated, constituting 78% of the total ARR. However, as Promon strategically diversified its customer base, this share has now decreased to 66%. Simultaneously, other verticals have witnessed an increase, underscoring Promon's successful expansion into diverse markets.

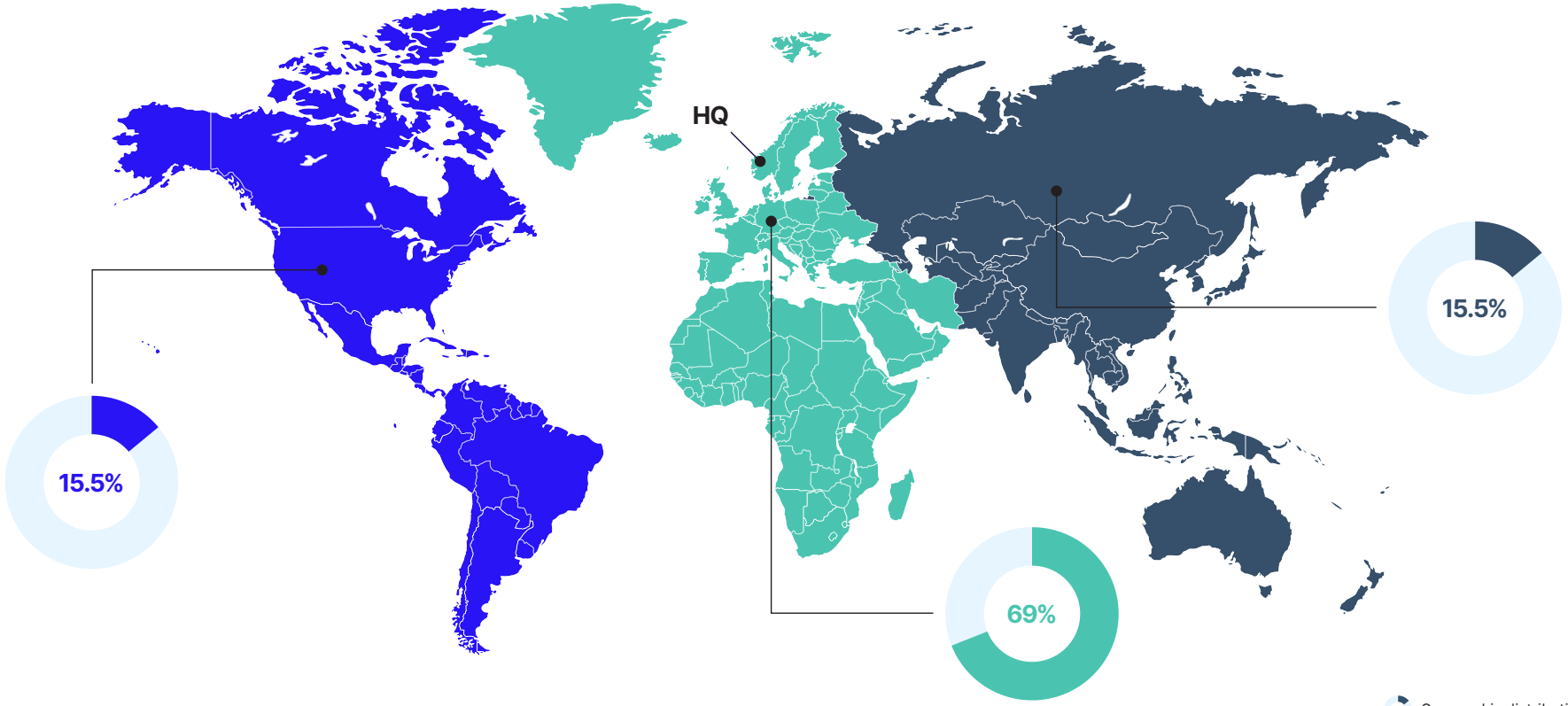


Geographic split of ARR

PROMON

Geographically, ARR is categorized into three regions: EMEA, APAC, and the Americas. Notably, the Americas have been steadily increasing their share of the total ARR since 2021, signaling a robust growth trajectory. EMEA and APAC have, although making up a smaller share of ARR, also increased at decent rates. This geographical distribution highlights the evolving landscape of Promon's market presence and underscores the company's growing footprint in the Americas.





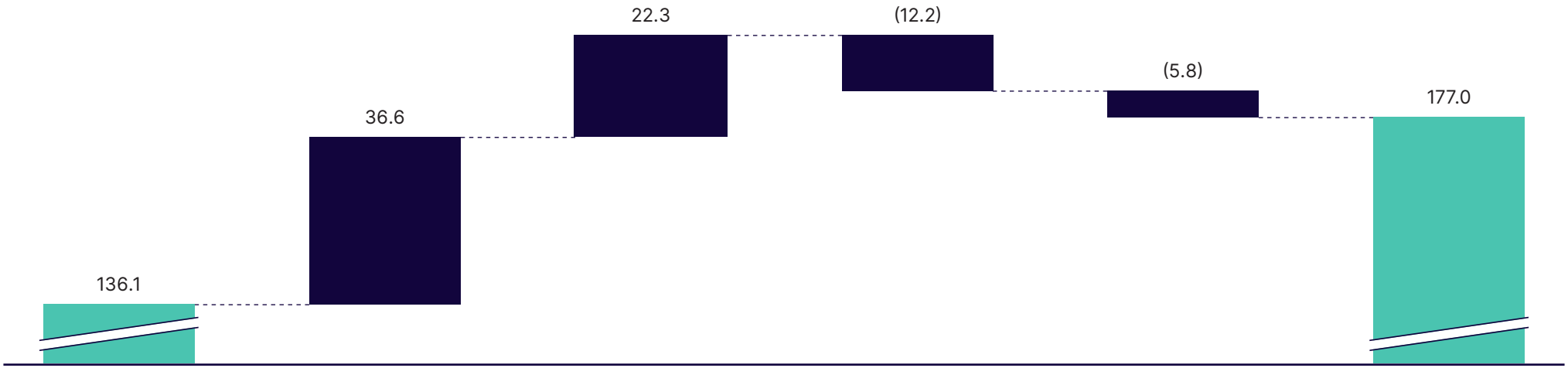
Geographic distribution of FY23 ARR

Breakdown of ARR

PROMON

ARR development between 2022 and 2023 (NOKm)

In examining the development of ARR between 2022 and 2023, net new ARR can be broken into new ARR of NOK 36.6m, expansion ARR of NOK 22.3m, downsell ARR of NOK (12.2m), and churn ARR of NOK (5.8m), resulting in net new ARR of NOK 40.9m. These figures highlight a robust retention of customers, with a Gross Revenue Retention (GRR) standing at 95% and an impressive Net Revenue Retention (NRR) at 110%. These stellar retention rates underscore the company's ability to not only maintain but also expand its customer base, reflecting its strong value proposition and customer satisfaction.



New ARR is ARR from new customer acquisitions

Expansion ARR is an increase in ARR for current customer accounts (Upsell)

Downsell ARR related to a decrease in subscription spending for current accounts

Churn ARR represents the revenue lost due to customers no longer continuing their subscription

Revenue and expenses

PROMON

Revenue

Total revenue is composed of License revenue, One-time fees, and other revenue. License revenue primarily arises from Promon's SHIELD™ SaaS solution, accounting for approximately 99% of the total revenue generated in both FY21 and FY22. Revenue has seen an increase the last fiscal years, being close to a direct derivative of ARR growth with some delay.

Expenses

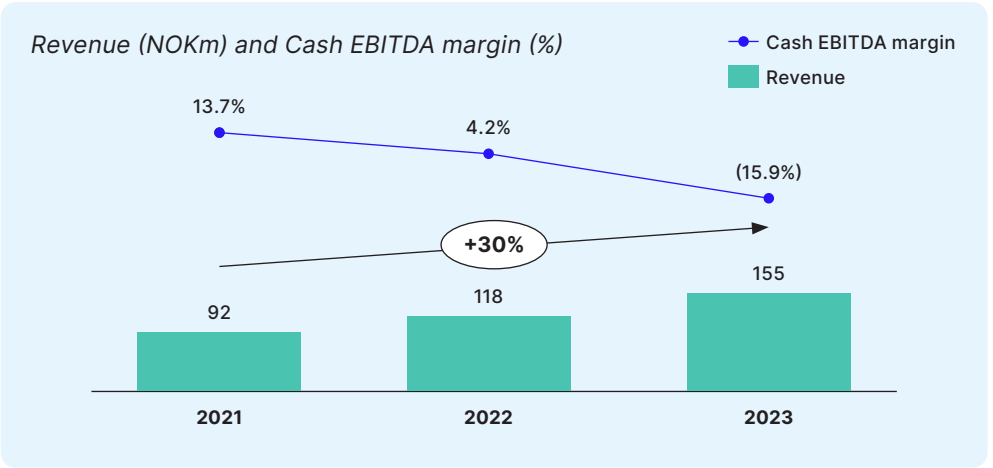
For simplicity, the cost structure can be divided into six different categories: Payroll expenses, marketing, software and licenses, Third-party consultancy, travel costs, and others.

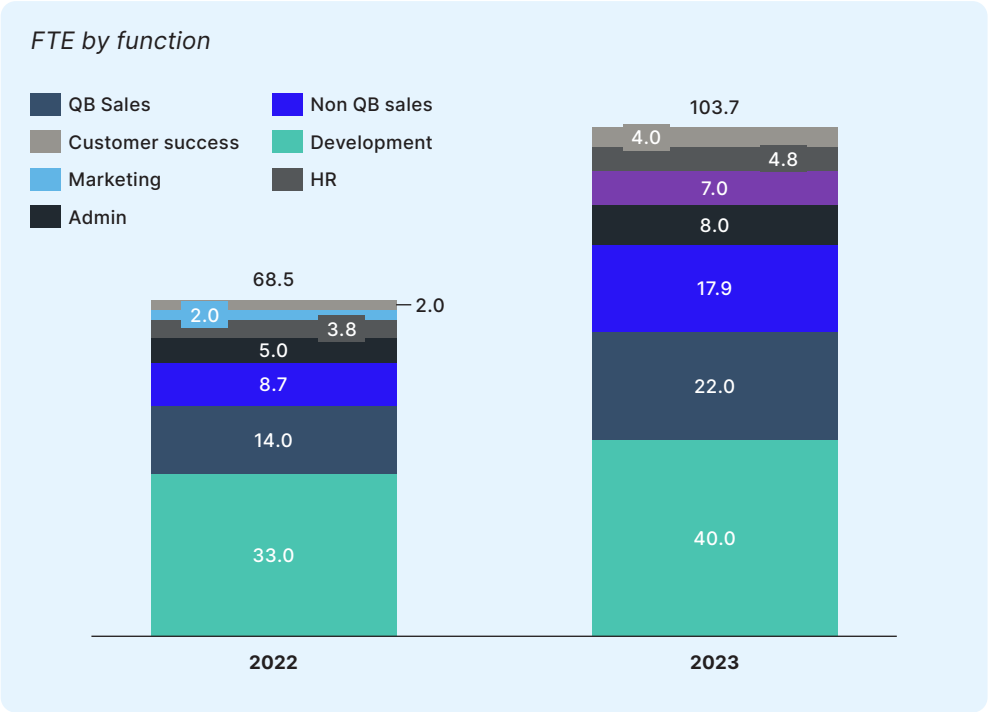
Payroll

Payroll expenses encompass all employee-related costs across various departments and serve as the predominant cost driver for Promon. As a highly technical company, Promon relies on technical solutions that need a significant number of developers for their development and maintenance. Moreover, the company has experienced a surge in its direct sales organization. As Promon continues to grow, payroll expenses remain the primary cost driver in the foreseeable future.

Cost and revenue relationship

As a SaaS company, Promon's expenditures are relatively independent of their sales figures. While S&M cost increases/decreases measures will impact sales growth in the long run, the immediate effect on sales is minimal due to the subscription-based structure of the SaaS business model. This dynamic suggests a lag between the implementation of cost initiatives and the impact on





Income statement

Income statement (NOKm)	2021	2022	2023
License revenue	92.0	116.4	153.0
One-time fees	0.0	1.2	0.9
Other revenue	0.1	0.1	0.8
Total revenue	**92.0**	**117.6**	**154.7**
COGS	(0.0)	(0.0)	(0.0)
Gross profit	**92.0**	**117.6**	**154.7**
Payroll expenses	(57.0)	(78.4)	(135.2)
Marketing	(4.6)	(6.5)	(9.0)
Software and licenses	(2.7)	(4.8)	(5.8)
Third-party consultancy	(9.6)	(13.5)	(11.7)
Travel costs	(0.7)	(4.1)	(6.3)
Other	(4.8)	(5.3)	(11.2)
Cash EBITDA	**12.6**	**4.9**	**(24.5)**

Balance sheet and ownership

PROMON

Balance sheet

Promon operates an asset-light business model, with few fixed assets. This means most of their assets are current assets. The three largest assets being accounts receivable, cash and cash equivalents and intangible assets (consisting of capitalized R&D expenses).

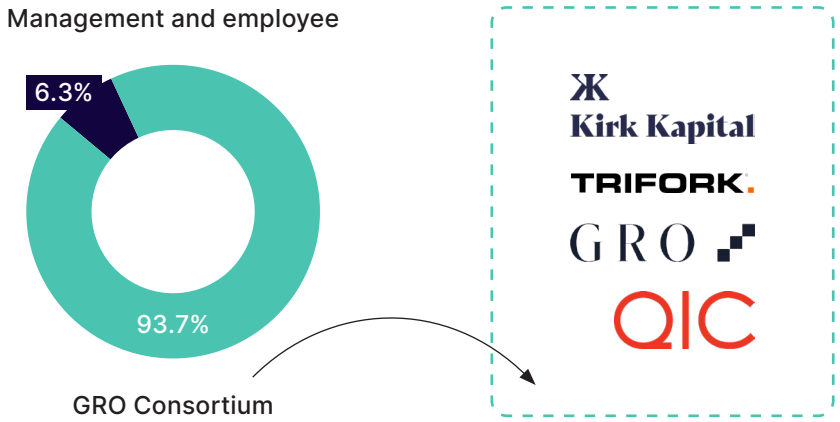
The main driver behind Promon's liabilities is other short-term debt. Other short-term debt constitute approximately 90% of Promon's total liabilities. This significant portion primarily stems from the company's practice of having customers prepay for a year of services. While revenue recognition occurs gradually as the services are delivered, the prepayments generate short-term liabilities for Promon, as the company has received payment for services that are yet to be provided.

Promon has opted to operate with no leverage, relying entirely on equity to fund its operations and growth. Promon has been able to sustain this due to their strong cash-flow generation business model with little need for CAPEX. This highlights the scalability of their business model as they do not need to take on large investments to grow further. As such, management expects an operating cash flow conversion rate from cash EBITDA of 90%.

Balance sheet (NOKm)	2023
Total intangible assets	51.8
Total fixed assets	6.2
Accounts receivable	34.9
Other debtors	8.6
Cash and cash equivalents	45.9
Total assets	**147.4**
Total equity	48.8
Long-term liabilities	0.0
Accounts payable	3.3
Public duties payable	6.5
Other short-term debt	88.8
Total equity and liabilities	**147.4**

Ownership structure

The ultimate parent of Promon AS is Portalen Topco AS, which is owned by the GRO Consortium consisting of: GRO, Queensland Investment Company (QIC), Kirk Kapital, and Trifork. The GRO Consortium owns 969,395,720 shares (93.7%), with management and employees owning 65,316,353 shares (6.3%).



Comparable multiples

PROMON

The following list of comparable public companies is not exhaustive, and participants are encouraged to explore and propose other peers, if they believe they better fit the criteria

Company	Offerings	Market cap (NOKm)	EV (NOKm)	Sales growth	EBITDA margin	Rule of 40	NTM EV/ SALES	NTM EV/ EBITDA	NTM EV/ EBIT	NTM P/E
Cisco Systems, Inc.	Networking, security, Cloud	2,071,511	1,927,725	7.7%	30.9%	35.8%	3.6x	9.7x	10.5x	13.5x
Verimatrix SA	Data right management & cybersecurity	559	718	(3.7%)	(7.2%)	-17.2%	1.1x	27.4x	n.a.	n.a.
Gen Digital, Inc.	Cybersecurity & -privacy	144,471	237,766	22.1%	49.0%	64.0%	5.7x	9.6x	9.6x	9.9x
F5, Inc.	Cloud applications and cybersecurity	115,481	109,661	3.6%	25.9%	25.4%	3.7x	9.9x	11.1x	14.7x
Qualys, Inc.	IT security and compliance	65,284	60,482	13.2%	34.3%	42.6%	9.4x	22.5x	24.8x	32.1x
OneSpan, Inc.	Identity, security and productivity solutions	4,097	3,428	3.3%	(6.2%)	-5.5%	1.4x	9.3x	40.3x	15.3x
Fortinet, Inc.	Networking and security solutions	565,213	550,716	20.1%	25.4%	43.4%	9.0x	30.9x	33.6x	41.0x
NSFOCUS Technologies	Internet & application security	8,188	7,630	(11.5%)	(11.7%)	-22.7%	2.1x	15.4x	25.9x	29.3x
G-Able	IT infrastructure and security	901	553	12.8%	6.7%	18.9%	0.3x	4.3x	5.0x	10.1x
A10 Networks, Inc.	Cloud and security solutions	10,473	8,915	(10.2%)	19.1%	5.2%	3.2x	11.0x	12.7x	17.3x
Palo Alto Networks, Inc.	Endpoint-, network-and operations security	1,075,591	1,063,026	22.3%	12.9%	32.6%	11.9x	39.1x	44.8x	56.5x
Atende S.A.	IT integration, infrastructure, security, etc.	319	328	39.8%	7.3%	46.1%	n.a.	n.a.	n.a.	n.a.
Cloudflare, Inc.	IT modernization, security and compliance	351,313	348,787	33.0%	(5.5%)	18.7%	19.9x	108.0x	205.9x	168.6x
Datadog, Inc.	IT security, infrastructure, etc.	460,216	442,419	27.1%	0.1%	25.5%	16.2x	68.1x	76.2x	91.3x
SentinelOne, Inc.	IT threat prevention and detection	90,142	81,934	58.4%	(62.6%)	-10.2%	10.2x	n.a.	n.a.	n.a.
SecureWorks Corp.	Network-, OT-, and endpoint-security	6,153	5,630	(17.6%)	(25.8%)	-52.3%	1.5x	105.5x	111.2x	n.a.
Cyber Security Cloud, Inc.	Internal and web security solutions	1,877	1,767	n.a.	19.5%	n.a.	6.4x	n.a.	32.0x	50.5x
Appgate, Inc.	Cybersecurity solutions	628	1,880	(2.9%)	(61.3%)	-84.4%	n.a.	n.a.	n.a.	n.a.
Dynatrace, Inc.	IT Security, automation, infrastructure and business analytics	153,498	145,997	24.4%	12.0%	33.6%	8.5x	30.9x	32.2x	39.1x
Narf Industries, Plc.	Cybersecurity research and development	193	204	94.1%	(16.1%)	65.1%	2.4x	14.8x	27.5x	26.9x

Source: Capital IQ as of 28/02/2024

Acknowledgements

Case writers:

Søren Hummelgaard
Julie Klein-Ipsen
Mikkel Hvitfeldt Andersen

Special thanks to:

Maxwell Veyhe
Joakim Lassen
Frederik Knudsen
Henning Treichl
Amelie Dunder
Ane Hellum
Esben Vestergaard
Julie Jakobsen
Jakob Göte

PROMON

Corporate Partners

GRO

KIRKBI

Carnegie

ACCURA

BCG

pwc

aip

CAPITAL FOUR

N2F Nordic Secondary Fund

FINANSFORBUNDET