SFA | SINGAPORE FINTECH ASSOCIATION

CYBER SECURITY & QUANTUM COMPUTING PITCHBOOK

SFA CYBER SECURITY & QUANTUM COMPUTING PITCH BOOK

SFA is driving efforts at showcasing our members' solutions to other industries, enterprises/SMEs and other industry bodies and relevant agencies.

This is in line with our mission to:
(i) increase our members' chances of success, and
(ii) uplift our industry, and FinTechs in the Singapore ecosystem.

Our SFA members are driving innovation and unlocking new possibilities across the fintech landscape. We are excited to showcase these latest advancements in Cyber Security and Quantum Computing with all stakeholders and ecosystem players and together foster a more dynamic and resilient industry in Singapore and beyond.

- **Holly Fang, President, Singapore Fintech Association**

Cyber Sierra

Company Details

Category
Cybersecurity, Governance, Risk and Compliance (GRC) / RegTech

Business Model
B2B

Website
www.cybersierra.co

Contact Person
Pramodh Rai, Co-Founder and CEO

Subhajit Mandal, Co-Founder and COO

Business Email
platform.solutions@cybersierra.co

Business Phone Number
+65 9325 6401

Founded
2021 (Singapore)

Which countries do you operate in?
Singapore (headquarters), United States, Japan, India and the Middle East

Examples of FI clients
Regulated Enterprises: Global financial Institutions, Government and Defence Agencies

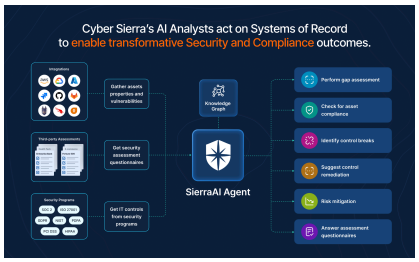
Pitch
Compliance teams are drowning in manual work. Every audit, assessment and certification requires hours spent reviewing documentation and gathering evidence. As compliance obligations increase, teams often need to increase headcount just to keep up.

Cyber Sierra's award-winning Sierra AI platform changes the equation.

The Sierra AI Platform's AI Analysts take on the operational work of compliance. The platform will integrate deeply to your pre-existing systems to:

- collect evidence
- assess controls
- answer questionnaires
- produce audit-ready reports.

Tasks that once took days or weeks can now be completed in minutes. Compliance and security teams can spend less time on repetitive work and more time on higher-value work like managing risk and strengthening controls.



Problem/Opportunity and Solution/Product
A security and compliance program is really many jobs running at once. Teams must keep hundreds of controls audit-ready, work through third-party assessments, keep risk registers current, and stay on top of the vulnerabilities surfacing across their organization. Cyber risk keeps rising and the deadlines never move, yet most of this is still done by hand, which is slow, fragmented and easy to get wrong.

Cyber Sierra brings it into one platform with dedicated modules for Governance, Risk, Assessment and Third-Party Risk Management. Each module has its own AI Analyst, so your team spends its time on more valuable work:

- **Gap Assessment:** maps your security policies against constantly changing regulations.
- **Continuous Control Monitoring (CCM):** spots control deviations and compliance breaches in near real time.
- **Evidence Auditor:** maps and audits evidence in minutes, not days.
- **Ask TracyAI:** answers thousands of questions instantly using context from your cyber posture.
- **Third-Party Risk Management (TPRM):** automates vendor reviews by evaluating the evidence third parties submit.

Recognized in the Gartner Hype Cycle for Cyber Risk Management 2024 and trusted by global enterprises and government agencies.

Protos Labs

PROTOS LABS

Company Details

Category
Adversarial Risk Intelligence

Business Model
B2B/ B2C

Website
www.protoslabs.io

Contact Person
Joel Lee (Co-founder & CEO)

Business Email
joel_lee@protoslabs.io

Business Phone Number

Founded
2022 (pivoted to Agentic AI in 2024)

Which countries do you operate in?
Singapore, United States, Thailand

Examples of FI clients
Deployed with Defence and Intelligence agencies and government since 2024; Expanded to commercial enterprises since Oct 2025; currently 12 POCs with F5000 companies (client names under NDA).

Advised by former CISOs from US, Israel and Singapore.

Pitch

Protos Labs is a Singapore-based Cyber AI company building the agentic investigation layer for adversary intelligence. Our AI agents conduct deep, multi-step investigations into threats, vulnerabilities, and actors — applying the tradecraft of a human intelligence analyst at machine speed. Not a SOC copilot, not a SIEM, not alert summarisation: a purpose-built investigation engine for the questions that matter.

The Problem

- Adversaries now operate at machine speed, while defenders remain constrained by manual workflows. The window from disclosure to exploit has narrowed sharply.
- Senior analysts are stuck on low-value collection and enrichment instead of judgement and decisions.
- Feeds, alerts, and advisories pile up — but raw data without context is just more noise.

Our Solution – Agentic AI platform for Adversary Intelligence

- A contextualisation layer that complements your existing feeds and tools, rather than displacing them.
- Multi-source ingestion across cyber, fraud, social media, and dark web sources — every threat, vulnerability, and actor mapped to your assets, industry, and risk profile.
- Deep, long-form investigations — AI agents pursue multi-step lines of inquiry across sources, pivoting on new evidence the way a human analyst would, to resolve complex adversary investigations end-to end.

Benefits

- Up to 15x faster investigation cycles — work that took analysts days closes in minutes, with the reasoning trail intact.
- A force multiplier for lean teams — cyber talent is scarce and expensive; our agents let a small team operate at the throughput of a much larger one.

Why Us — Credentials, not Claims

- Deployed with Defence and Intelligence agencies since 2024 — the few environments where adversary investigation is mission-critical, and where Cyber AI is held to the highest bar.
- Built by former Booz Allen cyber operators and advised by former CISOs from the US, Israel, and Singapore — grounded in genuine intelligence tradecraft rather than repackaged analytics.
- Recognised by leading AI and cyber organisations including Nvidia Inception, Microsoft AI Accelerate, and CSA (Singapore's cyber regulator).

10S Technologies

Company Details

Category
Cyber Security / Digital Identity / Fraud Prevention

Business Model
B2B / Enterprise SaaS / Licensing / Pilot Integration

Website
10stechnologies.com

Contact Person
Govind Yadav

Business Email
govind@10stech.com

Business Phone Number
+44 777 899 3807

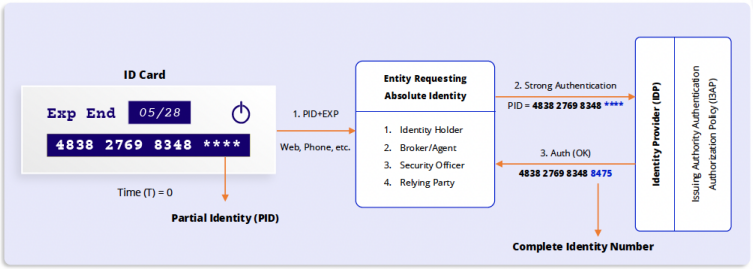
Founded
2025

Which countries do you operate in?
United Kingdom, Singapore, India; available for international pilots

Examples of FI clients
Available for FI pilot / sandbox evaluation

Pitch
10S Technologies is developing ZIEL™ / Dynamic Partial ID (DPID), a patent-pending identifier-security layer for banks, payment providers and digital-finance platforms. ZIEL reduces exposure of reusable customer identifiers by replacing static identifiers with dynamic, time-bound and relying-party-bound identity states, making captured identifiers structurally useless for phishing, replay, credential stuffing and account-takeover chains.

Problem/Opportunity and Solution/Product
Financial institutions have invested heavily in MFA, OTPs, device binding, fraud monitoring and behavioural analytics. However, many controls still operate after customer identifiers have already been exposed, harvested, replayed or socially engineered.
ZIEL addresses this architectural gap by ensuring that no complete reusable customer identifier is exposed to the user, browser, app, attacker or relying party in reusable form. Each interaction can generate a dynamic partial identifier, while the complete identifier is released or completed only after relying-party validation and policy checks.
Initial use cases include NetBanking and mobile banking login, account-access protection,s customer-ID harvesting prevention, recovery-path abuse reduction, card-present/card-not-present transaction protection and wallet/tokenised payment flows.



Supporting analysis: Comparative review of Online ID & NetBanking authentication models and identifier-exposure risk vectors:
Online ID: Link
Payment Industry: Link

Aires Applied Quantum Technology

Company Details

Category
Data Encryption (Post Quantum Cryptography)

Business Model
B2B/ B2C

Website
https://airesatech.com/

Contact Person
Ken Lin

Business Email
kenlin@airesatech.com

Business Phone Number
8022 8688

Founded
2021

Which countries do you operate in?
Singapore, United States, Thailand

Examples of FI clients
Banking, Insurance, Capital Markets, Payments, Crypto Exchange, Brokers, Platforms

Pitch
At Aires Applied Technology, we provide new age and innovative data encryption solutions for Cybersecurity. Our main focus and value preposition is in proprietary Deep Tech that is researched and developed in-house. As of End 2022, we have obtained our first Patent on Quantum Resistant Data Encryption, with 4 other patents being filed. We have also developed innovative and customized data encryption and key management solutions for clients including for cloud platforms and long-term data preservation.

Bitdefender

Bitdefender

Company Details

Category
Cyber Security & Quantum Computing

Business Model
B2B

Website
www.bitdefender.com

Contact Person
wtay@bitdefender.com

Business Email
Sales-apac@bitdefender.com

Business Phone Number
(+65) 60 18 39 22

Founded
2001 (Bucharest, Romania)

Which countries do you operate in?
Singapore, Indonesia, Australia, New Zealand, Malaysia, Thailand, Philippines

Examples of FI clients
Singlife, MSIG, Webull, Coinhako, Crypto.com

Pitch

Bitdefender provides cybersecurity solutions with leading security efficacy, performance and ease of use to small and medium businesses, mid-market enterprises and consumers. Guided by a vision to be the world's most trusted cybersecurity solutions provider, Bitdefender is committed to defending organizations and individuals around the globe against cyberattacks to transform and improve their digital experience.

Problem/Opportunity and Solution/Product

Financial institutions face sophisticated, persistent adversaries targeting credentials, infrastructure, and supply chains. Since reactive security is no longer sufficient, Bitdefender's Cybersecurity portfolio addresses this with solutions like:

1. GravityZone PHASR (Proactive Hardening and Attack Surface Reduction) dynamically profiles user behavior to enforce least-privilege controls and neutralize living-off-the-land attacks (LotL) before they happen.
2. GravityZone MDR provides 24/7 threat monitoring, triage, and response backed by Bitdefender's elite SOC
3. GravityZone XDR correlates telemetry across endpoints, network, identity, and cloud for unified threat visibility
4. Cybersecurity Advisory Services delivers strategic guidance on security architecture, risk posture, and regulatory alignment
5. Cybersecurity Offensive Services, including penetration testing and red team exercises, validates defenses against real-world attack scenarios and satisfies MAS TRM assessment requirements.

Cybersense Solutions

Company Details

Category
System Integrators, Cybersecurity Consultancy and Advisory, Regulatory and Compliance Advisory, Managed Security Services, Cybersecurity Awareness training

Business Model
B2B

Website
https://www.cybersensesolutions.com

Contact Person
Adrian Harris

Business Email
adrian.harris@cybersensesolutions.com

Business Phone Number
+65 9635 5364

Founded
2023

Which countries do you operate in?

Singapore, Thailand, Vietnam, Philippines, Indonesia

Examples of FI clients
Banking, Insurance, Capital Markets, Payments, Crypto Exchanges

Pitch
Real security begins with understanding your business, your people, and the unique pressures you face. Headquartered in Singapore and present across the Philippines, Indonesia, Vietnam, and Thailand, Cybersense Solutions partners with organisations across APAC to build cyber resilience that is both technically robust and deeply human. Our team of seasoned professionals brings industry-recognised expertise and a genuine commitment to translating complex threats into clear, actionable strategies

Problem/Opportunity
The threat landscape is evolving faster than most organisations can keep up with, and the stakes are no longer just technical. They are reputational, financial, and deeply personal. Cybersense Solutions meets organisations where they are, delivering integrated cybersecurity across four service pillars tailored to the complex needs of government entities and financial institutions.

Detack

Company Details

Category
Cyber Risk · Credential Security / Identity & Access · Penetration Testing & Security Audits

Business Model
B2B

Website
www.detack.sg

Contact Person
Philip Joslin (Managing Director, Detack Pte Ltd)

Business Email
phil.joslin@detack.sg

Business Phone Number
+65 8488 0003

Founded
Detack Pte Ltd – May 2024
(Detack Group – 25+ years)

Which countries do you operate in?
Singapore, Germany (HQ), USA, Australia, Romania, Switzerland

Examples of FI clients
AXA · HUK (DE) · Evonik · Equitable (US) · Piraeus Bank · UniCredit · LBBW Asset Management · Mount Alvernia Hospital · Hong Kong Baptist Hospital; global partnerships with two of the "Big Five" advisory firms

Pitch

25 years securing Europe's banks and insurers – now on the ground in Singapore.

Detack Pte Ltd is the Singapore home of the Detack Group. For a quarter of a century we have protected banks, insurers and fintechs across Europe's most demanding regulatory regimes – GDPR, DORA and NIS2 – helping them prove their security to regulators, not just claim it. That battle-tested expertise, and our patented technology, are now local in Singapore – ready for the institutions shaping Asia's digital-finance future.

What we bring: elite offensive security (Red Teaming, penetration testing, third-party risk) and EPAS (Enterprise Password Analytics Solution) – our patented platform that continuously proves your credentials are strong and uncompromised, without ever seeing them. Triple ISO-certified (27001 / 9001 / 22301), trusted in 30+ countries.

Problem/Opportunity

Asia's FIs are scaling faster than anyone – and attackers know it. Credential-based attacks – phishing, credential stuffing, account takeover – are the No. 1 breach vector. As you expand across cloud, SaaS, APIs, core-banking and legacy systems, MFA alone cannot cover every door. Regulators – MAS TRM, the MAS Notice on Cyber Hygiene and the PDPA – increasingly expect continuous, auditable proof. Europe shows where this is heading: under DORA, 'we have a policy' is no longer enough. The institutions that get ahead of it win trust, close enterprise deals faster and stay resilient.

The solution – EPAS

EPAS turns credential security from a blind spot into a board-ready KPI. A sealed, air-gapped appliance audits and enforces credential strength across your entire estate – cloud and on-prem directories (Active Directory, Entra ID), Linux, databases, payment and core-banking systems, APIs and service accounts. Patented blind auditing flags weak, reused or breach-exposed credentials without ever exposing the cleartext – privacy-by-design that fits the PDPA and regional data-sovereignty needs. Backed by one of the world's largest breach-intelligence datasets and AI, it deploys in 24 hours, agent-less, with no data leaving your organisation, and generates the audit evidence MAS, your board and your clients want to see.

The bottom line: European-grade, regulator-proven credential assurance – now in Singapore – that strengthens (not replaces) your MFA, IAM and PAM, and turns compliance into a competitive edge.

iProov

Company Details

Category
Biometric Verification Solutions

Business Model
B2B

Website
https://www.iproov.com/

Contact Person
Thao Pham

Business Email
thao.pham@iproov.com

Business Phone Number

Founded
2011

Which countries do you operate in?
Global coverage

Examples of FI clients
ING, UBS, MoMo, Union Digital Bank, Knab, Rabobank
More at:
https://www.iproov.com/industries/financial-services

Pitch
Deepfakes have become commonplace as generative AI enables attackers to industrialize digital impersonation at scale. iProov provides biometric solutions that enable the world's most security-conscious organizations to defend against this threat, establishing genuine human presence in digital interactions to ensure trust and security. iProov actively defends against injection attacks, face swaps, and synthetic identity fraud, setting the standard for biometric identity assurance.

Problem/Solution
Deepfake-driven account takeover, synthetic identity fraud, and AI-generated injection attacks are increasingly prevalent in everyday enterprise workflows and outpacing legacy verification controls. iProov provides biometric solutions that directly address these threats.

Real-time technical and human security: iProov's patented Flashmark™ technology confirms the right person is present — a real person, verified in real time. The iSOC provides continuous global monitoring of attack patterns, so clients benefit from collective threat intelligence rather than point-in-time detection.

Operational efficiency at scale: iProov delivers high-assurance onboarding for citizens and enterprises, integrating natively with Microsoft Entra, FIDO2, and global channel partner networks, minimizing operational overhead and unifying identity across physical and online environments.

Regulatory alignment: iProov maps directly to APAC frameworks, helping financial institutions demonstrate compliance with robust, auditable biometric assurance. Independent validation benchmarks include: FIDO Face Verification Certification Program; NIST 800-63-4; CEN TS 18099 Level 2 (High) and Ingenium Biometrics Level 4; and UK DIATF Gamma (0.4).

Proven at scale: Trusted by governments and financial institutions worldwide — including GovTech Singapore, Australian Taxation Office, U.S. Department of Homeland Security, U.K. Home Office and NHS, MoMo, and UnionDigital Bank — iProov secures over one million daily transactions.

Samta.ai

Company Details

Category
Cyber Risk Quantification (CRQ) | Return on Security Investment (RoSI) | AI Governance & Compliance | Digital Risk Protection | DFIR Readiness

Business Model
B2B | SaaS Platform Licensing | Enterprise & Government

Website
https://www.samta.ai

Contact Person
Harish Taori, Founder & CEO

Business Email
harish@samta.ai

Business Phone Number
+65 8118 6670

Founded
2022 | HQ: Singapore
Engineering Centres: Noida & Nagpur, India

Which countries do you operate in?
Singapore (Primary) | USA | Latin America | Southeast Asia | India

Examples of FI clients
CRQ platform built for and deployed at Financial institutions such as Banco Union, Coltefinanciera, Seguros Bolivar, REFINANCIA, Finesa, Grupo Gentera (Banco Compartamos, Aterna, Yastas, Concredito, Compartamos Peru) in Latin America and few clients in India and Philippines. Additional POC and pipeline engagements across the region. References available under NDA.

Pitch
Samta.ai (https://samta/ai) is a Data & AI Engineering company delivering audit-ready, explainable AI solutions for Banks and Financial Institutions across the USA, Southeast Asia, and India. Samta.ai built a Cyber Risk Quantification (CRQ) platform for a leading Latin American financial institution — translating cyber risk into financial terms so boards and CISOs can justify investments, optimize spend, and demonstrate measurable security impact. In addition, Samta.ai's "Assure" services provide the AI governance, Privacy & compliance frameworks, Model Assessments, Security and operational guardrails to deploy solutions safely in regulated financial environments.

Samta.ai operates from Singapore (HQ), with engineering centres in Noida and Nagpur, India — serving clients across Southeast Asia, USA, Latin America, and India. Governance is embedded by design, not bolted on after deployment.

Problem/Opportunity and Solution/Product
CISOs and boards struggle to answer: "**Are we secure enough?**"

The cybersecurity market exceeds $500B by 2028, with DFIR tools and services at $90B+. The average breach costs $4.45M, takes 277 days to detect, and SOC teams face 98% false positives. There are 6.75M unfilled security jobs globally. CISOs must justify investments, quantify risk in financial terms, and communicate exposure to boards and regulators — yet no single platform connects all the dots. Compounding this: 92% of enterprise AI initiatives stall due to security and governance gaps, leaving organisations exposed even as they modernise.

The CRQ platform, built for and proven number of financial institutions, quantifies cyber risk with numerical precision across assets, business units, and processes — translating technical exposure into board-ready financial impact.

Core capabilities: Risk Quantification at Scale; Investment Optimisation ranking controls by Return on Security Investment (RoSI); Human & Process Risk Insights (insider risk, workflow vulnerabilities); Executive-Ready Dashboards; and Scalable Assessment Models for any regulatory framework.

Samta.ai's Assure service wraps the deployment with: Data Governance & Policy; Security & Guardrails (RBAC, encryption, governed data exchange); Privacy & Compliance (GDPR, HIPAA, MAS FEAT); Model Assessments (explainability, bias detection, accuracy validation); and Operational Risk Controls with automated audit evidence. Result: 4x faster AI adoption, reduced compliance violations, and a CRQ platform audit-ready from Day 1.

SoftScheck Singapore

Company Details

Category
Cybersecurity Consultancy

Business Model
B2B

Website
https://softscheck-apac.com/sg/

Contact Person
Erika Zhang

Business Email
erika.zhang@softscheck-apac.com

Business Phone Number
8902 3530

Founded
2010

Which countries do you operate in?
Singapore, Malaysia, Indonesia

Examples of FI clients
DBS, UOB, Singlife, AIA, Mizuho, OKX

Pitch
softScheck is a cybersecurity consultancy that helps organisations find and fix their security weaknesses before attackers do. We pair offensive security, penetration testing and red-team simulation, with governance and compliance advisory, giving clients both the technical assurance that their defenses hold and the regulatory confidence to prove it.

Problem/Opportunity and Solution/Product
Organisations face rising cyber threats and tightening regulation, yet many only discover their weaknesses after an incident, and treat compliance as a paper exercise rather than proof of real resilience. softScheck closes that gap. Our offensive security team thinks like real adversaries, using vulnerability assessment, penetration testing and full red-team simulations to show how systems would actually fail under attack. Our GRC practice then turns those findings into defensible compliance, guiding clients through ISO 27001, SOC 2, MAS TRM and NIST CSF. The result is security that holds up in practice, not just on paper.

Sumsub

Company Details

Cyber Risk Category
Digital Security;
Identity and Access Management

Business Model
B2B

Website
sumsub.com

Contact Person
Penny Chai (VP, Sumsub)
Yvonne Goh (APAC, Sales)

Business Email
penny.chai@sumsub.com

Business Phone Number
+65 9114 8032 (Penny)

Founded
2015

Which countries do you operate in?
Global coverage

Examples of FI clients
sumsub.com/customers/

Pitch

Identity weaknesses account for almost 90% of cyber incidents, often involving compromised credentials, third-party vulnerabilities, and sophisticated deepfake attacks. Sumsub mitigates these threats by securing identity - the core vector of cyber risk. Our integrated platform delivers real-time biometric verification, advanced deepfake detection (99.98% accuracy), continuous behavioural monitoring, and compliance- ready cybersecurity controls (ISO 27001, PCI DSS, SOC 2). Trusted by over 4,000 enterprises globally, Sumsub reduces exposure to third-party breaches, automates fraud prevention, and delivers validated business outcomes - a 240% ROI within six months according to a study by Forrester.

Problem/Opportunity and Solution/Product

Cybersecurity teams increasingly confront sophisticated identity-based attacks, credential stuffing, and account takeover attempts that traditional security controls struggle to mitigate. Deepfake-driven fraud has doubled in the past year alone. Businesses also face heightened regulatory scrutiny from compliance frameworks that require robust fraud detection, real-time threat monitoring, and stringent cybersecurity protocols to combat synthetic fraud, phishing, and social engineering attacks.

Sumsub provides a comprehensive, identity-centric solution to directly address these challenges:

- **Deepfake & identity verification:** Sumsub instantly authenticates identities using advanced liveness and deepfake detection technologies, achieving a remarkable 99.98% accuracy, eliminating synthetic identities and deepfake-driven fraud before they penetrate your security perimeter.
- **Behavioural & device intelligence:** Leveraging AI-driven behavioural analytics, Sumsub's device intelligence systematically tracks device behavior and network-level data beyond basic IP addresses, proactively detecting unauthorized or spoofed devices and ensuring rapid identification of unauthorized access attempts and compromised accounts in real-time.
- **Compliance assurance:** Fully compliant with major cybersecurity standards (ISO 27001, PCI DSS, SOC 2), Sumsub ensures continuous adherence to evolving cybersecurity and regulatory requirements, dramatically reducing compliance-related overhead.
- **Award-winning innovation:** Over the past three years, we've received more than 30 industry awards globally, including the 2025 Asia FinTech Awards for RegTech of the Year.
- **Proven economic impact:** Independently verified by Forrester TEI, Sumsub's clients realize substantial cost savings, improved security efficiency, and measurable economic returns, with an average 240% ROI achieved within just six months.

Tosba Technologies

Tosba
DIGITAL. AI. CYBERSECURITY.

Company Details

Category
Cybersecurity Certification Preparedness, Compliance with Regulations, Risk Assessment and Management Services, Consulting, Third-Party Risk Management

Business Model
B2B, B2C

Website
https://tosba.tech

Contact Person
Hasan Selcuk BEYHAN

Business Email
contact@tosba.tech

Business Phone Number
83162929

Founded
2020

Which countries do you operate in?
Singapore
Germany
France
Türkiye

Examples of FI clients

Pitch
Tosba Technologies is an IT and cybersecurity consultancy helping businesses innovate, scale and operate securely in an era shaped by AI and quantum computing.
We develop cutting-edge mobile and web applications in-house, and are known for our hands-on expertise. Our solutions address real-world challenges and are powered by advanced technologies—including AI, Blockchain, and AR/VR. As these same technologies reshape the threat landscape, we help clients stay ahead of both AI-driven attacks and the looming risks posed by quantum computing to today's encryption standards. We deliver secure, scalable, and forward-thinking outcomes for our clients.

Problem/Opportunity and Solution/Product
Many corporations, especially FinTechs, often struggle with aligning their technology initiatives with business goals.
They lack the in-house expertise to lead complex development projects, adopt modern technologies like AI, or ensure their systems are secure against growing cyber threats. At the same time, hiring experienced full-time CTO and CISO leadership can be expensive and difficult to justify for growing businesses.

We address these challenges through flexible, hands-on consultancy in software development, technology leadership and cybersecurity. This enables us to offer, amongst others:
CISO-as-a-Service (CISOaaS)
Proactive cybersecurity oversight tailored to your risk profile.
Our services also address emerging security priorities, including:
- AI security, governance and risk assessments
- Protection of AI models, data and applications
- Defence against AI-enabled cyber threats
- Post-quantum cryptography readiness and migration planning
- Security awareness, incident management and compliance

CTO-as-a-Service (CTOaaS)
Strategic technology leadership on a flexible basis.
We help you design and manage technology roadmaps, modernize your infrastructure, lead dev. teams, and integrate emerging technologies like AI—without the need for a full-time CTO.
Our CTO-as-a-Service offering includes:
- Software and product strategy
- Architecture and technology selection for modernisation
- AI adoption and responsible implementation
- Development team and outsourcing management
- Coordination between business, technology and cybersecurity

V-Key

Company Details

Category
Digital Identity
Cyber Security

Business Model
B2B/ B2C

Website
www.v-key.com

Contact Person
Peter Mah

Business Email
peter.mah@v-key.com

Business Phone Number
+65 9792 1001

Founded
2011

Which countries do you operate in?
APAC, Middle East, Europe, and Americas

Examples of FI clients
Leading Financial Institutions, Digital Banks, eWallets, Government Agencies and Mega Apps

Pitch
V-Key ID is a privacy-first digital identity solution that unifies digital identity across platforms—enabling seamless access with just one registration. Built on V-Key's patented virtual secure technology, V-OS, it helps businesses prevent breaches, build user trust, reduce login friction, and deployment costs with strong passwordless authentication.

Problem/Opportunity and Solution/Product

AI-driven threats fuel identity fraud and expose new security vulnerabilities, banks, fintechs, and government agencies are under growing pressure to secure digital access without compromising user experience. Meanwhile, users navigate multiple usernames, passwords, and verification steps across banking apps, government portals, and financial platforms, resulting in fragmented experiences, lower engagement, and increased security risk.

Businesses face:

- High drop-off rates during onboarding
- Siloed and repetitive identity verification
- Growing pressure to meet privacy and regulatory compliance demands
- Increased risk from passwords and device-tied biometrics
- Rising AI-powered fraud targeting digital identities

Wultra

Company Details

Category
User Authentication, Digital Identity, Mobile App Security, Digital Onboarding, Passwordless Multi–Factor Authentication

Business Model
B2B

Website
www.wultra.com

Contact Person
Sanjeev Velayuthan

Business Email
sanjeev.velayuthan@wultra.com

Business Phone Number
+65 9789 0091

Founded
2014

Which countries do you operate in?
Europe, MENA, and ASEAN markets with offices in Prague and Singapore

Examples of FI clients
Banks, fintechs, and financial institutions across 25 countries

Pitch
Wultra equips banks and fintech companies with seamless authentication and digital identity solutions that strengthen security today while supporting the transition to a post-quantum future. Trusted by financial institutions in more than 25 countries, Wultra combines a developer-friendly architecture with a passwordless user experience, helping organizations meet evolving regulatory requirements, strengthen resilience against emerging threats, and build digital trust across all channels.

Problem/Opportunity and Solution/Product

As financial services become increasingly digital, banks and fintech companies face growing challenges from AI-powered fraud, including deepfakes, identity impersonation, account takeover, and sophisticated phishing attacks. At the same time, organizations are beginning their transition to post-quantum cryptography to ensure long-term security and resilience.

Wultra helps banks and fintech companies secure their digital channels with phishing-resistant, passwordless, and post-quantum-ready solutions. The platform supports the entire digital journey, from onboarding and identity proofing to user authentication, transaction authorization, and electronic signatures, delivering a seamless and secure user experience. This enables organizations to strengthen digital trust today and prepare for the security and identity challenges of tomorrow.

In addition, Wultra assists financial institutions in addressing local regulatory requirements related to digital identity security, strong customer authentication, transaction protection, fraud prevention, and operational resilience. By aligning security capabilities with evolving regulatory expectations.

Zavior

Company Details

Cyber Security Category
Risk Management, Data Protection & Privacy, Software / Hardware Asset Management, Identity Management, Incident Response Management,
Third-Party Risk Management

Business Model
B2B

Website
www.zavior.ai

CONTACT PERSON
Glenn Tan

Business Email
contact@zavior.app

Business Phone Number
+65 8787 3518

Founded
2024

Which countries do you operate in?
Singapore

Examples Of FI Clients
Fintech SaaS Startups

Pitch
Zavior is an integrated cyber security, data protection, and technology-risk platform built for Singapore's financial sector. Zavior helps financial institution vendors to close enterprise deals and meet regulatory requirements by automating the compliance process. Achieving relevant certification such as ISO 27001, Cyber Essentials and Trust Mark, Data Protection Trustmark among others.

Problem/Opportunity and Solution/Product
Zavior will be your single source of truth to manage compliance tasks and business operations functions using AI and integrations.
Zavior enables teams to:

- Manage your Compliance Project from Start To End
- Review & Generate Data Protection / Security Policies
- Delegate Compliance Tasks Automatically Throughout Organization
- Manage Risk - 3rd Party, Supplier & Vendor Risk
- Manage People through Integration with Office 365, Google Workspace