فنتك السعودية
FintechSaudi

Digital Identification

Wealth Management

Insurtech

Business and Accounting

Capital Market

Cyber Security

Fintech Saudi Deep Dives:

Cybersecurity Solution Opportunities in KSA

In collaboration with

Deloitte.

info@fintechsaudi.com

fintechsaudi.com

@FintechSaudi

Contents

Introduction

Business Model Considerations

Regulation

Introduction

This report was developed by Fintech Saudi in collaboration with Deloitte as part of a series looking at areas of opportunity in the Saudi fintech industry. We hope this report proves to be valuable to our community and early stage entrepreneurs looking to establish and scale fintech companies in Saudi Arabia

What are Cybersecurity Solutions and why do Companies Need Them?

Cybersecurity solutions are critical services which protect business IT systems and data from cyber threats (e.g. cyber hacking, data breaches). These solutions are essential in enabling businesses to shield the integrity, confidentiality and availability of their information. Listed below are few specific examples of why businesses require cybersecurity solutions:

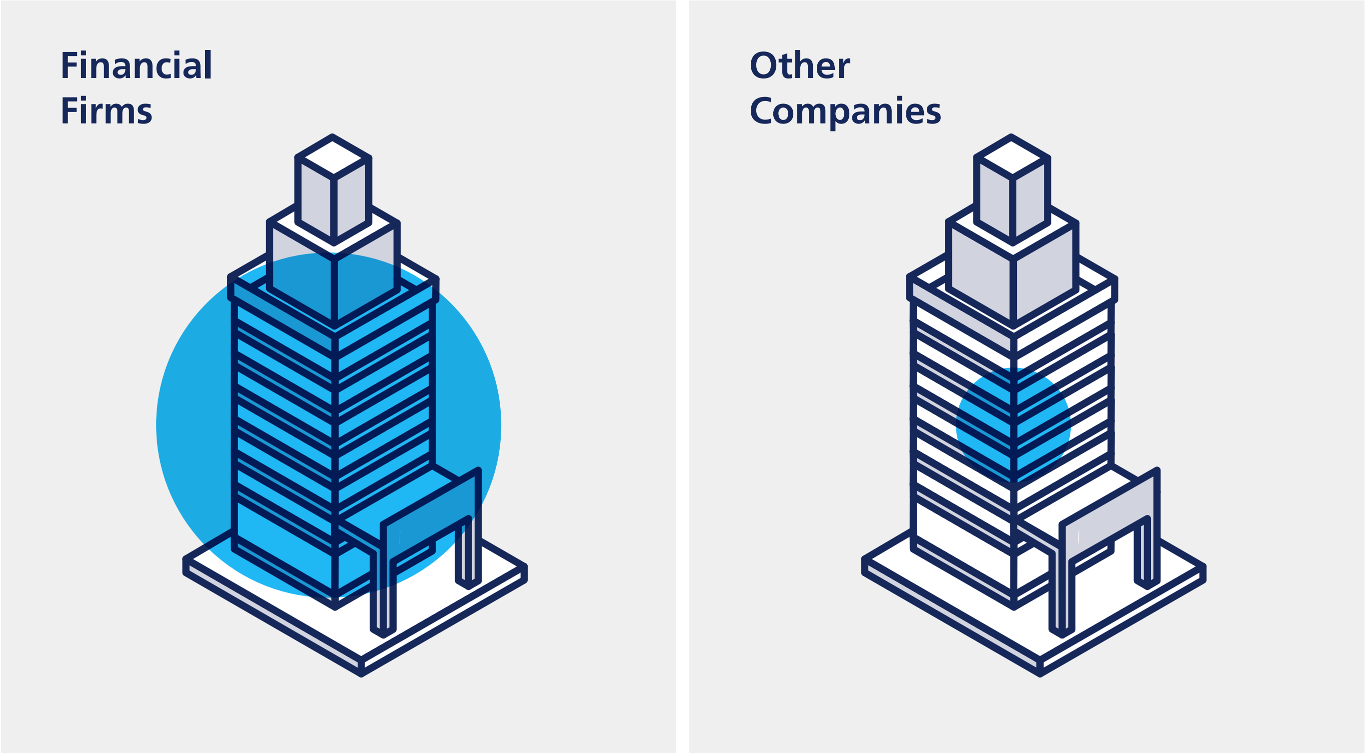
Maintain reputation and trust amongst their customers, employees, vendors and counterparties by ensuring data is protected and safe

Prevent the loss of their competitive edge by controlling the exposure of critical data (e.g. source files, intellectual property) to spyware

Protect day-to-day operations and productivity by preventing downtime due to targeted cyber-attacks (e.g. DDoS)

Why is this an Interesting Area for Entrepreneurs?

The current scenario in the Saudi market in regards to cybersecurity is:



● The likelihood of getting hit by a cyberattack

Cyberattacks are 300 times more likely to hit financial firms than other companies.[1]

Cybersecurity is a growing threat for global financial institutions, yet most of them are ill-prepared to respond within their current infrastructure.

[1] Business Insider – Cyberattacks on Financial Institutions

Why is this an Interesting Area for Entrepreneurs?

$18.5 m

The average annualized cost of cybercrime for financial services companies globally has increased to US$18.5 million[2]

16.59%

The size of Saudi Arabia's cybersecurity market in 2019 was SAR10.9B ($2.9B) and that market is expected to grow at a CAGR of 16.59% through 2023 to an estimated SAR21 billion ($5.6 billion)[3].

Banks across KSA have been increasingly investing in technological advancements in order to adopt a proactive approach to cyber security

It is evident there is demand by businesses in the Saudi market to enhance their cybersecurity to shield their integrity, data and availability of information. Entrepreneurs have an opportunity to develop and provide an effective solution that can combat the increasing cyber threats whilst reducing operational cost

[2] Accenture – Cybercrime on Financial Services Companies

[3] USSABC Economic Brief: Saudi Arabia's Emergence in Cyber Technology

What are the Current Challenges?

Saudi Arabia is currently the target of the highest number of cyberattacks in the Middle East, with over 160,000 daily hits[4]. The financial services industry faces the highest impact of cyber threats with cyber attackers increasingly targeting multiple banks simultaneously.

Despite the threats KSA is facing, there is a shortfall between the demand and supply for cyber security in KSA. This shortfall has also led to an estimated 95% of local cyber security companies focusing on providing cyber services/operations, whilst only 5% are focused on developing cyber products to tackle the evolving cyber threat challenges that businesses in KSA face[5]. Key threats include:

- **Advanced phishing** – Machine learning is being utilized to quickly craft and distribute convincing digital messages which increase the threat of malware and exposure of sensitive data
- **IoT (Internet of Things) interconnectivity** – the proliferation of insecure devices on an IoT (Internet of Things) network, coupled with legacy systems, are making businesses highly susceptible to cyber-attacks and data breaches, as accessing once device opens the flood gates to accessing all devices on the same network
- **Data infrastructure** – Both cloud and physical data storage have cyber security challenges. Physical data storage facilities are susceptible to targeted attacks whilst cloud infrastructure can by targeted by cyberattacks. As companies reliance on the use of data increases, the impact of disruptions to data infrastructure also increases.

[4] Oxford Business Group – Saudi Arabia Cybersecurity
[5] Deloitte Cybersecurity Subject Matter Experts Panel

How can Fintech Solutions Address Challenges?

Businesses can leverage fintech solutions to enhance their cybersecurity and protect their organization from data breaches, reputational fallout and operational downtime. The potential benefits of fintech cybersecurity solutions for businesses include:

- Utilizing AI (Artificial Intelligence) technology to recognize, monitor and analyze transactions to protect capital and sensitive information
- Deploying AI (Artificial Intelligence) and machine learning systems to secure cloud environments against the most typical means of malware penetration
- Automation of monitoring and preventing cyberattacks, reducing the cost and manpower required to prevent cyberattacks

Currently the biggest companies tend to purchase cyber security solutions from international companies. There is therefore an opportunity for domestic cybersecurity companies that solve local problems and ensure full compliance with local cyber security regulations.

Business Model Considerations

Business Models to Consider for the Saudi Market

1

Fraud Protection for Vulnerable Individuals

Vulnerable individuals are at most risk of fraud. This is a particular risk in Saudi Arabia due to the high levels of financial illiteracy.Fraud detection solutions can address this by monitoring transactions to identify suspicious activity on an account. In the case of vulnerable individuals, the solutions could be used to alert appointed guardians or family members to the activity.

2

Phishing / Fraud Check Databases

National Cyber Security Center has reported that phishing e-mails in Saudi Arabia have exceeded 26 million emails in the past few years.[6] These in particular may target vulnerable adults or individuals who are receiving emails in an unfamiliar language. A phishing / fraud database can help with identifying suspicious emails and could check communication in real time.

[6] Ministry of Communications and Information Technology

Business Models to Consider for the Saudi Market

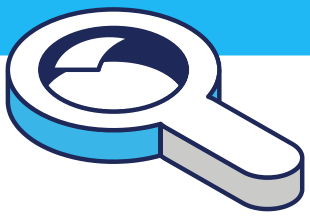
Escrow Accounts

Escrow accounts are where funds are held in trust whilst 2 or more parties complete a transaction. For example an investor may hold funds in escrow whilst they complete the purchase of a property transaction. Escrow accounts provide parties with security and trust when dealing with unknown parties. Historically escrow accounts are expensive and therefore have only been used for large transactions. However fintech solutions may look to develop low cost escrow solutions that can be used for smaller transactions such as purchasing a car. This avoids one party having to transfer cash to the other before they have checked what they are buying reducing the risk of fraud.

Automated Data Destruction

Data breaches are a significant issue for companies and government bodies. Data may be released accidently or may be obtained by hackers. Fintech companies can protect against data breaches by coding data so if a breach occurs, the data is automatically destroyed.

Case Studies



We have identified fintechs that are providing cybersecurity solutions globally that entrepreneurs interested in this area can learn from. The table below provides a high-level overview of their backgrounds, value propositions, target customers and pricing models used:

Case Studies: Praetorian

What is their mission?
To make the world a safer and more secure place

What service do they provide?
Offer clients the means to find, fix, stop, and ultimately solve cybersecurity problems across their entire enterprise and product portfolios.

How much funding have they received?
Raised $10M in Series A funding from Bill Wood Ventures and McKinsey & Company

What has their growth looked like?

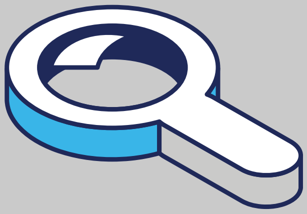
- Named an Inc. 5000 Fastest Growing Private Company for 7th Consecutive Year
- 237% growth rate experienced over the last three years
- 24 employees

What is their value proposition?

- Track vulnerabilities to closure across lifecycle
- Machine learning aided vulnerability identification
- Integrate with 3rd party bug tracking software
- Benchmark results over time across product portfolio
- Automated analysis through continuous testing

Who are their customers?
All businesses

What is their pricing model?
Feature pricing



Case Studies: Acunetix

What is their mission?
Provide a trustworthy web security solution that protects all assets, aligns with policy, and fits perfectly into the development lifecycle

What service do they provide?
Finding and detecting vulnerabilities at the earliest stage by using a web vulnerability scanner.

How much funding have they received?
$40M investment injected

What has their growth looked like?
Currently work with more than 1000 companies all over the world

What is their value proposition?
- Prevent potential attacks

- Manage web and network security
- Automate scanning
- Detect SQLi, XSS, and other issues
- Integrate with SDLC

Who are their customers?
Small businesses, and web professionals

What is their pricing model?
Tiered pricing

Case Studies: Sonrai Security

What is their mission?
Deliver the best Cloud data control solution in the industry

What service do they provide?
Deliver identity and data protection for public Clouds

How much funding have they received?
$38.5M investment injected

What has their growth looked like?

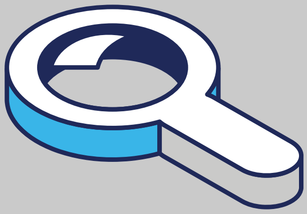
- Closed 2020 having achieved a number of critical milestones, including more than 3X customer growth, a number of large enterprise client deployments and a wide range of new product innovations
- Achieved strategic growth by becoming an Advanced Technology Partner with AWS and achieving ISV Accelerate status. The company also added Microsoft Azure and Google Cloud to its growing list of partners. Noted technology integrations include Hashicorp, IBM Qradar, Slack, and Jira

What is their value proposition?

- Find and remove previously invisible identity risk
- Prevent crown-jewel data loss
- Unify compliance and platform configuration monitoring
- Increase DevOps velocity

Who are their customers?
Businesses utilizing public Cloud (e.g. AWS, Azure, Google Cloud)

What is their pricing model?
Contact vendor for details



Case Studies: CrowdStrike

What is their mission?
Protect our customers from breaches

What service do they provide?
Unify technology, intelligence from across the globe to immediately prevent and detect threats

- Cloud native to eliminate complexity and simplify deployment to drive down operational costs

What has their growth looked like?

- 3.41% monthly website visits growth
- Transitioned from $52M revenue in 2017 to $250M revenue in 2019

How much funding have they received?

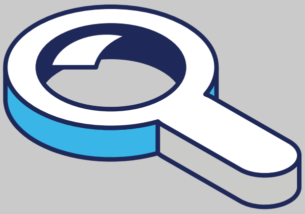
- In 2012, received $26M through Series A funding
- In 2013, received $30M through Series B funding
- In 2015, received $100M through Series C funding
- In 2017, received $125M through Series D funding
- In 2018, received $200M through Series E funding

What is their value proposition?

- Leverage AI (Artificial Intelligence)to offer instant visibility and protection across the enterprise
- Prevent attacks on endpoints on or of the network
- Correlates 2 trillion security events a week

Who are their customers?
All businesses

What is their pricing model?
Contact vendor for details



Case Studies: ReSec

What is their mission?
Provide complete protection – without asking employees and users to radically change behaviors or to work with overly burdensome and restrictive policies

How much funding have they received?
$11.8M investment injected

What has their growth looked like?
14 employees across 2 locations

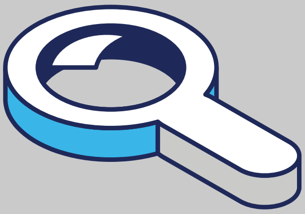
What service do they provide?
Provide 360 degree security for total protection against all types of known and unknown malware threats including viruses, ransomware, and phishing regardless of their delivery method

What is their value proposition?

- Isolate suspicious elements and guarantee all users receive clean and trusted files
- Create a non-intrusive user experience with no latency during file transfer and no impact on network performance
- Smooth and rapid deployment, easy customization, and seamless integration with existing infrastructure

Who are their customers?
All businesses.

What is their pricing model?
Contact vendor for details



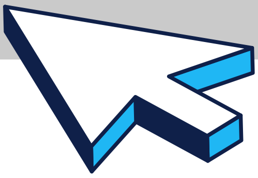
Regulation

How are Cybersecurity Solutions Currently Regulated in KSA?

As long as the fintech companies are not offering products and services that include regulated activities, fintech companies offering cybersecurity solutions are not regulated by Saudi Central Bank (SAMA), and therefore, can immediately apply for a Commercial Registration (CR) with the Ministry of Commerce and begin operations once the CR is received.

However, they would still need to be compliant with existing regulation such as regulation related to the use and transfer of financial data. The solutions would also need to comply with the framework set out by the National Cybersecurity Authority.

For more information on regulation clarity, please refer to the Fintech Access Guide **here** and Fintech Regulatory Assessment Tool **here**.



We hope this report was insightful for entrepreneurs and start-ups looking to create, establish, and scale their cybersecurity solutions in KSA.

If you found this report to be helpful or would like to learn more, please reach out to us at info@fintechsaudi.com

فنتك السعودية
FintechSaudi

About Fintech Saudi

Fintech Saudi is an initiative launched by the Saudi Central Bank (SAMA) in collaboration with the Capital Markets Authority (CMA) under the Financial Sector Development Program to support the development of the Fintech Industry in Saudi Arabia. Fintech Saudi's ambition is to transform Saudi Arabia into an innovative fintech hub with a thriving and responsible fintech ecosystem.

Fintech Saudi seeks to achieve this by supporting the development of the infrastructure required for the growth of the fintech industry, building capabilities and talent required by fintech companies and supporting fintech entrepreneurs at every stage of their development.

To learn more visit https://fintechsaudi.com or @fintechsaudi (Twitter)

Deloitte.

This presentation has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved. Deloitte & Touche (M.E.) (DME) or its affiliated entities would be pleased to advise readers on how to apply the principles set out in this presentation to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this presentation.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories, serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 280,000 people make an impact that matters at www.deloitte.com.

DME is a licensed member firm of Deloitte Touche Tohmatsu Limited (DTTL) and is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides audit and assurance, tax, consulting, financial advisory and risk advisory services through 25 offices in 14 countries with more than 3,300 partners, directors and staff. It has also received numerous awards in the last few years which include, Middle East Best Continuity and Resilience provider (2016), World Tax Awards (2017), Best Advisory and Consultancy Firm (2016), the Middle East Training & Development Excellence Award by the Institute of Chartered Accountants in England and Wales (ICAEW), as well as the best CSR integrated organization.