SECURE GROUP

Secure Communication Solutions for Your Industry Needs


Secure your business
data - it’s your most
valuable resource.

INDEX

WHY YOU NEED TO SECURE YOUR COMMUNICATIONS

Mobility has become the standard in communication. People cannot imagine themselves being physically restrained by a location to make a call, send an email, or engage in a chat session. Everyone has their smartphone with them at all times, enabling them to be connected to the world around: personal- and business-wise. Communication has become much more mobile, yet much more exploitable.

The threat landscape is evolving, and nowadays, cyber attacks are much more complex as they utilize whole networks of devices and try to break in through multiple end-points simultaneously.

Companies such as Google and Facebook, that facilitate much of today's communications, keep stacks of data on users and use it to create behavioral profiles of people. Their end-goal is better-targeted advertising, yet it comes at the price of privacy intrusion. However, such data could be collected and leveraged by other, ill-intended third parties.

What's evident by the news is the fact that technologies are now put to use by governments to produce cyber warfare for geopolitical digital wars. Cyber attacks are originating from everywhere – Russia, China, North Korea, and the USA are fighting for dominance over the Internet. In this online war, no one is safe, as was proved by recent scandals such as Brexit, the Facebook data leaks, and national power grid's glitches.

Government-owned attacks are mass collecting data to understand peoples' psychographics and use this information to destabilize society and gain political advantage.

HIGH STAKES

A failure to secure corporate data could have disastrous consequences.

The evolving threat landscape also puts powerful cyber weapons in the hands of hackers and parties trying to leverage corporate information. According to the 2018 Global Applications and Network Security Report[1], the average cost of a cyberattack on an enterprise is $1.1 million.

The techniques used include zero-day exploits, malware attacks, phishing, wiretapping, DDoS, MiTM, and online hacking. Such attacks are capable of turning any smartphone or mobile device into a spying tool, listening and watching the user's every move. To prevent this, enterprises must secure not only the network but its various end-points and ensure their employees are using security-hardened devices.

1 | https://www.techrepublic.com/article/cyberattacks-now-cost-businesses-an-average-of-1-1m/

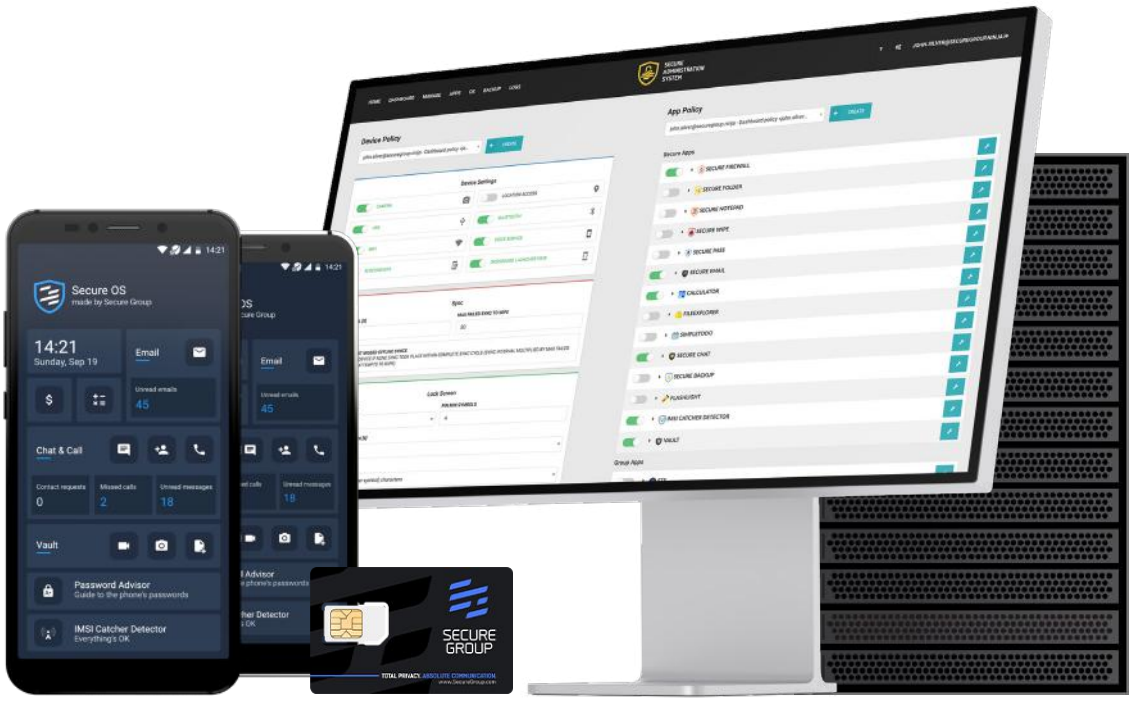
OUR SOLUTIONS FOR YOUR BUSINESS COMMUNICATION

Different industries have different communication needs. As a result, they face different threat models – which, in turn, calls for different security setups. There is no one-size-fits-all solution to secure your business communications. That's why Secure Group designed its products to be flexible, scalable, and meeting the needs of different sectors.

Our range of solutions starts with end-to-end encrypted communication apps and ends with a self-hosted enterprise secure communications centers.

To be able to answer every business's needs, we also provide the ability to integrate your corporate apps within our solutions, create custom applications and features, and even develop custom hardware models.

- End-to-end Encrypted Communications
- 360-degree Secure OS
- In-house Built Secure Hardware
- Instant Connectivity
- MDM with High Visibility
- Self-Hosted Enterprise Solutions



CONSULTING & ACCOUNTING

Companies in the consulting and accounting sector handle sensitive corporate information daily. This includes the financial books of clients, confidential business plans, personal information and credentials. This data is a goldmine for cybercriminals who can profit directly from it by using it to commit fraud or blackmail, or by reselling it to competitors. Hence, it is vital for companies in the sector to communicate, transmit, and store this data securely.

Confidentiality is part of the service clients pay for. Activities like accounting, audits, and consulting require elevated access to the books and records of client companies. If such information falls into the wrong hands, this may have disastrous business consequences for clients, and by extension for the consulting or accounting firm. Leaks happen at an alarming rate:

160 MILLION

compromised records with sensitive information per year.

- The total number of compromised records containing sensitive information in 2015 was 160,017,976[1].
- Every three months, there are over 100,000 reported cyber attacks against consulting companies in the USA alone[2].
- The cost attributed to account takeover (cybercriminals taking over businesses with the help of stolen credentials) is $ 5.1 billion in US alone[3].

These numbers are just the tip of the iceberg. They reveal that accounting and consulting companies are behind in the adoption of cybersecurity measures, compared to other high-stake industries such as banking and pharmaceuticals.

1 | https://www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_ tid%5B%5D=2122
2 | https://www.ft.com/content/f52f6fee-ccf4-11e6-864f-20dcb35cede2?mhq5j=e
3 | https://www.cpomagazine.com/cyber-security/account-takeover-fraud-is-the-new-normal-you-can-fight-it-without-losing-good-customers/

Industry Pain Points

As in many other industries, attacks in the accounting and consulting industry focus on employees and exploit their access to sensitive data or the corporate database. The main target of cybercriminals is the data of third-party entities – the clients. It could be collected by obtaining the clearance and credentials used by accountants and auditors to provide easy access. Other problems the industry faces:

- Emphasis on securing endpoints such as employee personal devices, rather than on corporate networks.
- Need for secure storage – cloud services provide convenience, but little in the way of security guarantees.
- Storing information on-premises instead of on the cloud collides with the need for employees to be able to access it from different locations and at different times.

These challenges outline the need for secure communications and storage of messages and documents on mobile devices.

Suggested Solution

Secure Group's approach to security combines strong encryption, securing app and device storage, and fixing the many inherent vulnerabilities of smartphones with modifications going as deep as the OS kernel and the boot-up process. In short, we protect sensitive information in transit, within the apps, and on the device. Only the user has the key to access communications.

- Use Secure Group's communication apps suite for end-to-end encrypted messages, calls, and emails.
- Transfer documents securely through the encrypted file-sharing functionality.
- Benefit from the device's and the apps' have encrypted storages: if the phone is stolen, the data from it still cannot be extracted.
- Trust the devices firewall to prevent phishing attacks; even in the extreme case that malware finds its way on the device, it cannot extract data from the apps.

BANKING & FINANCIALS

The financial and banking industry is among the primary targets of any crime, including cyber. The motive for fast capitalization is leading in such cases.

The client information that banks store is of high interest because it could be used to commit identity theft and fraud. To counter these threats, the banking industry needs to secure its internal network and communications.

At the same time, successful breach costs companies in the sector much more than the sums of money they will potentially have to restore. The reputational damage from the implication that a bank is ill-equipped to protect its customers' assets could cost it its business. Nevertheless, breaches do happen with alarming frequency:

68%

of banking and financial institutions admit they have been hacked.

- Financial institutions account for 35% of all data breaches[1].
- 68% of companies in the sector report they have been hacked at one point or another[2].
- Banks rarely announce the cost of breaches, but several cases have shown it can be in tens of millions US dollars.

Financial and banking institutions have responded accordingly to the threats by investing in cybersecurity. Companies in the sector have also been at the forefront of adopting security practices such as link encryption, two-factor authentication, EMV chips, etc. However, smartphones and mobile banking services have changed the industry landscape. They have also introduced new security pain points related to the inherent flaws in mobile devices.

1 | https://www.forbes.com/sites/insights-klgates/2019/01/15/what-financial-services-executives-need-to-know-about-data-security/#60a9a43d1e43
2 | https://www.imperva.com/lg/lgw.asp?pid=533

Industry Pain Points

Due to the essence of banking and financial companies' business, every part of it is a potential target for cybercriminals. The latter have adopted increasingly sophisticated, multi-step attacks that use an arsenal of techniques to extract pieces of data from various points. Once pieced together, this data can be used to inflict severe financial and reputational damage.

- Protecting data from such attacks calls for a holistic approach to cybersecurity which leaves no attack surface uncovered.
- Communications are always under threat of eavesdropping and interception due to the nature of shared information.
- Constant attempts to impersonate clients, steal their credentials, and get to even more valuable data.
- Phishing and spear-phishing attacks against bank employees and clients to steal credentials, infect devices with malware.

Suggested Solution

Secure Group has a range of products that offer strong resistance against online and offline hacking attempts, as well as enterprise-level solutions that can facilitate secure communications within an institution. Banks and financial institutions can:

- Use our encrypted apps suite to ensure the confidentiality of communications.
- Secure mobile devices against physical tampering through complex authentication algorithms and triple password protection employed by our software to guarantee the identity of the user.
- Benefit the security-hardened design to withstand malware, phishing attacks, and compromise of software.
- Reduce the attack surface of the encrypted mobile desices: through our mobile device management solution – Secure Administration System (SAS), admins can granularly control features and policies.
- Deploy our solutions on the organization's infrastructure, ensuring higher system integrity and data security. The technique helps banks and financial institutions establish control over internal sensitive communication, and visibility into various user groups.

PHARMACEUTICALS

Where information is of high value, cybercrime is sure to follow. The pharmaceutical industry is a primary example of that. Drug formulas, patents, and R&D data are some of the most valuable assets in this trillion-dollar industry. It is of vital importance for companies to protect their intellectual property and communications.

According to the European Federation of Pharmaceutical Industries and Associations:

$985
MILLION

is the cost of bringing a new drug to market.

- It costs an average of $985 million to bring a new drug to market.
- The time it takes to bring a new drug to market is 12-13 years on average.
- Only 1 in 10,000 synthesized drugs makes it to consumers.

Because of the above, snatching a market-ready formula – possibly, before it is patented – is a huge benefit for a competitor. It would allow the company stealing the design to save money and time while sparing itself the risk of investing in dead-end research. At the same time, a breach is a major setback for any company engaged in rigorous R&D activities.

Thus, it is not a very big surprise that two-thirds of pharmaceutical companies report serious data breaches. A quarter admit to have been hacked.

Industry Pain Points

The big problem of pharmaceutical companies is data leaks. The latter happens through deliberate outside attacks and insiders. Because of that, it is a necessity for pharmaceutical companies to protect their networks and communications from outside interference. Also, they must enforce strict clearance levels internally. Secure communications are one of the pillars of any holistic strategy for protecting intellectual property.

- Leaks happen through outside attacks, with deliberate or unintentional employee cooperation.
- Complications if the company's operations are spread geographically over multiple locations: headquarters and R&D centers can be in different countries; the company can be present in multiple markets.
- Need to secure incoming and outgoing messages against eavesdropping and interception.
- Necessity for control over employee communication devices to help prevent internal leaks.

Suggested Solution

Our products offer different levels of security and control while remaining scalable and compatible with any infrastructure and setup. Our solutions for the pharmaceutical industry's communication needs allow organizations to:

- Rely on the VoIP encrypted group and video calls to facilitate safe long-distance communication with other locations of the organization.
- Use a fleet of secure communication devices to protect sensitive data.
- Assign different clearance levels for various user groups.
- Use our mobile device management solution: Secure Administration System (SAS), to control features and sensors on an admin level granularly. Assign policies to single or whole fleets of devices, to further limit the attack surface.
- Deploy a self-hosted version of our solutions that guarantees higher system integrity and data security. The technique helps companies establish control over internal sensitive communication and visibility into various user groups.

ENERGY

The energy industry is a volatile one. A shift in one company's operations could cause a domino effect and disrupt entire markets and economies. In a sector like this, information is a high-value asset, and the security of communications is a vital part of protecting that information.

77%

of energy companies register a rise in successful cyber attacks.

Due to the geopolitical significance of natural resources and energy, the industry faces high-profile cyber adversaries, including governments. Companies in the sector have reportedly registered a 77% rise in successful cyberattacks against them in the past year[1].

At the same time, the sector requires stakeholders and executives to be on the move constantly. Traveling means switching networks, carriers, operators, and regulations all the time, as you go over state and national borders. This gives too many third parties potential access to communications that ought to be confidential.

For example, an executive from an energy company might have to undertake a trip to a foreign country to negotiate a deal, or to attend an industry summit. The moment they land on foreign soil, their smartphone connects to the local network, run by the local carrier. Like any mobile operator, including the ones in the persons' home country, this is a company that has elevated access to that person's communications.

1 | https://www.tripwire.com/company/press-releases/2016/04/tripwire-study-energy-sector-sees-dramatic-rise-in-successful-cyber-attacks/

Industry Pain Points

The energy industry faces many of the same challenges as accounting and consulting, and banking and financials. Securing communications is a must due to the nature of the shared information. So is the necessity to use devices that can resist hacking attempts. There are several extra pain points added by frequent traveling:

- Local carriers and, by extension, foreign governments can access the communications data if it's not encrypted.
- The same have access to metadata about the communications: the time a message was sent, who it was sent to, from what specific location, etc.
- Carriers can locate a person by monitoring which cell tower their device is connected to at any given moment.
- They can also push software, including malware, on the device.
- Network operators can hamper communication by cutting off a specific device's access to the network.

Suggested Solution

Naturally, a security-wary traveler has to seek a way to remove local network operators from the equation. And if they are not able to do that – at least hamper the carriers' ability to access communications by encrypting them. With Secure Group's solutions, we offer a use-ready device for many of the challenges outlined above:

- Leverage the instant connectivity and unlimited data coverage worldwide that the Secure multi-IMSI SIM card provides. Due to the card having multiple IMSIs, it can switch between providers to offer the best signal.
- Remain connected even if a carrier decides to shut down its network for a user.
- Secure all incoming and outgoing communications and the device's storage with state-of-the-art encryption.
- Avoid wiretapping attempts through device's built-in IMSI-Catcher Detector.

SECURITY & DEFENSE

Secure communications are of fundamental importance for the security and defense sector. The sector is where most advancements in cryptography came from because data leaks could be fatal nation-wise and globally. On top of its encrypted products and services, Secure Group offers innovative approaches to connectivity and infrastructure independence that bring security one step further.

As the value of data is rising, the threat landscape is evolving rapidly. Mobile technologies, due to their architecture, are the most easily exploitable end-points, carrying large amounts of sensitive information.

$120 BILLION

were spent globally in 2019 to combat cybercrime.

The state of the inudstry calls for a holistic approach to mobile security, which combines strong encryption with minimizing the role of third-party operators and server infrastructure. Security companies need strong end-to-end encryption and secure devices, designed to withstand hacking attempts and physical tampering. On top of that, they need MDM capabilities to micromanage the solutions and different user groups.

Industry Pain Points

Mobile communications are a tricky field regarding security, to begin with. The way the regular cellular infrastructure operates leaves a number of attack surfaces and vectors and gives elevated access to multiple third parties. There are several general concerns about the security of mobile communications:

- Network operators have elevated access to mobile communications' content and metadata.
- IMSI-catchers – the surveillance technology used by law enforcement for wiretapping purposes – is now widely available to other parties, including criminal organizations.
- Vulnerabilities in the SS7 protocol used by all networks offer almost unlimited options for location tracking of devices and, by extension, individuals.
- Communication apps and services rely on third-party infrastructure, with little or no guarantees that messages aren't stored and read.
- Mobile devices are inherently vulnerable to hacking and malware infections.

Suggested Solution

Secure Group's products are designed to offer a combination of security, control, and versatility. Our software uses strong encryption to secure communications. Our devices have zero-attack-surface. They are all micro-manageable and customizable through SAS. We have also developed a way to make the service deployable on different infrastructures, as well as to make the apps compatible with equivalent services by third-party providers. Our solutions enable organizations to:

- Run a secure communications center by self-hosting our solutions and operating a network of secure communication devices. Ensure higher system integrity and data security and establish visibility into various user groups.
- Rely on the phones for secure communications – all ingoing and outgoing communications, plus the storage, use strong end-to-end encryption.
- Resort to the device's duress features if necessary – phone's storage and memory can be erased remotely with SAS, or automatically if the device is isolated from the network or in case of physical tampering.
- Request a custom solution. For example, we can design and develop rugged hardware models, ensuring that they will withstand extreme field conditions. Secure Group's hardware models are in-house built, security hardened, and tested by rigorous quality assurance procedures to guarantee zero-day-integrity.

LEGAL PROFESSIONALS

Law firms, lawyers, and other legal professionals are usually a target for cyber attacks, due to the sensitive information they possess in regards to their professional activities.

96%

of devices that are taken away are then searched for sensitive data.

Lawyers are obligated to protect the confidentiality of their clients' data, and law firms have to pay closer attention to confidentiality than the average business. If law firms do not secure their client communications and other data, they could violate the attorney-client privilege, lose clients, be subject to malpractice actions, damage their reputation, and possibly also lose their license to practice law.

Unencrypted communication via regular smartphones can easily be intercepted by state agencies, spying parties, and even private individuals. While the law prohibits the wiretapping of lawyers and requires that intercepted communication that comes from lawyer-client communication to be destroyed, it does not fully guarantee their privacy.

Numerous clients refuse to share sensitive information on a mobile call or are afraid to drop an email. To practice the legal profession with the expected degree of reliability, you need to use mobile encryption to guarantee the secrecy of your conversations with clients and partners. With our multi-layered mobile solutions, you can rest assured that your data won't end up in the hands of third parties.

Pain Points

Nowadays, law enforcement officers no longer have a monopoly on surveillance technology. Stingrays and IMSI catchers, SS7 hacks, and malware infections are all also available to cyber criminals. Here's why confidential communication is so important for legal professionals and law firms:

- Industrial espionage occurs in many sectors, and the nature of the information shared with lawyers makes them potential targets for eavesdropping.
- In criminal investigations, intercepted communication can help the claimant to prepare for the planned legal defense and perhaps even refute it.
- If a client approaches a lawyer for advice about a potential seizure, that communication alone is enough for law enforcement officers to freeze the client's accounts.

People who have legitimate reasons to worry about surveillance need a complete approach to mobile security. It boils down to understanding surveillance technology and the vulnerabilities it exploits. Once you know what to look for, you can choose the right tools to secure your communications.

Suggested Solution

The above is an integral part of Secure Group's mission as a company. We believe that that technology should be a means to enable perfect communication secrecy, rather than a barrier.

Secure Group offers end-to-end encrypted communication solutions, designed to guarantee the confidentiality of peers' correspondence and protect sensitive data. It combines strong encryption for communications with modifications on the device that make it resistant to hacking. Organizations that choose us can:

- Rely on Secure Group's mobile solutions for communications – join P2P and group chats, make and receive VoIP calls, send emails, and transfer files thoroughly secured through end-to-end encryption.
- Use the IMSI-Catcher Detector to spot suspicious network activity that could be a symptom of wiretapping attempts.
- Count on the data-at-rest security techniques that encrypt the application's databases and the physical storage, ensuring no software or physical tampering can extract data from the device.
- Use the device's wipe capabilities to erase sensitive information if necessary; set up a duress password that can wipe the phone from the lock screen.
- Leave no trace online – the device doesn't feature Internet browsing or Google Services, which limits tracking options significantly.

SECURE YOUR BUSINESS DATA

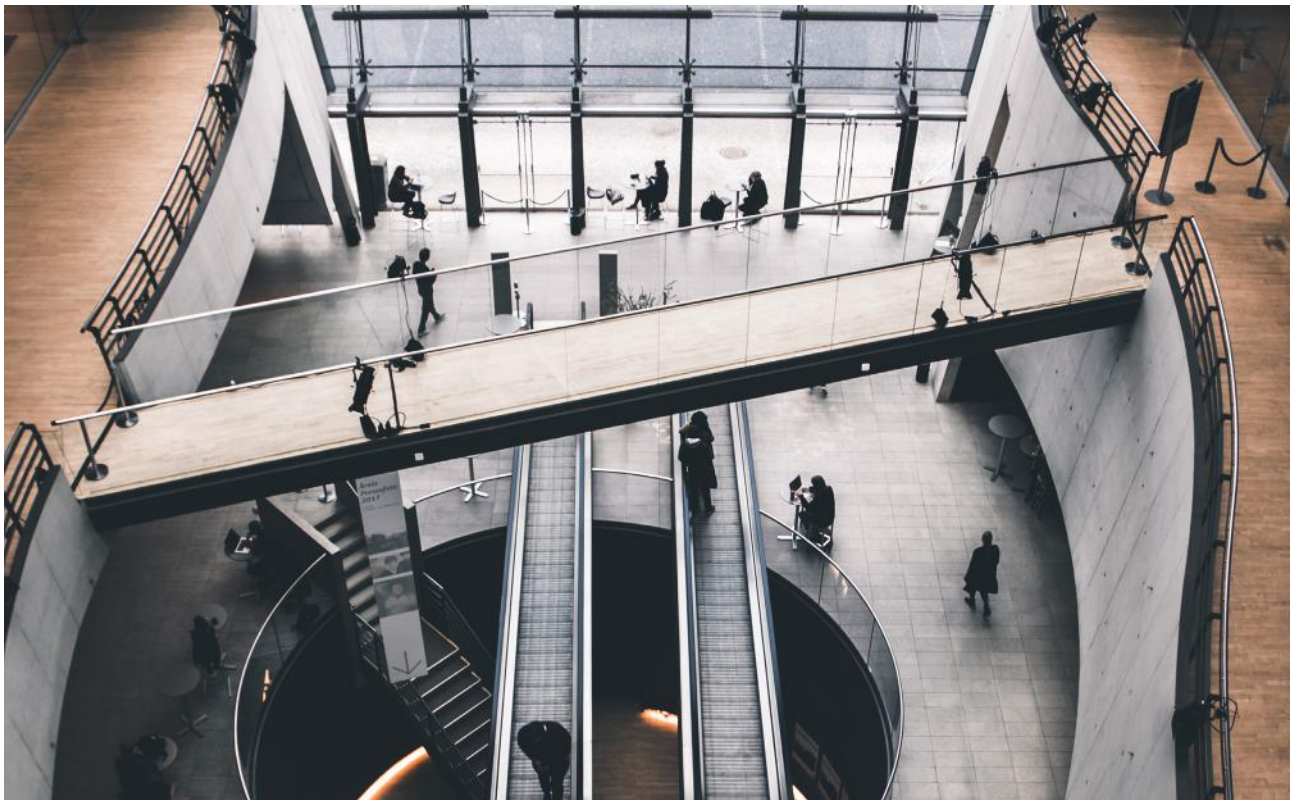
In a digital world, data is your most viable resource used to scale-up your business. This sensitive information is, respectively, a target to attacks, that aim to steal and leverage it for the means of third parties. Mobile technologies, due to their architecture, are your most vulnerable link.

To ensure your mobile data is thoroughly secure and your communications are absolutely private, Secure Group offers end-to-end encrypted mobile solutions with multiple defense layers countering any threat.

In this world, where the digital threat is evolving because the value of data is rising, our goal is to make cybersecurity as accessible as possible. This is why we've taken rigorous measures to ensure our solutions can be customized to fit perfectly the business needs of each organization.

With the state-of-the-art mobile security offered by Secure Group, data protection, and conversation privacy is but a choice.

Contact us to find one of our solution providers in your region, and choose to secure your business data today because tomorrow might already be too late!



CONTACT US

Contact number:
+359 2 42 44 222, ext. 609

Email:
sales@securegroup.com

Web:
www.securegroup.com

Address:
130 Simeonovsko Shosse Blvd.
Sofia, Bulgaria