



GlobeX Data®

Disclaimer

A final prospectus containing important information relating to the securities described in this document has been filed with the security's regulatory authorities in British Columbia, Alberta and Ontario. A copy of the final prospectus, and any amendment, is required to be delivered with this document. This document does not provide full disclosure of all material facts relating to the securities offered. Investors should read the final prospectus, and any amendment, for disclosure of those facts, especially risk factors relating to the securities offered, before making an investment decision.

This presentation provides a very brief summary of GlobeX Data Ltd. (the "Company") derived from the disclosure contained in the Company's final prospectus dated May 8, 2019 (the "Prospectus") that this information was derived from that contains "forward-looking statements". Forward-looking statements can be identified by words such as: "anticipate," "intend," "plan," "goal," "seek," "believe," "project," "estimate," "expect," "strategy," "future," "likely," "may," "should," "will" and similar references to future periods. Examples of forward-looking statements include, among others, statements regarding:

- Anticipated levels of expenditures for the next twelve months;
- Expectations of ongoing relationships with reseller and partners;
- Timing of completion of software integrations and updates;
- Management's belief that we have sufficient liquidity to fund the Company's business operations during the next twelve months; and
- Strategy for customer retention, growth, product development, market position, financial results and reserves.

Forward-looking statements are neither historical facts nor assurances of future performance. Instead, they are based only on management's current beliefs, expectations and assumptions regarding:

- the future of the Company's business;
- the success of marketing and sales efforts of the Company;
- the projections prepared in house and projections delivered by channel partners;
- the Company's ability to complete the necessary software updates;
- increases in sales as a result of investments software development technology;
- consumer interest in the Products;
- future sales plans and strategies;
- reliance on large channel partners and expectations of renewals to ongoing agreements with these partners;
- anticipated events and trends; and
- the economy and other future conditions;

Because forward-looking statements relate to the future, they are subject to inherent uncertainties, risks and changes in circumstances that are difficult to predict and many of which are outside of our control. The Company's actual results and financial condition may differ materially from those indicated in the forward-looking statements. Therefore, you should not rely on any of these forward-looking statements.

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. Actual results may vary from such forward-looking information for a variety of reasons, including but not limited to, risks and uncertainties disclosed in this prospectus. See "Risk Factors" on page 41 of the Prospectus.

These forward-looking statements are made as of the date of the Prospectus and are based on the reasonable beliefs, expectations and opinions of management on the date of this prospectus (or as of the date they are otherwise stated to be made). Although the Company has attempted to identify important factors that could cause actual results to differ materially from those contained in forward-looking statements, there may be other factors that cause results not to be as anticipated, estimated or intended. New factors emerge from time to time, and it is not possible for management to predict all of such factors and to assess in advance the impact of each such factor on the Company's business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statement. There is 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. We do not undertake to update or revise any forward-looking statements, except as, and to the extent required by, applicable securities laws in Canada.

Readers are cautioned against placing undue reliance on forward-looking statements.



For 10+ years GlobeX Data Ltd. and its sister companies have been providing Swiss-hosted cybersecurity and cloud privacy solutions for communications and secure data management.



GlobeX Data®



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

What We Do

We protect data and **communications** for consumers, enterprises and public entities.

Proprietary Technology and the Highest-Grade Encryption combined with Swiss Data Privacy Laws.



Sekur®

Secure private chat and email with Anti-phishing SekurSend and SekurReply technology, self-destruct timer, file transfer. encrypted voice recording transfer. Communications are transmitted within Swiss hosted secure servers.



SekurMail®

Secure and private email, collaboration suite, real-time archiving, Anti-phishing and SekurSend proprietary technology platform. Businesses can move their domain with SekurMail's Swiss hosted secure environment.



SekurMessenger®

Secure and private chat, self-deleting chat, voice recording, file transfer via any mobile device, tablet or desktop. Communications are transmitted only within the Swiss hosted secure servers.



SekurSuite®

Secure and private data backup and disaster recovery, file-sharing, password management, multiple users' management, access rights, file-sharing, and secure email hosted in Switzerland.

Why Switzerland



LONG DURATION
OF POLITICAL
STABILITY



LOW ENVIRONMENTAL RISK
AND INDEPENDENT ENERGY



MAXIMUM DATA
PRIVACY



NEUTRALITY



EXCELLENT
INTERNATIONAL
RELATIONS



INDEPENDENT OF BIG
PLAYERS (USA and EU)
No Cybersecurity Act of 2015
No CLOUD Act of 2019



LOW NETWORK
LATENCY

Global Cyber-threats Statistics

94%

Of cyberattacks begin with spear-phishing emails to infect devices with ransomware, induce damage and destruction (or loss) of data, downtime, lost productivity, post-attack disruption to the normal course of business, even reputational harm.

\$20B

Billion global ransomware damage costs by 2021.



Of reported security incidents were Phishing attacks

80%



Spear phishing addresses found through web searches

75%



Of malicious email attachments are Office files

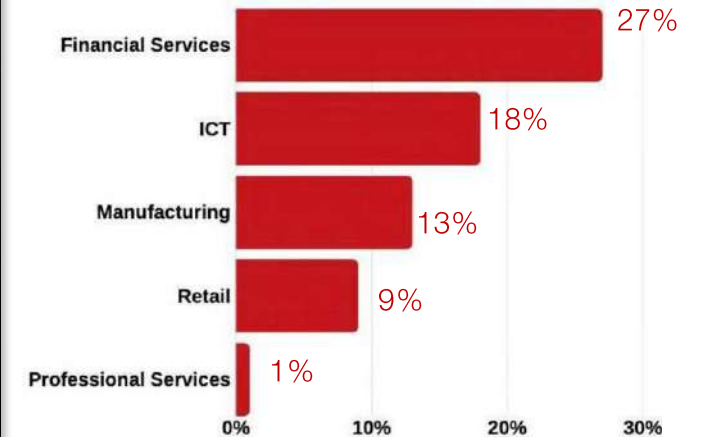
48%



Breach victims were small and medium businesses

43%

Volume of Cybersecurity Incidents by Sector



Cyber-attacks and theft of data are identified as two of the top 10 business risks most likely to happen.

“Global Risk Report 2020” by the World Economic Forum.

How sensitive online banking data is in the 21st century



\$1.8B

In BEC attack
Losses (4 times higher
than Ransomware)



75%

Rise in invoice
and payment fraud
BEC attacks in 2020



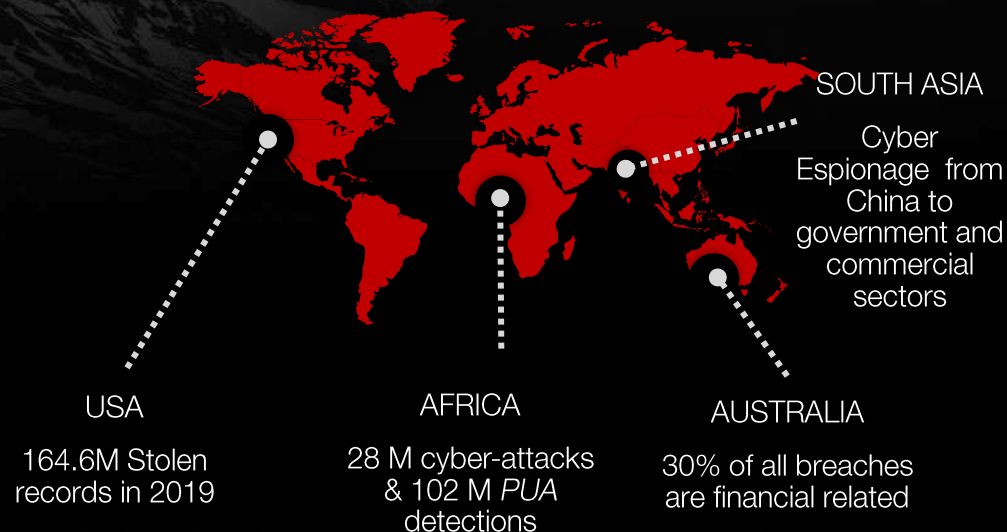
80%

Payment-card
related data breaches



56%

Of all data breaches
take <6 months to be
discover



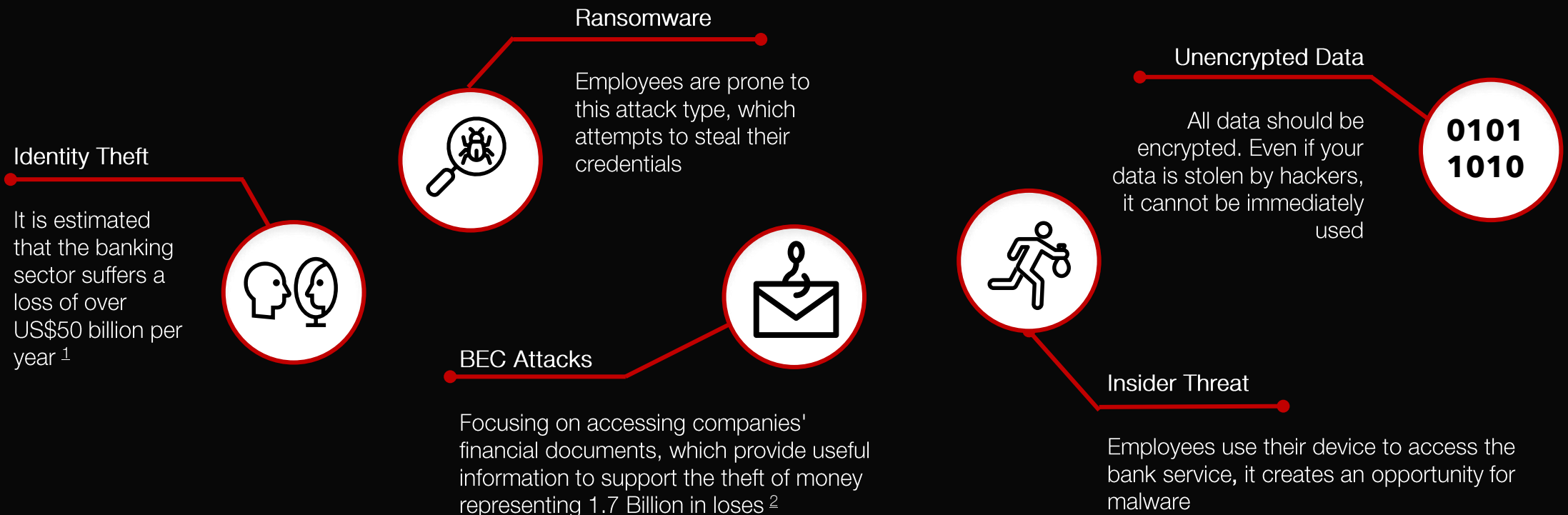
300

Times cyberattacks are more likely to hit
financial institutions than companies from
other industries.



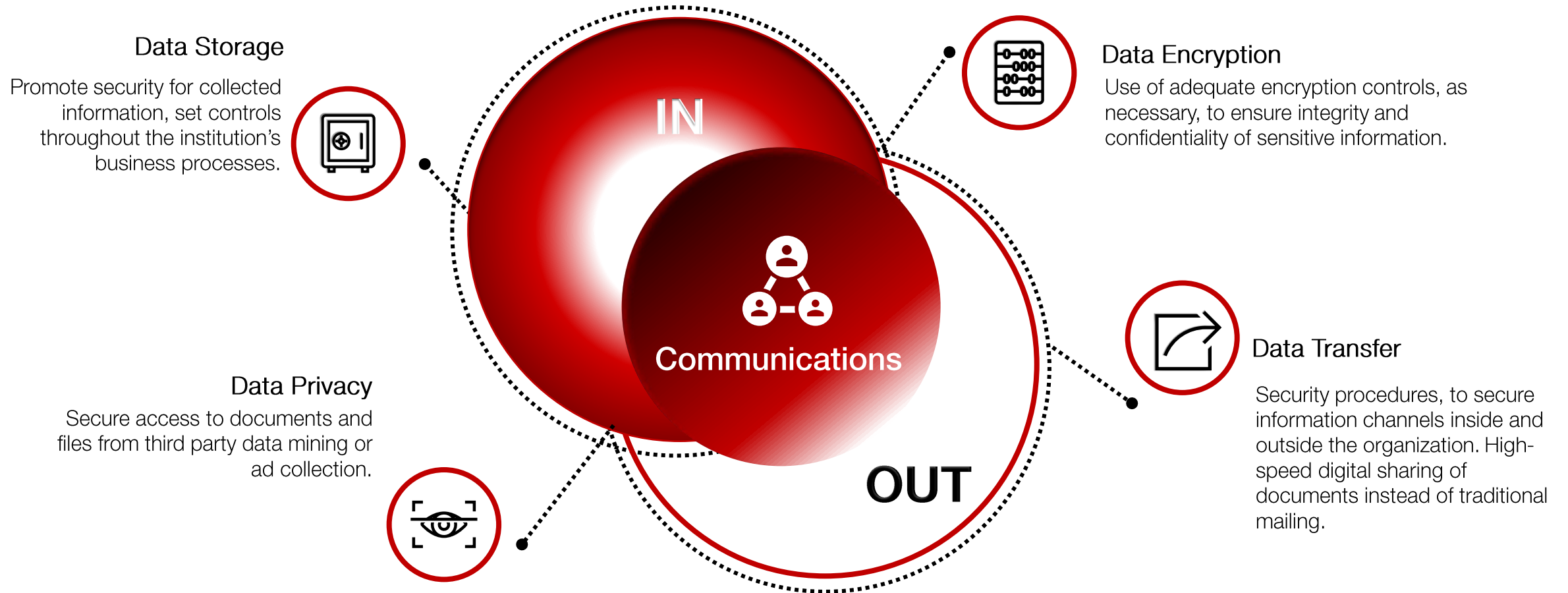
Security threats for financial information

Threats vary in style and intent. Distributed denial of service and payment system attacks are common, but attackers can also route through suppliers or seek to gain some advantage by taking **private data hostage at rest or in transit**.



Information Security

Protecting networks not only requires institutions to improve security of their own systems, but to change the security balance of the entire communications environment inside and outside the organization as well.



Because Privacy Matters

Trends in shift away from mega cloud providers and Big Tech, into more privacy and security focused solutions provider.



Privacy and Security by design.



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.

Communications common channels

Information about financials and operations must be exchanged in a secure manner. No matter the channel, the exchange must be reliable.

CLIENT FACING

Security should work painless for you, for partners and clients. Sensitive information should be protected inside and outside, at rest or whether the data is moving.



Email

Breaches happen because of how files are transmitted. An email or a message that contains an unencrypted file, or sensitive info, could cause a breach.



Messaging

Data is shared and accessed in different ways by different companies. Sometimes IM messages are an easy way to exchange information leaving security aside.



File transfer

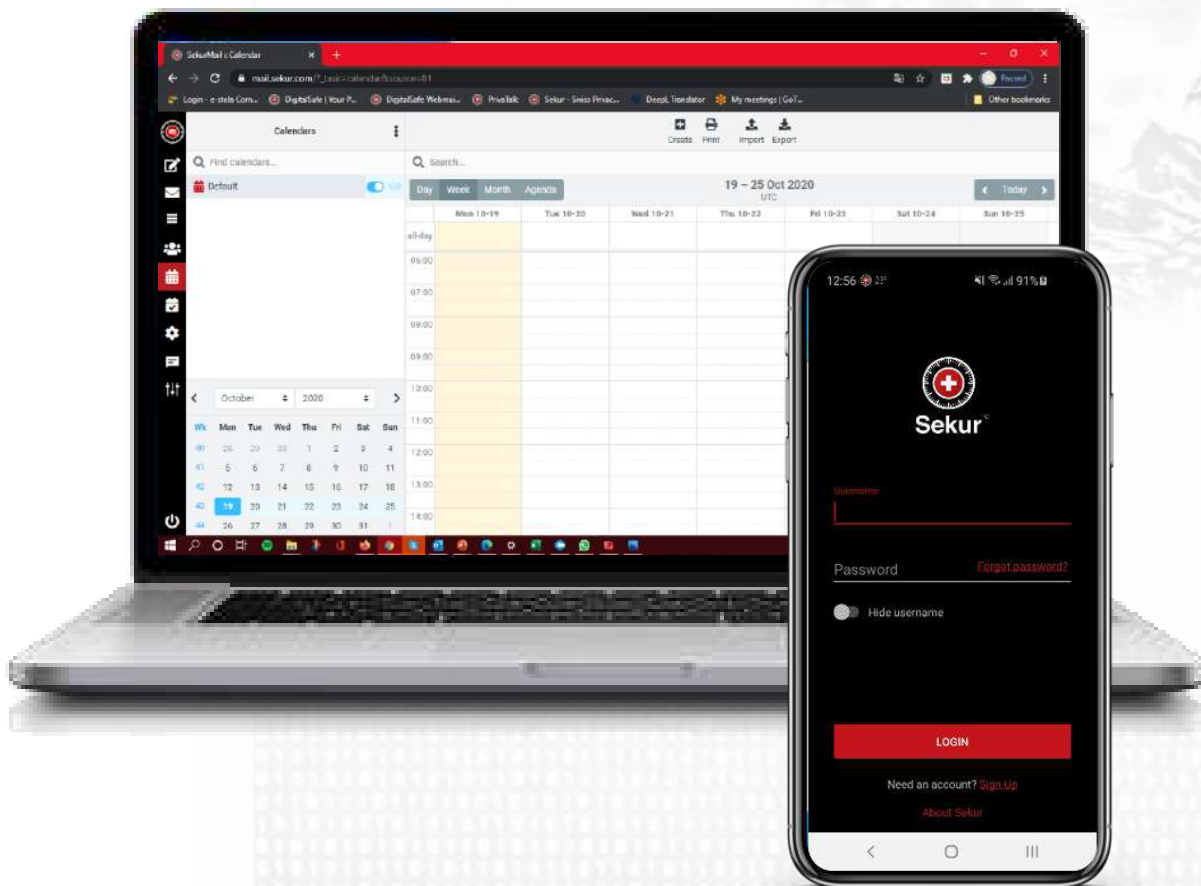
Breaches happen because of how files are transmitted. Data encryption allows contractors and customers to work without worrying about giving away confidential data.



Sekur[®]

Sekur is an Email and Messaging solution for security and Privacy in all your communications.

Sekur encrypts all your communications end-to-end including messages, group chats, files, recorded voice files and emails. Only you and the recipient of your message have access to the communications. Our SekurSend–Sekur Reply prevents from phishing or impersonation attacks.



Military level encrypted Chat.



Proprietary SekurSend – SekurReply Email.



Confidential contact search.



Time limit to self- destruct chats and emails.



Private communications in a private environment.



Unlimited size for SekurSend files.



SekurMessenger®

Sekur Messenger is a Swiss encrypted and private messaging app that offers maximum security using our own proprietary code.

Encrypts all your communications end-to-end including messages, group chats, files and photos. Self delete chats make sure nothing can be found on your device or on our servers. We do not store your messages on our servers.



Military level encrypted chats and file transfers.



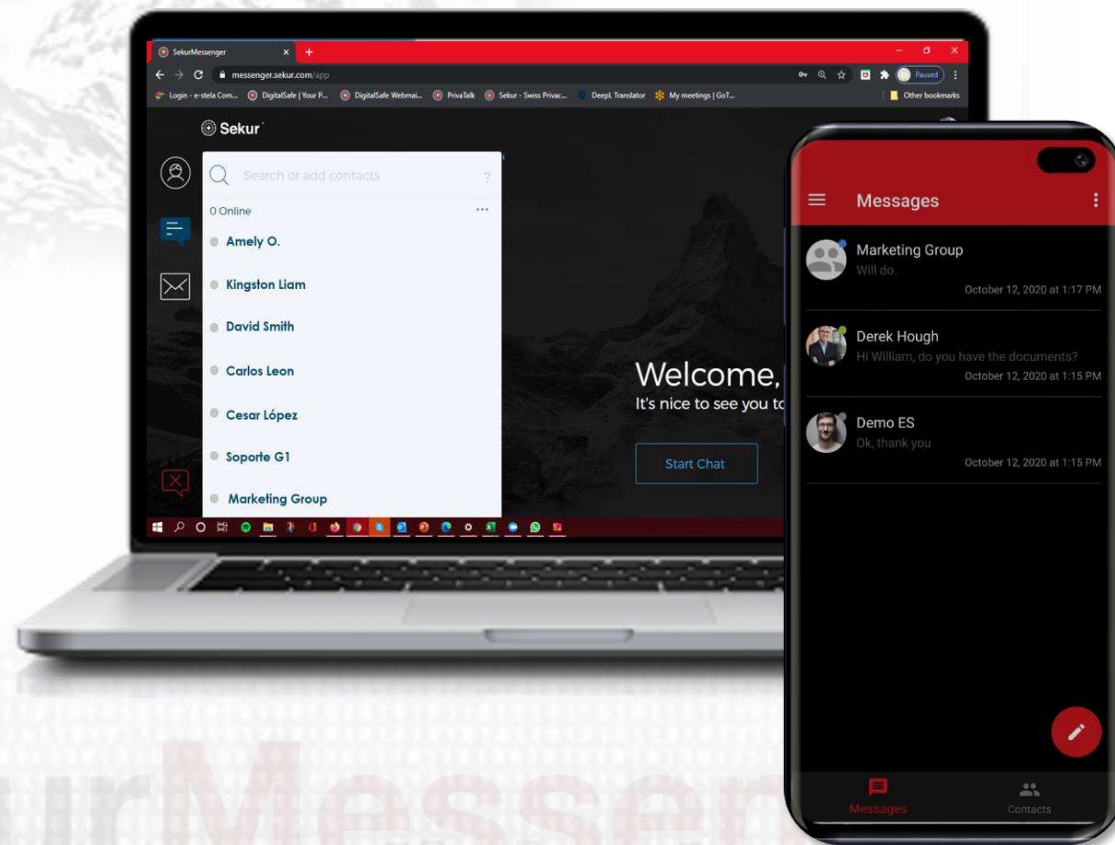
No message, voice or video data resides anywhere.



Confidential contact search by Sekur Number only.



Delete chats from all devices instantly.

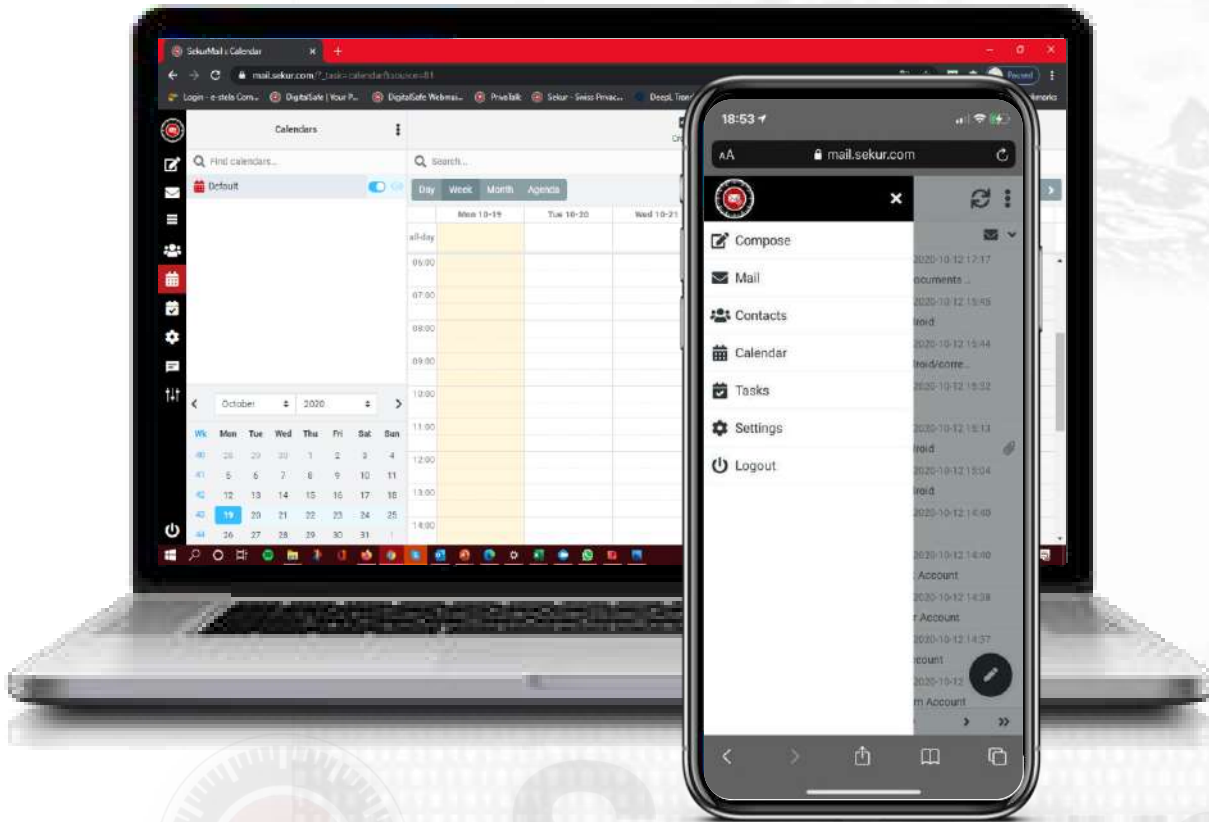




SekurMail®

SekurMail offers Private and Secure end-to-end encrypted emails from servers in Switzerland.

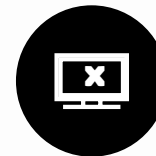
Works with any email address and supports unlimited external recipients with encryption inside and outside the organization using proprietary technology.



SekurSend↔Reply technology.



SekurSend to unlimited file size transfers.



Self-destruct function on external inbox using SekurSend.



Privacy by design no Open-Source code.



Messages do not leave the server and cannot be intercepted.



Real time Archiving API data export.



SekurPro[®]

SekurPro is a Swiss Hosted Private and Secure communications application offering.

Secure Voice and Video calling (web), Secure Chat with Self-Destruct feature, Secure Email and File Transfer via any mobile device, tablet or desktop.



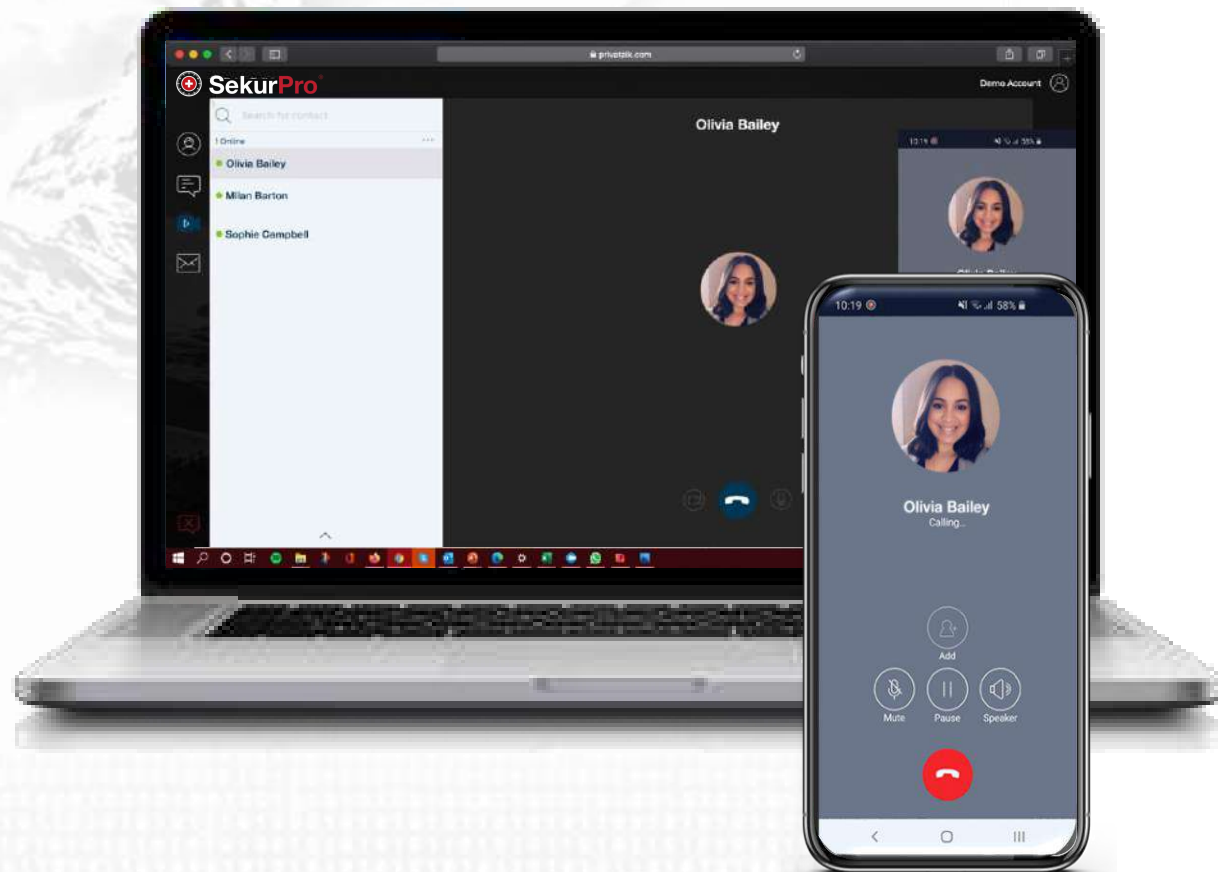
All conversations are directed through our servers in Switzerland.



Multiple users create a master account and invite and collaborate with business partners. It is perfect for small or large companies.



Encrypted private video calls with anyone on the Sekur network, we don't store any part of your conversation.

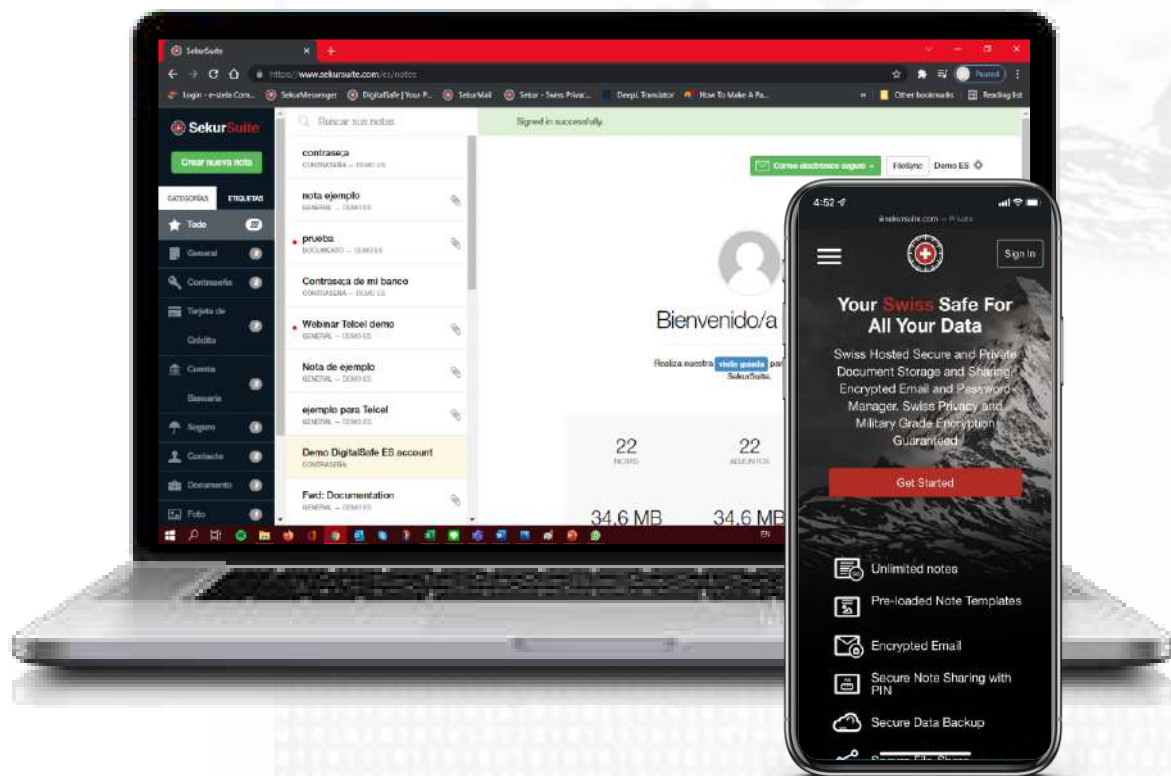




SekurSuite®

SekurSuite is your Swiss Safe For All Your Data.
Encrypted Password Manager, Secure Data Vault,
Secure File-share and Secure Email all in one.

Your information is completely confidential as your information is safely stored in Switzerland. Military Grade security, proprietary technology with Swiss Data Privacy.



Encrypted document management and file transfer tool.



Share files with PIN and time limit for days or even minutes.



Encrypted password manager with complexity meter and visualization cipher.



Transfer unlimited files unlimited size with SekurShare.



Create groups with granular access permissions that allow information control.



Tracking files once sent to verify views, downloads, access points.
















SekurSuite®

















Sekur[®]

Side Comparison for Messenger

There are several industries where secure messaging applications are a necessity. The information they share is highly confidential and they need to be sure to send such sensitive information in a secure application.

							
	SekurMessenger	Signal	Telegram	WhatsApp	Threema	Wire	Skype
 Sign Up to the App Anonymously No phone number needed.	✓	✓	✗	✗	✓	✗	✗
 Private Contacts No Phone Number Permissions to add new contact only by SM number. No contact or social mining.	✓	Limited Function	✗	✗	✗	✗	✗
 Self-Destructing Chats in All Devices Automatic deletion messages, photos, or files with a timer for all devices. Deletion to "bare-metal" in servers.	✓	✗	✗	Limited Function	Limited Function	Limited Function	✗
 End to End Encryption by Default Privacy and security by design beyond E2E.	✓	Limited Function	✗	Limited Function	Limited Function	Limited Function	✗
 Encrypted Chats with Non-App Users Communicate in a private session with anyone without recipient being an app user.	✓	✗	✗	✗	✗	✗	✗
 Service Runs its Own Servers Own server hosted in Switzerland. No third-party platform, no Big Tech platform (No AWS, Microsoft Azure or Google Cloud).	✓	✗	✗	✗	✗	Extra cost	✗

Side Comparison for Messenger
















								
		SekurMessenger	Signal	Telegram	WhatsApp	Threema	Wire	Skype
	No Third-Party Access No API's exposing code.	✓	✗	✗	✗	✗	✗	✗
	No User Data Collection No statistics or behavior analysis. No metadata collection.	✓	✗	✗	✗	✗	✗	✗
	No Open Source Protection for each individual account by segregating each user from the other users, creating several individual barriers of protection. Uses proprietary technology only.	✓	✗	✗	✗	✗	✗	✗
	No Access Data by the CLOUD Act. Entitles US to access data from US IT service providers even if the data is not stored in the US.	✓	✗	✗	✗	✓	✗	✗
	Not Subject to the PATRIOT Act. Any information that you provide to GlobeX shall remain in our Swiss data centers.	✓	✗	✗	✗	✓	✗	✗
	Proprietary technology VirtualVaults® & HeliX® wraps data transfer many times stronger than 2048 bit to avoid MITM. Stores data in multiple encryption environment for each user.	✓	✗	✗	✗	✗	✗	✗
	Swiss FADP Jurisdiction All data is protected under the Swiss Federal Act on Data Protection only.	Swiss	USA	USA / UK / Belize / UAE	USA	Swiss	USA	USA



















Sekur[®]

Side Comparison for Email

Modern email systems use HTTPS to secure message transmission, but the email providers themselves have some level of access to what you're sending. If you truly want to communicate with total privacy, you must encrypt your email communications both ways, without exposing your email to the open Internet.

						
	SekurMail	Gmail	ProtonMail	Outlook	Zoho Mail	Tutanota
 End to End Encryption for Everything Your account at rest, and in transit Emails, Contacts, Calendar, and Tasks are individually protected.	✓	✗	Limited Function	✗	✗	✓
 SekurSend - Encrypted Emails to Anyone Communicate in a private channel, within and outside of your organization without recipient sign up, using Helix proprietary technology protection.	✓	✗	Limited Function	✗	✗	Limited Function
 Email Protection by Personalized Keys Use SekurSend, with password protection, maximum number of reads by recipient, or time expiration.	✓	✗	Limited Function	✗	✗	Limited Function
 Send Unlimited Messages Unlimited encrypted email messages using proprietary technology, military-level encryption, and Swiss Privacy.	✓	✗	✗	✗	Limited Function	✓
 Automatic Server Key Exchange Key exchange on private servers to enable encryption and confidentiality.	✓	✗	✗	✗	✗	✗
 Sekur Reply Send encrypted email and receive a reply to it without having to ask the recipient to register to Sekur. Email does not go through open Internet to reach recipient.	✓	✗	✗	✗	✗	✓
 Advanced Filtering Rules to manage email behavior to handle incoming messages.	✓	✓	✓	✓	✓	✓
 Unlimited Secure File Transfer Encrypted and invisible to any ISP provider, using SekurSend feature.	✓	Limited	Limited	Limited	Limited	Encryption Not Using SekurSend
 Monitor Module Real time tracking views and Immediate recall of emails.	✓	✗	✗	✗	✗	✗

							
		SekurMail	Gmail	ProtonMail	Outlook	Zoho Mail	Tutanota
	Secure Calendar Create unlimited private calendars with customized views and advanced edition.	✓	Not Encrypted	Beta Version	Not Encrypted	Not Encrypted	✓
	Secure Task List Manage your everyday assignments in a secure and private environment.	✓	✓	✗	✗	✓	✗
	Automatic Data Export (ADE) Allow users to automatically export on premise or in any server they wish.	✓	Not Encrypted	Not Encrypted	Not Encrypted	Not Encrypted	Limited Function
	Email Migration Tool Easy migration from any Email provider.	✓	✗	✗	✓	✓	✗
	Private Domain Hosting Host any domain for business in Swiss hosted environment.	✓	✓	✗	✓	✓	✗
	NO Open Source Protection for each individual account using proprietary technologies VirtualVaults® & HeliX®.	✓	✗	✗	Not Encrypted/ Source Code Compromised		✗
	Service Runs its Own Servers Own server hosted in Switzerland. No third-party platform, no Big Tech platform (No AWS, Azure or Google Cloud).	✓	✗	✗	✓	✗	✗
	Data Not Accessible by the CLOUD Act. Entitles US to access data from US IT service providers or platforms (AWS, Microsoft, Google) even if the data is not stored in the US.	✓	✗	✗	✗	✓	✗
	Not Subject to the PATRIOT Act. Any information that you provide to GlobeX shall remain in our Swiss data centers.	✓	✗	✗	✗	✓	✓
	Swiss FADP Jurisdiction All data is protected under the Swiss Federal Act on Data Protection only.	Swiss	USA	Swiss	USA	India	Germany

Industries



Financial Services / Insurance



Government



Service Industry



Military / Security



Healthcare / Biotech



Logistics / Transport



Oil & Gas / Mining

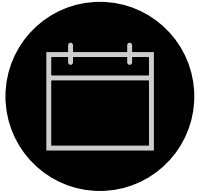


Telecommunications



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Distribution Model



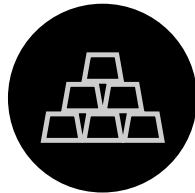
Monthly Recurring Revenues ("MRR")



Partners bear the cost of client acquisition

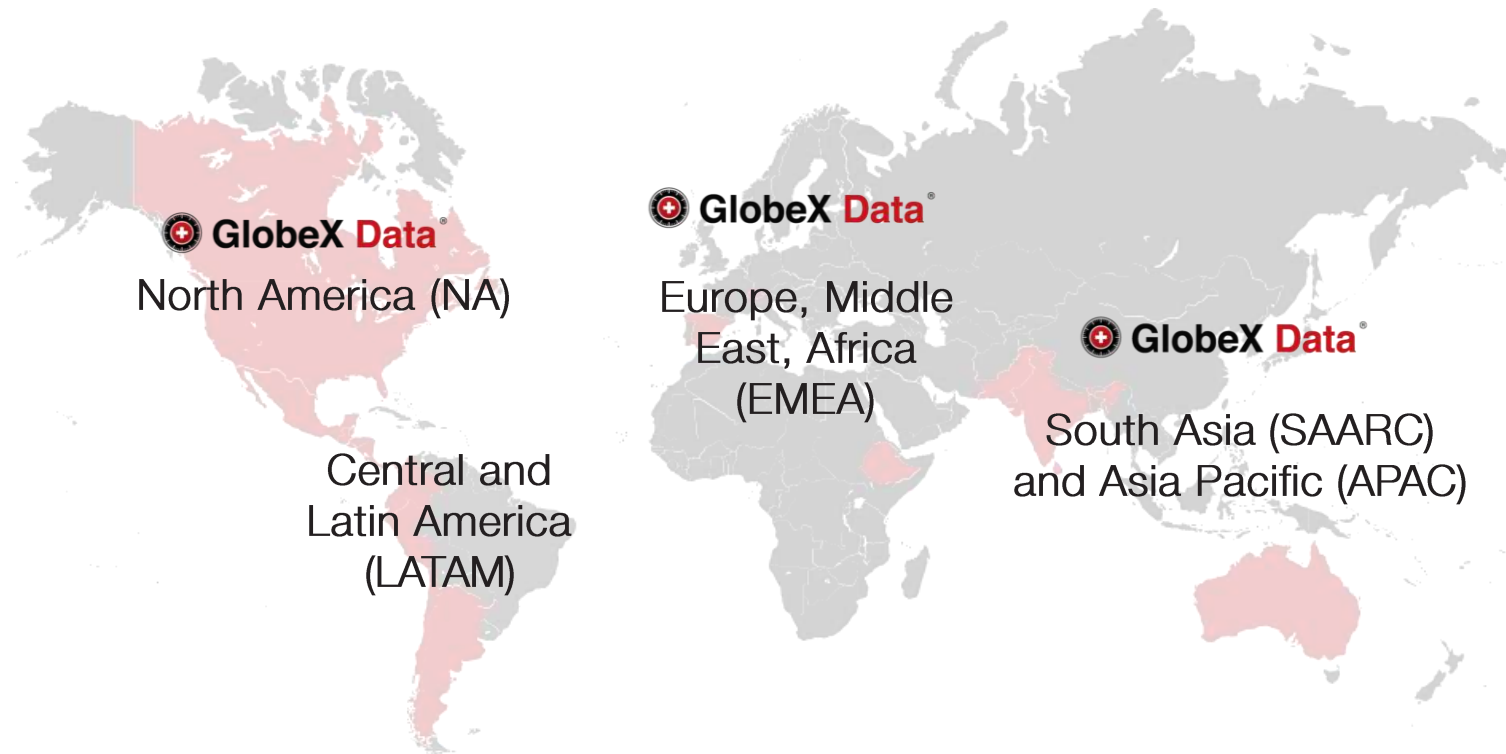


"Sticky" services. Once client uses services, they never leave.



Massive market of USD 500 Billion a year

ARPU US\$70/year Blended Direct and Wholesale



Global Partnerships

North America Partners (incl.
America Móvil 22+ MM
subscribers):



LATAM Partner
America Móvil:
300+ MM subscribers



Grupo Micronet 2000:
Cybersecurity Resellers in 10
countries in Central America
and LATAM



Micronet Spain 1000:
Cybersecurity resellers



Africa Partners with
Ethio Telecom 50 MM
subscribers



South Asia Partners:



SAARC and APAC Partners:
150+ MM subscribers

Our Unique Proposition



Compliance with the Swiss Federal Data Protection Law (FADP) and the Swiss Federal Data Protection Ordinance



Not Subject to U.S. Patriot act and U.S. Cybersecurity Act of 2015 or CLOUD Act of 2019



Proprietary technology such as VirtualVaults® and Helix® Technology
No Open Source



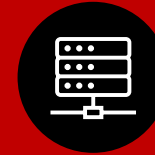
Industry's highest 2048-bit encryption standards and AES256 minimum encryption with biometric login credentials, triple-layer encryption



100% owned infrastructure No Amazon Web Services (AWS), Google infrastructure or Microsoft Azure cloud (unlike most competitors)



Unique environment for secure data and communication management with real privacy



All servers are inspected manually by internal engineering prior to configuration



Rich in features, unlimited scalability in more than 10 languages that serve consumers, SMEs and Governments

Share Structure as of Nov 2021



Listed on the Canadian CSE
exchange under ticker: **SWIS**



Listed on the US OTCQB
exchange under ticker **SWISF**



Listed on the Frankfurt Stock
exchange under ticker **GDT**

Outstanding Shares: **106,059,225**

Non-Tradeable Warrants: **11,275,000**

Tradeable Warrants: **5,692,000**
(Exercisable @ CAD 0.75/WT exp 07/2022)

Total Warrants: **16,875,000**

Management Escrowed Restricted Shares: **20,000,000**

Management Options:
12,000,000 (mostly at approx. US\$0.50)

Management and Directors Shares: **34,500,000 (33%)**

Cash on hand:
US\$ 7,250,000 No debt.



Directors and Executives Officers

Alain Ghiai - Founder, Chief Executive Officer, Director

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

Scott Davis, CPA, CGA- Partner, Cross Davis & Company LLP., CFO

Scott Davis is a Chartered Professional Accountant and a partner of Cross Davis & Company LLP Chartered Professional Accountants, 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 four years at Appleby as an Assistant Financial Controller. Prior to that, he spent two years at Davidson & Company LLP Chartered Professional Accountants as an Auditor, five years with Pacific Opportunity Capital Ltd. as an Accounting Manager and two years at Jacobson Soda and Hosak, Chartered Professional Accountants. Scott Davis obtained his CPA, CGA in 2003. Scott Davis has been a service provider to technology companies for over 8 years. He is working side by side with Alain Ghiai on the management of the finances of the Company.

Henry Sjöman, Director

Henry Sjöman has been an entrepreneur and angel investor since 1991. Henry 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 Sjöman co-founded Elcoteq SE in 1991, an electronics manufacturing company that was listed on Euro NASDAQ until 2010. He received his BSc, Telecom from the Kopings Tekniska Institut (Sweden), in 1974.

Henry is a Director of the Company, and a member of the Company's audit committee.

Amir Assar, Director

Amir Assar has over 27 years of experience in technology sales and leadership and is presently AVP Sales at Workday, Inc. (NASDAQ:WDAY), one of the leading software company in the world. Prior to joining Workday, Amir was one of the key executives at Adaptive Insights, where he was instrumental in establishing Adaptive as a leader in the financial data analytics market, culminating in an IPO filing in June of 2018 and eventual acquisition by Workday for US\$1.55 Billion in August 2018. Amir Assar started his technology career in 1993 at Actel Corporation as the Western USA Director of Sales. Actel was a leading provider of Field Programmable Gate Arrays (FPGA) and was acquired by Microsemi Corporation, 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 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 a fledgling start-up with no customers into a US\$300M business while transitioning it to be one of IBM's most successful acquisitions. He is married and lives with his wife in San Francisco, California.

Amir is a Director of the Company, and a member of the Company's audit committee.

BÖRSE
FRANKFURT
GDT

OTCQB
SWISF



GlobeX Data®

Swiss Secure Cloud and Communications

www.globexdata.com

www.sekur.com

www.sekursuite.com

corporate@globexdatagroup.com



[company/globex-data-ltd](https://www.linkedin.com/company/globex-data-ltd)



[@globexdata](https://twitter.com/globexdata)



[@globexdata](https://www.instagram.com/globexdata)