Rockstone Research

September 22, 2023

Report #1

Cybersecurity

The Swiss Fortress of Digital Security

GUARDIANS OF THE CYBERSPACE:
HOW TO DEFEND AGAINST CYBERCRIME AND SAFEGUARD PRIVACY WITHOUT BIG TECH GIANTS

In recent years, the digital world has witnessed a dramatic and alarming surge in cyberattacks and privacy abuses. The proliferation of these attacks and data breaches has sent shockwaves through governments, businesses and individuals alike. As the global population becomes increasingly interconnected and reliant on digital technology, the need for robust security products has never been more critical. Governments, businesses and individuals must take proactive measures to mitigate the growing threat of cybercrime and embrace the growing need for privacy. By recognizing the evolving nature of cyberthreats and taking preemptive steps to defend against them, we can hope to secure our digital future and protect the foundations of our interconnected world.

In an era where the digital realm is an integral part of our daily lives, the importance of cybersecurity and privacy cannot be overstated. With the growing complexity of cyberthreats and the ever-expanding attack surface, companies selling cybersecurity products find themselves in a position of significant relevance and opportunity.

According to McKinsey, the global addressable market for cybersecurity products stands at a staggering $2 trillion USD, yet vendors have only tapped into a mere 10% of this expansive market. Consequently, this vast gap presents an unprecedented opportunity for companies to expand their portfolios, foster innovation, and seize the immense growth potential within the cybersecurity industry.

Sekur Private Data Ltd. stands out among other cybersecurity and privacy companies through its exceptional product portfolio and a steadily expanding clientele. With innovative solutions tailored to address evolving digital threats and privacy concerns, Sekur has established a reputation for excellence in safeguarding sensitive information, positioning the company and its shareholders for promising growth prospects in the ever-evolving landscape of cybersecurity.

Company Details

Sekur Private Data

Sekur Private Data Ltd.
Suite 5600 –100 King Street West
Toronto, ON, M5X 1C9 Canada
Phone: +1 416 644 8690
Email: corporate@sekurprivatedata.com
www.sekurprivatedata.com

Listing Date: July 22, 2019

ISIN: CA81607F1036

Shares Issued & Outstanding: 119,632,941

Chart Canada (CSE)

Canadian Symbol (CSE): SKUR
Current Price: $0.20 CAD (09/21/2023)
Market Capitalization: $24 Million CAD

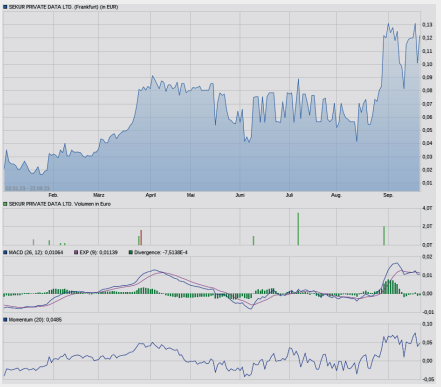


Chart Germany (Frankfurt)

German Symbol / WKN: GDT0/ A3DKJ0
Current Price: €0.122 (09/21/2023)
Market Capitalization: €15 Million EUR

All $-figures in CAD unless otherwise stated.

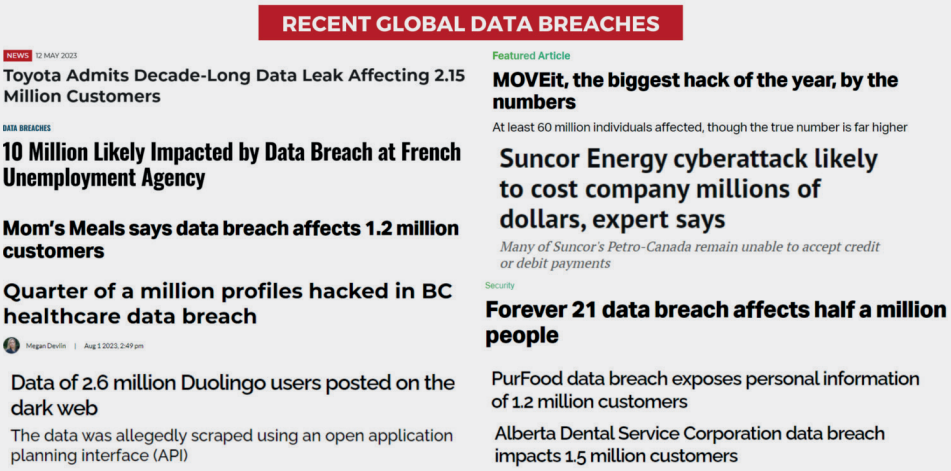
The cybersecurity industry has witnessed a wave of mergers and acquisitions (M&A) in recent years. Established technology companies and private equity firms are recognizing the immense value of security and privacy solutions and are actively investing in or acquiring companies active in this market. This influx of capital and expertise further validates the bright future of this thriving industry.

The first and perhaps most compelling reason for the bright future of cybersecurity companies is the escalating cyberthreat landscape. Cyberattacks have become more sophisticated, diverse and frequent than ever before. Hackers continuously develop new techniques to breach networks, steal data and disrupt operations. As long as cyberthreats persist and evolve, there will be an ongoing demand for innovative cybersecurity and privacy solutions.

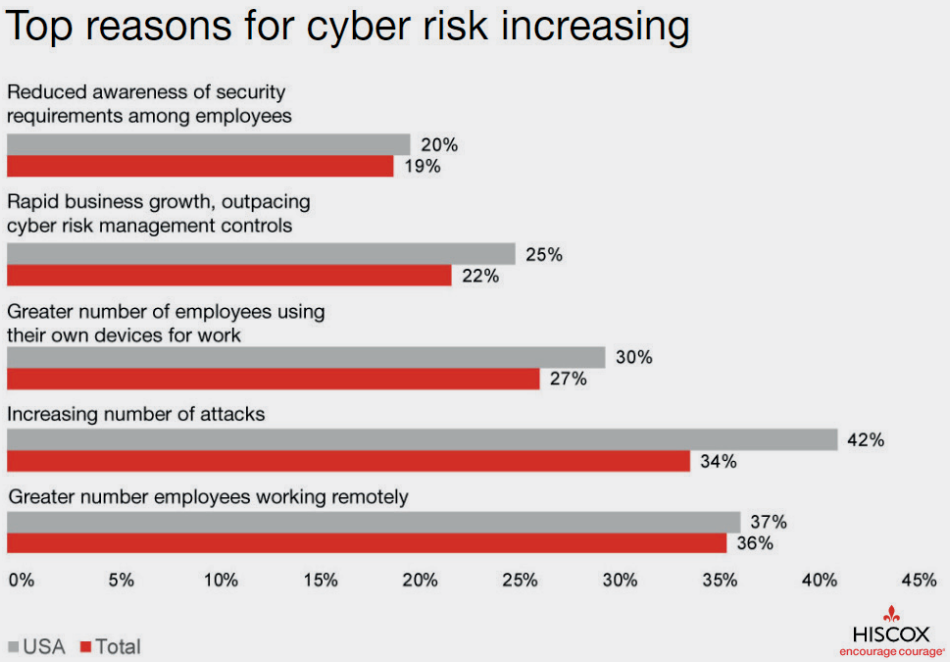
Individuals are increasingly aware of the importance of cybersecurity in their personal and professional lives. This heightened awareness drives demand for cybersecurity products. As governments and enterprises become more security-conscious, companies selling cybersecurity products will find a growing market for their offerings.

With ongoing innovation, adaptation to emerging threats, and a commitment to protecting digital ecosystems, the cybersecurity industry will continue to play a vital role in protecting our interconnected world.

"Security and cybersecurity incidents are costly, with losses increasing every year. For example, in 2022 the FBI Internet Crime Report showed losses in excess of $10 billion due to internet crime, up from $3.5 billion in 2019. Although these losses are staggering, they are almost certainly the tip of the iceberg. They only reflect losses that are reported to the FBI, and many victims – whether individuals or businesses – choose not to file complaints or report losses. Moreover, the FBI data does not include certain types of losses, such as ransomware payments. In addition to direct costs, victims often suffer indirect costs, such as revenue losses due to downtime, reputation or brand damage, and loss of trade secrets or intellectual property. These can easily exceed the level of direct costs. In light of these growing threats, it is no wonder that organizations in all industries continually rank security as a top priority for new spending." (Source: Avasant, 2023)



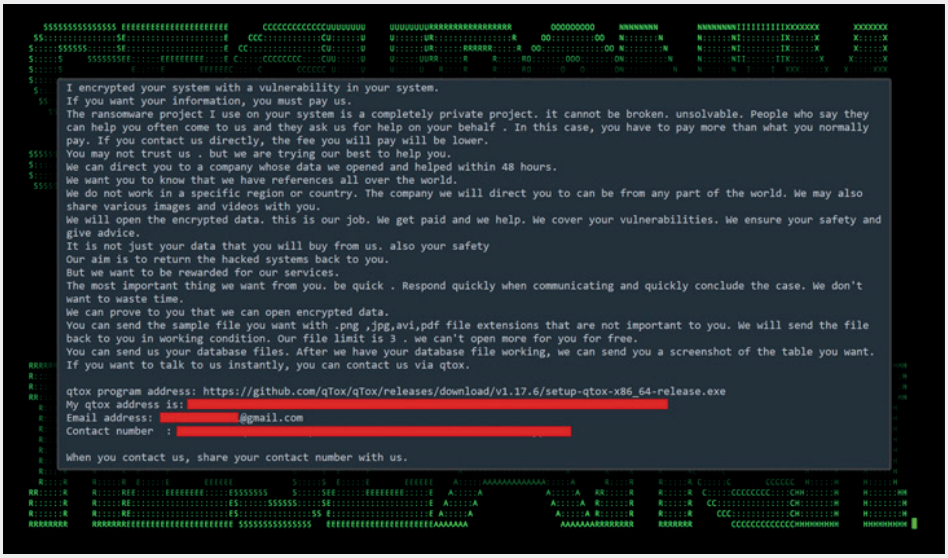
Above compilation of recent global data breaches from the article "Sekur: Safeguarding your digital world" (September 15, 2023). Most recently, two Las Vegas hotels fell victim to cyberattacks, shattering a public perception that casino security requires ad "Ocean 11"-level effort to defeat it. Both MGM Resorts and Caesars Entertainment have acknowledged recent attacks, leading to a range of disruptions including the inaccessibility of doors at the company's casinos and hotels, non-functional slot and ATM machines, malfunctioning elevators, and lengthy guest check-in delays. Caesars already paid roughly half of a $30 million USD ransom that hackers demanded after a cyberattack late this summer.



A 2022-survey from Hiscox revealed that US businesses are more concerned about cyberattacks (46%), than the pandemic (43%), or skills shortages (38%): The number of cyber attacks is on the rise in the US, with **almost half of all US businesses having suffered a cyber attack** in the past 12 months.

Based on research conducted in late 2022 by Enterprise Strategy Group, 65% of organizations plan to increase cybersecurity spending in 2023 with 40% of survey respondents saying that improving cybersecurity is the most important justification for IT investments.

"No matter the industry, small and medium sized enterprises (SMEs) are major targets for cyber-attacks. There is a misconception that large businesses are a large target, but the reality is that smaller organizations often do not have the proper security protocols in place leaving them more susceptible to attacks.... As of right now, small and medium sized enterprises spend only 10% of their annual IT budget on cybersecurity companies for services and solutions... this allocation does not match the rapid increase in cyber-attacks... It's clear that there's an anticipated increase in cybersecurity spending in 2023 and the years to follow. In our 2023 Cybersecurity Predictions, we noted that there's a growing in cyber attacks with a 15% increase from 2021 to 2022. In 2023, that's expected to spike. More sophisticated cyber attacks driven by Artificial Intelligence or geo-phishing will push companies to spend more." (Source: BIO-key, 2023)



If you encounter a message resembling the one displayed above on your computer screen, it indicates that your system has been compromised by a cyberattack, placing you or your organization in a precarious situation. Regrettably, countless individuals and businesses find themselves with limited alternatives and may feel compelled to engage with cybercriminals and fulfill their ransom demands. (Image from the article "Threat Actors Targeting Microsoft SQL Servers to Deploy FreeWorld Ransomware", September 2023)

"Cybercrime is a serious threat that needs to be taken care of... Over the past few years, businesses worldwide have witnessed a significant shift in priorities, with cyberattacks being one of the major concerns. Experts estimated that the total cost of cybercrime would reach $8 trillion (with a T, not a B) this year. No doubt, cybersecurity is top of mind for industry leaders. Moreover, cybercriminals are also becoming increasingly sophisticated, making mitigating those threats difficult. In fact, this is one of the main reasons why more and more businesses are falling prey to it. As a result, it's important for businesses to increase their investments in cybersecurity measures... The United States is the largest geographic region for cybersecurity spending in 2023... The United States is closely followed by Western Europe, which is currently the second-largest region regarding cybersecurity spending... Moreover, the Asia/Pacific region also saw a significant investment in cybersecurity this year... As of 2022, businesses around the world allocated 9.9% of their IT budgets toward cybersecurity... Moreover, a small business, on average, allocates around 5% of its IT budget toward cybersecurity. It highlights that SMBs still haven't understood the importance of cybersecurity... Around 47% of small businesses have zero budget for cybersecurity... It indicates that they are more vulnerable to cyberattacks and breaches... It is estimated that small and medium-sized businesses (SMBs) will spend $29.8 billion on managed security services in 2025. However, they were forecasted to spend $90 billion on cybersecurity. That's $33 billion up from $57 billion in 2020... A significant portion of organizations worldwide (73%, to be precise) plan to increase their cybersecurity spending in 2023... Among all the large enterprises, a mere 7% dare to take risks and invest less than $250,000 per year in cybersecurity... Meanwhile, 43% of large organizations find themselves in a middle ground, investing between $250,000 and $999,999 in cybersecurity annually... Google has announced its commitment to strengthen cybersecurity by investing over $10 billion within five years..." (Source, 2023)

Global cybersecurity spending will reach $219 billion USD this year and grow to nearly $300 billion USD in the next 3 years, according to the latest forecast from IDC Data and Analytics. This year's investments in cybersecurity hardware, software and services are expected to jump 12.1% compared to 2022 and outperform growth in overall IT spending. "Almost all industries and company size segments will see low double-digit growth through 2026, driven by the expansion of cloud and container deployments, the need to secure remote access to resources, and the compliance requirements of privacy and data protection legislation," said Serena Da Rold, Associate Research Director at IDC. Analysts expect the cybersecurity market to continue its run of sustained growth and that the biggest spenders will include organizations in banking, manufacturing, professional servies and governments, accounting for more than one-third of all cybersecurity spending this year. Software, the fastest-growing segment, will capture 47% of all spending this year, followed by services (39%) and hardware (13%), according to IDC.

Companies selling cybersecurity products are poised for a bright future driven by the ever-growing need for robust cybersecurity measures. As cyberthreats become more sophisticated and pervasive, organizations and individuals alike will increasingly turn to cybersecurity solutions to safeguard their digital assets and privacy.

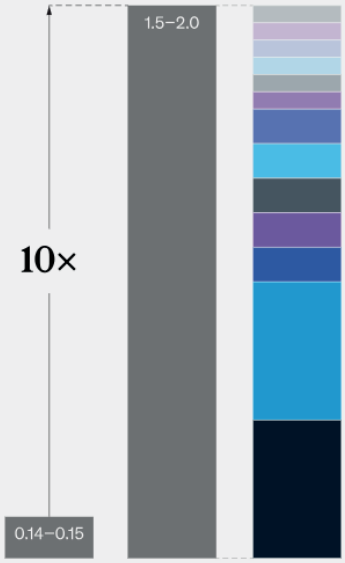
Excerpts from "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers" (McKinsey & Company, 2022):

"Cyberattacks are proliferating, causing trillions of dollars of damage every year. The cybersecurity industry has a chance to step up and seize the opportunity. As the digital economy grows, digital crime grows with it. Soaring numbers of online and mobile interactions are creating millions of attack opportunities. Many lead to data breaches that threaten both people and businesses. At the current rate of growth, damage from cyberattacks will amount to about $10.5 trillion annually by 2025 – a 300 percent increase from 2015 levels.

"In the face of this cyber onslaught, organizations around the world spent around $150 billion in 2021 on cybersecurity, growing by 12.4 percent annually. However, set against the scale of the problem, even this "security awakening" is probably insufficient. A survey of 4,000 midsized companies suggests that threat volumes will almost double from 2021 to 2022. According to the survey, nearly 80 percent of the observed threat groups operating in 2021, and more than 40 percent of the observed malware, had never been seen previously. These dynamics point to significant potential in an evolving market. Currently available commercial solutions do not fully meet customer demands... As a result, the gap today between the $150 billion vended market and a fully addressable market is huge. At approximately 10 percent penetration of security solutions today, the total opportunity amounts to a staggering $1.5 trillion to $2.0 trillion addressable market... This does not imply the market will reach such a size anytime soon (current growth rate is 12.4 percent annually off a base of approximately $150 billion in 2021), but rather that such a massive delta requires providers and investors to "unlock" more impact with customers by better meeting the needs of underserved segments, continuously improving technology, and reducing complexity – and the current buyer climate may pose a unique moment in time for innovation in the cybersecurity industry."

The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, $ trillion

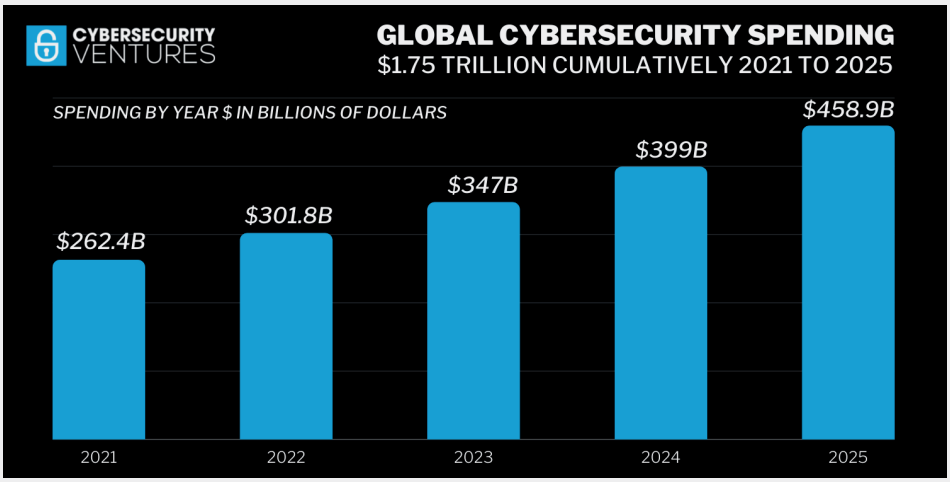


Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

McKinsey & Company

Huge gap to fill: The vended market represents the commercial aspect of the cybersecurity industry, where organizations and individuals can purchase a wide range of cybersecurity solutions and services to protect against cyberthreats. **The growth prospects for vendors in the cybersecurity market are exceptionally promising**, driven by the ever-expanding threat landscape, increasing digitalization across industries, stringent regulatory requirements, and the growing awareness of cybersecurity's critical role in safeguarding data, privacy, and digital assets.



"The imperative to protect increasingly digitized businesses, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion cumulatively for the five-year period from 2021 to 2025, according to Cybersecurity Ventures... With cybercrime predicted to cost the world $10.5 trillion annually by 2025, up from $3 trillion a decade ago and $6 trillion in 2021, commensurate growth in cybersecurity expenditure will be crucial to keep up... **Cybersecurity is the only line item that theoretically has no spending limit... There is a budget before a company suffers a cyberattack or a series of them, and then there's the actual spend that takes place afterwards. What business or consumer isn't going to do and spend whatever it takes to recover from being hacked?** Markets aren't sized by unlimited budgets or the extraordinary lengths that companies are willing to go to if push comes to shove, but it is one of the dynamics in the burgeoning cybersecurity space...While all other tech sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime..." (Source)

Users often enjoy the benefits of convenience, reliability, and scalability when using services from mega cloud providers and big tech companies. However, there are several problems and disadvantages associated with relying heavily on these companies. Users should be aware of the potential disadvantages associated with their dominance in the tech space:

Privacy Concerns

Mega cloud providers and big tech companies typically collect vast amounts of user data for various purposes, including targeted advertising. This raises significant privacy concerns as users might be uncomfortable with the level of surveillance and data tracking these companies engage in.

Data Security Risks

While these big tech companies invest heavily in security measures, they are still attractive targets for cyberattacks. A security breach can result in the exposure of sensitive user information, leading to identity theft, fraud, and other security-related issues. In recent years, large data hacks, mass virus infections and mass technical glitches have occurred, not only due to lack of security with open-source coding.

Service Outages

Even the largest cloud providers and tech companies are not immune to service outages. Users relying heavily on these services can experience disruptions in their daily operations when these companies encounter technical issues or downtime.

Limited Customer Support

Due to their scale, mega cloud providers and big tech companies may struggle to provide personalized customer support to all their users. This can result in frustration for users who encounter problems or need assistance.

Regulatory Scrutiny

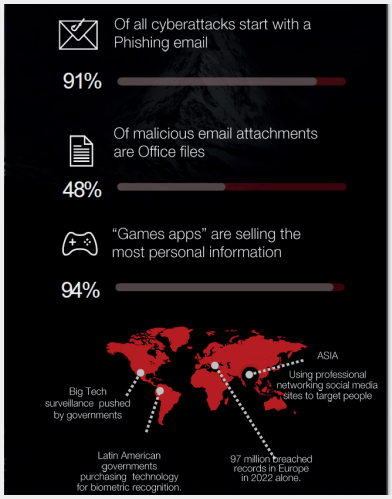
Mega cloud providers and big tech companies often face regulatory scrutiny and antitrust investigations. This can lead to legal challenges, fines, and changes in business practices that may impact the user experience.

Privacy & Security LANDSCAPE

100 B
Connections producing data expected in 2025.

80%
From the data collected from the apps has nothing to do with its functionality.

Sale
Data sale to third parties followed by influence voting manipulation are the most unacceptable uses of personal data collection.



1,557
Is the amount of demographic data gathered on average for each person.

83%
Use unsecured Social Messaging for their business communication.

1/3
More than one-third of cyberattacks during the first six months of 2022 were BEC (business email compromise) attacks.

Sekur Private Data Ltd. is a cybersecurity and internet privacy provider of Swiss hosted solutions for secure communications and secure data management.
The company distributes a suite of secure cloud-based storage, disaster recovery, document management, encrypted e-mails, and secure communication tools. Sekur Private Data Ltd. sells its products through its websites www.sekur.com and www.sekursuite.com, and approved distributors, and telecommunications companies worldwide. Sekur Private Data Ltd. serves consumers, businesses and governments worldwide. Sekur's corporate/investor website including news-releases: www.sekurprivatedata.com

Large data hacks, mass virus infections, mass technical glitches (44 million MS Office 365 with same username and password), open-source coding lack of security.

What WE DO

We protect data and communications for consumers, businesses, and governments.

SekurMail®
Send encrypted and private emails, to any ISP with added security features.

SekurMessenger®
Send encrypted chats to Sekur and non Sekur users with self-destruct messages.

Sekur®
Email and messaging combo plan for consumers.

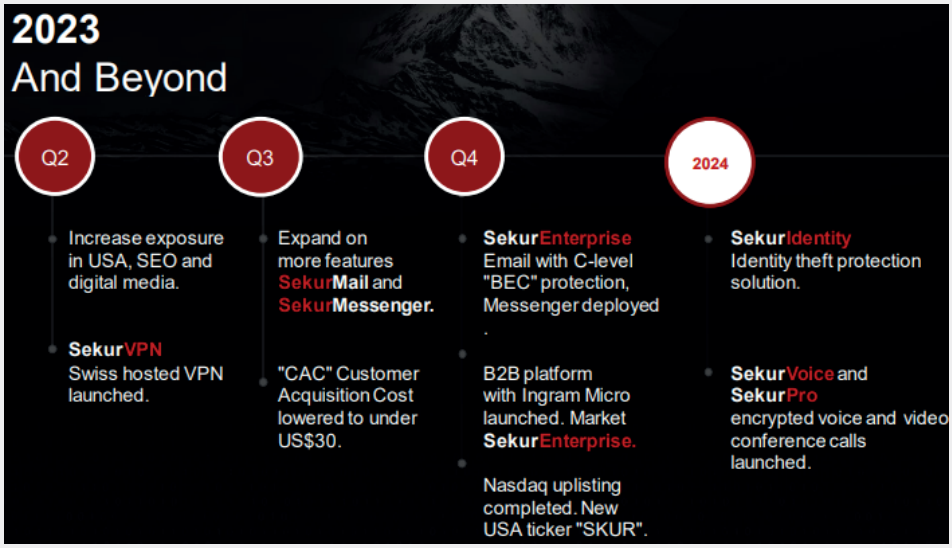
SekurPro®
Private video conferencing, encrypted calls, email and messaging for enterprise. (Launching Q3 2023)

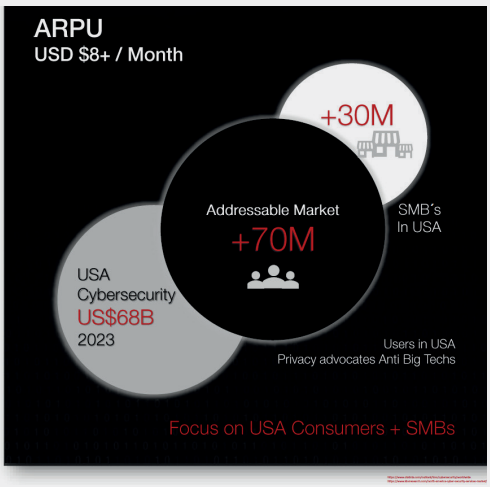
SekurVPN®
Swiss based secure VPN connection.

SekurVoice®
Communicate privately in a secure environment.
(Launching Q3 2023)

SekurSuite®
Private and secure document management, file share, password manager, email into one platform.

SekurIdentity®
Keep your personal information safe from theft.
(launching 2024)





Sekur Private Data Ltd. has been established to mitigate the disadvantages of big tech companies and mega cloud providers. Sekur protects data and communications for individuals, businesses and governments. Sekur offers privacy and security combined – with communication solutions end-to-end encrypted and without social exposure, location mining and big tech data mining intrusion. This protects users' privacy with no meta-data or cache in their devices. All conversations are locked in Sekur's VirtualVault® and Helix® technology. **In contrast to many other providers, Sekur owns 100% of the infrastructur (no Amazon Web Services, Google Cloud or Microsoft Azure).** All data traffic is hosted in Switzerland using closed source proprietary technology, independent platform away from big tech, military grade encryption and benefiting from Swiss Privacy Laws. All user data is protected by the Swiss Federal Data Protection Act (FADP) and the Swiss Federal Data Protection Ordinance, which offers some of the strongest privacy protection in the world for both individuals and entities. Sekur's state-of-the-art computer and storage servers are located in ISO certified, Swiss bank approved data centres with all the security and precautions you would expect from data centres in Switzerland serving some of the biggest banks and organizations in the world. Sekur's network is protected by an enterprise-class firewall and include SSL encryption to keep your data safe.

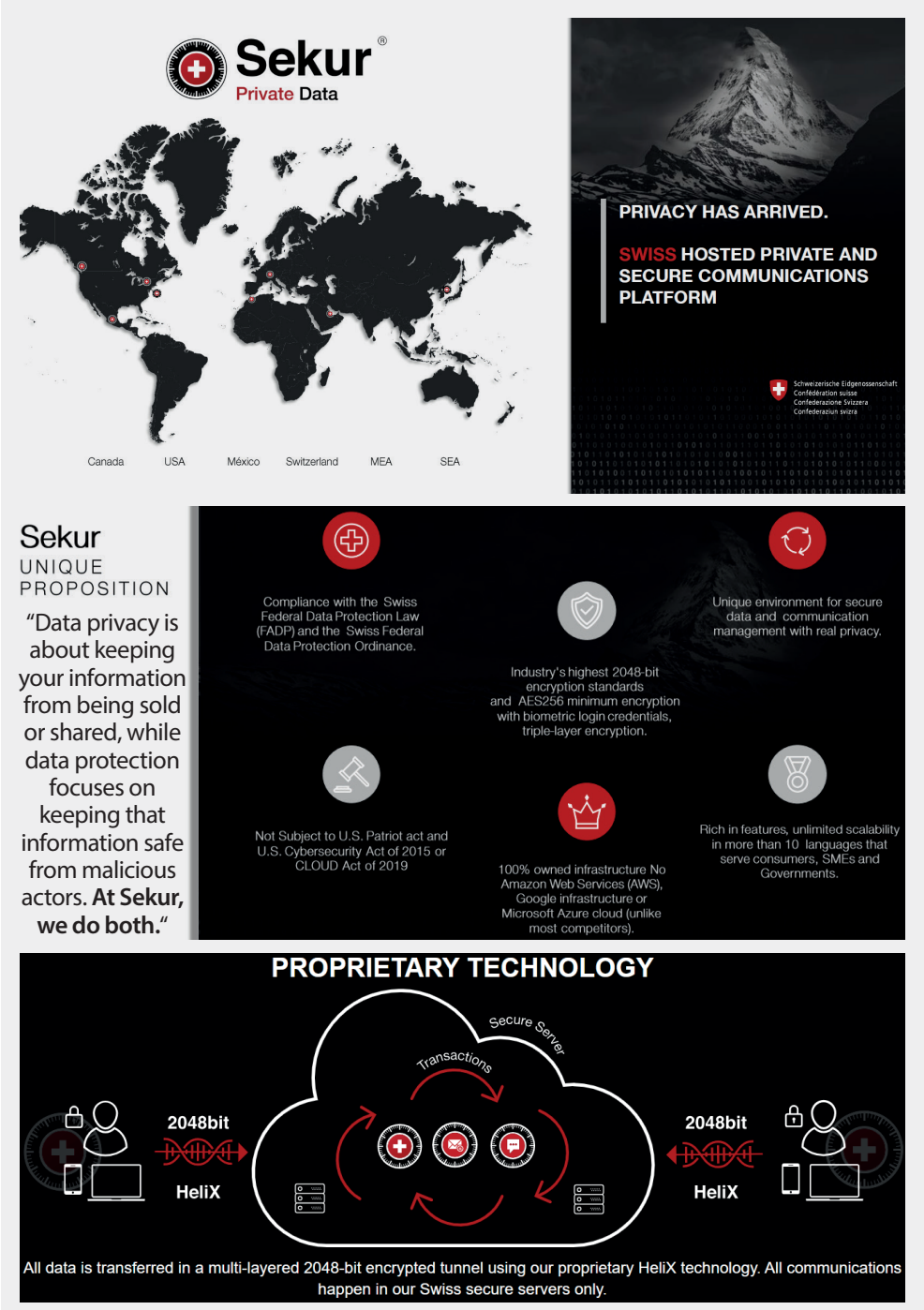
WHY SWITZERLAND

Switzerland has the world's strictest data privacy laws, the FADP Law. The purpose of the FADP is to protect the privacy, interests and fundamental rights of data subjects. At the end of September 2020, after legislative process of almost four years, both chambers of the Swiss Parliament approved the revised Federal Act on Data Protection (revised FADP). The revised FADP includes numerous adaptations to the EU's General Data Protection Regulation (GDPR), but retains its own basic concept and also deviates from the GDPR in various aspects. Examples of important changes in the revised FADP are: much stricter sanctions, extended duties to provide information, the duty to create a record of data processing activities, and the expansion of the data subject's rights.

Switzerland has a stable, prosperous and high-tech economy and enjoys great wealth, being ranked as one of the wealthiest countries in the world in per capita in multiple rankings. The World Economic Forum's Global Competitiveness Report currently ranks Switzerland's economy as one of the most competitive in the world. Switzerland is also home to several large multinational corporations and NGOs, including World Health Organization and the United Nations.

Strict Data Privacy Laws

Switzerland has the strictest privacy laws in the world. All user data is protected by the Swiss Federal Data Protection Act (FADP) and the Swiss Federal Data Protection Ordinance which offers some of the strongest privacy protection in the world for both individuals and entities.



Neutrality

Switzerland has a long history of neutrality – It has not been in war since 1815 and has remained neutral in any international political affairs.

Politically Independent

Switzerland remains independent in any government or political matter, is not a member of the EU and European Economic Area. Furthermore, it is listed among the top five countries in the "Economic Freedom" index.

Long-Lasting Stability

Switzerland has an unemployment rate below 5% and has the highest wealth per adult in the world. It is rated one of the top 5 most efficient economies in the world.

Low Network Latency

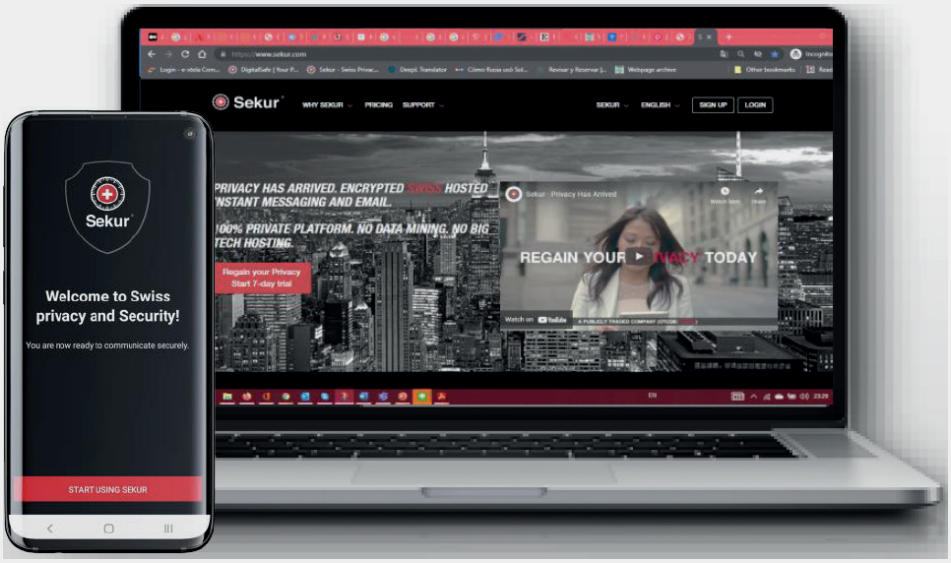
Switzerland's location is beneficial for any operation, due to the short distances within Europe and Switzerland being situated between the Asia/Middle East and North America.

Low Environmental Risks

Switzerland isn't prone to environmental risks, such as hurricanes, tsunamis, volcanos, earthquakes, forest fires or floods. In 2016, Switzerland made history when it became the first country to vote for implementing a green economy. New initiatives included a goal to reach OneEarth sustainability until 2050 by achieving "100% renewable energy, protection and restoration of 50% of the world's lands and oceans, and a transition to regenerative, carbon-negative agriculture".

THE OPPORTUNITY

"Cybersecurity has grown to represent a significant portion of a business's budget. In fact, Gartner estimates that over the next 5 years companies will spend $1.75 trillion on cybersecurity. This is a considerable increase for an industry that was only worth $3.5 billion in 2004... From 2020 to 2021, cybersecurity spending increased exponentially... In 2021 there was a considerable increase in spending to secure devices outside of company premises. It is predicted that by the end of 2024, mobile security spending will exceed $7.2 billion... Smartphones have become an integral part of life, therefore including mobile security in the corporate cybersecurity policy is now critical for most organizations. In fact, the lack of mobile security is predicted to be one of the fastest-growing threats in cybersecurity, because of the potential vulnerabilities it brings... As the technological landscape continues to evolve, and governmental regulations become more stringent, businesses are steadily growing their cybersecurity budget." (Source, 2022)



"79% of users in the Americas are concerned about their data privacy, 41% of U.S. users delete cookies frequently, and 30% of consumers have downloaded adblockers." (Source)

Sekur keeps your internet traffic private and secure: Privacy is the new security!

Privacy: Protects your personal information and communications from being accessed by unauthorized parties, such as hackers, advertisers, or rogue agencies.
Security: Encryption and other security measures to prevent your messages from being intercepted, modified, or tampered with, in transit or at rest.
Online Freedom: Empowers you to access information and communicate with anyone in the world, regardless of geographical or political barriers.

ONE OF THE PROBLEMS

Last month in August, US regulators announced a combined $549 million USD in penalties against 15 financial firms for "widerspread and longstanding failures" to maintain electronic records of employee communications, including al lowing the use of unsupervised side-channels such as messaging apps WhatsApp and Signal to discuss company business. The SEC (Securities and Exchange Commission) and the CFTC (Commodity Futures Trading Commission) disclosed charges and fines against Wells Fargo, Société Générale, BNP Paribas, Bank of Montreal, BMO Capital Markets, and other firms for using unapproved communication methods. **Last year in September, the SEC fined 16 financial firms a combined $1.1 billion USD** over failing to maintain and preserve electronic communications, including Barclays, Bank of America, Citigroup, Credit Suisse, Goldman Sachs, Morgan Stanley and UBS.

THE SOLUTION

Sekur has launched a compelling product portfolio for users (individuals, businesses and governments) to protect their data in order to maximize security and to comply with regulators.

Last year, the SekurMessenger was launched with América Móvil's Telcel mobile operator in Mexico, aiming to replace non-secure and non-private messaging applications not only for businesses but also for the mass market: "Recent data breaches in messaging applications and in particular in the WhatsApp application have created a certain urgency for businesses and data privacy advocates to protect their communications form cyber-attacks and identity theft via mobile and desktop devices... Telcel is the largest mobile operator in Mexico, with over 75 million mobile subscribers. América Móvil is the 7th largest telecom operator in the world with over 277 million mobile subscribers in over 20 countries throughout Latin America and Europe. Its shares trade in the New York Stock Exchange under ticker AMX... Once sales gain momentum in Mexico, the launch is planned to expand to other countries where America Movil operates through its Claro brand, such as Colombia, Peru and other Latin American countries, as the business grows over the coming years."

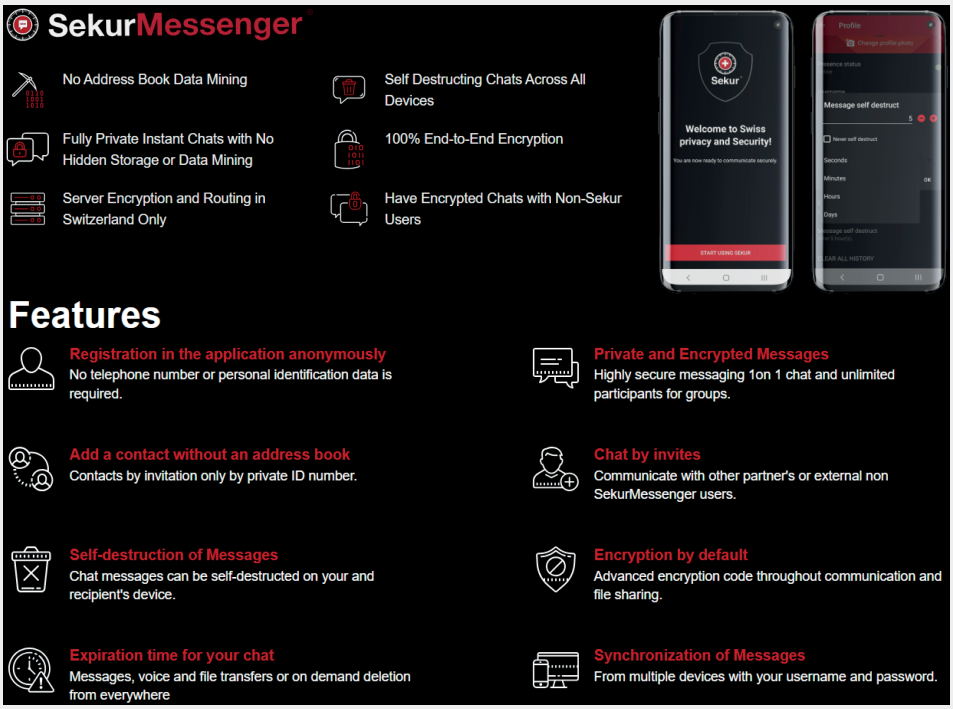
At Sekur, all the data, including the user authentication information, is transmitted over the internet and stored on its own servers in encrypted form. All connections to Sekur's servers, for all users, are protected with 2048bit SSL encryption. Passwords are encrypted with bcrypt algorithm. Locking the account after a predefined number of failed login attempts prevents brute force password guessing. Timing based password guessing is not possible due to nature of bcrypt encryption. When current session expires, browser window is redirected to login page in case computer is left unattended. Notes are stored on the server encrypted with

AES-256 encryption and encryption key is stored on a separate server, not accessible from the internet. For ultimate security and privacy, users can choose to have their own password be used to encrypt the data. In this case, it is not possible to decrypt user' private data without knowing the password. Not even Sekur personnel can decrypt the data. However, that also means user's password cannot be reset and data will forever be lost if password is lost.

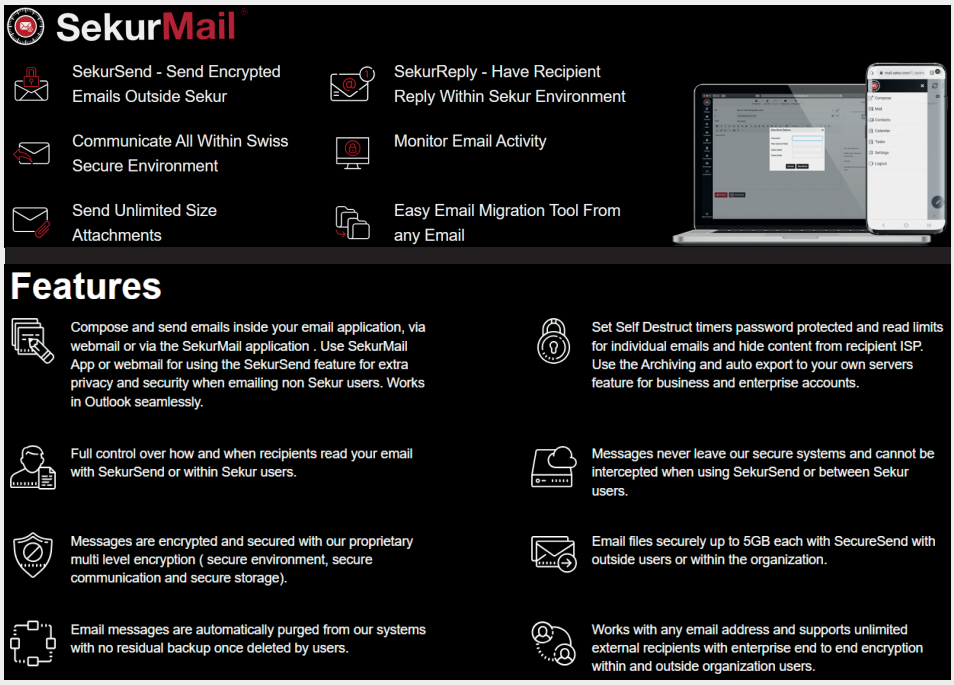
Sekur stores data in a world-class data warehouse located in Switzerland, renowned for its exacting standards and quality control. Sekur has the physical environment necessary to keep the servers up and running 24 hours a day, seven days a week, even in case of power shortages and major natural disasters. These world-class facilities are custom designed with raised floors, HVAC temperature control systems with separate cooling zones and seismically braced racks. These offer the widest range of physical security features, including state-of-the-art smoke detection and fire suppression systems, motion sensors, 24/7 secured access, video camera surveillance and security breach alarms.

In compliance with the **Payment Card Industry Data Security Standard** (PCI DSS), Sekur has a 24/7 third-party monitoring of its network infrastructure to check for known application and service vulnerabilities. The company also has a yearly on-site audit lasting multiple days where every aspect of the system is audited: from software development to hardware deployment, from personnel policies to passwords management. There are more than 200 criteria that Sekur has to meet in order to keep its compliance level.

Sekur prides itself in storing users' information in a politically and economically stable and neutral country. Switzerland does not abide by the USA PATRIOT ACT. This ensures that your information is safe from competing predators or agencies and entities with personal motives who would pry into your privacy and steal your data without your knowledge. Sekur has no servers based in the USA. All of Sekur's servers are based in Switzerland where the company runs its Swiss online backup digital vaults platform.



"Recent data breaches in messaging applications have created a certain urgency for businesses and data privacy advocates to protect their communications from cyber-attacks and identity theft via mobile and desktop devices." (Source)



SekurMessenger

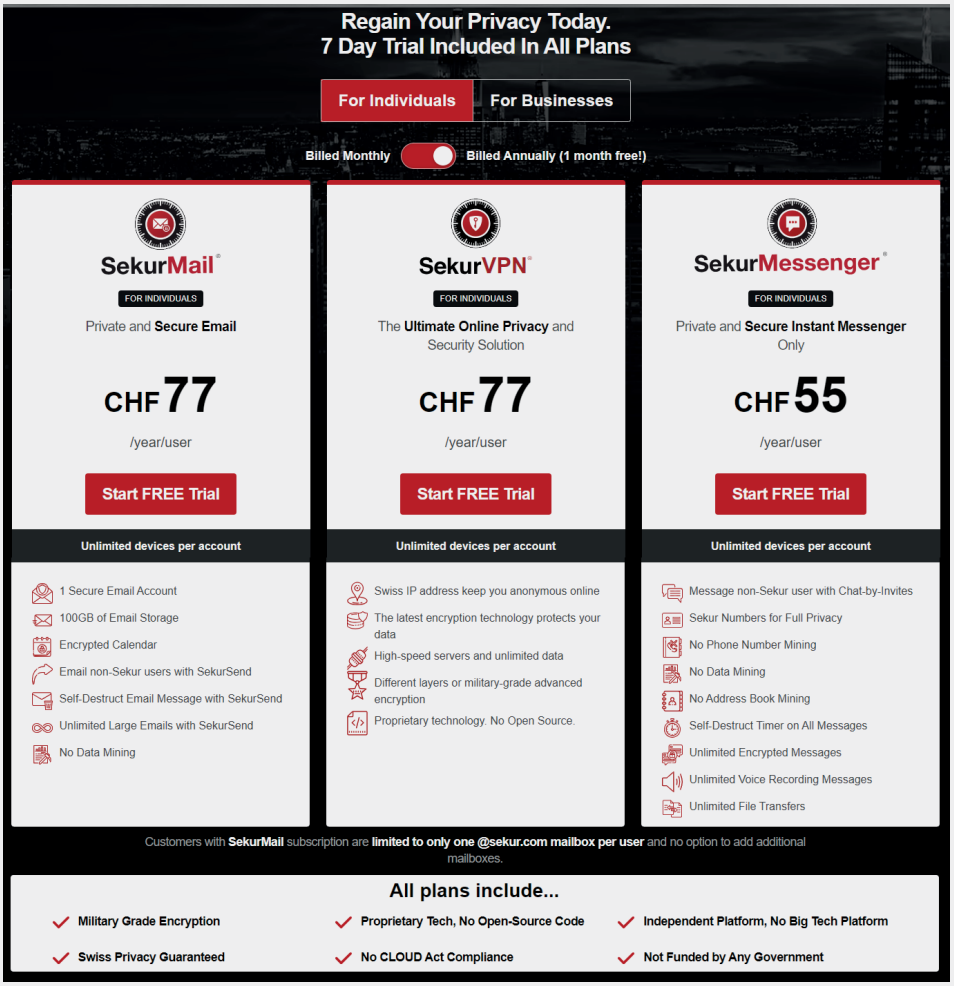
Encrypted messaging application designed for organizations that need to protect their flow of information and secure their communications between devices, with customers and partners. SekurMessenger is not just any ordinary messaging app. It is designed to provide military-grade encryption and privacy by design ensuring that only the sender and intended recipient can read the messages exchanged. It also employs multi-vault encryption layers, segregating users' data in virtual vaults and encrypting it with individual keys. This means that your data is safe even if one layer of encryption is compromised. Sekur does not collect or

store metadata of any kind, or share information with third parties, and guarantees privacy using its own servers. SekurMessenger works for both licensed users of the application and external users who do not have the app. SekurMessenger provides fully private instant chats with no hidden storage or data mining. This means that your conversations are kept completely private and cannot be accessed by anyone else. SekurMessenger uses end-to-end encryption to ensure that your messages are secure and cannot be intercepted by anyone else. One of the key features of SekurMessenger is that it is built on proprietary code without open source involved. This means that the code used to build SekurMessenger is not publicly available and cannot be modified by anyone else. This ensures that the service is secure and cannot be compromised by anyone.

SekurMail

For anyone who cares about online privacy and security, SekurMail offers an encrypted email service that is not only private by default, but a safe and powerful tool to communicate with everyone, within Sekur or outside of Sekur. SekurMail turns your email into a secure and private communications platform with the highest security and privacy standards using end-to-end encryption for messages between SekurMail users and with external users. Sekur's backend email servers provide the most secure environment for your digital communications. On top of the multilayer encryption, Sekur uses proprietary technologies, Virtual Vault and Helix, to encrypt all data stored on disks and all data that is transmitted across the network.Sekur executes all transmissions and exchange of data within its secure server platform environment. When a user accesses one of Sekur's services, the user connects first to the company's secure platform in its data center, and then the transaction happens within its own servers' environment. This eliminates the risk of data being intercepted from the sender's device, i.e. data cannot be read or accessed. All data in Sekur's storage systems is encrypted. This eliminates "BEC" (Business Email Compromise) and email phishing incidents.

According to a survey published on Forbes, 66% use a VPN to help protect personal data, 80% use a VPN for increased security and 33% use a VPN to mask their internet activity: "VPNs, or virtual private networks, have become indispensable tools in today's internet-driven world... Used to secure and encrypt your IP address on public networks, VPNs protect your online activity from tracking and exploitation by internet predators. Initially largely used by a subset of niche businesses, VPN use has increased in popularity in recent years. Adoption by businesses and everyday internet users alike increases every day. Protecting our online privacy and habits has become more important than ever..."



Since launching SekurVPN in April 2023 and customizing 'a-la-carte' bundles for consumers and businesses, approximately 50% of all customers have been buying bundles and 32% of customers purchased SekurVPN in the bundle or on its own. (Source)

SekurVPN

SekurVPN creates a secure, encrypted connection between your device and the internet, and lets you access the web safely and privately by routing your connection through a server and hiding your online actions. All of the data you send and receive is hidden from prying eyes. This includes your Internet Service Provider (ISP), potential hackers, and even government surveillance agencies. It also can help you bypass geographics restrictions and censorship. SekurVPN software client on the user's device encrypts the device's connection request sent to the associated VPN server. Once the connection is established, requests for information are encrypted and go from user's device to the VPN server. The VPN server decrypts the request and uses the internet to obtain the information. Once obtained, the VPN server then encrypts and returns the information, which is decrypted by the client software. Sekur uses its own VPN servers located in Switzerland. You can enjoy lightning-fast connections speeds anywhere in the world with Sekur's extremely simple app.

SekurSuite

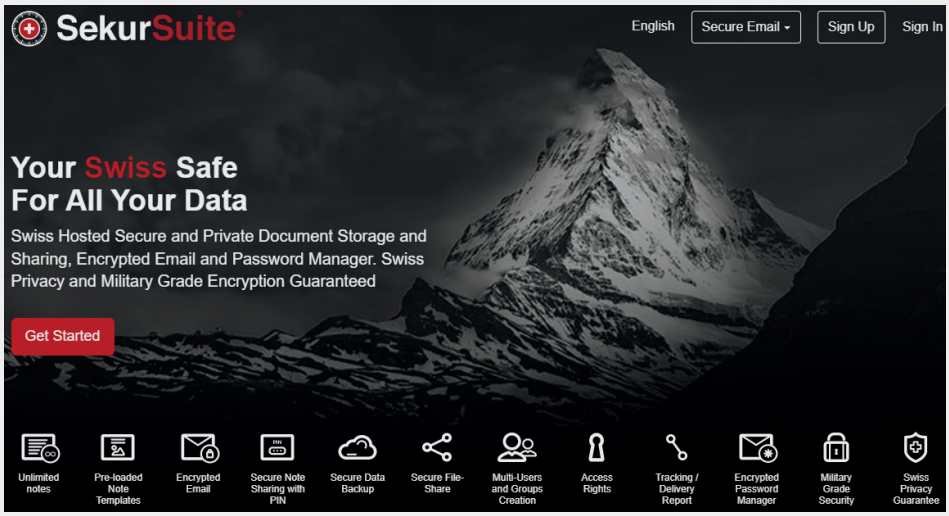
SekurSuite is Swiss-hosted secure and private document storage and sharing with encrypted email and password manager. Swiss privacy and military grade encryption guaranteed!

PRIVACY

Sekur's cybersecurity and privacy solutions are all hosted in Switzerland, protecting users' data from any outside data intrusion requests.

No USA PATRIOT Act, No CLOUD Act, No Cybersecurity Information Sharing Act

By having its own proprietary technology, Sekur is not subject to intrusive laws such as the CLOUD Act. This ensures that your information is safe from data predators and malicious actors using your personal data for commercial or criminal means without your knowledge. All communications data is stored in Switzerland. Self-destruct messages delete all messages from devices and servers in Switzerland to bare metal.



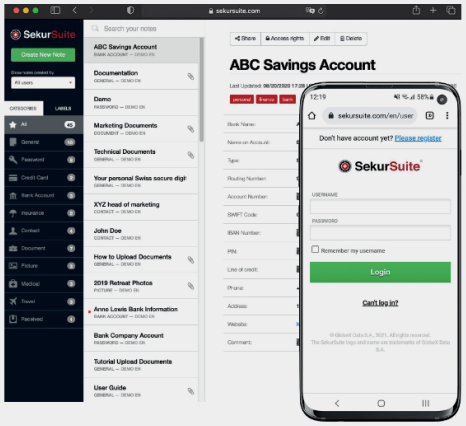
Secure And Private Document Storage And Sharing In Switzerland

Securely Manage and Create Encrypted Passwords, Store and Share Notes and Documents of all types, with the protection of Swiss Privacy Laws using Military Grade Encryption. Your data is fully encrypted in SekurSuite and scanned for viruses as you back it up.

Think of us as Your Swiss Safe in the cloud!

Get Started

Available on the App Store | Android app on Google Play



Pricing packages for Personal and Business use

Solo	Team	SME	Enterprise
100GB of storage 1 user	500GB of storage 5 users	2500GB of storage 25 users	Pricing available upon request.
$50 / month $550 / year if paid annually	$250 / month $2,750 / year if paid annually	$1,250 / month $13,750 / year if paid annually	
Includes all standard features	Includes all standard features **plus** Swiss Hosted Company Domain Secure Email Multi-Users and Groups Creation Access Rights	Includes all standard features **plus** Swiss Hosted Company Domain Secure Email Multi-Users and Groups Creation Access Rights	Includes all standard features **plus** Swiss Hosted Company Domain Secure Email Multi-Users and Groups Creation Access Rights
Get Started	Get Started	Get Started	Contact us

All packages include:

- Unlimited Notes
- Swiss Hosted Secure Email
- Secure Note Sharing with PIN
- Pre-loaded Note Templates
- Military Grade Security
- Encrypted Password Manager
- Secure File-share
- Swiss Privacy Guarantee
- Tracking/Delivery Report
- Secure Data Backup

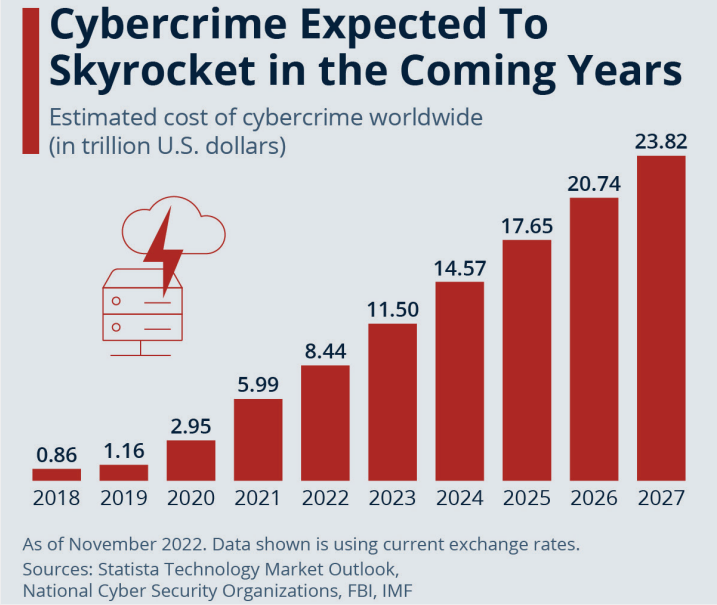
Your data stays private and secure in Switzerland!

Our state-of-the-art computer and storage servers are located in ISO certified, Swiss bank approved data centres with all the security and precautions you would expect from data centres in Switzerland serving some of the biggest banks and organizations in the world. Our network is protected by an enterprise-class firewall and all SekurSuite plans include SSL encryption to keep your data safe.

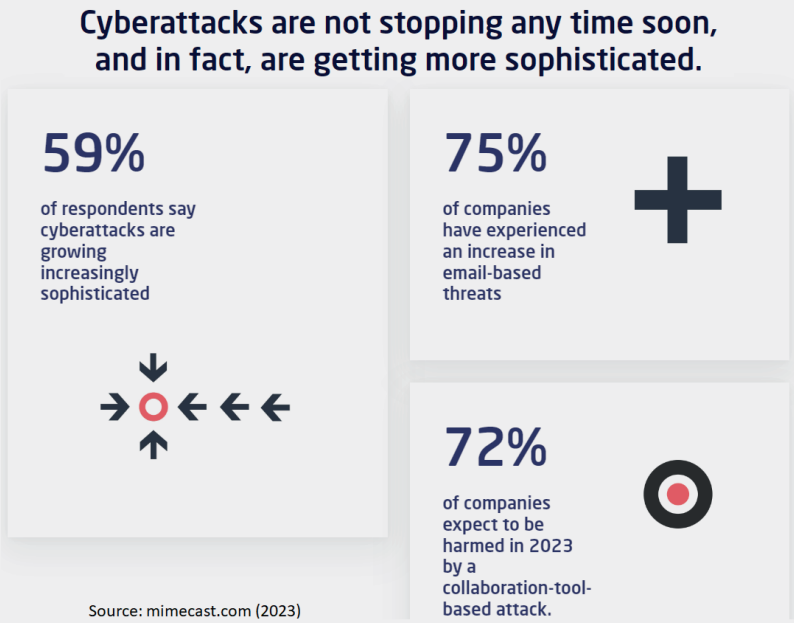
LATEST NEWS

On August 2, 2023, Sekur announced the signing of Reseller Agreement with Digital Smart Solution Sarl ("DSS"), an IT services consulting company based in Casablanca, Morocco. DSS intends to approach the first and third largest telecom operators in Morocco, along with several major banking groups and government organizations. This strategic move is prompted by the significant rise in cyberattacks on mobile phones and Business Email Compromise (BEC) attacks in the region. The targeted telecoms collectively boast a mobile subscriber base exceeding 20 million users, with businesses accounting for over 15% of this subscriber base.

Alain Ghiai, CEO of Sekur Private Data, said: "We [are] excited to expand into the Kingdom of Morocco as many international companies have their Africa headquarters in Morocco. According to market research, approximately 90% of African businesses are operating without cybersecurity protocols in place, making them vulnerable to cyber threats, such as hacking, phishing, and malware attacks. The economic consequences of digital insecurity are already substantial. This is where Sekur comes in, to ensure private and secure communications and prevent Business Email Compromise ("BEC") attacks with our SekurSend feature on SekurMail, and to offer a private and secure alternative to data mined messaging applications, with our SekurMessenger and our Chat by Invite unique privacy function. We will also offer our SekurVPN as there is a growing market demand for VPNs. Our prime directive is to provide private and secure communications for everyone, and, as we are not connected to any Big Tech cloud platform, we offer a truly independent, private and secure means of communications without any data mining, through our proprietary technology and our secure servers based in Switzerland. We look forward to offering true data privacy to all Moroccan businesses and government organizations, and protect their intellectual property, and their privacy, from data miners, malicious hackers and rogue agents of foreign powers."



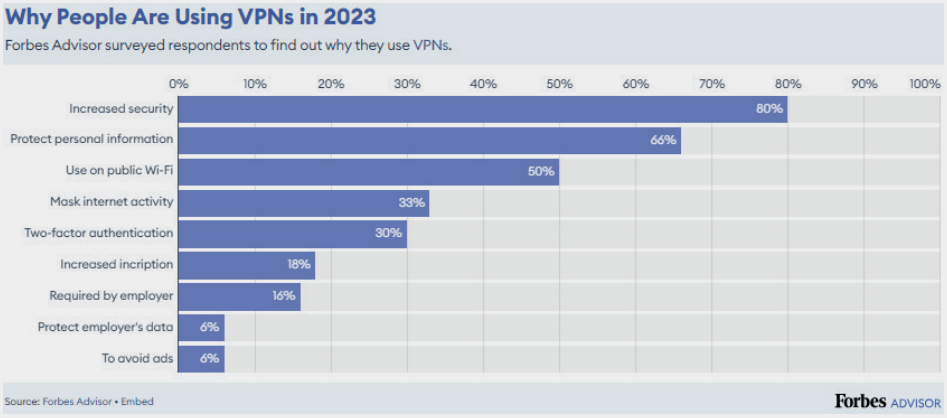
"**According to the BR and the Tagesschau, there were cyber attacks on three IT service providers of the ITZ Bund, which is responsible for 200 federal and state authorities, by the end of April.** The attacks "very likely" leaked large amounts of e-mail communication and probably also personal data. Now the picture is clear as to why exactly the external service providers Materna, Init and adesso were attacked. To the BR or the Tagesschau there is probably a message from the Federal Information Technology Center (ITZ Bund) from the end of April with a warning about the attacks. It describes the attacks, their scope and the loot. The cyber thieves are said to have captured a large number of e-mails. Personal data, telephone numbers and offices are probably also included. Information about current projects and sometimes entire email histories also ended up with the attackers through attached documents." (Source, 2023)



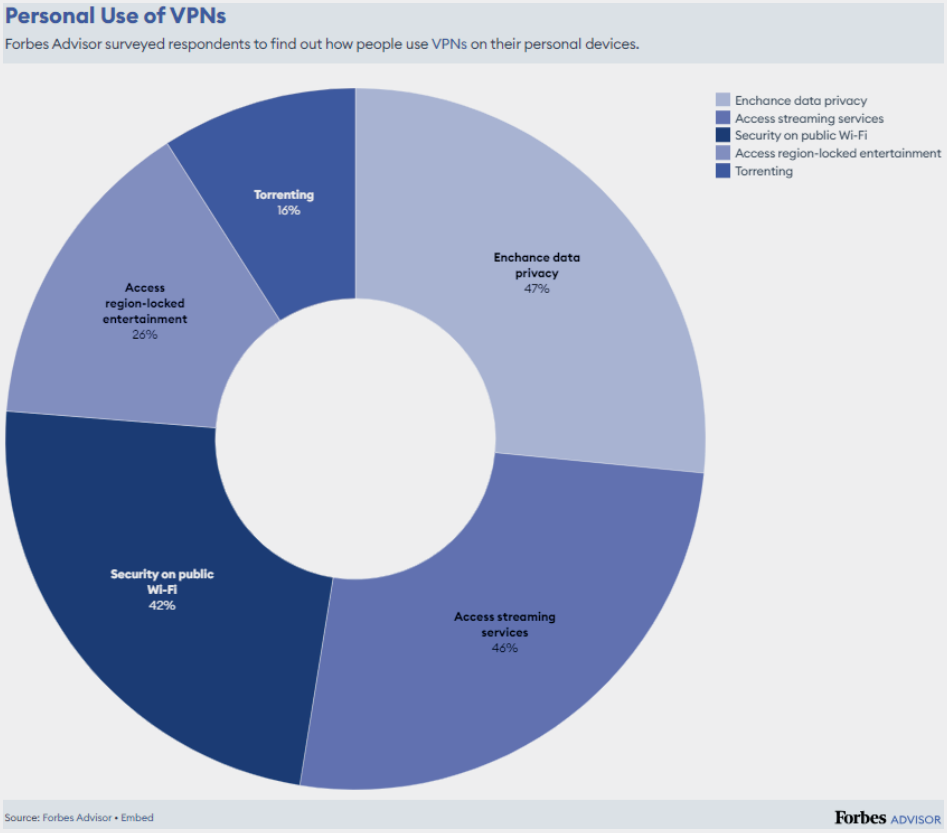
"**As humans become more dependent on digital technology to live, work, and play, the risk of cyberattacks has increased substantially.** According to a study conducted by Comparitech, more than 71 million people are victims of cybercrime each year. Further, the number of cyberattacks has continued to increase year over year... Cybercrime rates have increased by 300% since the beginning of the COVID-19 pandemic. Organizations lose more than $17,000 every minute due to phishing. 17% of all data breaches involve malware infections. More than 700 million ransomware attack attempts occurred in 2021. Criminal hacking causes more than 45% of sensitive data leaks. Malware attacks cost companies an average of $2.6 million." (Source, 2023)

On September 20, 2023, Sekur announced that new subscriber sign-ups for its Swiss hosted privacy VPN, SekurVPN, has increased by over 100% month-over-month: "Sekur is registering a surge in signups for its VPN solution, as cyberattacks become more and more commonplace and digital identity theft is rampant. The Company expects exponential growth in the coming months and years for its SekurVPN solution and is adding enterprise features and other upgrades... Sekur plans to launch a full-scale campaign for its VPN solution sometime in late October or early November as it is preparing the final touches on its digital ads. There are other plans as well with resellers to launch SekurVPN later this year. Additionally, Sekur is pleased to report that website traffic for Sekur.com has increased by approximately 100% in the last month and by 650% in the last two weeks, and is registering a conversion rate of 5% on its organic search site visits. The Company believes that in the coming 12 months, its web traffic will be such that its customer acquisition cost could drop down dramatically as the organic search increases exponentially. As Sekur increases SMB marketing to businesses, spending per customer is expected to increase as SMBs have multiple users in their business. Spending per user is also expected to increase as the Company launches its SekurVoice voice calls encrypted solutions and SekurPRO, its video conferencing and complete private and secure communications suite, in Q1 2024."

On June 14, 2023, Sekur announced that, since it has started optimization and SEO in January 2023, its Customer Acquisition Cost "CAC" was lowered to US$32 per Customer in June, month-to-date, while Life Time Value metrics "LTV" per customer has increased again. In January 2023, The Company has embarked on a reduction of its Customer Acquisition Cost ("CAC") in order to focus on targeted digital marketing, such as Google Ads and META campaigns, and optimization of its Sekur website. Previously, the Company announced that is was targeting a CAC of US$75 or lower by the end of 2023, and a CAC of US$60 or lower for 2024 from direct marketing, not counting B2B partnerships, which would



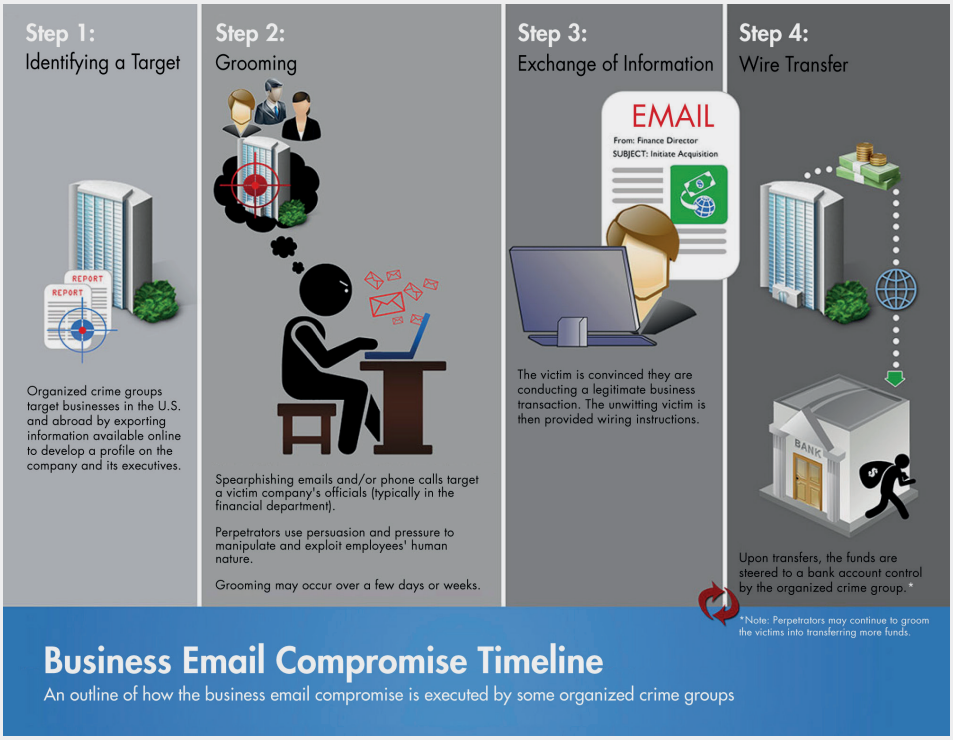
"VPNs aren't only popular in the United States [as shown in above and below figures]. While two-thirds of surveyed internet users within the United States reported using a VPN at some point in their lives, about a third of the rest of the world's population has also adopted VPN use... **33% of All Internet Users Use a VPN:** This number only continues to climb. Studies suggest that by 2027, the value of the VPN marketplace will climb to $107.5 billion... Paid VPNs, in general, tend to offer more features and better security than free ones... **The Average Cost for a VPN Is $6.50 per Month:** The cost of a VPN ranges from free to about $13 per month." (Source: Forbes, 2023).



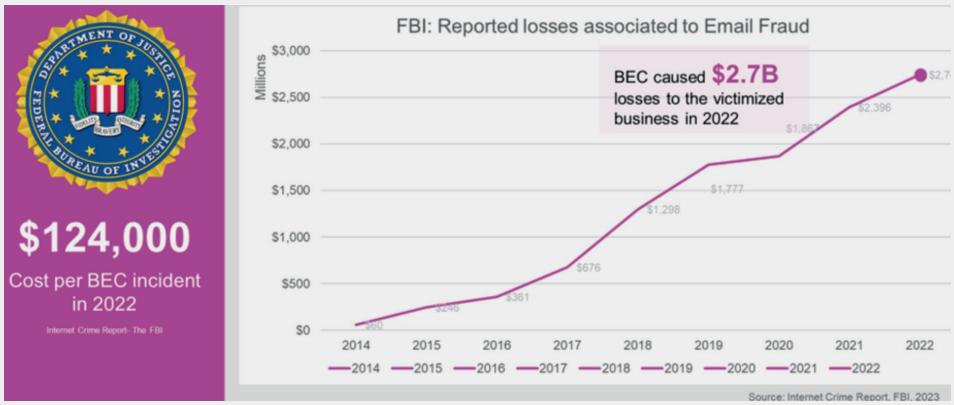
"SekurVPN uses its own proprietary infrastructure and does not use any Hyperscaler or Big Tech hosting providers, unlike most other VPNs. It offers Swiss IPs only, and this guarantees that it is using only SekurVPN's own servers and routing. Other VPNs offer 100s of locations and are using Big Tech providers, compromising users' privacy. SekurVPN never monitors users' activity and never shares any data with third party service providers. By being a pure VPN, without bundled outside services, such as anti-virus, and ad-blockers, SekurVPN keeps users' information private without sharing their data with third party service providers. With SekurVPN, users do not register their phone number on the App or the web, rendering users invisible from hackers or snoopers. No phone number to register, anonymous Swiss IPs only, no data mining or traffic sharing with anyone... SekurVPN is extremely easy to setup and deploy." (Source)

lower the CAC overall. The Company is targeting consumers and SMBs at this time and is improving its website content in order to inform SMBs and visitors on the benefits of using the Sekur privacy and security communications platform. **Alain Ghiai, CEO of Sekur Private Data, said:** "We are very happy to be well ahead of our plans for our CAC reduction. The Company has a specific plan to tweak the CAC for the next quarter and increase the digital marketing budget gradually from August 2023 onward. Right now, if we count the money we are spending on digital marketing, and the organic growth from the SEO efforts, we are tracking a CAC of between US$30 to US$35. This is an amazing achievement in such a short time, and I want to congratulate our entire marketing team for their progress so far. A CAC of US$75 or lower is very attractive as we can scale and grow exponentially with the proper budgets put in place, and a CAC of under US$50 is extraordinary for us, so if we are under any of these numbers, we will do very well..."

On June 6, 2023, Sekur announced that it is on track to launch its Sekur Enterprise Solutions by the end of July 2023. The Company's offering for SMBs, large enterprises and government organizations, will include full users' management, message and email archiving features and admin dashboard for mass on-boarding and management of employees. Sekur Enterprise Solutions will also include a new email feature, to be launched and announced in the coming weeks, allowing large organizations to host C level emails on Sekur's private and secure network offering the Company's SekurSend feature, while keeping the rest of their employees on their existing email hosting company, eliminating costly email migrations, while protecting C level communications to the highest level. This split-level email system also allows C level employees to maintain the same company domain name as the rest of the employees, while C levels are hosted on the SekurMail privacy platform. This feature is very much in demand as small and large businesses have recently been the target of Business Email Compromise (BEC) attacks. A BEC attack is a type of cybercrime where malicious hackers use email to trick someone into sending

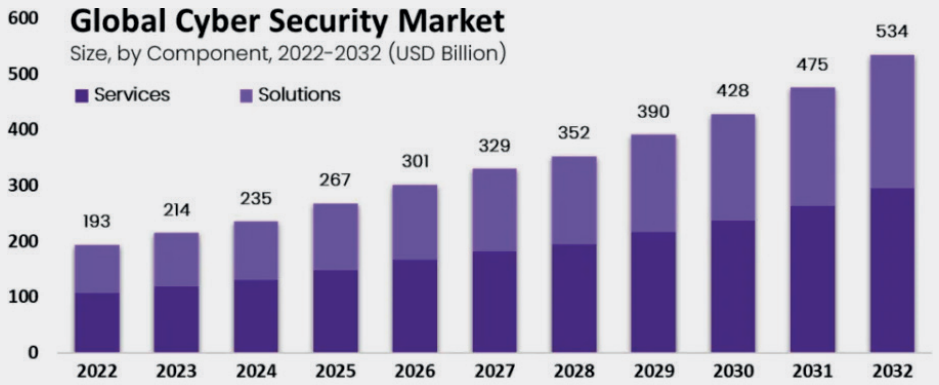


"Business email compromise (BEC) – also known as email account compromise (EAC) – is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business – both personal and professional. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request." (Source)



The $2.7 billion USD represents a 12.5% increase in losses in just one year in the USA due to BEC attacks. (Source: FBI 2022 Internet Crime Report) "The BEC scam has continued to evolve, targeting small local businesses to larger corporations, and personal transactions. Between December 2021 and December 2022, there was a 17% increase in identified global exposed losses." (Source: FBI, 2023) According to latest data from Perception Point, a 20% growth in the prevalence of Business Email Compromise (BEC) attacks along with a 41% surge in phishing attacks from H2 2022 to H1 2023 is reported: "Additionally, the report observed a 75% increase in attacks targeting cloud collaboration apps and storage, including Microsoft 365 apps, Salesforce, Slack, AWS S3 Buckets and others... **The total number of cyberattacks rose by 36% in H1 2023. Email continued to be the main vector for delivering malicious content, with as many as 1 in every 100 emails sent in the first half of 2023 found to be malicious...** We expect cybercriminals to continue sharpening their tools in order to target a wider range of communication and collaboration channels, which is likely to fuel an unprecedented surge in attacks in 2023. Organizations should adopt proactive security measures and embrace emerging technologies and holistic, managed services to strengthen their ability to prevent and remediate such pernicious cyber threats."

money or divulging confidential company info. BEC scams are on the rise due to increased remote work – there were nearly 20,000 BEC complaints to the FBI in 2021, according to the FBI Internet Crime Report. C-Level employees are particularly targeted in BEC attacks. According to this article on TechTarget, BEC exploits often begin with the attacker using a social engineering scam to trick a C-level target into downloading malware, clicking on an infected link or visiting a compromised website. Once the C-level manager's account has been compromised, it can be used to trick another employee into sending money to the attacker. A popular BEC strategy is to send an official-looking email to someone in the company's finance department. Typically, such an email will say there is a time-sensitive, confidential matter that requires payment to be made to a customer's, partner's or supply chain partner's bank account as soon as possible. The attacker hopes that the unsuspecting person in finance will think they are helping their company by facilitating a quick transfer of funds – when, in reality they are sending money to the attacker's bank account. The Company's enterprise solutions will be priced differently than its consumer versions, with SekurMail being US$10/month/user, with alias emails at US$7/month/alias, SekurMessenger priced at US$9/month/user and SekurVPN at US$9/month/user. New solutions such as SekurVoice and SekurPro will add encrypted voice and video to the mix of offerings and are planned to be priced at US$20/month/user and US$25/month/user respectively. Yearly pricing will be 11 times monthly to offer 1 free month of service. Businesses will be able to customize bundles for each solution, as they are today. Customers can now simply go to the Sekur website and select either SekurMail, SekurVPN or SekurMessenger and select any add-on offered for any or both of the other 2 solutions not selected as the primary choice. Add-ons are offered at a discount when bundled with any single solution. The Company is already seeing the advantages of offering the add-ons, as over 50% of their customers choose to bundle solutions. **Alain Ghiai, CEO of Sekur Private Data said:** "We are very excited to be on track to launch our Sekur Enterprise Solutions, which will improve our existing Business Solutions, and offer more features to larger enterprises and government organizations. We have a high demand in Latin America for these features and we will be ready for the US market as we launch our B2B platform in Q4 2023. Offering SMB and Enterprise solutions is part of the core strategy of the Company for Q4 2023 onward, as these solutions increase our average spend per customer and create a more stable and stickier customer base, while still catering to the vast consumer market. There are over 30 million small businesses in the USA alone, and we plan to target a percentage of these businesses, protecting them from such things as BEC attacks..."



The market for cybersecurity and privacy solutions has been growing rapidly in recent years and is expected to continue its expansion in the foreseeable future. This growth is primarily driven by the increasing frequency and sophistication of cyberthreats, as well as the growing dependence of businesses, governments, and individuals on digital technology. According to Fortune Business Insights, the global **data privacy software market** size is projected to reach $25.85 billion USD by 2029, at a CAGR of 40.8% during the forecast period 2022-2029: "North America is expected to hold the largest market share... The increasing concerns regarding personal and confidential data breaches are driving organizations to adopt data privacy software... The growing data privacy concerns have forced governments of various countries to implement data privacy enforcement laws and regulations... As the number of IoT devices and applications continues to rise, it is anticipated that the market for data privacy management applications will also grow, leading to significant expansion in the industry in the years ahead."

On May 25, 2023, Sekur announced its financial results for the first quarter of 2023, with sales increasing by 50% compared to first quarter of 2022. Alain Ghiai, CEO of Sekur Private Data said: "We are pleased to show our shareholders that our plan to increase sales while reducing expenses is materializing. Sales were up 50% Q1 2023 vs Q1 2022, expenses were down by 55% in Q1 2023 vs Q1 2022 and we finished Q1 2023 with a solid balance sheet. We intend to continue to follow our plan for 2023, which is to improve our solutions, reduce our Customer Acquisition Cost ("CAC") and increase in proportion our digital marketing budgets, as the CAC goes down. Our CAC is going down as per our recent news, release issued on May 9, 2023, and we are continuing to work to reduce it further. We have achieved great results so far, lowering in some campaigns our CAC as low as US$28. The plan is to increase digital marketing as we lower our CAC and scale up from there. We are expecting increased sales for 2023 vs 2022, thanks to a lower CAC and the launch of new solutions and various improvements to our existing ones. We also want to thank all our shareholders for their support, and we look forward to presenting even better financial results for 2023."

On March 16, 2023, Sekur announced that it has been named on a lits of the "5 Best Cyber Security Companies to Watch 2023" by the Silicon Review magazine. The article can be viewed here.

LATEST INTERVIEWS

Yesterday, Sekur's CEO, Alain Ghiai, was interviewed by Rich TV Live.

Alain is interviewed regularly as part of the "Hack of the Week" series on NewToTheStreet.com.

Recently, Alain was interviewed by the renowned Cybercrime Magazine.

In June, Alain discussed decreased customer acquisition costs and its global vision on The Street Podcast.

Alain talked about the importance of Swiss privacy with Roman Balmakov from The Epoch Times' Facts Matter.

LATEST ARTICLES

The 15 articles published about Sekur in 2023 have reached 215,650 pageviews on Benzinga as of today.

Additional select articles include:

"Sekur: Safeguarding Your Digital World"
(Zimtu Capital, September 2023)

"Redefining Digital Security: The Rise of Sekur Private Data Ltd."
(Tech Times, August 2023)

"Securing Your Digital Footprints: Sekur Private Data Ltd. Charts the Future"
(Hackermoon, August 2023)

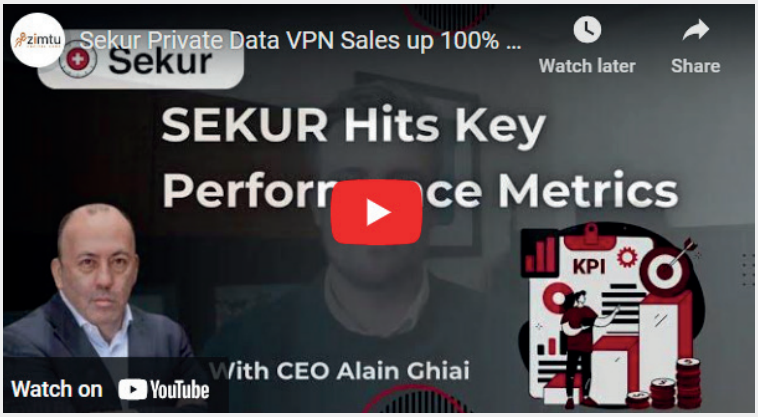
"Sekur Private Data Ltd.: Bridging the Gap between Privacy and Technology"
(Next Gen Hero, August 2023)

"Reshaping Digital Privacy: Sekur's Solution to Cybersecurity Threats"
(Daily Caller, April 2023)

Click above image or here to watch the interview.

Click above image or here to watch the interview.

Click above image or here to watch the interview.



Click above image or here to watch the interview.

MANAGEMENT & DIRECTORS

ALAIN GHIAI
Founder, President, CEO, Director

Alain founded Sekur Private Data Ltd. and has served as CEO and Director since March 2017. He has served as President and Corporate Secretary of the company since June 2018. Alain also founded **GlobeX Data S.A.** ("GDSA") and has served as its CEO and Director since 2007. He also founded **GlobeX Data Inc.** ("GlobeX US") and has served as its CEO and Director since 2012. Alain attended the California College of Arts in San Francisco, where he obtained his Bachelor of Architecture in 1994. Alain has over 15 years of experience in the software industry and has been instrumental in the development of the company and its public listing in 2019.

SCOTT DAVIS
CFO

Scott is a Chartered Professional Accountant and a partner of **Cross Davis & Company LLP**, a firm focused on providing accounting and management services for publicly listed companies. His experience includes CFO positions of several companies listed on the TSX Venture Exchange and his past experience consists of senior management positions, including 4 years at **Appleby Global Group Services Ltd.** as an Assistant Financial Controller. Prior to that, he spent 2 years at **Davison & Company LLP** as an Auditor, 5 years with **Pacific Opportunity Capital Ltd.** as an Accounting Manager and 2 years at **Jacobson Soda and Hosak**. Scott obtained his CPA, CGA in 2003. Scott has been a service provider to technology companies for over 8 years. He is working side by side with Alain on the management of the finances of Sekur Private Data Ltd.

HENRY SJÖMAN
Director

Henry has been an enterpreneur and angel investor since 1991. He has been involved in the electronics and telecommunications industry since 1974, building a substantial part of all Blackberry and Nokia phones at one time through his network of manufacturing worldwide. Henry co-founded **Elcoteq SE** in 1991, an electronic manufacturing company which was listed on Euro-NASDAQ until 2010. He received his Bachelor of Science in Telecommunication from the Kopings Tekniska Institut (Sweden) in 1974. Henry serves as a Director of Sekur Private Data Ltd. and is a member of the company's audit committee.

AMIR ASSAR
Director

Amir has over 27 years of experience in technology sales and leadership and is presently AVP Sales at **Workday Inc. (NASDAQ: WDAT)**, one of the world's leading software companies. Prior to joining Workday, Amir was one of the key executives at **Adaptive Insights**, where he was instrumental in establishing the company as a leader in the financial data analytics market, culminating in an IPO in June 2018 and the acquisition by Workday for $1.55 billion USD in August 2018. Amir started his technology career in 1993 at **Actel Corp.** as Western USA Director of Sales. Actel was a leading provider of Field Programmable Gate Arrays (FPGA) and was acquired by **Microsemi Corp.**, a California-based semiconductor and systems solutions provider for the aerospace, defense, communications, data center and industrial markets. From there, Amir went on to work for several successful emerging technology companies in the Silicon Valley, including **Annuncio Software** (acquired by **PeopleSoft**), **NetScaler** (acquired by **Citrix**), **DataPower** (acquired by **IBM**), and IBM where he held senior sales management and leadership positions. At DataPower, he was part of the original sales leadership team that built the company from fledgling start-up with no customers into a $300 million USD business while transitioning it to become one of IBM's most successful acquisitions. He is married and lives with his wife in San Francisco, California. Amir serves as a Director of Sekur Private Data Ltd. and is a member of the company's audit commitee.

DR. CLAUDIO ALBERTI
Director

Caudio has served as CTO and Co-Founder of **GenomSys**, a Swiss company specialized in the compression and transport of genomic sequence data since 2017. He is a major contributor to MPEG-G, the new ISO/IEC standard for representing genome sequencing data and is currently editor of the second part of the project "Coding of Genomic Information". After earning a Master's degree in Engineering from the Politecnico di Milano (Italy) and a Doctorate from the EPFL (Lausanne, Switzerland), he designed and developed solutions for digital media processing and information security companies. He currently collaborates on developing compliant genome processing applications to MPEG-G with genomic competence centers such as the Swiss Institute of Bioinformatics, the James Hutton Institute (UK) and the Carl R. Woese Institute for Genomic Biology (University of Illinois at Urbana Champaign).

DISCLAIMER AND INFORMATION ON FORWARD LOOKING STATEMENTS

Rockstone Research, Zimtu Capital Corp. ("Zimtu") and Sekur Private Data Ltd.. ("Sekur") caution investors that any forward-looking information provided herein is not a guarantee of future results or performance, and that actual results may differ materially from those in forward-looking information as a result of various factors. The reader is referred to the Sekur´s public filings for a more complete discussion of such risk factors and their potential effects which may be accessed through its documents filed on SEDAR at www.sedar.com. All statements in this report, other than statements of historical fact should be considered forward-looking statements. Much of this report is comprised of statements of projection. **Statements in this report that are forward looking include** that with the growing complexity of cyberthreats and the ever-expanding attack surface, companies selling cybersecurity products find themselves in a position of significant relevance and opportunity; that Sekur stands out among other cybersecurity and privacy companies through its exceptional product portfolio and a steadily expanding clientele, and that with innovative solutions tailored to address evolving digital threats and privacy concerns, Sekur has established a reputation for excellence in safeguarding sensitive information, positioning the company and its shareholders for promising growth prospects in the ever-evolving landscape of cybersecurity; that as long as cyberthreats persist and evolve, there will be an ongoing demand for innovative cybersecurity and privacy solutions; that heightened awareness drives demand for cybersecurity products; that as governments and enterprises become more security-conscious, companies selling cybersecurity products will find a growing market for their offering; that with ongoing innovation, adaptation to emerging threats, and a commitment to protecting digital ecosystems, the cybersecurity industry will continue to play a vital role in protecting our interconnected world; that 65% of organizations plan to increase cybersecurity spending in 2023; that there's an anticipated increase in cybersecurity spending in 2023 and the years to follow; that cyberattackes are expected to spike in 2023 and spending will increase this year and in the years to follow; that more sophisticated cyber attacks driven by Artificial Intelligence or geo-phishing will push companies to spend more; that experts estimated that the total cost of cybercrime would reach $8 trillion this year; that it is estimated that small and medium-sized businesses (SMBs) will spend $29.8 billion on managed security services in 2025, and that they were forecasted to spend $90 billion on cybersecurity; that a significant portion of organizations worldwide (73%, to be precise) plan to increase their cybersecurity spending in 2023; that Google has announced its commitment to strengthen cybersecurity by investing over $10 billion within five years; that the imperative to protect increasingly digitized businesses, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion cumulatively for the five-year period from 2021 to 2025; that cybercrime is predicted to cost the world $10.5 trillion annually by 2025; that cybersecurity is the only line item that theoretically has no spending limit; that global cybersecurity spending will reach $219 billion USD this year and grow to nearly $300 billion USD in the next 3 years; that this year's investments in cybersecurity hardware, software and services are expected to jump 12.1% compared to 2022 and outperform growth in overall IT spending; that almost all industries and company size segments will see low double-digit growth through 2026; that analysts expect the cybersecurity market to continue its run of sustained growth and that the biggest spenders will include organizations in banking, manufacturing, professional servies and governments, accounting for more than one-third of all cybersecurity spending this year; that software, the fastest-growing segment, will capture 47% of all spending this year, followed by services (39%) and hardware (13%); that companies selling cybersecurity products are poised for a bright future; that organizations and individuals alike will increasingly turn to cybersecurity solutions to safeguard their digital assets and privacy; that as the digital economy grows, digital crime grows with it; that damage from cyberattacks will amount to about $10.5 trillion annually by 2025; that threat volumes will almost double from 2021 to 2022; that the total opportunity amounts to a staggering $1.5 trillion to $2.0 trillion addressable market; that the current buyer climate may pose a unique moment in time for innovation in the cybersecurity industry; that the growth prospects for vendors in the cybersecurity market are exceptionally promising; that Switzerland isn't prone to environmental risks, such as hurricanes, tsunamis, volcanos, earthquakes, forest fires or floods; that over the next 5 years companies will spend $1.75 trillion on cybersecurity; that it is predicted that by the end of 2024, mobile security spending will exceed $7.2 billion; that the lack of mobile security is predicted to be one of the fastest-growing threats in cybersecurity; that businesses are steadily growing their cybersecurity budget; that once Sekur's sales gain momentum in Mexico, the launch is planned to expand to other countries where America Movil operates through its Claro brand, such as Colombia, Peru and other Latin American countries, as the business grows over the coming years; that Sekur expects exponential growth in the coming months and years for its SekurVPN solution and is adding enterprise features and other upgrades; that Sekur plans to launch a full-scale campaign for its VPN solution sometime in late October or early November as it is preparing the final touches on its digital ads; that there are other plans as well with resellers to launch SekurVPN later this year; that Sekur believes that in the coming 12 months, its web traffic will be such that its customer acquisition cost could drop down dramatically as the organic search increases exponentially; that as Sekur increases SMB marketing to businesses, spending per customer is expected to increase as SMBs have multiple users in their business; that Spending per user is also expected to increase as Sekur launches its SekurVoice voice calls encrypted solutions and SekurPRO, its video conferencing and complete private and secure communications suite, in Q1 2024; that Sekur has the physical environment necessary to keep the servers up and running 24 hours a day, seven days a week, even in case of power shortages and major natural disasters; that Sekur's products ensures that your information is safe from competing predators or agencies and entities with personal motives who would pry into your privacy and steal your data without your knowledge; that Sekur ensures that only the sender and intended recipient can read the messages exchanged; that the data which Sekur stores is safe/Secure, and that your conversations are kept completely private and

cannot be accessed by anyone else, and that the service is secure and cannot be compromised by anyone; that Sekur provides the most secure environment for your digital communications; that Sekur eliminates the risk of data being intercepted from the sender's device, and that "BEC" (Business Email Compromise) and email phishing incidents are eliminated; that Sekur never monitors users' activity and never shares any data with third party service providers; that by having its own proprietary technology, Sekur is not subject to intrusive laws such as the CLOUD Act, USA PATRIOT Act or Cybersecurity Information Sharing Act; that DSS intends to approach the first and third largest telecom operators in Morocco, along with several major banking groups and government organizations; that Sekur ensures private and secure communications and prevent Business Email Compromise ("BEC") attacks; that Sekur will also offer our SekurVPN in Morocco; that Sekur offers a truly independent, private and secure means of communications without any data mining; that Sekur looks forward to offering true data privacy to all Moroccan businesses and government organizations, and protect their intellectual property, and their privacy, from data miners, malicious hackers and rogue agents of foreign powers; that Sekur has a specific plan to tweak the CAC for the next quarter and increase the digital marketing budget gradually from August 2023 onward; that if Sekur's CAC numbers are under $50 USD, the company will do very well; that Sekur's enterprise solutions will be priced differently than its consumer versions; that New solutions such as SekurVoice and SekurPro will add encrypted voice and video to the mix of offerings and are planned to be priced at US$20/month/user and US$25/month/user respectively; that Sekur has a high demand in Latin America for these features and Sekur will be ready for the US market as it launches its B2B platform in Q4 2023; that offering SMB and Enterprise solutions is part of the core strategy of Sekur for Q4 2023 onward, as these solutions increase Sekur's average spend per customer and create a more stable and stickier customer base, while still catering to the vast consumer market; that cybercriminals are expected to continue sharpening their tools in order to target a wider range of communication and collaboration channels, which is likely to fuel an unprecedented surge in attacks in 2023; that Sekur's plan to increase sales while reducing expenses is materializing; that Sekur's plan is to increase digital marketing as we lower our CAC and scale up from there; that Sekur is expecting increased sales for 2023 vs 2022, thanks to a lower CAC and the launch of new solutions and various improvements; that Sekur looks forward to presenting even better financial results for 2023; that the market for cybersecurity and privacy solutions is expected to continue its expansion in the foreseeable future; that the global data privacy software market size is projected to reach $25.85 billion USD by 2029, at a CAGR of 40.8% during the forecast period 2022-2029, and that North America is expected to hold the largest market share; that it is anticipated that the market for data privacy management applications will grow, leading to significant expansion in the industry in the years ahead. **Such statements involve known and unknown risks, uncertainties and other factors that may cause actual results or events to differ materially from those anticipated in these forward-looking statements. There can be no assurance that such statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Risks and uncertainties include:** The receipt of all necessary approvals and permits for conducting business; uncertainty of future capital expenditures and other costs; financing and additional capital requirements for maintenance or expansion of business activity may not be available at reasonable cost or at all; legislative, political, social or economic developments in the jurisdictions in which Sekur carries on business may hinder progress or business; operating or technical difficulties or cost increases in connection with existing products or proiects in development; the ability to keep key employees and operations financed; share prices of Sekur and other companies may fall as a result of many factors, including those listed here and others listed in the companies' and other cybersecurity and privacy company disclosure; and the vended prices of offered products may not be sufficient to continue economically; the promised product features may prove incorrect, unsafe/unsecure and users may experience data breaches or othe rkind of cyberattacks; the security features may prove insecure, in which cases Sekur may face litigation or other kinds of legal challenges; regulators may hinder users to use Sekur's products; that the laws in Switzerland or elsewhere may change to the disadvantage of Sekur conducting business; that users may find Sekur's products not useful and discontinue the service; that Sekur will not find new users to keep operations financed; that Sekur will not make any profits and will go bankrupt or delist its shares from the stock exchange, and that investors may lose all of its investment into Sekur; that Sekur's share price will fall dramatically or the stock gets halted for a long time, i.e. investors can not trade their stock anymore; that Sekur will not have sufficient funds to fund its operations; Sekur's continued operation as a going concern is dependent upon its ability to generate positive cash flows and/or obtain additional financing sufficient to fund continuing activities and acquisitions. According to Sekur: "While we continue to review our operations in order to identify strategies and tactics to increase revenue streams and financing opportunities, there is no assurance that we will be successful in such efforts; if we are not successful, we may be required to significantly reduce or limit operations, or no longer operate as a going concern. It is also possible that operating expenses could increase in order to grow the business. If we do not start generating and significantly increase revenues to meet these increased operating expenses and/or obtain financing until our revenues meet these operating expenses, our business, financial condition and operating results could be materially adversely affected. We cannot be sure when or if we will ever achieve profitability and, if we do, we may not be able to sustain or increase that profitability. Important risk factors that could cause the Company's actual results and financial condition to differ materially from those indicated in the forward-looking statements include, among others, the following: speculative nature of investment risk; history of operating loss; going-concern risk; the Company's reliance on resellers and other distribution channels to sell its products; dependency on large channel partners; dependency on key personnel; dependency on third parties; software bugs; competition; security threats; research and development; commitments; obsolescence; growth; dilution; unissued share capital; liquidity and future financing

risk; market risk for securities; and increased costs of being a publicly traded company. Although management believes that the above risks fairly and comprehensibly illustrate all material risks facing the Company, the risks noted above do not necessarily comprise all those potentially faced by the Company as it is impossible to foresee all possible risks. Although the Directors will seek to minimise the impact of the risk factors, an investment in the Company should only be made by investors able to sustain a total loss of their investment. Investors are strongly recommended to consult a person who specialises in investments of this nature before making any decision to invest. Any forward-looking information in this MD&A is based on the conclusions of management. The Company cautions that due to risks and uncertainties, actual events may differ materially from current expectations. With respect to the Company's operations, actual events may differ from current expectations due to economic conditions, new opportunities, changing budget priorities of the Company and other factors." For more details on risk factors and uncertainties, visit www.sedar.com and read the "Management's Discussion & Analysis" forms along with its financial statements. **Accordingly, readers should not place undue reliance on forward-looking information.** Rockstone and the author of this report do not undertake any obligation to update any statements made in this report except as required by law.

DISCLOSURE OF INTEREST AND ADVISORY CAUTIONS

Nothing in this report should be construed as a solicitation to buy or sell any securities mentioned. Rockstone, its owners and the author of this report are not registered broker-dealers or financial advisors. Before investing in any securities, you should consult with your financial advisor and a registered broker-dealer. Never make an investment based solely on what you read in an online or printed report, including Rockstone's report, especially if the investment involves a small, thinly-traded company that isn't well known. **The author of this report, Stephan Bogner, is paid by Zimtu Capital, a TSX Venture Exchange listed investment company.** Part of the author's responsibilities at Zimtu Capital is to research and report on companies in which Zimtu Capital has an investment. So while the author of this report is not paid directly by Sekur Private Data Ltd. ("Sekur")., the author's employer Zimtu Capital will benefit from appreciation of Sekur's stock prices. The author currently does not own any equity of Sekur, however he owns equity of Zimtu Capital Corp., and thus will benefit from volume and price appreciation of the stock. Sekur pays Zimtu to provide this report and other investor awareness services. According to the news-release on August 31, 2023: "Zimtu Capital Corp. (TSXv: ZC; FSE: ZCT1) (the "Company" or "Zimtu") announces it has signed an agreement with Sekur Private Data Ltd. ("Sekur") to provide specific services from its Zimtu-ADVANTAGE program (https://www.zimtu.com/zimtu-advantage/). Zimtu will receive $50,000 from Sekur for the duration of the 3-month contract." Also note that the referenced video interviews and articles have been sponsored by Sekur Private Data Ltd. **Overall multiple conflicts of interests exist.** Therefore, the information provided in this report should not be construed as a financial analysis or recommendation but as an advertisement. Rockstone's and the author's views and opinions regarding the companies that are featured in the reports are the author's own views and are based on information that was received or found in the public domain, which is assumed to be reliable. Rockstone and the author have not undertaken independent due diligence of the information received or found in the public domain. Rockstone and the author of this report do not guarantee the accuracy, completeness, or usefulness of any content of this report, nor its fitness for any particular purpose. Lastly, Rockstone and the author do not guarantee that any of the companies mentioned in the report will perform as expected, and any comparisons that were made to other companies may not be valid or come into effect. Please read the entire Disclaimer carefully. If you do not agree to all of the Disclaimer, do not access this website or any of its pages including this report in form of a PDF. By using this website and/or report, and whether or not you actually read the Disclaimer, you are deemed to have accepted it. Information provided is educational and general in nature. Data, tables, figures and pictures, if not labeled or hyperlinked otherwise, have been obtained from Stockwatch.com, Sekur Private Data Ltd. and the public domain. The cover picture (amended) has been obtained and licenced from KanawatTH.

Author Profile & Contact

Stephan Bogner (Dipl. Kfm., FH)
Rockstone Research
8260 Stein am Rhein, Switzerland
Phone: +41 44 5862323
Email: sb@rockstone-research.com

Stephan Bogner studied Economics, with specialization in Finance & Asset Management, Production & Operations, and Entrepreneurship & International Law, at the International School of Management (Dortmund, Germany), the European Business School (London, UK) and the University of Queensland (Brisbane, Australia). Under Prof. Dr. Hans J. Bocker, Stephan completed his diploma thesis ("Gold In A Macroeconomic Context With Special Consideration Of The Price Formation Process") in 2002. A year later, he marketed and translated into German Ferdinand Lips' bestseller "Gold Wars". After working in Dubai's commodity markets for 5 years, he now lives in Switzerland and is the CEO of Elementum International AG specialized in the storage of gold and silver bullion in a high-security vaulting facility within the St. Gotthard Mountain in central Switzerland.

Rockstone Research is specialized in capital markets and publicly listed companies. The focus is set on exploration, development, and production of resource deposits, as well as technology ventures. Through the publication of basic geological, technological, and stock market knowledge, the individual company and sector reports receive a background in order for the reader to be inspired to conduct further due diligence and to consult with a financial advisor.

All Rockstone reports are being made accessible free of charge, whereas it is always to be construed as non-binding research addressed solely to a readership that is knowledgeable about the risks, experienced with stock markets, and acting on one's own responsibility.

For more information and sign-up for free email newsletter, please visit:
www.rockstone-research.com