SERBUS LIMITED

PORTFOLIO

MOBILE DEVICE SECURITY

SERBUS

securing the remote worker

2021 V1.1

CONTENTS

SERBUS

securing the remote worker

SECURING THE REMOTE WORKER

ABOUT US

Who We Are

Established in Mar 2010, the founders, and co-directors, are former UK Special Forces

The cornerstone of our excellent team is the culture that runs at its core. All team members are selected on attitude first and professional skills thereafter.

This approach has made Serbus the high-performing company it is today.

What We Do

Secure Mobile Communications.

What Matters To Us

Uncompromising Excellence.

How We Do It

We focus on you.

- You will meet a friendly, diverse and highly professional team
- We each understand our vital role within the team
- We know the importance of our actions
- We strive for excellence
- We establish your operational needs
- We produce your system design
- We build and commission your system
- We support you during the build
- We support you when the system is operational
- We are with you for the journey

Our personnel are security cleared in accordance with UK Government standards.

We focus on security - leaving you to get on with your business

SERBUS SECURE

SECURE COMMUNICATION, MOBILE DEVICE SECURITY, SECURE HOSTING

What is Serbus Secure?

Serbus Secure is a fully managed suite of secure communication, enterprise mobility and mobile device security tools.

Why Serbus Secure?

Simply installing an end-to-end encrypted messaging app, such as WhatsApp, on your devices does not constitute mobile device security.

Mobile device security takes a centrally managed and multilayer approach.

Consideration should be given to:

- Permitted applications
- Permitted web browsing
- Security of communication
- Device restrictions & monitoring
- Server location, security & monitoring
- How your data is handled and who has access to your data
- How to ensure centralised management, control and compliance of your mobile devices

With Serbus Secure you can be sure that your devices are secure, your teams are equipped with the tools to work remotely and securely, and your fixed infrastructure will be protected from the threats of unmanaged and unprotected mobile devices.

Serbus Secure is available as an on-premise, hosted or hyrbid solution. It is also available as a fully managed **Operational Capability as a Service (OCaaS)**, where we look after all of your hosting requirements, leaving you to get on with your core business.

SECURE VOICE & MESSAGING

GOVERNMENT GRADE END-TO-END ENCRYPTION

At the heart of our systems is a secure voice & messaging application. The application is approved by the National Cyber Security Centre (NCSC), which is the UK's independent authority on cyber security.

Key Features

- Voice, messaging and video
- Full conferencing facility (Audio, video & screen share)
- Share images, documents and video files
- Compatible on iOS, Android and Windows PC
- Centrally managed address book
- Press to talk (PTT)

Security

- Centrally managed (by Serbus or your organisation)
- Absolute control of your cryptographic material
- Monthly, over the air, crypto updates
- Choice of server hosting locations (or host your own)
- End-to-end encryption (between sender and recipient)
- Independently certified
- Closed communities / security domains (can be inter-connected)(NCSC), which is the UK's independent authority on cyber security.

Secure Comms Partners

We are pleased to offer Government grade secure voice and messaging, in association with our valued partners Armour Comms and Cryptify.

Armour Comms

cryptify

MOBILE DEVICE SECURITY

Our mobile device security provides an enhanced level of protection from threats that lead to data breaches, from a loss of data as a result user error and from gaps in your security systems.

Supported devices include IOS and Android smartphones, tablets and laptops.

Mobile Device Management

With our mobile device management you can centrally control the security settings of your mobile devices, manage permitted applications, control confidential information, remotely lock/wipe devices and ensure your mobile device security is compliant with the National Cyber Security Centre best practice and guidance.

Endpoint Security

Equipping and enabling a remote workforce also means allowing remote access to your fixed network and infrastructure. Endpoint security provides protection for your organisation by monitoring the devices, files and processes that are accessing the network.

Endpoint security constantly scans your remote connections and can provide early warning when a threat is detected. Your security teams, or Serbus, monitoring the network will then be alerted and can intervene before any damage is done.

If you chose our fully managed service (OCaaS), our team of highly experienced engineers will keep your network safe on your behalf, leaving you to get on with your business.

VPN

Our VPN connection prevents unauthorised eavesdropping of your traffic, allows remote workers secure access to your network and ensures your sensitive data is transmitted safely. A well implemented VPN also masks your IP address when using the internet, which further contributes to the safety and security of your remote work force.

Threat Defence

Threat defence provides continuous protection of your mobile devices. This protects against iOS and Android threats, so that vulnerabilities resulting from user behaviour and security gaps can be minimised.

Secure Web Browsing

Secure web browsing enables your teams to remain productive and secure, whilst providing access to essential web based material and content. This protection keeps your teams, and their devices, safe from a multitude of internet-based threats.

SECURE HOSTING

ON PREMISE, HYBRID, OR MANAGED SERVERS

Your operational requirements will determine the optimal server technology, server location and security environment.

Serbus is highly experienced at building, deploying and supporting entire systems that are physically located at the customers premises, or hybrid solutions with servers located at multiple sites.

Operational Capability As A Service (OCAAS)

Serbus also offer a fully managed Operational Capability as a Service (OCaaS), where we look after all of your hosting requirements, leaving you to get on with your core business.

- Fully managed, ticketed, service support desk
- Secure hosting environment
- Infrastructure backup and restore, aligned to NCSC Good Practice Guide (GPG)
- Protective monitoring/system monitoring (SIEM) and regular vulnerability assessments (VA's)
- Independent system penetration testing
- Maintenance and support by fully vetted staff
- Serbus has no access to sensitive business information

SERBUS SECURE

PRICING

Serbus Secure is a bespoke solution built to meet the exact needs of your organisation. Customer specific requirements include, but are not limited to:

- Number of users.
- Secure voice and messaging application only or enhanced device security, with centralised device management and access to the Serbus support desk.
- BYOD, customer or Serbus supplied devices.
- Type of devices (iOS or Android).
- On premise hosting, Serbus hosting or a hybrid solution.
- Secure browsing.
- Device monitoring.
- Access to business specific applications.
- Integration with additional customer services.

Indicative Pricing

Year one pricing, excludes airtime.

1. Small deployment of 10 users

Entire system built and managed by Serbus. System to include secure voice and messaging, Serbus hosted servers, centrally managed security with MDM enrolment, Serbus support and system administration, Serbus supplied iPhones, 24hr device monitoring, with threat defence.

Price £30,000.00 + VAT

2. Medium deployment of 150 users

Entire system built and managed by Serbus. System to include secure voice and messaging, Serbus hosted and AWS hosted servers, active monitoring of AWS hosted elements, centrally managed security with MDM enrolment, Serbus support and system administration, Serbus supplied iPhone XS, 24hr device monitoring with threat defence, supply of CMS laptop, secure internet browsing, system design documentation for accreditors, hand delivery of devices, user training.

Price from £220,000.00 + VAT (subject to hosting requirements)

A fixed price, no obligation, quotation will be provided following detailed discussions regarding your specific requirements.

PARTNERS & SUPPLIERS

Serbus work with industry leading partners to ensure we are always using the latest technology and tools. Serbus take these tools and integrate them into our Serbus Secure platform to deliver a highly secure, fully managed system that provides a seamless user experience.

Airbox

Airbox provides a comprehensive suite of Situational Awareness tools for both desktop PCs and mobile platforms. Airbox software is trusted by Law Enforcement, Military, Special Forces, Search & Rescue, Fire and Medical Emergency Services around the world.

Armour Comms

Armour Mobile provides secure voice calls, video calls, messaging and group messaging, voice and video calls, file attachments and the option for messages to automatically delete once read or after a set time.

Cryptify

Cryptify Call provides end-to-end, encrypted, secure voice and messaging on managed and unmanaged BYOD and business devices running IOS and Android. It also runs on Windows PCs for use from offices or deployed operational control rooms.

Garrison

Ultra Secure Browsing - Garrison's technology isolates your endpoint from risky websites, remotely transforming all web content to a verifiably safe format. Garrison SAVI® (Silicon Assured Video Isolation) delivers a truly isolated browser in an integrated, user-friendly experience.

Getac

As one of the leading rugged computer providers, Getac offers extensive rugged computing product lines including laptops, tablets computers. Getac serves a wide range of vertical markets including military & defence, law enforcement, public safety, emergency services, utility, natural resources, oil and gas, telecommunications, transportation and industrial manufacturing.

Instant Connect

Next-generation Push-to-Talk. The Instant Connect Enterprise™ dynamic frontline communications platform provides seamless mission-based talk groups – connecting team members sharing tasks, workflows, and missions – for today's fast-moving workforces. The software can provide voice and data services connecting any mix of mobile, radio, IP, and telephony devices.

Mobile Iron

Mobile device management (MDM) is the foundation for a secure mobile enterprise. It provides a comprehensive way to quickly onboard and secure a vast range of employee devices coming into the enterprise.

Samsung

A complete suite of enterprise mobility solutions designed to keep your work phones, tablets, and wearables under IT control. Protect confidential files, credit card transactions, passwords, and all critical data.

TAK

CivTAK - The Android Team Awareness Kit (ATAK), for civilian use, or Android Tactical Assault Kit (also ATAK) for military uses - is a suite of software that provides geospatial information and allows user collaboration over geography.

Galaxkey

Email Encryptio - Every message you send is carefully wrapped in three layers of protection. Works with all popular systems (Outlook, iOS, Android, Windows) to protect your emails in transit and at destination.

Zello

Zello Push-to-Talk (PTT) Mobile App

- Talk in real-time to individuals and groups anywhere in the world.
- Use any smart device and mix all WiFi/data networks.
- Configure settings and channels of up to 10,000 users.
- Customize with accessories, like headsets, microphones, and rugged devices.
- Mix and match any device, network, and accessory combination.
- Cloud, or on-premise, hosting.

CASE STUDY 1

COMMERCIAL INSURANCE

The Client

A UK industry leader in commercial insurance.

The Brief

In 2018 our client came to us after their compliance and information security teams identified potential security weaknesses across particular job functions, in relation to the storage and transfer of customer data within the business.

With the GDPR deadline fast-approaching, they enlisted Serbus to present a solution that would ensure full compliancy when it came to their employees use of mobile devices throughout the business.

The Consultation

To better understand how the company functioned, what their current processes were, and how their people used mobile devices on a day-to-day basis, we went to meet with the client for half a day. This provided valuable insight for our project management team and established the understanding needed to create a bespoke Serbus Secure solution for our client.

Following our consultation, we presented our recommendations to the client which included a managed MDM, secure voice and messaging, secure browsing and a VPN for secure connectivity to business critical tools. The suite of products provided enhanced productivity for the employees and ensured compliance requirements were met across the entire mobile workforce.

Cont...

COMMERCIAL INSURANCE - CONT

We also set up a complimentary trial of key components of the Serbus Secure solution within a cross-section of their workforce. This afforded us the opportunity to demonstrate the effective integration of Serbus Secure and provided the client with preliminary insight into how the solution could be implemented within day-to-day business activity.

The Implementation

The initial trial lasted 10 working days with 20 devices. The client was very satisfied following the trial period, and asked us to scale up the project to 85 devices on a 12 month contract, with the Serbus support team managing the entire system, which included the MDM, crypto keys and key monthly updates.

Over the last 12 months the system has grown to 223 managed devices across both mobile devices and Windows desktops and additonal services have been added which are now hosted on-premise. We have supported the client as the requirement has grown and provided training and support, as required, to their IT teams and end users.

The client can now conduct all calls securely, hold secure conferences, send secure messages, share files and access business tools whilst working from their mobile devices.

The Feedback

In a recent review with our account management team, the client reported the following:

> “Since using Serbus Secure we have been so impressed with how simple and easy to use the product is and the ease of centrally managing the team’s devices. Our team have commented that they now feel much more comfortable sending and receiving sensitive information from their mobile devices and have also noted the high quality of the secure voice and video conferencing.”

Additionally, the client has told us that the implementation of Serbus Secure has improved productivity across their sales team, as the team no longer has to use protracted and inefficient ways of sending and receiving client data while on the road.

CASE STUDY 2

VC BACKED FINTECH PROVIDER

The Client

A VC backed FinTech provider with 4 years trading history, a senior leadership team of 8 executives and an account management team of 32.

The Brief

In early 2020, one of the UK's fastest-growing, London-based, FinTech companies approached us to assist in strengthening the safety of their information security.

In a highly-regulated industry, it was vital to our client that they ensure security and compliance when handling data within their organisation. They also wanted to ensure that their mobile workforce were given the tools to communicate and transfer sensitive data securely when working remotely and from their mobile devices.

The Consultation

We went to meet with the client for half a day to establish how the business operated from an internal communications perspective. Our consultation highlighted the nature of the information being held, sent and received by both the senior leadership and account management teams.

This afforded our project management team excellent insight that allowed them to create a custom Serbus Secure solution that would best protect our client, and ensure that their processes were compliant and in accordance with FCA regulations.

The Implementation

It was proposed and agreed that the client would start with 20 Serbus Secure configured iPhone 8 devices that would be used for business purposes only. Two completely

FINTECH - CONT

separate, secure domains were created; one for the senior leadership and one for the account management team. Each domain was provided with secure voice, messaging and conferencing at the core of their systems.

Secure email was also implemented, along with Threat Defence and a secure VPN to ensure that devices remained safe and secure when users were working remotely, sending emails and browsing online. The client's system and devices were ordered, delivered, and operational in 20 business days.

In the light of working restrictions imposed as a result of the recent COVID-19 pandemic outbreak, our client has since added more devices and an additional domain for their business operations team, to better ensure a safe, secure and compliant home-working situation for employees.

The Feedback

With a total count of 47 mobile devices operational and managed by the Serbus support team, our client has shared the following feedback on our service over recent months:

"After our initial meeting with Serbus we were very impressed with how quickly they put together such a detailed and thorough proposal that took into account our business needs."

"Serbus Secure is such a brilliant fit for our leadership team to communicate business critical information in a timely way when we are rarely in the same place."

"We love the secure conferencing facility. We can now make important business decisions, host team meetings and share important data while everyone now needs to work from home."

"Serbus support team has been really flexible and responsive whenever we have required to adapt the way we work or setting up new users."

CASE STUDY 3

PHARMACEUTICAL

The Client

A fast-growing, innovative, UK pharmaceuticals company.

Established 5 years ago and now operating with 30 staff across two sites, with a recent turnover of £35 million.

The Brief

In the Summer of 2019, our client came to us for assistance at the same time that they were bringing a new product to market.

The product itself was set to provide a radical and innovative edge to the industry. Having been beaten to market with previous products, due to lapses in their company information security, they were keen to prevent further IP losses by tightening their communication systems and process.

The Consultation

We met with the client and were quickly able to ascertain that their IP could be potentially compromised through the sharing of critical data between employees. Their product was being designed, tested and developed across two company sites, between multiple teams, and was therefore a key target for industrial espionage.

Off the back of our meeting, having ascertained the client's needs, our experts designed and implemented a Serbus Secure system that gave the client a centrally managed MDM, secure voice and messaging, group messaging, secure conferencing, threat defence and a mobile VPN.

To ensure data remained securely on their site, we built a bespoke on-premise system that would enable our client's research, design and operations teams to collaborate and communicate securely.

PHARMACEUTICAL - CONT

The Implementation

The client was provided with their brand-new, Serbus Secure iPhone 8 devices; 18 in total to span 3 teams. A secure mobile VPN provided additional security when using the IOS and Android applications; strengthening the devices against malicious targetted and untargetted attacks.

Secure voice and messaging provided the teams with instant secure voice calls, secure messaging and secure conference calls to conduct their day-to-day work safely and securely.

Secure conferencing gave the teams the ability to hold project meetings without the risk of cyber attacks that are all-too common with other mainstream video conference platforms. We joined the 3 domains to allow different parts of the business to communicate both within their own teams and the wider company. A gateway was also installed at the client's telephone exchange in order to provide mobile devices the ability to directly and securely communicate with landlines.

The MDM gave their IT team the ability to only allow white-listed applications to be installed on their mobile devices, again reducing potential attack vectors and the potential for accidental information loss. Threat defence also actively scanned for threats to mobile security via apps or external hardware, eradicating any chance of successful industrial espionage attempts and subsequent loss of IP.

The Feedback

In a recent report from the client to our account management team regarding their experience of the Serbus Secure solution and of our service, they said:

"The secure voice and messaging application is so easy to use and has such strong call quality that we now use it as our primary way to communicate across our business."

"Serbus Secure gave us the ability to get our new product to market without the fear of losing our IP to a rival company. This meant we could spend extra time refining the quality of the product in the knowledge we didn't have to rush it to market."

SERBUS
securing the remote worker

Contact Us

Serbus Limited
The Granary
White Hall Farm
Hampton Bishop
Hereford
Herefordshire
HR1 4LB
UK

+44 (0)1432 870 879
info@serbusgroup.com
www.serbusgroup.com

CYBER
ESSENTIALS
PLUS

QMS
ISO
9001 : 2015
REGISTERED
Certificate No. 286172018

Crown
Commercial
Service
Supplier