Join the Most Senior-Level Gathering of RegTech Leaders in the World

22 SEPTEMBER 2020 - LONDON

Register Now

www.GlobalRegTechSummit.com
The CYBERTECH100 is an annual list of 100 of the world’s most innovative CyberTech companies selected by a panel of industry experts and analysts. These are the companies every financial institution needs to know about as they consider and develop their information security and financial crime fighting strategies.

There’s plenty of interest and hype about CyberTech in financial services given the increased risk of data breaches and cyber attacks, but much of it is superficial, incoherent or self-serving and fails the needs of decision-makers in incumbent financial institutions who require independent facts, figures and analysis.

The CYBERTECH100 list will help senior management filter through all the vendors in the market by highlighting which business models have market potential and are most likely to succeed and have a lasting impact on the industry.

CRITERIA

The criteria assessed by the Advisory Board and FinTech Global team include the following:
• Industry significance of the problem being solved
• Growth, in terms of capital raised, revenue, customer traction
• Innovation of technology solution
• Potential cost savings, efficiency improvement, impact on the value chain and/or revenue enhancements generated for clients
• How important is it for a financial institutions to know about the company?

PROCESS

<table>
<thead>
<tr>
<th>RESEARCH CYBERTECH UNIVERSE</th>
<th>NOMINATE COMPANIES</th>
<th>CONDUCT INTERVIEWS &amp; SURVEY</th>
<th>IDENTIFY CYBERTECH 100</th>
<th>PUBLISH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyse universe of CyberTech solution providers on RegTech Analyst’s database and external sources</td>
<td>Shortlist candidates that meet criteria along with companies nominated via the website</td>
<td>Undertake in-depth interviews or surveys with founders and CEOs of shortlisted companies</td>
<td>Determine which companies excel in terms of the criteria and can be classified as CyberTech innovation leaders</td>
<td>Announce results to media and finalists</td>
</tr>
</tbody>
</table>
Understand how using technology can help insurers deliver superior customer experience amid social distancing

FREE TO ATTEND TWO DAY DIGITAL EVENT - 21 & 22 JULY

Register for Free

www.VirtualInsurTechForum.com
AlgoSec Security Policy Management Solution (ASMS) intelligently automates and orchestrates network security policy management to make enterprises more agile, more secure, and more compliant — all the time. Through a single pane of glass, users can determine application connectivity requirements, proactively analyze risk from the business perspective, and rapidly plan and execute network security changes — all with zero-touch deployment and provisioning, seamlessly orchestrated in multicloud network environments.

Alyne is a next generation Regulation Technology (RegTech) company, offering organisations extensive capabilities in managing their Cyber, Governance, Risk and Compliance processes through a Software as a Service platform. Alyne enables industries of all sizes to gain actionable insights through its content-rich library of structured controls and risk information, all mapped to relevant regulations, laws and industry standards. The company’s technology is powered by industry experts, empowering risk and assurance professionals to easily understand complex data and manage Risk and Compliance processes effectively.

AnChain.AI combines the time-tested pedigree of the cybersecurity and the meticulous polish of big tech to provide to the blockchain the first true enterprise-grade security and analytics arsenal – Blockchain Ecosystem Intelligence. Using its proprietary AI and machine learning, the company brings transparency to the pseudonymous blockchain ecosystem, affiliating nameless wallets with real-world enterprise and entities, and flagging patterns of suspicious behaviour before they can financially impact business operations. With industry-leading data labelling, fraud detection alerts, address identification and seamless built-in case management, the Blockchain Ecosystem Intelligence is an all-purpose platform for a modern blockchain enterprise.
A NASSCOM Emerge 50 company, Astra is a security suite consisting of security audits, a Web Application Firewall, a Malware scanner and other security tools. The company's flagship product, ASTRA, brings together an extensive feature set of manual/automated penetration testing tools, while performing a comprehensive vulnerability assessment and proactively responds to threats. Astra stops 1 million+ threats on its customer's web applications every day. The VA/PT product has uncovered 100,000+ vulnerabilities in client applications. Many prestigious brands like Gillette, Carrier, African Union, Ford, Oman Airways, Cosmopolitan, Hotstar, Kotak Securities, Dolls Kill, Invicta, Akeneo (Founded by former CTO of Magento) and thousands of other brands use Astra's security solution.

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend® Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes extensive network, endpoint, application, and data deceptions designed to misdirect and reveal attacks efficiently from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts and native integrations that automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 125 awards for its technology innovation and leadership.
Leading Experts in Post-Quantum Cryptography from Theory to Deployment

PQShield provides quantum-secure cryptographic solutions for software, software/hardware co-design and data in transit. This is particularly important where long lifecycle, performance and lasting confidentiality are a priority, now and for years to come. We need to be prepared for the threat landscape of the future. Consider the proliferation and lifecycle of connected systems across telecoms, automotive, smart environments and financial institutions - the need for advanced post-quantum protection is evident.

Our leading team of cryptographers are building next-generation technologies for all parts of the security ecosystem. PQShield is a major contributing participant to the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardisation process. During the transition from older cryptographic standards to new post-quantum cryptography, interoperability with legacy systems is important. Our solutions provide fast time to market and compliance with both existing and upcoming cryptography standards.

Solutions

PQSoC

PQSDK
Comprising of implementations of post-quantum primitives fully integrated with OpenSSL API and applications such as PKI (CA), S/MIME electronic mail and VPN solutions.

PQE2E
A software development toolkit for enabling ‘data in transit’ messaging solutions using post-quantum algorithms, leveraging a new, provably secure, Signal-derived protocol.

Contact us

Email: contact@pqshield.com  
Call: 01865 339 569  
Visit: www.pqshield.com
Auraya is a world leader in voice biometric technology with the mission of empowering people and organisations to interact and engage with convenience and security in all channels and languages. ArmorVox™ is Auraya’s next-generation voice biometric engine designed for telephony and digital channel implementations. ArmorVox allows partners to provide frictionless customer experience and improved security using machine learning algorithms and patented features like automated tuning, speaker-specific thresholds and background models, impostor mapping, synthetic voice detection and voice collection process from browsers. Powered by ArmorVox, EVA is a cloud-based voice biometric extension for telephony and digital channels. EVA provides voice identification & verification and fraud detection capabilities and solution application customisations using standard Amazon Connect orchestration resources to modify call flows, functionality, business rules, reporting and agent screen displays. Auraya provides its technology via a global network of partners that incorporate ArmorVox into their secure, customer-facing applications and fraud detection solutions.

Barac is a UK company that has developed a unique technology that protects organisations from malware attacks hidden inside encrypted traffic. Barac’s unique security technology, uses AI, Machine Learning and behavioural analytics, to locate and stop cyber-attacks hidden in encrypted traffic in real-time, without having to decrypt. The solution looks at 200 different indicators. It has a detection rate of 99.997% accuracy, and only 0.00006% false positives. The company also provides real-time visibility, reporting and audit across all the TLS and SSL traffic, including policy violations such as key strengths and certificate validity. Barac is integrated with existing security infrastructures and can use switches or firewalls to block attacks in real-time, and can forward alerts and logs to a SIEM or SOC, such as Arcsight, Qradar, Splunk, FortiSiem, Logrhythm or Securonix.

Bitglass’ cloud security solutions enable enterprises to secure any SaaS apps, web traffic, IaaS instances, data lakes, on-premises apps, and private cloud apps built on any platform. Bitglass’ cloud-first security platform provides end-to-end visibility and control over corporate data, limits sharing, prevents data leakage across all apps, and ensures that data is always safe and secure. This is imperative as organizations continue to enable bring your own device (BYOD). In fact, 85 percent of organizations allow BYOD for at least some of their stakeholders. This means that sensitive data is moving beyond the protective perimeter of traditional tools like corporate firewalls far more often. As such, cybersecurity technology must evolve to become data centric. Bitglass can protect data on any device, at any time, and from anywhere in the world – without the need for cumbersome, agent-based deployments.
Bridewell Consulting is a flexible and adaptable cyber security and data privacy company with offices in London, Reading and Newport. Bridewell is CREST and NCSC certified, as well as one of seven companies on the ASSURE framework in the UK. The company partners with its clients becoming an indispensable part of their team, ensuring that they have the most up to date advice to meet regulatory requirements and assist in selecting and configuring best in class security controls.

Build38 is a global provider of mobile application protection solutions. Its service represents a new generation of in-app and app-hardening technologies that protects apps from known and unknown attacks and opens the market to data intensive new digital business models. Build38 protects and monitors applications across various industries including Automotive, Financial, Public Transport and Healthcare creating the SELF-DEFENDING app.

Callsign is an identity fraud, authorisation and authentication company, with solutions for businesses across all digital sectors. The company solves challenges that organisations face in getting their users onto and interacting with their digital platforms easily and securely. Callsign provides solutions to some of the world’s largest banks and offers “bank grade” identification to public and private sector clients of all sizes to ensure that their legitimate customers can access their services easily, whilst at the same time blocking fraudsters. Callsign’s modular solution includes intelligent analytics e.g. behavioural biometrics, device fingerprinting, location analytics and telco data; feeding into a decisioning module which orchestrates dynamic, and contextual user journeys; and active authenticators e.g. swipe. Companies are faced with the challenge of having to prioritise fighting fraud, regulatory compliance, user experience and managing costs. Callsign has removed the need to compromise with an agile solution that is adjustable to customers evolving business needs.
Cobwebs Technologies is a global leader in automated web intelligence solutions. With offices in Singapore, Frankfurt, London, New York, Tel-Aviv professional investigators on six continents use the company’s solutions successfully to maximize efficiency and boost their results. Cobwebs’ web intelligence platform can be used by every team at a financial institution which conducts research on the open web, deep-web, and dark web to ensure safe business.

Currently financial professionals, among them compliance officers, front desk, anti-fraud teams, and security & investigations teams, are expected to carry out law-enforcement grade investigations, but often times lack the tools, training, and time to do so. Cobwebs provides law-enforcement grade web Investigations tools to financial professionals, giving them the power to conduct automated deep due diligence on any counterparty, ensuring that they can meet their business goals in a safe, compliant manner.

Cobwebs extracts targeted intelligence from the web’s big data using the latest machine learning algorithms and uses AI to generate hidden network risks, negative sentiments, and other insights which help detect front-men, fraud, shell companies, and other fincrime activity. The system emphasizes a user-friendly interface that turns any financial professional into a top-rate investigator.

What makes Cobwebs’ solution stand out is that the platform uses AI technology to “think” like a professional financial investigator allowing any counterparty to be searched and analyzed. As opposed to “static” risk screening solutions, Weaver searches both standard PEP and sanctions lists, alongside deep, smart searches of social media, blogs, darkweb, and other deepweb sources providing access to local data across the globe. This ensures that true best efforts are made in the risk assessment process, and peace of mind for a financial institution that all possible data on their client was gathered, analyzed and provided with the relevant insights.

The company has global presence with several law enforcement, regulatory and financial institutions using its platform, including in the EU, Asia, Latin America, Africa, and North America.

Cobwebs has a Cloud partnership with Microsoft, for the Azure Cloud service, as well as Amazon AWS cloud, and has partnerships with research institutes, among them the institutes for financial crime and counter-terrorism investigations.

The company won the Frost and Sullivan 2019 best technology award.

Cobwebs is targeting commercial banks, private banks, insurance, private equity funds, and other financial institutions worldwide as clients.

Weaver Financial Investigations Platform employs a suite of artificial intelligence-based technologies to automate and enhance every aspect of due diligence including ranging from machine learning, NLP, optical character recognition, big data, blockchain analysis, facial recognition, and other crucial modules for automated Web investigations. The system deploys dozens of algorithms to analyse hidden links and connections relating to any research Subject.

Weaver Financial Investigations Platform is the ultimate automated deep due diligence engine and allows financial professionals to gather data simultaneously on a counterparty from all levels of the web. The powerful web intelligence solution monitors online activity, collecting and analyzing data of endless digital channels – from the open, deep and dark web, using traditional ‘static’ compliance resources and databases to crucial dynamic new media data streams.
**The Challenge**
A tier 1 highly reputable private bank came under scrutiny from a European Regulator after it was suspected that numerous clients from the Russian and Middle East markets were suspected of having ties to money laundering and terror financing.

Following several reviews, it appeared as though standard checks were made during the onboarding process, but these were not sufficient in uncovering the harmful ties of the customers which could be the source of suspicious transactions being investigated. The bank, forced with business-damaging de-risking and prolonging their already inconvenient onboarding times, faced serious business continuity risks in its crucial markets, alongside reputational damage, should it fail to satisfy the regulator.

**How we solved it:**
Following a successful pilot program, Cobwebs Technologies deployed its Weaver Financial Investigations Platform with the Bank’s first and second lines of defense. Cobwebs Financial Investigators were embedded with the bank for several days, providing training and certification in conducting full-proof KYC and automated network risk analysis as it related to the Bank’s specific customer base.

- Deploy a new multilayered screening approach to new customers
- Review the entirety of the existing client profile to identify high-risk connections using link analysis
- Integrate dynamic risk sources alongside static screening databases
- Reduce onboarding times by 80 percent
- Increase the output of compliance and KYC functions by 250%
- Reduce onboarding costs incurred by the customer by 60%

**Outcome**
- Bank Compliance and Business continuity enhanced with Cobwebs
- Reduced onboarding times and costs
- Improved accuracy in identifying actual money laundering risks
- Less de-risking
- Greater confidence in accepting global business opportunities
- Reduced risk of regulatory penalties
- Enhanced research capabilities for discovering new, safe customers
- Stringent employee vetting processes
How Cobwebs is stopping the game of whack-a-mole in the fight against money laundering

Money laundering in global financial markets is like “whack-a-mole”, when you stop one scheme, another just pops up, according to Daniel Nisman, the head of financial sector solutions at web intelligence company Cobwebs.

Governments around the world have spent a lot of time, effort and funding to create regulations to try and crack down on money laundering and corruption. However, the financial market is still plagued with vulnerabilities. The United Nations estimates that between $800bn and $2trn is laundered through banks each year. Financial institutions are being put on the frontlines to fight this fraud and are expected to conduct law enforcement-grade investigations and intelligence-driven risk assessments on their counterparties. The Northern European money-laundering scandal of 2017, where €200bn was reportedly found to have been processed illicitly through Baltic branches of Nordic banks, shows there are still major issues in the system.

“Something’s definitely not working,” Nisman says. “Traditional banking, which is the most heavily regulated, is still the most favoured conduit for criminals trying to launder dirty cash.” One of the reasons for this, is that most of the criminal organisations laundering money know all of the vulnerabilities in financial institutions. Most of the time, if the offender, and source of dirty cash on a politically exposed persons list or watchlist, they will just go through a connected network to launder illicit funds.

When taking on a high-opportunity, but high-risk clients, a financial institution has one of three options, Nisman states. They can choose to have no dealings with any client in a high-risk jurisdiction or sector because they don't want to take the chance, but this loses them clients and business. The next option is to do nothing and “put your head in the sand, but that puts you at significant risk,” he says. The final choice is to spend a lot of time and money on enhanced due diligence, but often times they too are based on rudimentary, manual checks that scratch the surface of the web, by straining onboarding times and budgets. These limited options have a major impact on business.

“In some financial sectors, we’ve even seen shrinking, for example, in the private banking sector in Europe, because of de-risking they’re actually shrinking, as they’re giving up on business.” This is due to firms just not wanting to take the risk or have the right tool. Cobwebs is helping financial firms solve their money laundering issues through a combination of cybersecurity and regulation technology.

“Cobwebs plugs the remaining gap in the RegTech market, which is the whole aspect of client onboarding, client reviews, and client risk assessments, in a manner that enables business.” The company’s technology helps firms be better adapted to preventing money laundering during the onboarding and client review process, and other financial crime risks among counterparties.

Its technology differs from other due diligence solutions by searching and deeply analyzing data all three layers of the web. These are the surface web, which includes search engines and blogs, the deep web, which spans forums and social media, and then the dark web. Traditional KYC methodologies typically don’t go this far; it consists of checking static watchlists, then possibly
going to explore google, conducting manual analysis and searching, but that only reaches around 4% of the internet, Nisman says. Various studies conducted by leading institutions on the matter still point to technology, automation, and static data sources as key concerns among compliance officers.

“If I have a corporate client domiciled in a designated high-risk jurisdiction, I can plug that company into the system, it will immediately and automatically plot out the network of the company, who are their directors, who are they working with, what negative reputation is there on any of those nodes of that network,” Nisman explains.

Not only does the platform look into what is being said but also accounts for who it is by and whether its painting a positive or negative picture of the customer. It helps to uncover a person’s seemingly hidden networks, eliminating the most common money laundering tactics.

Launderers will use complex networks to exploit vulnerabilities from very creative methods and entry points. These often rely on getting access as customers by exploiting local partners of financial institutions, “they will even stoop to trying to insert moles into sensitive employment positions,” Nisman says. This is where solutions like Cobwebs can help ensure correct due diligence, risk assessments and background checks on all aspects of their business to make sure they’ve protected their entry points.

Cobwebs is removing that valve by giving gatekeepers of the financial market the tools and expertise to expose harmful networks without incurring a financial and time burden. “Cobwebs is one of the only providers, if not the only provider, that is offering a dedicated financial investigator academy to complement the technology it provides,” he says. The company is launching the academy to teach its clients on how to conduct automated web investigations, reduce false positives, and improve their fight against money laundering.

The company’s expertise is another key ways in which it is unique to other players in the market, Nisman adds. Not only has the company created a team with expertise within financial due diligence and the needs of the financial market, but it has also gathered a wealth of cyber expertise from a range of industries, including military intelligence, government/regulatory, and law enforcement. With the expertise, the Cobwebs Investigator Academy (CWIA) will further ensure businesses are best prepared for fighting money laundering.

The company “goes where other similar companies are too afraid to go in terms of dynamic media sources.” Other businesses are doing network analysis, but few are covering all three areas of the web. For example, some only go through corporate registries, but these are static and can even be tampered with in some places, including via legal action. Likewise, there are solutions which will do media reviews or others that explore the dark web, but not all together, making it hard for deep due diligence.

"We have a very bold vision, and that enhances the integrity of the traditional financial market across all different types of financial institutions,” continues Nisman. “So it forces the money launderers, to basically find other sources of what I call the oxygen for their operation. I always say money laundering is the oxygen that allows criminals to breathe. We want to take away that main artery in the traditional financial sector.”

Regulators around the world have been trying their hardest to satisfy growing public outcry over the continued harm to the integrity of their financial markets. There are numerous regulations coming into the market as a result. The Fifth Anti-Money Laundering Directive (5AML) was enforced in the European Union on January 10 2020 and despite only just being introduced, 6AML is already pitched for a December 2020 implementation. The market is not short of regulations, but there is so much these legislations can achieve and this can be seen by the sheer number of money being laundered and companies being hit with fines. Businesses are on the frontline and increasing regulation is not the solution to the money laundering problem.

“You can’t be too specific with the regulations, because otherwise it could be bad for business and it could also create too much of a checkbox approach and still allow money launderers to get around those restrictions,” Nisman concludes. “They can’t have a one size fits all approach in such a dynamic market, where there are so many different kinds of financial instruments that are being used. The solution is to unleash the creativity and ingenuity of the private sector, to ensure that financial institutions have the tools and training they need to succeed in driving safe, compliant business.”
Cardabel is a startup company focused on detecting and preventing loss from capital markets frauds and operational errors. Founded by industry veterans with decades of experience in financial technology and in particular applying mathematical models towards capital markets trading, it has developed a software product that uses new proprietary research in machine learning models that creates dynamic patterns used to detect anomalies in trade data. The software is an end-to-end solution, automating the process from trade inception to reporting and resolution. Cardabel is currently being used worldwide by asset managers, investment banks and trading organizations for all asset classes, ranging from money market, equity, FX, derivatives to physical commodities. Cardabel helps anti-fraud, compliance and internal audit teams broaden their scope of anomaly detection while reducing false alerts.

CleanCloud is a public cloud infrastructure management platform with two products:
- Inspect, cost management and optimization platform for AWS and Azure cloud, with dashboards, reports, and daily and automatic recommendations to reduce costs; and
- Score, compliance product for the AWS cloud with +100 verifications for the main frameworks and benchmarks, including PCI, GDPR and Brazilian regulations like its Central Bank and LGPD.

Commissum is a specialist Information Assurance company that fully understands the business and technological implications of the modern networked world, its risks, and the resulting balance of opportunity versus exposure. The Commissum team has the knowledge and essential experience required to ensure clients can confidently take advantage of the opportunities offered while meeting the legal, commercial and corporate governance responsibilities demanded of company management in this environment. Commissum’s service offering comprises five core areas of expertise: analysis, delivery, testing, operations and security awareness. This comprehensive coverage of the Information Security spectrum allows it to meet all of the Information Risk and Assurance requirements an organisation may have.
Corsha is a cybersecurity company with deep technical expertise in data protection, cloud, blockchain, encryption and orchestration technologies. All of its technology is developed in-house and the company has multiple patents on file. Corsha’s Streaming Authentication solution is a new unique technology that secures machine-to-machine communications, such as APIs. It can operate at the speed and scale of modern cloud deployments. In essence, the solution provides multi-factor authentication (MFA) for machine communications, similar to the use of MFA for humans (e.g., use of a security code at login). Our solution is fully automated, cloud-native, highly secure, and platform agnostic. Corsha can enable financial institutions to move to the cloud with confidence by providing security that is uniquely fitted to large at-scale cloud deployments.

Covr Security helps companies in heavily regulated industries to on-board and retain customers with one of the market’s most user-intuitive, password-less multi-factor authentication solution. Covr Security provides mobile, multi-factor authentication in the cloud to a wide range of industries that depend on strong customer authentication: banks, payment networks, credit card companies, eID providers, IoT companies and mobile carriers. The company’s three-layered authentication solution is truly customer-friendly and built on modern, patent-pending encryption technology. Its MFA technology supports a variety of individually independent proofs of identity for authentication and authorization: the smartphone’s biometrics like facial recognition or fingerprint activation, and 6-digit PIN codes.

Cryptosense provides the first application security software dedicated to the detection and remediation of crypto vulnerabilities. The Cryptosense software helps protect the majority of interbank messages worldwide, more than half of all global Forex trades and the world’s largest financial transactions database. It also helps test the cryptography used by the world’s largest cloud providers. A spin-off of the French national institute for computer science research (Inria), Cryptosense’s patented, state-of-the-art technology helps some of the world’s largest organizations eliminate the vulnerabilities caused by crypto misuse in their applications and infrastructure, and comply with custom or public crypto standards. Its solutions are offered in SaaS or on-premise and are deployed with an international clientele, in particular in the financial, industrial and government sectors.
Crysp's Trust Intelligence Platform leverages advanced analytics and behavioural biometrics to reduce fraud by using innovative device identification, device reputation and smart authentication solutions. Crysp enables FinTechs, EdTechs, eCommerce, online gaming & betting organizations improve online trust by proactively identifying bad actors (users and machines).

Crysp technologies have currently been deployed on 200M+ devices and are helping clients:

- Reduce misuse of promotions and cashbacks;
- Detect account takeovers and identity theft;
- Detect new account registration fraud;
- Reduce chargeback and friendly fraud;
- Reduce false declines and reviews;
- Reduce reseller fraud;
- Detect bots and machine behaviour;
- Reduce customer friction and improve genuine customer adoption;
- Block previously blacklisted fraudsters from returning;
- Enhance effectiveness of existing anti-fraud solutions.

Cyberint transforms cybersecurity into a business enabler by turning intelligence into action, proactively protecting digital businesses against cyber threats. As a partner to businesses worldwide, Cyberint's intelligence-driven detection and response protects organizations with a unique combination of a market-proven threat intelligence suite and domain expert cyber analysts, while reducing organizations’ TCO. We serve more than 100 brands worldwide across industries as diverse as financial services, retail, gaming, entertainment, and media.

Cyberlumeneer's CORE addresses the growing need for operational efficiency and monitoring by visualizing information that can be confusing and often overwhelming. Translating this into accurate and action-based reporting and visibility across numerous security controls, through one secure portal. A cloud based, secure by design, modular platform that has been custom built from the ground up by security experts. It provides a holistic view of an organization's operational security environment, including: asset management and best practice compliance; attack footprint mapping; security control management and action-based reporting.
Cybersec Innovation Partners (CIP) is a specialist technology business that concentrates on the critical area of ensuring the integrity and resilience of the business's PKI and encryption systems and processes. Unmanaged PKI is a key weakness that can be exploited by cyber criminals as well as being the cause of operational outages. CIP's core product is Whitethorn®. It provides complete digital certificate and key discovery and life cycle management. Visibility of all digital certificates and keys is essential to address the risks of being compromised. It provides Indicators of Compromise at a unique level of detail which can complement existing cyber security tools and SOC capabilities.

Based in London, CIP has a network of cyber and encryption specialists in the UK, Europe and the Americas. It is supported by globally recognised executives and advisers with experience in consulting, technology as well as extensive experience in financial services.

CyberSmart effortlessly solves the pain of cyber security for SMEs. The company offers an accessible SME focused platform that allows a company to check, fix, assurance and insure themselves against cyber risks. CyberSmart is a data driven mobile and desktop application and cloud cybersecurity platform for audit, certification, continuous protection and compliance. It helps businesses stay safe and secure to world-leading cyber security standards while making it easy for non-IT experts to understand and manage their cyber security.

Cybersprint empowers cybersecurity professionals, from CISO to analyst, to prioritize relevant risks. Using real-time, continuous digital footprint monitoring and detection, the company offers full visibility, from risk to root cause and remediation, taking into account brand, organisation, infrastructure, VIP's, 3rd parties and more. The company's AI correlates dozens of data sources, uses a multitude of scanners, to make risk relevant.

Most importantly, Cybersprint automatically handles attacks, incidents and risks. This saves security departments an enormous amount of time, and they need to focus much less on “fire extinguishing”. The time they save is invested in structural improvements. In this way, Cybersprint provides greatly increased resilience, and a smarter deployment of scarce security personnel.
CYE was founded in 2012 by the founder of the IDF's red team unit and grew to become a market specialist in red team (black-box) cyber security assessments and cyber maturity programmes. The company's technology leverages advanced AI and analytics to continuously assess behaviours and events, automatically block threats before they occur, and enable the organisation to focus resources and efforts where they matter the most. CYE operates globally with offices in five locations and support clients (Fortune500, with a strong foothold in the banking and insurance sector) throughout their cyber security journey with a range of tailored solutions.

CyGov is the developer of a cutting-edge cyber risk management platform—built from the ground up—that gives organizations of all sizes unparalleled understanding of their digital and compliance risk. This platform streamlines information, feeding into one, clear and actionable interface, allowing companies to see the gaps—and close them.

The CyGov solution automates and centralizes security-related data, actively collecting it from internal and external sources, painting an ever-more accurate picture of an organization's current and future risk profile.

By adopting the CyGov platform, organizations achieve the capacity—in real time—to see, review and update a comprehensive cyber security profile and implement optimal remediation measures. This provides an unmatched level of continuous, ongoing risk awareness—covering procedural, systems and human risk factors. The technology saves time, money and strengthens organizations for greater cyber resiliency in a world where risks are changing by the second.

Cymulate is a SaaS-based breach and attack simulation platform that makes it simple to test, measure and optimize the effectiveness of your security controls any time, all the time. With just a few clicks, Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you’re exposed and how to fix it—making security continuous, fast and part of every-day activities.
CyNation is an Integrated Risk Management company focused on managing the risks inherent in third-party ecosystems. Its solutions are trusted by banks, insurers, asset management firms and innovation centres across Europe. CyNation helps companies in industries that typically have large, third-party networks, are data-rich and highly regulated. These sectors face a high volume of data flows, interconnected processes, lack of transparency, compliance and third-party risk.

The company’s CyDesk solution is an integrated risk management platform that automates digital risk management, providing advanced, prescriptive analytics that identify, analyse and manage risk factors across third-party ecosystems. As these ecosystems can be large and complex, it also mitigates risks stemming from fourth parties and shadow vendors.

Deceptive Bytes provides organizations & MSSPs with its Active Endpoint Deception platform that enables them real time prevention against unknown & sophisticated cyber attacks in an ever growing advanced threat landscape. The solution helps security & IT teams reduce alert fatigue, operational burden and overall costs, allowing organizations to increase security and to focus on their business rather than recovering from cyber attacks.

Deceptive Bytes’ technology uses malware own defenses & techniques against it. The solution dynamically responds to malware as it evolves, based on the current stage of compromise, making malware believe it’s in an unattractive/hostile environment to attack & reducing its motivation and by changing the outcome of the attack.

Recognized as a Gartner Cool Vendor in 2019.

DivvyCloud helps enterprise customers change the world by empowering them to gain the freedom to innovate using cloud services without the resulting chaos and risk. DivvyCloud keeps companies out of the news by protecting cloud and container environments from misconfigurations, policy violations, threats, and Identity and Access Management (IAM) challenges, all of which can lead to the massive data breaches (like Capital One, Marriott, and Instagram) talked about in the news almost daily. With automated, real-time remediation, DivvyCloud customers achieve continuous security and compliance, and can fully realize the benefits of cloud and container technology.
Enveil is a pioneering data security company protecting Data in Use to enable secure search, analytics, sharing, and collaboration. Leveraging advances in homomorphic encryption to ensure nothing is ever revealed during the entire processing lifecycle, Enveil enables secure and private data collaboration through a market-ready, flexible, and adaptable trust framework. Organisations can securely collaborate in a completely decentralized manner while each entity retains positive control of its data assets.

Enveil’s business-enabling and privacy-preserving capabilities for secure data search, sharing, and collaboration protect data while it’s being used or processed – the ‘holy grail’ of data encryption. Enveil ZeroReveal® allows analysts at financial institutions to securely derive insights, cross-match, and search third-party data assets without ever revealing the contents of the search itself or compromising the security or ownership of the underlying data.

These secure and private Intra/Inter-Bank search capabilities enhance intelligence-led decision making by allowing users to securely derive insight from multiple data sources, even when using highly sensitive or regulated indicators.

Enveil’s groundbreaking use of homomorphic encryption means encrypted operations are run on any type of data at scale, with processing times that ensure minimal impact on user experience. While homomorphic encryption has been a topic of academic research for decades, Enveil’s solution breaks through this computation barrier bringing homomorphic encryption from the realm of the theoretical to the commercially practical. Enveil allows data to be securely used where it is and as it is today, delivering nation-state level security without requiring any system overhauls.

Enveil is a leader in the category of Privacy Enhancing Technologies (PETs), delivering the first and only NIAP Common Criteria-certified Data in Use security capabilities. The company’s flagship line of ZeroReveal® solutions leverage homomorphic encryption to enable secure search, analytics, sharing, and collaboration of sensitive data assets. By decoupling from the storage technology layer, Enveil is able to sit above the data, allowing organizations to retain control of their data assets while leveraging existing storage methods and access controls mechanisms. The Enveil ZeroReveal® solution facilitates encrypted search as a two-party, proxy layer software system. The ZeroReveal® Client application lives within the Enterprise’s trusted environment while the ZeroReveal Server application lives within the environment of the Data. The solution can be deployed in any configuration, including one-to-many or many-to-many. The deployment model is optimized for highly distributed, decentralized multi-party, and/or hybrid cloud deployments.

Enveil focuses exclusively on solutioning to secure Data in Use and integrates with existing at-rest and in-transit data security solutions, acting in a complementary capacity to provide full lifecycle security via standard APIs. Using proprietary technology that has led to 17 patent applications to date, Enveil uses homomorphic encryption techniques to achieve unmatched levels of scale – the solution has been proven to perform robustly and at speed over terabytes of data on cloud platforms, over commodity hardware, and on special purpose platforms like FPGAs and GPUs.
TOTAL FUNDING - $15M

Investors:

Enveil announced a $10 million in Series A funding in February 2020 and is using the capital to globally advance the business-enabling capabilities of its ZeroReveal® product line.

Zulfe Ali, Managing Partner at C5 Capital: “Enveil is stepping up to solve a fundamental security challenge: preserving privacy while ensuring that data remains usable. By empowering organizations to secure data throughout its lifecycle, Enveil’s contributions go beyond adding business value and ensuring compliance – we believe the company’s innovative use of Privacy Enhancing Technologies will positively impact enterprise and consumer privacy and security across verticals.”

Jorn Lambert, EVP, Digital Solutions at Mastercard: “In our ever-expanding digital world, exponential amounts of data are being produced, which can help companies innovate and provide better products and services to consumers. In doing so, companies have a responsibility to individuals, to one another, and to society as a whole to be good stewards of the data they manage and use for those consumers. We look forward to partnering with Enveil to explore solutions that advance these standards to enable critical business functions.”

TRACTION/GROWTH

• The company opened a UK office in 2020 to expand its profile in Europe and support ongoing customer deployments and business development opportunities in the region

• Enveil recently announced a new encrypted machine learning product, ZeroReveal® ML

• Enveil’s solutions are applicable across multiple verticals including Financial Services, Healthcare, Audit/Compliance, and Cloud Security. The majority of the current commercial use cases for Enveil’s enterprise-ready, Common Criteria-certified capabilities are focused on enabling organizations to perform homomorphically encrypted operations over unencrypted data.

PARTNERSHIPS

Enveil is an Advanced Technology Partner and a Public Sector Partner within the Amazon Partner Network (APN), and can deploy natively over AWS Commercial, GovCloud, and C2S.

Enveil is a Co-Sell Ready Partner within the Microsoft Partner Network and can deploy over Azure, Azure GOV, and Confidential Computing Environments.

Thales

Enveil is Thales eSecurity ASAP Partner and has completed integrations with products including Vormetric, SafeNet, SafeNetAT, and Thales Federal.

MANAGEMENT BIO

Dr. Ellison Anne Williams - Founder & CEO

Dr. Ellison Anne Williams is the Founder and CEO of Enveil, the pioneering data security company protecting Data in Use. Building on more than a decade of experience leading avant-garde efforts in the areas of large-scale analytics, information security, computer network exploitation, and network modeling, Ellison Anne founded the startup in 2016 to protect sensitive data while it’s being used or processed – the ‘holy grail’ of data encryption.

Leveraging her deep technical background and a passion for evangelizing the impact of disruptive technologies, Ellison Anne has helped define and advance the Data in Use security space and cultivated Enveil’s capabilities into category-defining solutions that enable secure search, analytics, sharing, and collaboration. In addition to her ongoing contributions as a cybersecurity mentor, speaker, and thought leader, Ellison Anne has been recognized as an SC Media Reboot Leadership Innovator Award winner, a Woman to Watch in Security, and a CyberScoop Leet List Honoree.

Under Ellison Anne's leadership, Enveil has been recognized with a number of awards including: SC Award Winner “Best Cloud Computing Security Solution”, SINET 16 Innovator, Cybersecurity Breakthrough Awards “Overall Encryption Solution of the Year”, Maryland Cybersecurity Awards “Cybersecurity Innovator of the Year”, Cybersecurity Impact Award Winner, FCA TechSprint Winner, and RegTech 100. Just four months after founding the company, Ellison Anne presented the company's groundbreaking technology at the 2017 RSA Innovation Sandbox, becoming the youngest company ever selected to participate in the esteemed competition, and was ultimately recognized as one of the winners.

Ellison Anne started her career at the U.S. National Security Agency and the Johns Hopkins University Applied Physics Laboratory and is accomplished in the fields of distributed computing and algorithms, cryptographic applications, graph theory, combinatorics, machine learning, and data mining. Ellison Anne holds a Ph.D. in Mathematics (Algebraic Combinatorics), a M.S. in Mathematics (Set Theoretic Topology), and a M.S. in Computer Science (Machine Learning).
CLOSING THE LAST GAP IN DATA SECURITY

Enveil closes the gap in data security by protecting data while it is being used, allowing organizations to securely search, share, and collaborate with sensitive data without risk of compromise or incidental exposure.

By decoupling from the storage technology layer, Enveil is able to sit above the data, requiring no changes to the underlying environment, and allowing organizations to retain positive control of their data assets while enabling secure sharing and collaboration.

NATION-STATE LEVEL SECURITY FOR THE PRIVATE SECTOR

Enveil is the only Data in Use security company to achieve NIAP Common Criteria security certification, verifying its capacity to provide nation-state level protection for sensitive data assets in the global marketplace.

DELISTING PRIVACY-PRESERVING CAPABILITIES ACROSS VERTICALS

Secure Data Collaboration  Secure Data Monetization  Continuous Monitoring  Insider Threat  Secure Cloud Processing  Edge/IoT Compute

Enable secure and private data sharing and collaboration to enhance intelligence-led decision making.

Monetize data assets and realize new revenue sources without compromising privacy or security.

Reduce liability and enhance data governance by enabling secure watchlist tipping and alerting.

Keep insider threat monitoring encrypted throughout the processing lifecycle.

Confidently process sensitive workloads and data in the Cloud by ensuring interactions remain encrypted during processing.

Never reveal Intellectual Property, or PII when searching untrusted or third-party data sources.

ABOUT ENVEIL  Enveil is a pioneering data security company protecting Data in Use to enable secure search, sharing, and collaboration. Founded by a seasoned team of PhD mathematicians and computer scientists, Enveil is revolutionizing data security by eliminating the Data in Use vulnerability that people have been chasing for more than 20 years. Learn more at www.enveil.com.
Enabling secure and private data sharing and collaboration

Enveil ZeroReveal® solutions enable entities to securely leverage external and cross-jurisdictional data assets in place without revealing the contents/interests of the search or the results returned.

CASE STUDY

Each year, large Financial Institutions spend hundreds of millions completing KYC (Know Your Customer) and Customer Due Diligence (CDD) processes to enhance intelligence-led decision making. The effort validated how homomorphic encryption can uniquely enable intelligence-led risk decisions to address key challenges in the financial sector. Analysts were able to securely and private cross-match and search regulated data across privacy jurisdictions in a business-relevant timeframe while ensuring sensitive assets remained protected during processing in accordance with regulatory requirements.

The use case also validated Enveil’s capabilities as a foundational component of a trust framework enabling Financial Institutions expand data inputs in order to better understand customer risk and make faster, better informed onboarding decisions. It further lays the groundwork for future intra- and inter-bank applications of these innovative cryptographic techniques.

Enveil was recently asked to examine how this collaborative gap might be overcome by leveraging advancements in Privacy Enhancing Technologies. Utilizing the data security company’s breakthroughs in homomorphic encryption, Enveil worked alongside market participants to develop a flexible and adaptable trust framework capable of facilitating secure and private Know Your Customer (KYC) checks on new and existing customers, however, no framework exists to collectively mitigate risk through the sharing of customer risk intelligence across privacy jurisdictions or between entities. This lack of access to existing intel often forces institutions to make risk-rating decisions based on incomplete information.

Enveil’s capabilities as a foundational component of a trust framework enabling Financial Institutions expand data inputs in order to better understand customer risk and make faster, better informed onboarding decisions. It further lays the groundwork for future intra- and inter-bank applications of these innovative cryptographic techniques.

A PRIVACY ENHANCING TECHNOLOGY-ENABLED SOLUTION

Powered by homomorphic encryption, Enveil ZeroReveal® protects searches, watchlists, and analytics during the entire processing lifecycle, enabling secure collaboration while maintaining a natural and defendable separation. With Enveil, data owners maintain control of their data assets and access to it. By leveraging this decentralized data model, participants are never required to move/consolidate data assets, make changes to their data environment, or re-encrypt their data.

- **Auditability:** without requiring ownership transfer of sensitive data assets
- **Secure Interactions:** with datasets on third-party systems to verify sensitive, questionable inputs
- **Improved Quality:** and efficiency of suspicious activity detection & reporting, KYC, and CDD
- **Mutually Beneficial:** capabilities that are accessible to all participating parties
- **API-based Interfaces:** for interactions without requiring changes to underlying infrastructure

WWW.ENVEIL.COM
Every company is faced with the challenge of how to securely save, manage, and share digital data. DRACOON, the market leader in the field of enterprise file services in the German-speaking region, has made it its mission to give the world back control of its data with the help of its platform.

DRACOON has been named a leader by independent analysts and various certifications confirm that the platform meets the highest standards of security. DRACOON features built-in client-side encryption and thus offers maximum protection of both sent and saved files, because the owner is the only person who has the decryption key. The granular user and rights management system makes it possible to define individual permissions for all of the files saved to the platform.

The universal API makes it possible to integrate external services and applications – from secure email communication to the complete modernization of the company’s file services.

Egress' vision is for a connected world in which people communicate efficiently and securely. To achieve this, the company provides human layer security to protect individual users and stop breaches before they happen. Its patented technologies are built using leading-edge contextual machine learning and powerful encryption that mitigate modern risks in ways that other solutions simply can’t achieve.

Today, Egress provides intelligent email security and collaboration solutions that prevent accidental and intentional breaches, protect sensitive data, and equip CISOs and their teams with the detailed reporting required for compliance purposes.

Egress is headquartered in London, with regional offices in the UK, the US, Canada and the Netherlands.

EverCompliant, the leading provider of cyber risk intelligence and transaction laundering detection and prevention, offering unparalleled visibility into the largest source of data in the world – the internet – to inform risk assessment, guide go-to-market strategies, and uncover new opportunities. EverCompliant gives payment processors, acquiring banks, payment facilitators and other marketplaces the flexibility to tailor their merchant risk profiles to prevent bad actors from infiltrating their systems and ensure only legitimate transactions get processed.

EverCompliant's technology uses artificial intelligence (AI) and advanced machine learning (ML) to power the cyber intelligence platform in order to assess hundreds of millions of domains. These insights shine a light on hidden relationships and risks, identifies an entity's full Digital DNATM, and reveals new opportunities to scale businesses efficiently and confidently.
Every company has forgotten about potentially toxic data lurking in the shadows; information that's been exported to a spreadsheet, edited, emailed, and then left in a folder somewhere. But within the bad data lies valuable knowledge and insight too.

Working with some of the most demanding companies in defence, banking and pharmaceuticals, Exonar tackles this problem by revealing everything within an organization's data estate, at scale, and in clever ways that competitors can't, or don't, do.

Exonar then enables companies to categorise, move or delete their data at scale, from files through emails to databases, to effectively 'spring clean' it and assure regulatory compliance. In addition, the company can create a single view of connected data, which further distils knowledge, and transforms data from a risk to an asset.

Expanse protects the world's most important organizations by discovering risks on the internet no one else can find. We build a system of record that is the authoritative source for an organization's global Internet assets. Expanse Expander enables organizations to discover, monitor and track their internet assets automatically, anywhere in the world, and reduce their risks and exposures. Expanse Behavior helps organizations continuously analyse suspicious traffic patterns and exposed services to ensure compliance with security and IT policies. And Expanse Link empowers organizations to reduce their supply chain risk by accurately identifying and driving remediation of exposed assets and services associated with strategic suppliers. Born from DARPA, Expanse was founded in 2012 and is backed by more than $135m in funding.

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyses all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, ExtraHop helps the world's leading enterprises including Credit Suisse, Fiserv, and BECU to rise above the noise of alerts, organizational silos and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.
EyesClear gives banks a crystal clear and real-time view of payments and trade transactions coming in and going out of the bank. It provides fraud and compliance managers with a forensics tool to perform detailed analysis of clients’ transactions together with versatile reporting and alerting capabilities. The solution is plug and play and has therefore no impact on existing critical systems and operations. This makes EyesClear an ideal independent solution for tackling fraud, ops-system glitches and money laundering.

Additionally, for business units such as foreign exchange and trade finance, EyesClear is the ultimate scouting tool for new clients and new businesses. With built-in features as well as extensive user customisation capability, compliance or business units can easily find anything from suspicious transactions to missed FX opportunities.

EyesClear ensures excellent balance between convenience and security for clients due to its top down approach in tackling risks and identifying opportunities.

FourStop GmbH (4Stop) founded in 2016, specialises in providing leading global KYB, KYC, compliance, anti-fraud technology and data science all available from a single API. They establish a true all-in-one solution for optimal risk management and fraud defence world-wide in a fail-safe, future-proof, simplistic and real-time manner. 4Stop’s platform brings together their proprietary real-time anti-fraud technology paired with thousands of aggregated global data points and hundreds of premium KYC and KYB data sources, with one-click, real-time activation. They are making it effortless for businesses to capitalise on advanced automated data-driven due-diligence to maximise onboarding, life-time value and fraud prevention with minimal to zero-touch on their business operations. Companies can confidently anticipate risk and are empowered to make well-informed decisions, backed by quantifiable data to accelerate their business performance. 4Stop has been developed with a full understanding of compliance needs, both locally and globally.

Futurae, a global cybersecurity company, offers a modular two-factor authentication and transaction signing suite for high security, which never compromises on customer experience. Futurae supports financial organizations with regulatory compliance (e.g., GDPR, PSD2/SCA).

Futurae offers a full range of authentication methods for complete flexibility of web and mobile banking products: Novel Adaptive Authentication (Zero-Touch), One-Touch, QR-Code, TOTP, Single Device, Authentication for Smart Home devices (voice banking), as well as Hardware Tokens. Offering its leading-edge technologies as a SaaS offering or on-premise installation, as well as through a secure mobile app, mobile SDKs, or customized White Label solutions. Futurae’s human-centric technologies enable swift integration into existing infrastructure via REST APIs or WebWidget.

Futurae is incorporated in Zurich by best-in-class cybersecurity and usability researchers. Currently the company serves customers in the financial and insurance industries like major international retail banks, private banks, asset managers, family offices, stock exchanges and FinTechs.
Governor Software supports senior risk and compliance executives at financial institutions maintain governance and oversight, through clear visualisation of their regulatory obligations and risk appetite. Founded in 2015 by CEO Richard Pike, the Governor Software team have first-hand experience of the production and oversight of governance information within financial institutions.

The company enables firms to visualise their obligations and integrate the connecting risks, regulations, frameworks and policies across the organisation. This is done by aggregating, integrating and visualising each one alongside performance information across the entire organisation. All within a single platform, Governor allows risk management from one central location and ensures accountability. Governor’s information architecture allows for flexibility in reporting and provides real-time feedback in the form of dashboards and notifications tailored for management.

Greenbone Networks is a vulnerability management specialist and enterprise IT solutions provider based in Germany. Its Greenbone Security Manager (GSM) analyses IT network devices, identifying security vulnerabilities, providing detailed reports and instructions to resolve security issues before attackers are able to exploit them, ensuring organisations remain resilient in their cybersecurity.

The company was founded in 2008 by leading experts in the field of network security and open source software with the goal of engineering products and concepts that are able to cope with the present and future challenges of cybersecurity. Greenbone has a comprehensive quality assurance process for its customers and is particularly concerned with providing a verifiable product rather than a black box.

Greenbone's vulnerability management solutions are deployed in more than 30,000 installations and integrations across a broad range of industries and company sizes, and its vulnerability management software has been downloaded more than 2.5 million times.

Hoxhunt is the leading provider of security engagement platforms worldwide. Hoxhunt’s security engagement training turns employees into a strong security shield by empowering them with the skills and knowledge to identify and report cyber threats. The Hoxhunt training provides gamified simulation, best-in-class real-time reporting of threats with its unique incident response module to equip security teams with the necessary intelligence to mitigate attacks and breaches faster. Hoxhunt works with Global 2000 organizations from a variety of industries, such as financial services, manufacturing, telecommunication, retail, and much more, to help the customers educate their employees better and thus reduce risk related to human error.
ID R&D is a NY-based software company with global technological leadership in voice biometrics, voice and face liveness detection, and continuous multimodal authentication. ID R&D breaks through in a crowded cybersecurity market with science-driven biometric products that enable frictionless authentication while dramatically increasing security in mobile apps, web apps and conversational interfaces like chatbots. ID R&D's AI-driven capabilities include IDLive Face, a truly passive facial liveness product that detects spoofing attacks during remote onboarding and authentication without the user having to do anything. Liveness detection occurs in the background, making it easy and effortless for the customer while preventing fraudsters from knowing when it's happening. The solution is ISO/IEC 30107-3 compliant, having passed iBeta Level 1 testing with a perfect score.

Since 2014, Illusive has been a pioneer in deception-based cybersecurity. Previously, deception took the form of honeypots—systems that emulate valuable corporate resources and attract attackers. Illusive believed that instead of studying the attacker, the attacker needed to be stopped—with lightweight, high-fidelity technology. Illusive disrupted the deception market with technology that, instead of mimicking corporate assets deep within the network, engaged attackers at the edge. With "deceptions everywhere", regardless of where the attacker first landed he could be caught early in the process, long before reaching valuable systems and data. The entire network becomes a trap.

A current focus for the company is to empower incident responders after attack detection with instant, comprehensive, easy-to-interpret forensic data for rapid triage of the attack, and for rich understanding of malicious tactics to improve future cyber resilience.

imVision enables digital and highly automated organizations, who heavily base their business and services on APIs to protect against API breaches such as data theft, fraud, and account takeover. The API Anomaly Management Platform (AMP) is an API threat protection platform, that leverages algorithms from a NLP domain to automatically learn API's business logic, enabling early detection and prevention of abnormal API usage. Unlike legacy web security solutions, AMP can detect the unknown API attacks while requiring zero human configuration and tuning alongside zero-latency addition.

imVision's product is commercially deployed, on-premise and on hybrid cloud, with Global Fortune 500 customers, performs business logic analysis by inferring meaning from sequences of API calls. This enables early detection and prevention of API attacks before the damage was done, demonstrating highly accurate detection using its “meaningful anomaly” model and leading to a 90% operational cost reduction.
Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person's online and real-world identities. Jumio's end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including informed AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 225 million identities issued by over 200 countries and territories from real-time web and mobile transactions.

Established in 2010 with 1,001-5,000 employees, Jumio operates globally in subsectors of threat management/security operations, fraud prevention, risk assessment/risk management.

Kriptos - ADC (Automatic Data Classification), is a cybersecurity software that analyses, classifies and labels documents automatically based on their sensitivity level (Confidential, Restricted, General Use, Public) using artificial intelligence. The company allows businesses to:

- Improve cybersecurity tools, budget & strategies (The technology is compatible with any DLP/CASB solution)
- Optimize cybersecurity policies (Generate cybersecurity Culture through visual labels)
- Identify risky Users and Areas (Train and protect critically users first)
- Certify regulatory compliance (ISO27001, PCI, NIST, GDPR, HIPPA and more)

Founded in 2018 with 11-50 employees, Kriptos focuses on subsectors of identity & access management, data security/data governance, endpoint security, cloud security, employee risk, risk assessment/risk management and operates in the United States and Latin America.

Using its proprietary and pioneering technology, KYND makes complex cyber risks simple to understand and manage for every organisation, regardless of size, means, or industry. With KYND cyber risks associated with operating online can be checked with just a domain name, providing instant results and saving users valuable time.

Using a simple traffic light system, the KYND risk profile highlights, in red or amber, risks that leave it open to cyber-attacks covering email security, ransomware vulnerabilities, data breach risks, and exposure to phishing and malware attacks. It also provides clear and easy-to-understand recommendations and guidance on how to mitigate these cyber risks.

KYND has multiple uses from one-off reports to continuous monitoring and is used by or on behalf of clients all over the world helping reduce cyber risks simply and quickly.

Established in 2018 with 11-50 employees, KYND operates in the United Kingdom and Portugal within subsectors of threat management/security operations, data security/data governance, email/communication security, fraud prevention, risk assessment/risk management.
Ledger is the global leader in security and infrastructure solutions for safeguarding critical digital assets from cryptocurrencies and DApps to CBDCs and STOs. With a team of over 200 professionals around the world, Ledger offers a variety of products and services that protect critical digital assets for individuals, companies and connected devices. Whether you are an individual, enterprise or industry, Ledger has the solution to protect and manage your digital assets. Ledger created a unique digital security ecosystem that provides protection and is built on verifiable trust across its people, hardware and software. Ledger empowers its users by giving them the right security tools to manage and control their critical digital assets. With its meticulous approach to security and ease of use, Ledger puts its customers at the core of everything it does.

LogicGate is a leading provider of cloud-based solutions for automating governance, risk and compliance (GRC) processes. LogicGate empowers customers to shift strategies from reactive to proactive, enabling them to build risk management programs tailored to their business needs. Its proprietary Risk Cloud platform, an end-to-end suite of risk management solutions, blends the right mix of flexibility and out-of-the-box functionality for organizations to manage their risk with confidence. Companies like SoFi, CAPCO and Blue Cross Blue Shield of Kansas City, rely on LogicGate to accurately predict the path of risk and, when needed, rapidly pivot GRC processes without the support of consultants or corporate IT.

Lucideus is a global leader in Enterprise Cybersecurity Risk Quantification (CRQ) platforms incubated from IIT Bombay and backed by Cisco’s former Chairman and CEO John Chambers. It protects multiple Fortune500 companies and governments around the world with its SAFE platform. The platform is a category leading, enterprise grade Cyber Risk Quantification (CRQ) platform which helps businesses measure and mitigate cyber-risks in real-time. It gives decision makers a company-wide, objective view into cybersecurity risk posture and a data-driven approach to cybersecurity. For customers and partners alike, SAFE is the only Cyber Risk Quantification (CRQ) platform which helps businesses measure trust across 5 vectors - people, process, technology, cybersecurity products and external threats, thereby providing a unified and real-time measurement of the risk posed by each.
Maxeler Technologies specializes in solution for high computing problems in multiple markets, such as finance, HPC and defence. For the last 17 years Maxeler Technologies has been providing unique solutions based on both hardware and software for a wide range of problems. MaxIDS is hardware-based Snort rule IDS, providing traffic analysis on high speed network channels. A unique solution that can be deployed everywhere and is nearly untampered due to its secured by design nature. The combination of hardware platform for high performance together with programmability provided by the company’s proprietary toolchain gives a unique advantage to its clients. The company counts CMS, JP Morgan and Citi bank among its customers.

Mitiga specializes in incident response and breach readiness for organizations designing their cloud migration, or already active at the cloud. From capital market banks and insurance firms, to FinTech and welfare and asset management companies, our clients rely on us for custom-crafted operational cybersecurity resilience in the form of pre-incident methodologies that accelerate post-incident business bounce-back and a state of business-as-usual, down to hours. Our team of ex-military cybersecurity intelligence backgrounds are at your disposal and ready to be deployed for active incidents including: ransomware attacks, data breaches, insider attacks, malware attacks, DDoS, APT’s, business email compromise, cloud misconfiguration breaches and application attacks.

Founded by a team of cybersecurity serial-entrepreneurs that have sold companies to EY & Synopsis, we combine a granular understanding of financial market security risks, with military-grade technology, strategy and leadership. Mitiga is backed by and partnered with world-leading cybersecurity VCs.

MYKI is a decentralized password management & authentication solution for individuals, enterprises, and managed service providers. It allows users to privately store passwords, payment card information, IDs, and 2FA secrets offline, across their trusted devices. The company’s mission is to help users reclaim ownership of their digital identity.
NanoLock Security protects IoT and connected edge devices against persistent cyberattacks by insiders, outsiders and supply chain attackers. NanoLock provides a device-level, Security-by-Design solution with powerful flash-to-cloud defense that secures the entire chain of device vulnerability—from deeply embedded endpoints in the device, to the cloud—with no additional device costs and zero computing power. NanoLock’s patented technology is securing a root-of-trust in the flash memory from leading memory vendors and is crucial to the success of industries like telecom, smart cities, utilities, industrial, automotive and more. NanoLock Security is the 2019 winner of the prestigious “4YFN Barcelona Startup of the Year” award.

NanoLock’s founding team and senior management is made up of veterans from the cybersecurity domain, representing a wealth of deep knowledge about management and security of next generation edge devices. NanoLock has offices in the United States, Israel and Japan.

Nethone is a Know Your Users™ (KYU) company that enables business from around the world to better understand end-users and prevent them from online fraud. By using AI & Machine Learning technology Nethone is able to detect and prevent card-not-present fraud, including protection against account takeover. Nehtone can help to lower clients’ rejection rates, costs of manual review, and fraud risk, without affecting the service UX.

Nethone makes a significant change, through: Profiling, which enriches the context of the user’s understanding with 5000+ attributes; Providing clients with a broad subset of structured data to determine online fraud risks; Focusing on frictionless transaction flow; Mitigating sophisticated fraudulent attacks; Easy integration.

Founded by data scientists, security experts, and business executives, Nethone is one of the fastest-growing technology companies in CE, which secures transaction attempts and logging into online accounts for e-commerce, digital goods, travel, and financial industries.

Netography delivers real-time protection/defense against millions of network-based threats across an organization’s entire infrastructure, both on-premises and in the cloud. As a result, network and security teams can have shared visibility into their security posture and effectiveness of their security controls at any and every point in time.

Netography’s Security Platform provides cross-network visibility, encompassing cloud and on-premises environments. With the network-wide visibility that Netography delivers, organizations can protect themselves, via instant and automated remediation, against a broad set of security threats, resulting in a 90-percent reduction in MTTR (mean time to resolution). Netography helps companies verify the effectiveness of their existing security and tools, share the same data in real-time across NetOps and SecOps teams, and easily protect their entire infrastructure as they scale, without adding expensive hardware.
Neuralys helps teams determine the real impact of a vulnerability. The company's platform enables cross-collaboration among all these different business units, combining all vulnerability tools and also the information from the multiple teams in one place, automating correlation, and empowering those teams to work together on the customization, prioritization, and attestation of what they found. Neuralys also enables them to standardize the multiple scopes and methodologies that they use without the collaboration challenges that they usually have since they are running different security tools. It's tough for them to share evidence across all those teams.

nsKnox is a cyber-fintech company focused on Corporate Payment Security, founded and led by Alon Cohen, Founder & former CEO of CyberArk (NASDAQ: CYBR). nsKnox solutions protect corporations and banks against cyber-fraud carried out by insiders or outsiders, preventing significant financial losses and reputational damage.

Leveraging its ground-breaking Cooperative Cyber Security™ (CCS) technology to combine the cyber strength of multiple organizations, nsKnox's solutions detect and prevent finance and operations infrastructure attacks, social engineering, business email compromise (BEC) and other Advanced Persistent Fraud attacks.

Backed by Microsoft Ventures, Viola Ventures and IDB Bank, nsKnox has offices in New York, London and Tel Aviv.

Paladin Cyber provides comprehensive cyber protection for small and medium businesses through differentiated insurance programs and easy-to-use technology.

Paladin Shield is an easy-to-use cybersecurity suite that allows businesses to address both their technical and human-driven cyber risks. It includes endpoint protection in the form of a Browser Extension, a portal for non-expert administrators to customize protection with ease, and a full employee training & assessment platform. Through its modern risk management capabilities, Paladin provides unique product differentiation and superior loss results to carrier partners.
PerimeterX is the leading provider of application security solutions that keep businesses safe in the complex digital world. Delivered as a service, the company’s Bot Defender, Code Defender and Page Defender solutions detect risks to customers’ web applications and proactively manage them, freeing customers to focus on growth and innovation. The world’s largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers’ digital experience. PerimeterX was named a Leader in Bot Management by Forrester Research and received differentiated ratings, the highest ratings possible, in 7 out of 9 rating categories including in the attack detection, attack response, threat research, feedback loops, performance metrics, vision, roadmap and market approach criteria. PerimeterX has operations in Tel Aviv and Miami and has over 200 customers in production. The fast-growing list of PerimeterX customers includes companies in the Fortune 500, the Alexa Top 1000 and the Internet Retailer 100.

Polyverse enables customers and partners to harness its leading-edge cybersecurity technology to build diversity and uniqueness across multiple system dimensions, increasing the complexity and cost for attackers and stopping cybersecurity attacks before they start. Polyverse turnkey solutions install in minutes within your existing architectural infrastructure and carry extremely low ongoing operating costs. Polyverse technology is validated by the U.S. Department of Defense to mitigate against zero-day memory exploits. The solution has been independently validated by Mitre, DISA, OSD, Navy, DARPA, Iomaxis and Plex on behalf of the US Department of Defense. Founded in 2015 by bringing together top talent from Microsoft, Amazon, Google, and SUSE, Polyverse is led by founder and CEO Alex Gounares. CNBC named Polyverse as one of the top 100 startups in the world.

Post-Quantum protects the world's information against today's threats and tomorrow's challenges. It ensures its clients can carry out their operations safely and securely, with trust and confidence in all their activities. Specialising in innovative identity and cyber-security solutions, PQ brings its expertise in cryptography and data protection to solve access, approval, and oversight challenges for clients across sectors. The company leverages innovative technologies – from multi-party computing to blockchain – to create new approaches to identity, and implement end-to-end solutions that enforce data policies, manage risk, and create trust. PQ binds identities to actions to ensure accountability, and segregates access to sensitive data to prevent privilege abuse.
Originating from the University of Oxford, PQShield is a world leader in Post-Quantum Cryptography. The company provides quantum-secure cryptographic solutions for software, software/hardware co-design and data in transit. This is particularly important where long lifecycle, performance and lasting confidentiality are a priority, now and for years to come.

PQShield helps customers transition their product lines from legacy RSA and Elliptic Curve cryptography to quantum-secure standards by offering ready-made and tailored IP for secure elements, IoT firmware, PKI and server technologies, and end-user applications.

The Quantum world is nearly upon us and it contains both great opportunity and vast security implications. Consider the proliferation and lifecycle of connected systems across telecoms, automotive, smart environments and financial institutions - one working quantum computer in the wrong hands is enough to put our whole online system at irreversible risk and cause tremendous damage. The need for advanced post-quantum protection is evident.

The PQShield's world-class team of cryptographers is building next-generation technologies for all parts of the security ecosystem. PQShield has unrivalled domain expertise in the design and implementation of quantum-resistant cryptography for software and hardware applications.

PQShield's solutions provide fast time to market and compliance with both existing and upcoming cryptography standards.

**PRODUCT DESCRIPTION**

PQSoC: A Post-Quantum System on Chip crypto coprocessor toolkit. Full system emulation and standard development tools ease adoption. Available as modular IP or self-contained solution.

PQSDK: Comprising implementations of post-quantum primitives fully integrated with OpenSSL API and applications such as PKI (CA), S/MIME electronic mail and VPN solutions.

PQE2E: A software development toolkit for enabling ‘data in transit’ messaging solutions using post-quantum algorithms, leveraging a new, provably secure, signal-derived protocol.

**TOTAL FUNDING**

PQShield has the financial support of Oxford Sciences Innovation (OSI), Kindred Capital, Crane and Angel Investors - and has also attracted significant Innovate UK project funding.

**TRACTION/GROWTH**

- First customer from the OEM world to be announced soon as well as partnerships with world leader security companies
- PQShield is a major contributing participant to the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardisation process. There are 26 main NIST semi-finalists – PQShield & advisors are co-authoring ten of them
- PQShield is the biggest spinout of Oxford University's Mathematical Institute, and home to the brightest talents in cryptography
- PQShield is developing new PQ-secure technologies to be applied in IoT, Automotive, Telecom, Financial and Healthcare industries
- The company's projected revenue in 5 years is $20-$50m

**MANAGEMENT BIO**

Dr Ali El Kaafarani is the Founder & CEO of PQShield, a spinout of the University of Oxford, and the Mathematical Institute where he is a Senior Industrial Fellow. Dr El Kaafarani has over 10-years of academic and industrial experience in Cryptography, having also worked at HP Labs in Bristol in addition to being an Oxford University academic. He founded PQShield in 2018. PQShield is now a leading authority in the cryptography community, contributing to various international standardisation efforts of the next generation of cryptography.

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.
PQShield is protecting the businesses of tomorrow
Quantum computers will change the cybersecurity threats that businesses face, but PQShield is stepping up to ensure companies stay ahead of the curve.

Doctor Ali El Kaafarani is trying to make companies safe from the future digital threats posed by quantum computers through PQShield, the cybersecurity startup he is the founder and CEO of.

Back in 2015, El Kaafarani became painfully aware of just how badly businesses cut it when it came to their digital defences. He had just finished a stint with Hewlett Packard Labs and had seen first-hand how businesses were fighting back waves of hack attacks. Yet, when he returned to the University of Oxford’s Mathematical Institute as a research fellow it became clear to him that companies were not doing enough. Not even close. “It was shocking, really,” says El Kaafarani. “The industry is like ten, 15 years behind what academics are saying about broken schemes or things that will go wrong.”

The way he saw it, a lot of businesses had simply adopted an attitude of patching their digital defences when they absolutely needed it, thinking that it would cost too much to give their cybersecurity a complete overhaul. “They just left it until the last minute and when things went wrong, then they said ‘okay, let’s change it,’” El Kaafarani says. While this might have worked for businesses in the past, the tech world is set for a massive paradigm shift.

Quantum computers will change everything. The idea behind the technology has been around since the 1980s. Rather than using only the traditional zeroes and ones, these computers would also use quantum bits, or qubits, when they process programs. Qubits can represent zeroes and ones at the same time in a state called superposition. What that means is that these machines will be able to crunch computational problems at a fraction of the time it would take any other device that has come before it, in some cases slaying billions of years of processing time into minutes. This could result in a significant cybersecurity threat for companies running on old software. Simply put, it means that the encryption many businesses use to keep their systems safe could be cracked really easy with a quantum computer.

Tech giants like IBM and Google as well as governmental bodies around the world are working on creating the first quantum computer. “Everyone wants to win this race,” says El Kaafarani. While the technology has yet to materialise, it is on the way.

In 2015, about the time that he had joined the University of Oxford, the US National Security Agency issued a public warning that quantum computers were inbound and that organisations better get their ducks in a row or risk suffering seeing their security compromised in a not too distant future. “So at that point, it was clear that the risk is real,” he continues. “And since cryptography is all about mitigating the risk, there’s no logical reason to not to be ready for the quantum era.”

El Kaafarani’s first project at the University of Oxford was leading a post-quantum cryptography project. About a year into the project, they realised that the project would work better as a commercial enterprise. “At the math departments, you want to hire PhD students or postdocs, which is fun, but that’s not how we can build a product,” he remembers. “If you want to build a product, you have to hire practitioners who
have been doing this for years. And that’s when the idea became clear in my head that we should spin out from the University of Oxford [and launch] a startup specialised in post-quantum crypto."

"It was shocking, really. The industry is like ten, 15 years behind what academics are saying about broken schemes or things that will go wrong."

Not resting on his laurels, El Kaafarani launched PQShield in May 2018. A few months later, the company’s first engineer joined the budding business. The company now employs about a dozen workers. “So a bunch of bright minds and brilliant cryptographers who are actually the designers of a bunch of schemes that are being standardised at NIST (National Institute of Standards and Technology),” he says. “We have people who really know what they’re talking about when they talk about the standardisation process because they are heavily involved in this standardisation process.”

Backed by this impressive team and the financial support of angel investors, Oxford Sciences Innovation (OSI), Kindred Capital, and Crane, the company set out on its journey. El Kaafarani also hints that more news about additional funding might be in the pipeline.

Of course, a company is all about the products. The team started off by looking at what the biggest risks were. It became clear to them that most quantum attacks would happen in retrospect. What that meant was that hackers may be able to harvest secure data today, but that this encrypted information would just read like complete gibberish until they got their hands on a quantum computer. When that happens, which El Kaafarani believes could be in the next decade, the confidential data could be compromised. “We wanted to solve that challenge,” he says.

The startup provides quantum-secure cryptographic solutions for software, both software and hardware co-design and data in transit. The hardware solutions are designed around RISC-V architecture and completely built in house. RISC-V is an open standard instruction set architecture based on established reduced instruction set computer principles available through open source. The solution can bridge the gap between legacy systems and post-quantum systems. The idea is that the company will license the design of the chips to people producing the hardware. PQShield also offers implementations of post-quantum primitives and a software development toolkit for enabling ‘data in transit’ messaging solutions using post-quantum algorithms, leveraging a new, provably secure, Signal-derived protocol.

But having tools on offer isn’t enough, PQShield also had to convince prospective clients that they actually needed the solution. This proved a bigger challenge than expected. “We don’t have quantum computers yet, so why should they care?” El Kaafarani says a lot of potential clients seem to think. When faced with that argument, the PQShield team try to explain that while quantum computers are some time off, bad actors can already harvest encrypted data now. When the technology does arrive, it’s just a matter of time before they can decrypt that data. In other words, sceptical clients must be certain that their privacy policies and the legislation that they must comply with do not say that they have to keep the data secure for three, five, ten years or however long it will take to launch a quantum computer. Yet, given NIST published another whitepaper in late May 2020 that offered an updated roadmap on how companies can prepare for the oncoming paradigm shift, it’s clear that there are reasons to take the cybersecurity risks of quantum computers seriously.

El Kaafarani compares it with having car insurance. “If you don’t drive a car and you never get into the car, then you don’t need car insurance to help you if you have an accident,” he says. “But when you have a car you need insurance. This doesn’t mean that the accident should happen tomorrow. But this means that or there is a chance that this might happen. With quantum computing, it’s even worse, we now know that it’s happening soon, we just don’t know exactly when”

At the moment, PQShield is at the beginning of its commercialisation journey and El Kaafarani hints that it is soon going to announce the first big customer in the OEM world. Yet, while the company’s journey is just getting started, it’s safe to say that the future has already arrived for PQShield.
PPC Protect is the pre-emptive ad fraud and ad safety solution for Google Ads media buyers. Utilizing true machine learning and advanced neural network analysis, PPC Protect analyses paid media web traffic in real time using a mixture of purpose-built algorithms, self-learning datasets and natural language processing to determine ad placement quality.

Founded in 2016, PPC Protect has gone from strength to strength over the past few years, winning multiple awards for its technology, including being named as one of the UK’s top 20 startups and recently being recognized as one of the 22 most promising cybersecurity scaleups within the UK.

Precognitive provides a multi-dimensional fraud prevention platform that uncovers suspicious activities in real-time before fraudulent transactions occur. By combining device intelligence, advanced behavioural analytics, machine learning, and a real-time decision engine, its technology detects and prevents all types of digital fraud including payment fraud, bot attacks, card testing, account opening, account takeover and return abuse. The company's easy-to-deploy solution has an unrivalled level of accuracy in fraud detection and prevention, creating an immediate positive impact by significantly reducing fraud-related revenue loss and operational costs, while also increasing customer satisfaction and revenue through higher approval rates for genuine transactions.

Precognitive takes a consultative approach, leveraging its highly experienced staff to evaluate and address clients’ specific goals and requirements. Through constant innovation, Precognitive outmanoeuvres fraudsters, pre-empting bad behaviour while safeguarding businesses and consumers.

Proteus-Cyber are specialists in Data Privacy, the GDPR, CCPA, LGPD, PDPA, RGPD regulations, plus others and own the award-winning software Proteus®NextGen Data Privacy™ Software that provides everything you need to manage your data privacy compliance in order to avoid a data breach. It really is the Gold Standard of data privacy compliance. With In-built Privacy Impact Assessments & Data Privacy Impact Assessments (PIA/DPIA), Proteus can automate parts of the process to enable the DPO to perform mapping of personal data and assess what personal sensitive data exists, how and why it is processed, and more importantly, how it is secured.

Proteus®NextGen Data Privacy™ is a Fully integrated enterprise scalable software solution with features like, Data Discovery & Categorisation, Automated PIA/DPIA & risk assessments, 3rd party audits, DSAR management, privacy-by-design, Breach notification, Free privacy research, Threat-intelligence, Pro-active Breach protection, Cookie management, Consent, Easy reporting and supported in over 100+ languages.
QOMPLX makes technology that helps the world’s leading companies identify and defeat sophisticated cyber adversaries including cyber-criminal groups and nation-state actors. These groups are exploiting critical IT infrastructure including Microsoft Active Directory to establish long-term residence on sensitive networks, often disguised as privileged users or applications. With QOMPLX, financial institutions can integrate disparate data sources across their enterprise to spot malicious activity and the earliest stages of a cyber attack. The company’s advanced streaming analytics technology uses rules, algorithms, simulations, and machine learning tools to help financial institutions identify attacks on Active Directory and other core infrastructure in near real-time. QOMPLX’s advanced algorithms, simulations, and machine learning tools help the world’s most demanding firms solve the toughest challenges in cyber security, insurance underwriting and finance.

Quantum Xchange gives commercial enterprises and government agencies the ultimate solution for secure communications. Its complete key management system, Phio Trusted Xchange (TX), is uniquely capable of making existing encryption keys quantum safe and supports both post-quantum crypto (PQC) and Quantum Key Distribution (QKD) for true crypto agility and quantum readiness. As the operator of the first quantum fiber network in the US, Quantum Xchange also holds the unique distinction of being the only company in the world to make QKD commercially viable by solving the distance and delivery limitations inherent with all other offerings. With a dynamic security infrastructure in place, organizations can enhance their existing encryption environment, select the level of protection needed based on their risk tolerance, and seamlessly scale to QKD at any time, across any distance, between multiple transmission points.

QuintessenceLabs is the global leader in quantum-enhanced cybersecurity solutions. Founded in 2008, it delivers unique products that integrate quantum technology with high-value security technology, including the world’s fastest true random number generator, an advanced key and policy manager, and integrated encryption solutions - all of which keep organizations secure today and prepared for tomorrow. QuintessenceLabs also stands at the forefront of development in quantum key distribution, using the laws of physics to protect our information from the security threat of quantum computers. The company is headquartered in Canberra, Australia.
Red Sift is a data-driven cybersecurity business that uses machine learning to help organizations of all sizes and sectors address day-to-day security challenges. It offers a dashboard of tools that analyze and synthesize data from core business processes - such as email - to help users better manage their online security.

Red Sift's mission is to democratize the technology essential for cybersecurity. Founded in 2015 by serial entrepreneurs Rahul Powar and Randal Pinto, Red Sift is headquartered in London, UK, and boasts an impressive client roster including TransferWise, Telefonica, Action for Children, and top UK law firms.

Resolver offers integrated risk management software for mid to large-sized organizations including solutions for risk management, corporate security, business resilience, and IT risk. Resolver enables its clients to drive user adoption, share data more effectively, streamline operations and provide more actionable insights throughout the organization. Over 1,000 organizations worldwide depend on Resolver’s security, risk and compliance software with around one million people using its tools each day. The company serves customers across a number of industries and business needs, such as finance, critical infrastructure and high tech.

RiskSense®, Inc. provides full spectrum vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. The RiskSense platform continuously correlates customer infrastructure with comprehensive internal and external vulnerability data, threat intelligence, human pen test findings, and business asset criticality to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation activities to achieve security risk goals.

By leveraging RiskSense threat and vulnerability management solutions, organizations significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, heighten response readiness, lower costs, and ultimately reduce attack surface and minimize cyber risks.
Rubica is mobile cybersecurity for remote working and BYOD environments. The company is the first consumer-friendly and enterprise-grade cybersecurity product built with a “mobile-first” approach. As more businesses shift to virtual environments and people work remotely, Rubica is the premium solution to protect their digital identities, privacy, data, and devices. Rubica secures your devices (laptops and mobile phones), internet connection and accounts, no matter where you connect from – Wi-Fi, cell, office, remotely. Unlike antivirus or a corporate VPN, Rubica security actually protects people from malware, phishing, mobile-app-based threats and 52 other kinds of emerging threats. Rubica uses encrypted VPN technology, an enterprise-grade security stack with IDS/IPS capabilities, real-time threat intelligence, and Security Operations Center (SOC) analysts to offer advanced cybersecurity for businesses of all sizes.

SCYTHER enables you to turn cyber threat intelligence into reality through a common platform, providing a single pane of glass to identify security blindspots. With SCYTHER, security teams can quickly create realistic adversarial campaigns that cover the spectrum from simple to APT-level complexity and stealth. The company is providing all the building blocks for red, blue, and purple teams: a common platform and workflows to test and validate their security controls and investments against real world threats targeting their enterprise, tailored to what is specifically targeting them. The campaigns are created through a simple to use, drag and drop timeline that includes pre-saved actions that replicate real-world TTPs from the MITRE ATT&CK framework and an SDK to build your own modules and TTPs.

SECBERUS is a Cloud Security Posture Management (CSPM) and Reporting Platform. The company creates solutions with the most advanced technology and best user experience to simplify cloud security and compliance, bringing organizations confidence in the cloud, today and tomorrow. SECBERUS Cumulus Cyber-IQ allows enterprises to enforce strategic multi-cloud, multi-vendor security practices via continuous infrastructure security and compliance assessments across the entire CI/CD cycle. SECBERUS is built to ingest any data source and, as a result, produce cloud-agnostic security and compliance policies. SECBERUS continuously audits an organization’s cloud infrastructure against common compliance standards such as PCI DSS, HIPAA, SOC2, CIS, ISO 27001, and FedRAMP to provide a real-time compliance posture that can be reported via one-click PDF reports.
Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to infuse security early in the application development process. With its flagship product, SD Elements, Fintech companies can automate manual processes for security and compliance to improve time to market for new technology. Their expertise in strategic advisory empowers organizations to embrace DevSecOps and helps them build a security culture. Security Compass is the trusted solution provider to many leading financial organizations, technology enablers, and renowned global brands.

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over a million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard’s patented rating technology is used by over 1,000 organizations for self-monitoring, third-party risk management, board reporting and cyber insurance underwriting; making all organizations more resilient by allowing them to easily find and fix cybersecurity risks across their externally facing digital footprint. SecurityScorecard is the only provider of instant risk ratings that automatically map to vendor cybersecurity questionnaire responses - providing a true 360-degree view of risk. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every company has the universal right to their trusted and transparent Instant SecurityScorecard rating.

Simudyne is a simulation technology company based in London. It uses advanced analytics and AI alongside agent-based modelling and simulation to help institutions, exchanges and governments solve complex problems and make better decisions. Institutions drive better financial results by weaving modelling and simulation into the fabric of their decisions. Simudyne augments traditional decision making and uncovers more optimal forward paths using realistic environments and properly calibrated models. With a realistic simulated environment, institutions can test their decisions to understand the best path forward before committing people and resources. Agent-based models make this kind of realistic simulation possible. Agents are independent components of software code that interact with one another, forming new data, prices, effects, results and anything else that needs to be embedded into a simulation to make the best possible decisions.
Source Defense secures websites, enables secure digital innovation, and ensures customer and payment data privacy via a real-time prevention solution against website supply chain attacks. The company provides its customers with a fully automated and dynamic set of rules and policies that control access and permissions of all Javascript based 3rd-party tools operating on a website.

Spitch provides customer service automation and identity and access management solutions for companies in the financial sector and other industries that help reduce costs, increase sales and improve customer satisfaction. Spitch’s omnichannel conversational platform allows to automate the processing of typical calls, automate regulatory compliance based on real-time and offline speech analytics, support secure homeworking for contact centre agents, including identification and ID verification by hybrid voice biometrics, fraud prevention, productivity monitoring, etc. Spitch’s high-precision conversational AI makes it possible to delegate routine functions to virtual assistants and ensures that human specialists have enough time to address more complex tasks creatively. Spitch solutions are easy to implement on-premise or in cloud. Alongside high accuracy and rich functionality, Spitch offers a bespoke approach ensuring that clients see measurable business benefits from day one.

swIDch is a cybersecurity startup that helps businesses to identify and authenticate its users through a patented algorithm, one-time authentication code that is generated in a networkless environment, to tackle problems of identity theft and CNP frauds. swIDch provides simplicity and security in the authentication process in the most cost-effective way. The algorithm creates OTAC (One Time Authentication Code) which is dynamic numbers generated on a user’s mobile for each transaction without a network connection. OTAC is a unique code that cannot be duplicated and identifies users for granting individuals unhackable access to any device, system, or service. In terms of payment, users can generate dynamic PANs (Primary Account Numbers) in the same format of card numbers, CVV/CVC, and expiry date. This can eliminate CNP fraud since there is no access surface for hackers.
Symphonic is an integrative solution based on standard technologies such as Java. The company is, however, able to use information sources from any digital resource to inform the decisions the software generates on whether access is properly permissible. This can and has included Blockchain, AI, and Big Data.

**PRODUCT DESCRIPTION**

Symphonic provides intelligent control of user’s ability to access data & services, by deploying its sophisticated authorization software solution. Policies can be defined by business users easily and at speed creating fine-grained authorization. Policies are built in a powerful user interface that is visual and easy to navigate. The company’s Policy Decision Point (’PDP’) which evaluates the bank’s policies for access in milliseconds, is scalable and can be deployed on-premises or in the cloud (or hybrid architectures). It can dynamically retrieve data from new, legacy or cloud data sources and services ensuring that intelligent decision making uses a variety of context-relevant information.

Symphonic has been designed from the ground-up to support emerging and maturing technologies such as cloud, containerisation, orchestration, serverless, configuration-as-code, and DevOps, while maintaining support for legacy architectures. The company recognises the shift in enterprise organisations to API-first architectures, and the growing desire of these organisations to exploit these data services in dynamic authorization and decisioning.

Large banks with complex architectures have turned to Symphonic to address these challenges, reducing complexity, lowering costs, and improving their regulatory compliance posture while driving improvements to fraud and risk processes.

**TRACTION/GROWTH**

- Symphonic has grown from a core team of about 10 to a team of over 30 in the last 12-18 months
- The company’s software is used by clients globally including major financial institutions and large organisations in other sectors
- The company is looking to expand its US and APAC client base, and expand further within Europe
- Symphonic has been selected for Tech Nation Cyber 2.0 among 22 high-growth UK scale-ups.

**PARTNERSHIPS**

- Ping Identity (Technology Partner)
- RAIDIAM (Consulting Partner)
- ProofID (Integration Partner)

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.
Watching the door is no longer enough
Symphonic Software has gone from being a cybersecurity research project to offering a contextualised data user experience to massive banks and governments around the world.

“We are like a club doorman,” says Derick James, CEO and founder of Symphonic Software, the dynamic authorization solution provider. While some doormen might only subjectively assess whether or not the guest is of legal drinking age before letting them in, the doorman in this analogy is considerably busier because he’s making sure people only do what they are allowed to do. “What we do is we apply rules at each stage,” James explains. “You can dance now, or stop dancing if you’re wearing stilettos. Have a cocktail if you’re over 21 or stick to a mineral water. If you then replace the club with the company’s digital solution and the drinks and the dancing with the data, then you basically have the idea.

Or to put it in another way, Symphonic’s software provides a contextualised user experience where their clients set rules for who can access what data and when. For example, with modern digital banking there are many rules in place for how customers can access their accounts. A customer who regularly pays the same payee can easily do so, but there is more risk involved when they pay someone new, which is why users are often asked to authenticate themselves again. Symphonic provides software that allows rules to be implemented to check various data in real-time with a view to minimising the risk of fraud.

The company was launched in 2014, having spun out of a research project from one of Edinburgh’s leading Universities. “The idea came from the notion that information access was being opened up much more widely,” James explains. Before the internet, computers might have been linked within a company, and data perhaps only shared with other company functions. Over time, this landscape has grown considerably in scale and scope.

As companies have grown in complexity and digital traffic ever increases, businesses have begun to open up data assets to partners, customers and suppliers. Often, this opening up of their digital infrastructure was protected by developers hand-crafting rules into each application which is error-prone, inconsistent, laborious and inefficient in times of change. At the same time the rules about what data different people could access have been increasingly subject to regulators’ scrutiny. Eventually, the application by application approach just becomes too complicated and the risks of inappropriate access is difficult to manage. “It used to be the case that if your username and password were right, you were in and then after that nothing was checked at all, or if it was very little,” James continues. This has created considerable risk now that lawmakers are imposing strict data privacy laws such as the EU’s General Data Protection Regulation (GDPR) and Open Banking / PSD2, and consumers in any case want more control of their own data.

Symphonic’s idea was to create a solution that took all of those rules out of the applications and essentially created a digital shield around the infrastructure that supports customers’ services and data. Instead of having to build these rules into each application, clients could use Symphonic to incorporate the new rules into the shield. “Symphonic does not touch or see the data,” James explains. “Our software gets in between a request to see the data and the data itself and applies rules to determine whether or not this is allowed.” One of the key advantages of this is that it brings consistency into the approach to prevention of fraud and cybersecurity breaches.

To get the startup off the launchpad, Symphonic raised a £280,000 seed round in 2014 in order to fund initial market testing of the company’s solution. “That allowed us to get our first customer traction,” he says.

From its early engagement in health, where data is just as sensitive as financial data, Symphonic has expanded extensively into finance. Moreover, it has worked with both smaller and larger banks, including some of the UK’s leading banking organisations. Symphonic also signed technology partnerships with companies like Janrain, which was later acquired by Akamai, and Ping Identity. “That let our partners distribute parts of our technology allowing us to expand overseas,” James says.

“Our strong customer traction gave us the opportunity to really scale the business and to expand the team significantly,” he recalls.

After further rounds in 2015 and 2017, the scaleup raised a £2m round in 2019. Maven Capital Partners led the latest raise. The capital injection was also supported by Symphonic’s earlier investors Edinburgh-based Par Equity and the Scottish Investment Bank. “That enabled us to double the size of our engineering team, to bring in further sales, marketing, finance and operations experience and to start really driving the business forward,” James says.

Today, Symphonic has customers in Australia, the US, and Europe. Having originally targeted the health and finance sectors, the company is now protecting data for consumer goods, marketing services and insurance companies as well as some government departments. “So we are diversifying our geography and our sector penetration, as we continue to grow,” James concludes.

Six years into the company’s history, it seems as if Symphonic’s doorman is about to get really busy.
How Symphonic helps banks securely boost their digital transformation

As banks across the world modernise their services with technology, Symphonic is providing them with the tools to do that efficiently and securely.

Global competition has forced financial services organisations to undergo massive digital transformation. However, the COVID-19 pandemic could speed up the process. As they do, they will need a secure way of how to share their data.

The move towards less physical interactions in the banking sector has been happening for some time but has accelerated in the face of the current crisis. Cash is quickly being replaced by electronic payments, branch visits have dropped significantly and call centres are being overwhelmed by a massive increase in calls.

While it's hardly surprising that businesses have recognised the need to accelerate their journey to digital, the transformation presents an enormous challenge for both IT and the business. Teams need to refine the optimum customer journeys that satisfy user and business need and then work back to identify which of the bank's systems need to provide the data. This data is then used to make a decision on when to allow a transaction, deny it or allow with some conditions (e.g. send a one-time password to the customers mobile before they can proceed).

Streamlining customer journeys is becoming more critical in digital channels as these grow. Poor digital experiences when dealing with banks are common. Being unable to pay an important bill due to a misplaced password or pin, is one example. Having a fraud block on a credit card when travelling despite having purchased a flight or booked a hotel at that destination with the same card is another.

Digital consumers are significantly less tolerant of these experiences. It's becoming easier than ever to switch so banks have to deliver or risk losing customers. Customers don't care about the reasons for poor digital experiences. And often, despite good intentions, the reliance is on a mix of old systems not designed or to be flexible to the demands of modern customer interaction.

At its core, the technical challenge is to provide an agile platform that can connect to all the systems required to access data needed to make the right authorization decision. Such a platform empowers banks to react quickly to evolving needs of customers, regulators and themselves.

For example, everyday transactions like a retail customer transferring money from one of their accounts to a friend's account appear simple. But to mitigate the risks appropriately, checks have to be made on many levels, all without compromising speed of service. This can include checks on customer and beneficiary accounts for KYC and AML purposes and checks on a host of other transaction characteristics, some of which are now enshrined in regulation. More sophisticated customer journeys will also bring in data from cloud services for things like risk scores, geo-location and customer consent data to make more context aware decisions in real time.

There are thousands of other potential customer journeys modern banks must accommodate. Beyond the checks mandated by the bank, customers are increasingly given controls to self-manage their access arrangements. New product offerings allow customers to set dynamic payment thresholds or manage permissions of family members. Embedding these regulatory checks and self-service controls into individual applications can quickly become opaque and difficult to understand, and costly to change. With the pace of change quickening, managing the basics of who can access what and under what conditions is becoming a major challenge and a risk to the business. This is only set to become a bigger challenge in the aftermath of COVID-19 as customers use more digital services and the bank's workforce increase their home working patterns.

That's where Symphonic comes in. The company's vision is to see authorization being a key, core architectural component of every enterprise. Symphonic's platform has been designed in collaboration with banks and has been implemented in some of the world's most advanced
and complex banking architectures. It has enabled banks to deliver personalised customer experiences, driving improvements in customer advocacy.

Symphonic is the leading authority in policy-based authorization management for financial services organisations. The software platform is developed with modern organisations’ technical needs in mind. The team behind it has leveraged its significant experience of the sector to provide a cutting-edge solution for pro-active, forward-looking banks.

They have already delivered pioneering projects for banks in Europe, Australia, and the US becoming a key component used by the banks in satisfying the new regulatory requirements.

Digital Transformation needs Dynamic Authorization

The scope of customer service digitisation and complexity of applications within organisations has been accompanied by security concerns around data breaches and privacy threats. This calls for an intelligent platform to drive a Dynamic Authorization approach that can analyse an array of factors to determine whether an access request should be authorized or not.

In response, Symphonic has combined its technology and security expertise to develop an integrated access management solution that provides organisations with centralised visibility and control over who they share their data and services with and how. "Symphonic has been helping banks across the world to protect data and services through the growth of digital self-service – to meet customer needs; exploit existing IT real estate; and manage risk," says Derick James, CEO of Symphonic.

Designed for flexibility and agility, Symphonic differentiates itself from its competition through its centralisation of authorization into a single set of policies, which can be reused by the myriad of applications in banks. This enables Symphonic to assure organisations that their policies are applied consistently and with agility across all applications and with clear visibility on the access policies that have been implemented.

The Trust Framework, a unique Symphonic feature, has powerful integration capabilities and provides the foundation for the access policies. The framework provides a complete map of a client’s enterprise data and services ecosystem, cataloguing the information related to resources being protected, users, and data points that need to be interrogated to provide contextual information when making dynamic authorization decisions.

From these building blocks, the Symphonic Policy Manager provides a platform for staff outside of the IT function to simply and easily create, adjust and manage the policies needed to ensure that access to data and services meets not only regulatory requirements, but also the needs of the bank.

Subsequent control is managed in real time by the Symphonic Decision Engine which evaluates access requests coming from the bank’s internal and external users and ensures enforcement of the bank’s policy rules. The Decision Engine captures real-time context surrounding a transaction, calculates the right decision and ensures compliance with the customer and bank’s requirements.

Transform, centralise and reduce cost

Symphonic introduces a new, modern capability into client organisations. Working collaboratively with a client, Symphonic’s onboarding process begins by analysing the technical landscape of the client’s IT assets. In partnership with the client, the goal is to map the business and regulatory demands onto the bank’s specific infrastructure and systems, so that these can be described as policies and can be implemented to support their requirements and fit with their operating models.

PSD2 is also driving uptake by having introduced the need for an intelligent authorization service that checks internal fraud and risk systems, cloud-based risk assessment sensors, and evaluates user and target characteristics in payment processes. Lynne Cameron, Tesco Bank’s head of financial crime and customer security comments, “Through a collaborative approach, Symphonic provided a sophisticated orchestration layer and policy decision platform enabling us to meet demanding regulatory requirements.”

Symphonic is uniquely placed to support banks as they modernise their services to address increasing traffic on all channels including web, mobile and API. By creating a reusable set of centralised policies, Symphonic’s clients have a platform that supports consistency, agility and visibility at greater speed and reduced cost – the key to successful digital transformation.

Banking industry veteran George Kelsey, CTO EMEA of Ondot Systems who formerly led innovation at RBS and Tesco Bank, is one of the market stakeholders that recognises the value of this new reusable centralised approach “Abstracting and centralising authorization and entitlement from disparate systems and data stores is the first step in simplifying the increasingly complex technical and business landscape companies face today,” he says. “Applying visible and auditable policies to authorization and entitlement and being sensitive to the ever-changing context of the customer and other dynamic factors is the next intelligent step forward. Symphonic delivers both of these steps with a system designed for scale and speed.”

If you are part of a team delivering strong customer experiences for your customers and want to build your knowledge, why not schedule a 30-minute workshop with Symphonic’s subject matter experts – an opportunity to learn from each other and discuss the art of the possible.
Sytorus is a market leader in data protection and privacy management software and solutions helping businesses and organisations comply with privacy regulations including GDPR, CCPA and HIPAA with an unrivalled combination of technology, expertise and experience. The company’s PrivacyEngine™, a SaaS privacy management platform built by technologists and data protection subject matter experts provides a complete solution for managing all aspects of data protection programs, including privacy compliance, staff management and vendor management. Founded in 2013, Sytorus operates globally in EMEA, Americas and Asia Pacific providing solutions to SMEs and Enterprise companies that go beyond demonstrating compliance for key stakeholders and regulators to delivering real business value, preventing data breaches, addressing regulatory risks and enhancing reputational management.

Theta Lake is a purpose-built risk and data privacy solution that automates detection of conduct, data leakage, regulatory, and data privacy risks in what is shared, shown, spoken, or written in modern communications. Natively integrated with leaders in unified communication (Cisco Webex, Microsoft Teams, RingCentral, Zoom, LogMeIn, Slack), Theta Lake’s multi-patent pending AI analyzes audio, video, collaboration chat, and other UC content, powers risk insights, and prioritizes risk review for comprehensive supervision coverage. With long-term SEC 17a-4 compliant archiving, legal hold, and robust eDiscovery capabilities, Theta Lake adds efficiency and scale to the compliance review and supervision process, driving down the cost of compliance. This means organizations can more confidently expand their external facing modern digital communication programs, such as video and collaboration chat, knowing that they can apply strong security, compliance, and supervision controls. The Theta Lake Compliance Suite is SOC 2, Type 2 compliant.

ThreatMark makes sure that the organizations can trust online users for every single action and transaction in the digital world through uniquely deep behavioural profiling that is impossible to fake and gives businesses superpowers over fraudsters and cybercriminals, while saving them money. ThreatMark is a rapidly growing cybersecurity company aiming to become a global leader in threat detection, smart authentication and fraud prevention. ThreatMark’s Anti-Fraud Suite can detect traditional as well as modern threats that jeopardize online banking and transaction systems. Its solution is a full-stack fraud detection system based on modern cognitive security user-centric approach. A combination of evidence-based cyber threat detection capabilities and behavioural profiling including behavioural biometrics supported by machine learning makes a perfect fit for combating the ever-changing threat landscape of modern banking applications.
PRODUCT NAME: Redflags™ Real Time Security Awareness
EXPECTED REVENUE IN 2020: Up to $250k

Founded in 2016 by the ex-global Heads of IT and InfoSec from the Cyber arm of BAE Systems (previously Detica), Think Cyber Security offers the next generation in Security Awareness. The company’s RedFlags™ software product applies behavioural and learning science theory, in a highly innovative approach, to deliver context-sensitive just-in-time guidance.

Redflags™ offers the toolkit financial services firms need to manage operational risk from cyber-attacks that target staff, meet compliance goals, keep content refreshed and relevant, while allowing staff to get on with their jobs to achieve business goals.

When 90% of cyber-attacks start with the human user, and technical controls can never be 100%, organisations need their staff to be the last line of defence. Sadly, organisations using traditional computer-based security awareness training face an uphill struggle to engage users to get the courses completed, and then find that content is quickly forgotten. The ISF found that less than 15% of staff changed their behaviours after traditional awareness training.

ThinkCyber solves the problems of engagement, retention and awareness, but most importantly moves beyond these to drive secure behaviours, reducing operational risk for its customers.

Redflags™ is a Microsoft .Net client application and an AWS hosted web content service. As the company increases its data sets it is applying Machine Learning techniques to further optimise delivery of awareness content.

The Redflags™ platform draws on Stanford Professor BJ Fogg’s theories on behaviour change as well as Thaler and Sunstein’s Nobel prize winning “Nudge” theory.

PRODUCT DESCRIPTION

ThinkCyber’s Redflags™ applies the theory and evidence of behavioural science to uniquely deliver real-time, context aware-guidance – at the point the user is at risk. Short, actionable and highly relevant content educates the user. Gentle and timely “nudges” strengthen behaviours, reduce risk and offer security teams visibility. Full metrics on and measurement of engagement offer unique insights. Based on clients’ usage statistics, average engagement levels with Redflags™ stand at 88%, resulting in halved click rates in just three months.

The security awareness market has been lacking in innovation. ThinkCyber takes a highly innovative new approach that is more in tune with the way corporate IT users work and behave. By delivering the right guidance, in the right way, at the right time, the Redflags™ toolkit changes user behaviour and drives out risk:

- **Redflags™ Security Stories** - Engage your employees with short but interesting and relevant tips and “security stories”
- **Redflags™ Alerts** - Send a real-time alert, in an active push format, to inform your users an incident is happening now
- **Redflags™ Phishing Threat Awareness** - Keep the threat of phishing front of mind and real, through highlighting engaging and interesting real examples on a regular basis
- **Redflags™ Behaviour Change Triggers** - Drive enduring behaviour change by gently “nudging” secure decisions at exactly the time you need to – at the point of risk
- **Measurement and Reporting** - Across all of the Redflags™ toolkit, your security awareness team gains visibility of engagement, dwell times on content, click throughs and answers to questions

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.
TOTAL FUNDING - £320,000

- The company was funded by friends and family, angel investors, as well as grants and awards such as Innovate UK
- ThinkCyber raised £260,000 from Angels Den at £2m pre-money valuation and £80,000 from Innovate UK grants
- The company is looking to raise £500,000 at the end of 2020 at £5-7.5m pre-money valuation to boost sales and marketing efforts

TRACTION/GROWTH

- ThinkCyber serves three live customers (including TescoBank and Cambridge University). Currently over 5,000 users are on the platform.
- ThinkCyber was shortlisted as finalist in the SC Awards 2020; was one of just two international (seven in total) finalists in the NYC Mayor’s office Cyber Moonshot Challenge; selected as finalists at the Duke of York’s Pitch@Palace 9.0; finalist in National Cyber Awards 2019
- The company was a member of the first cohort of the UK Government’s flagship cyber scale-up accelerator LORCA and is part of the latest TechNation Cyber cohort
- In Q1 2020 the company introduced NCSC-accredited Security Stories content for users
- The company is targeting a revenue of $20m+ by 2025 with employee count of 101-250
- ThinkCyber is actively looking to acquire investment banks, insurance companies and retail banks as clients

PARTNERSHIPS

- ThinkCyber is in the process of establishing partnerships with Big Four consultancies

MANAGEMENT BIO

Tim Ward - CEO & Founder
Tim Ward is CEO and Co-Founder of ThinkCyber. Tim has 20+ experience years in both consulting and corporate IT at Logica, PA Consulting, Sepura; and was Global Head of IT for the cyber division of BAE Systems (Detica). Tim studied Computer Science with AI at the University of Leeds, holds an MBA from the Open University and a Post Graduate Diploma in Entrepreneurship from Cambridge University.

Dr Mike Butler - CTO & Founder
Mike Butler is CTO and Co-Founder of ThinkCyber. Mike is an experienced IT and Information Security professional with 15+ years of experience across the security, technology and telecommunications industries including as Global Head of InfoSec at BAE Systems AI (Detica). Mike is a Certified Information Security Manager (CISM) and winner of a CISM worldwide achievement award. He holds a PhD in wireless communications and MSc in Communications Systems and Signal Processing.
Traditional Security Awareness is not enough

*Despite the world becoming more reliant on technology, humans still play a major role in cybersecurity.*

Traditional security awareness is not enough. Despite the world becoming more reliant on technology, humans still play a major role in cybersecurity.

The world is focused on battling online threats with new technology; however, good defence requires not only teaching employees to be more aware of their online behaviours, "but actually driving them to change their online behaviours to be more secure," according to Mike Butler, co-founder and CTO of Think Cyber Security.

Cyber criminals are constantly adapting and evolving their methods, finding new ways to get past systems and a business' security. When a company fixes one vulnerability, criminals are bound to uncover another pretty quickly. It's a constant battle, which is unlikely to disappear. A recent study from Infosys of 867 senior executives across 847 firms, revealed that the lack of security awareness of staff was their second biggest cybersecurity concern, with 76% of respondents stating their concern. Attacks from hackers was the only threat to receive more worry. Despite the clear need to improve staff knowledge in relation to digital threats, there are very few companies looking to change employee behaviours.

Companies solely relying on technology are bound to run into problems. Technology can become outdated pretty quickly, forcing companies to bolster their solutions or implement new tools. This costs a lot of money, and for a small business, that isn't always easy to get. However, encouraging secure behaviours and making employees more alert to risks can stop issues missed by technology and could potentially save cash. The problem is, there are not many solutions available in the market which help to improve staff behaviour and the ones which are available, are pretty limited, Butler said. This was one of driving factors that led to Butler and fellow co-founder Tim Ward to create Think Cyber at the end of 2016.

"Ultimately human risk is behaviour based, so if you can change behaviour, you can reduce that risk."

The world is focused on battling online threats with new technology; however, good defence requires not only teaching employees to be more aware of their online behaviours, "but actually driving them to change their online behaviours to be more secure," according to Mike Butler, co-founder and CTO of Think Cyber Security.

A company can have strong security and firewalls in place, but if employees are still unaware of risky behaviour, a business is still vulnerable. The risk humans pose to companies has not gone unnoticed. A survey from Infosys of 867 senior executives across 847 firms, revealed that the lack of security awareness of staff was their second biggest cybersecurity concern, with 76% of respondents stating their concern. Attacks from hackers was the only threat to receive more worry. Despite the clear need to improve staff knowledge in relation to digital threats, there are very few companies looking to change employee behaviours.

Think Cyber's Mike Butler said, “In practice, no solution and particularly no technology can be 100% effective all the time. Your people are the last line of defence and they're always going to be the ones who are there at the end when all the other defences have failed. It’s just part of any sensible kind of layered defence. You want to do a mix of things. You want to invest in some technology, but you also want to think about the human interaction and how you can influence your people to behave securely.”

There is clearly a need for companies to be pumping funds into their cyber defences; however, technology is not the only answer to stopping the criminals. A company's staff play a very important part in the security of a business, but they are often considered to be the weakest link. Multiple studies have found that as many as 90% of data breaches are caused by human error including by insurer Willis Towers Watson, and similarly, a report from Kaspersky Labs found in its study that 90% of cloud data breaches were due to attacks that target employees.

A company can have strong security and firewalls in place, but if employees are still unaware of risky behaviour, a business is still vulnerable. The risk humans pose to companies has not gone unnoticed. A survey from Infosys of 867 senior executives across 847 firms, revealed that the lack of security awareness of staff was their second biggest cybersecurity concern, with 76% of respondents stating their concern. Attacks from hackers was the only threat to receive more worry. Despite the clear need to improve staff knowledge in relation to digital threats, there are very few companies looking to change employee behaviours.

Think Cyber's Mike Butler said, “In practice, no solution and particularly no technology can be 100% effective all the time. Your people are the last line of defence and they're always going to be the ones who are there at the end when all the other defences have failed. It’s just part of any sensible kind of layered defence. You want to do a mix of things. You want to invest in some technology, but you also want to think about the human interaction and how you can influence your people to behave securely.”

There is clearly a need for companies to be pumping funds into their cyber defences; however, technology is not the only answer to stopping the criminals. A company's staff play a very important part in the security of a business, but they are often considered to be the weakest link. Multiple studies have found that as many as 90% of data breaches are caused by human error including by insurer Willis Towers Watson, and similarly, a report from Kaspersky Labs found in its study that 90% of cloud data breaches were due to attacks that target employees.

A company can have strong security and firewalls in place, but if employees are still unaware of risky behaviour, a business is still vulnerable. The risk humans pose to companies has not gone unnoticed. A survey from Infosys of 867 senior executives across 847 firms, revealed that the lack of security awareness of staff was their second biggest cybersecurity concern, with 76% of respondents stating their concern. Attacks from hackers was the only threat to receive more worry. Despite the clear need to improve staff knowledge in relation to digital threats, there are very few companies looking to change employee behaviours.

Think Cyber's Mike Butler said, “In practice, no solution and particularly no technology can be 100% effective all the time. Your people are the last line of defence and they're always going to be the ones who are there at the end when all the other defences have failed. It’s just part of any sensible kind of layered defence. You want to do a mix of things. You want to invest in some technology, but you also want to think about the human interaction and how you can influence your people to behave securely.”
He said, “we wanted to create a platform that we thought would actually make a difference to the security risk from the human side.” There were a few tools in the market which were trying to improve the human-risk within cybersecurity, but Butler felt, in his experience as a global head of infosec, they were not achieving much. “The first generation of security awareness solutions were primarily computer-based training systems, which a company would put their staff through annually, to meet compliance”, he said.

“A second generation, which is where the majority of the market is currently, are richer tools and simulations, such as phishing tests. These are better at showing people risks online but don’t change their behaviours across the breadth of security risks. These types of services also struggle to engage the customers to finish or remember what they are told.”

Next generation security awareness

Think Cyber hopes to be the third generation, offering technology which actually changes the behaviour of staff, so they actively avoid risks. Butler said, “Ultimately human risk is behaviour based, so if you can change behaviour, you can reduce that risk. Information security is about managing risk.”

Think Cyber aims to improve the cybersecurity of businesses by changing how their employees behave, making sure they avoid typical pitfalls that lead to data breaches. The technology offers real-time, context aware-guidance, which highlights areas of risk for users and helpfully “nudges” them to improve their interactions with business systems – at the point of risk. The platform, Redflags™ can also give real-time alerts on incidents happening, as well as, drip-feeding relevant tips and security stories.

The company doesn't bombard employees with information and complex explanations of conduct, as that would be counterproductive. Butler said, “if what you're asking them to do is too difficult, it just doesn't happen.” To ensure an employee does take note of what is being said, the information needs to be straightforward, give the user motivation for doing it and provide the advice at the right time. The aim of the platform isn't to make everyone experts in security, because at the end of the day “security isn't most people's primary job.” The trick is just making them more aware when they need to be.

"When we started the business and worked with academics on our Innovate UK funded research projects, the message that really resonated with us was, that just because we understand how all these attacks work and how to spot phishing, most people don't, and they probably shouldn't spend a lot of time thinking about it."

Working out how to engage with employees at the right time, but not being overbearing and annoying was one of the major challenges the company faced when building its platform and also the subject of their Innovate UK research projects. “The behavioural science was very clear – behaviour change requires timely prompts.” This was why the company chose to give employees helpful advice at the point of risk, when needed. The issue with swamping employees with advice is that they are likely to become annoyed and ignore it, or it risks interfering with their daily tasks. People need to have the ability to stop advice coming through and chose when to engage.

One of the other aspects Think Cyber took into account when building its solution, is to not overburden companies. Think Cyber looks at everything in terms of campaigns, so instead of trying to fix everything at once, which is often a disaster, it engages with clients and finds out what their biggest risks are, Butler stated. This way, a company can prioritise their training, whether its boosting awareness of phishing, lost laptops or removable technology like USBs. It also stops users being overwhelmed and trying to change all aspects of their behaviour at once.

Working with Tesco Bank

Tesco Bank turned to Think Cyber to improve the cyber awareness of their employees, having chosen to move away from traditional modular/compliance-based training.

“Tesco Bank saw our product as offering a completely new way to engage staff on security topics. During a pilot of 100 colleagues, 88% of staff said that they preferred the Redflags approach to learning compared to the more traditional method of delivering cyber awareness”, said Butler.

Tesco Bank and Think Cyber were introduced through a network of cyber security companies that Think Cyber had built through their involvement in the UK government’s cybersecurity accelerator programme LORCA. After an introduction to the Tesco Bank CISO, the founders of Think Cyber worked closely with security awareness practitioners which led to a pilot test of Think Cyber's Redflags™ product.

During the pilot test, Think Cyber engaged with the bank to explore specific kinds of behaviours and risks they were experiencing and the certain procedures they wanted their staff to follow. After the trial, the CyberTech company got positive feedback from Tesco Bank staff on the user acceptability of the solution.

The initial trial deployment at Tesco Bank not only helped boost security awareness for colleagues but also saved them time, as Butler notes “It removes inertia and stops the staff from having to take time out of their day to log into a computer-based training platform to do some kind of security awareness.”

Instead, the technology pushes advice messages out proactively, helping colleagues improve their behaviours, whilst having a limited impact on their ability to deliver their day jobs.

Following the success of the pilot Think Cyber have now commenced full deployment. Tesco Bank have expressed interest in more advanced behavioural nudges provided by the Redflags™ toolkit to further drive secure behaviours. Think Cyber very much hopes that the partnership can extend further, and the two businesses can work on more initiatives in the future.●
ThreatQuotient’s mission is to improve the efficiency and effectiveness of security operations with a platform that accelerates and simplifies investigations and collaboration within and across teams and tools. Integrating an organization’s existing processes and technologies into a unified workspace, ThreatQuotient’s solutions reduce noise, highlight top priority threats and automate processes to provide greater focus and decision support while maximizing limited resources. ThreatQuotient’s threat-centric approach supports multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability management, and also serves as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA.

Torsion is an information security and data governance software provider, created in 2014, to solve the problem of sprawling access to files and folders by integrating with collaboration systems such as Sharepoint, Teams and Office 365, to monitor and control access. Torsion works with collaboration tools to automatically monitor and detect any inappropriate access, out of date folders and permissions, or the movement of files. If anything doesn't look quite right it will promptly alert a business user associated with the file and shut down any potential breaches. Other than that, it can run seamlessly in the background until and unless it is required. Owners or creators of files and folders can certify and revoke access themselves, taking the responsibility away from the IT function.

Trust Exchange is a “network effect” software platform that allows companies to connect, collect, and collaborate to improve the quality and timeliness of mission critical business information. The Trust Exchange platform has been utilized by organizations of all sizes in many industries including banking, healthcare, pharma, public safety and retail. The platform employs advanced network effect mechanics to solve the exponential scale problems encountered by traditional providers. Information is gathered from a variety of sources including the Internet, news outlets, public data feeds and the companies themselves. From this information Trust Exchange garners actionable intelligence regarding a company’s performance and reputation.
Tu Identidad was founded by a group of former senior bankers, lawyers, and IT specialists who decided to change a paradigm in the process to complete the Know Your Customer (KYC) for a person and the Know Your Business (KYB) for a company without friction and at a significantly lower cost. On one hand, for KYC, the company's tool allows the individual to upload their official ID, proof of address, email, and biometrics in its mobile device. On the other hand, for the KYB, it allows its enterprise customers to upload deeds of incorporation, powers of attorney, tax IDs, proof of address, and stakeholder’s identifications. In both cases, Tu Identidad performs all validations in seconds and completes the background checks to guarantee that everything is correct and corresponds to the information recorded in the sources such as state information repositories. Both regulated and non-regulated customers are using the company's solution.

TypingDNA is a behavioral biometrics company, protecting online users based on how they type on their keyboards. TypingDNA has developed technology that expands the limited biometric authentication options without requiring specialized sensors or advanced hardware. TypingDNA provides a commercial authentication API suitable for securing login, enforcing reset passwords, and online biometric authentication. The product can be integrated into any corporate or consumer app, including SaaS, web apps, online learning, and payment providers, to enable two-factor authentication. Organizations around the world use the company's AI-based typing biometrics technology to improve online security through passive and frictionless authentication. TypingDNA's API is implemented by companies in various industries such as Financial and Banking Institutions as well as cybersecurity companies and educational organizations.

Veriato is a global leader in AI-powered insider threat security and employee productivity monitoring solutions. Veriato provides next-gen, metrics-driven monitoring for employees whether they're in the office or working remotely. In the quickly evolving work-from-home business model, brought about by the pandemic, it's critical that management has visibility to determine who's thriving and who is struggling in their remote work environment. Veriato's insider threat intelligence platform provides proactive threat hunting capabilities, by integrating User Behaviour Analytics, User Activity Monitoring, and Employee Risk Scoring. Veriato enables companies to reduce risk by changing their security posture from reactive threat containment to proactive threat hunting and threat avoidance. Veriato is used by thousands of financial institutions, corporations, and government entities in over 100 countries, to reduce risk, protect against insider threats and monitor the productivity of remote employees.
VIPRE is a leading provider of cyber security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats and data leakage. With over twenty years of industry expertise, VIPRE is one of the world's largest threat intelligence clouds, delivering protection against and training on today's most aggressive online threats. Its award-winning portfolio includes comprehensive endpoint, email and web security, along with security awareness training and SafeSend, a unique Outlook plugin helping to prevent accidental data loss.

WALLIX Group is a European cybersecurity solutions vendor specialist in privileged account governance in response to recent regulatory changes and the cyber security threats affecting all companies today. WALLIX's solutions help users defend against cyber attacks, theft and data leaks linked to stolen credentials, and abused privileges. It is the first market solution to have been awarded first-level security certification (CSPN) by France's National Cybersecurity Agency (ANSSI) and thus meets all the criteria for regulatory compliance. Listed on the Euronext under ALLIX and distributed by a network of more than 170 resellers and trained and accredited integrators, WALLIX accompanies more than 1,000 companies in securing their digital future.

Wandera provides a unified, cloud-delivered security solution that secures the new way of working. The service was designed to protect remote workers and devices from cyber threats, to enforce acceptable usage policies, and to enable zero trust access to all applications. Wandera operates a globally distributed Security Cloud that is optimized for the modern enterprise, where fewer applications are hosted on-premises and more users are working remotely. Unified security capabilities include threat protection, content filtering, and zero-trust network access. The Wandera Security Cloud enables threat defense, secure network connectivity, and robust data policies through a single cloud security platform.
xorlab’s defense system understands people’s communication relationships and behaviours. xorlab uses that understanding to proactively protect organizations against spear phishing, zero-hour malware attacks, accidental data loss, data exfiltration and non-compliance. With hundreds of signals gathered from every email, xorlab provides a level of visibility and control that allows security teams to efficiently automate threat analysis, prioritization and remediation, and realize a positive ROI on email. One mid-size private bank, for example, estimates that it can reduce its security operation efforts by up to 360k per year with xorlab, which is equivalent to 2 FTE.

xorlab was founded by ambitious security and software engineers with the mission to redefine corporate cyber defence. The company started with email because that’s where the majority of companies suffer the most with 90% of all security breaches involving email at some point during the attack.

ZeroFOX, the innovator of social media and digital security, protects modern organizations from dynamic security, brand and physical risks across social, mobile, web and collaboration platforms. Using targeted data collection and artificial intelligence-based analysis, ZeroFOX protects modern organizations from targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. Recognized as a Leader in Digital Risk Monitoring by Forrester, the patented ZeroFOX SaaS platform processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, HipChat, Instagram, Reddit, Pastebin, Tumblr, YouTube, VK, mobile app stores, the deep & dark web, domains and more.
ABOUT US

This summary was produced by FinTech Global. FinTech Global is a specialist data and research provider. FinTech Global offers the most comprehensive data, the most valuable insights and the most powerful analytical tools available for the global FinTech industry.

We work with market leaders in the FinTech industry – investors, advisors, innovative companies and financial institutions – and enable them to get the essential intelligence they need to make superior business decisions.

We cover every industry development, every investment, every exit and profile of every company in every FinTech sector around the world.

For more information, please visit:

For more information contact info@fintech.global