THE FUTURE OF SECURE COMMUNICATIONS

How BlackBerry's SecuSUITE is changing the way governments and enterprises communicate

In an increasingly dangerous world, governments today are facing an unprecedented challenge: how to keep their citizens and institutions safe while still allowing for the free flow of information. To meet this challenge, governments must find effective ways to protect sensitive communications without getting in the way of critical government operations and missions.

The Myth of Secure Voice Communications

Worldwide, communications — from phone calls to text messages — are being compromised and intercepted at rates never seen before, putting people and missions at extreme risk. Meanwhile, communication pathways are changing rapidly. Rather than traditional landlines, most people today use mobile and wireless networks to communicate.

That shift doesn't make communication safer, but actually broadens the "attack surface." In fact, it's surprisingly easy to eavesdrop on or monitor modern mobile devices, even over the latest LTE and 5G networks. The vulnerabilities of these systems are well known and are routinely compromised using methods ranging from fake cell towers and other "man-in-the-middle" (MITM) interceptions to identity spoofing in which cybercriminals fool you into sharing information with people you think are trustworthy, but are really imposters with nefarious aims.

Government employees may not think about security when using mobile devices. And while the interception of a single conversation by itself may not be of concern, when aggregated and analyzed with other communications, they can have devastating results.

Fighting Back

For years, governments have been actively seeking to protect against these security threats and vulnerabilities. Many have developed sophisticated and highly specialized systems for securing top secret and classified information and communications.

For the most part, however, these legacy systems are both expensive and hard to operate. Most require special equipment — such as bulky "Frankenstein" phones — that stand out in a crowd and can compromise sensitive missions.

To work around these limitations, government employees and contractors often resort to using burner phones and other devices that are purported to evade hackers and eavesdroppers. Lacking a secure communications capability, some users have taken the risky route of using their personal devices — often with uncertified applications — for sending texts and making calls. Beyond this, they have confined their sensitive conversations to protected facilities — or more often, simply tried to avoid speaking or texting about sensitive and classified topics altogether. All of these options are less than ideal and can place severe limitations on critical missions.

Many competing solutions claim to deliver secure voice communications, but most offer little more than consumer-level messaging solutions with encryption capabilities added on top. Few of these solutions are suitable for higher-level sensitive or classified communications.

Hacking Your Phone

It's easier than you think to break into cell phones and mobile networks. Witness the recent wave of intercepted mobile and wireless communications.

- U.S. congressman's communication line hacked
- U.S. President's Chief of Staff's cell phone compromised
- Multiple rogue cell towers discovered in Washington, D.C.
- Russia targets NATO soldiers' smartphones
- Bank accounts hacked using SS7 vulnerability to intercept security codes
- Secretive cellphone surveillance uncovered by Canadian police
- Canada's two largest telecoms vulnerable to international hackers
- FBI investigates texts impersonating U.S. Vice President's Press Secretary sent to members of Congress

"A voice or text conversation over a consumer messaging app should be considered as a conversation between two individuals in a public space, such as a bus stop or coffee shop. Some level of anonymity and privacy should be expected, but there are some enterprise conversations that must take place in a private room."

– Gartner[1]

Introducing BlackBerry's SecuSUITE

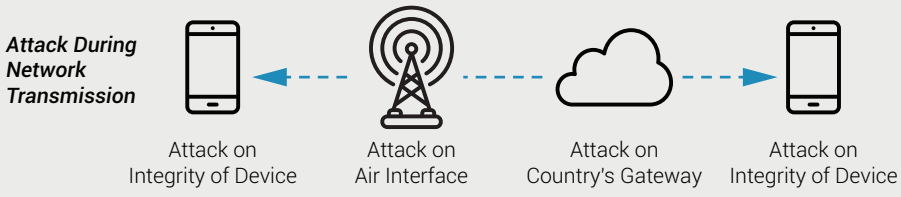
Now there is a better way to protect against cyberattacks and to secure communications in the most sensitive missions and locations. It's called SecuSUITE® and it's from BlackBerry, a world leader in secure communication services. SecuSUITE was built from the ground up with an overarching purpose: protect the most sensitive and mission-critical communications for governments.

Most people know BlackBerry as the maker of the legendary email-friendly smartphones. For decades, it had produced the most secure commercial mobile devices on the market. Building on that legacy, SecuSUITE voice and text communications provide protection on standard iOS® and Android™ devices at all security levels, from Sensitive But Unclassified (SBU) and Controlled Unclassified Information (CUI) to Top Secret.

SecuSUITE is trusted by governments, world leaders, and business executives around the globe. Driving their trust is a wealth of certifications and independent approvals secured from multiple government agencies, including the U.S. National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and the government of Canada.

Common Attack Vectors

- **International Mobile Subscriber Identity (IMSI) catchers** enable surveillance by appearing as a valid cellular service
- **Man-in-the-middle attacks** are possible on certain Wi-Fi routers, Mi-Fi networks, or any use of unsecured TCP/IP networks
- **A Signal System 7 (SS7) vulnerability** allows bad actors to steal data, eavesdrop on calls, and intercept text messages and location data
- **Mobile Devices:** Lack of password, no encryption, connection to public Wi-Fi, no VPN



[1] Gartner, December 2018. https://www.gartner.com/en/documents/3896166/market-guide-for-instant-communications-security-and-com

High Security Voice and Messaging for iOS and Android

SecuSUITE features a mobile application that allows users to conduct secure voice and data communications using off-the-shelf devices, including most commercially available phones running iOS and Android. The solution takes the complexity of specialized hardware of legacy communications systems out of the picture, vastly improving ease of use and mission flexibility. The SecuSUITE mobile app is simple to use: it mimics a traditional phone client, complete with dial pad, call log, and integrated text messaging.

End-to-End Security

SecuSUITE creates a hyper-secure network connection between every user of the application. Underpinning the solution is BlackBerry's secure server, SecuGATE™, which authenticates users and creates a fresh pair of encryption keys before sending the voice and data through the SecuSUITE app.

Both the SecuSUITE client and the SecuGATE server have been independently tested and approved for use on U.S. government devices.

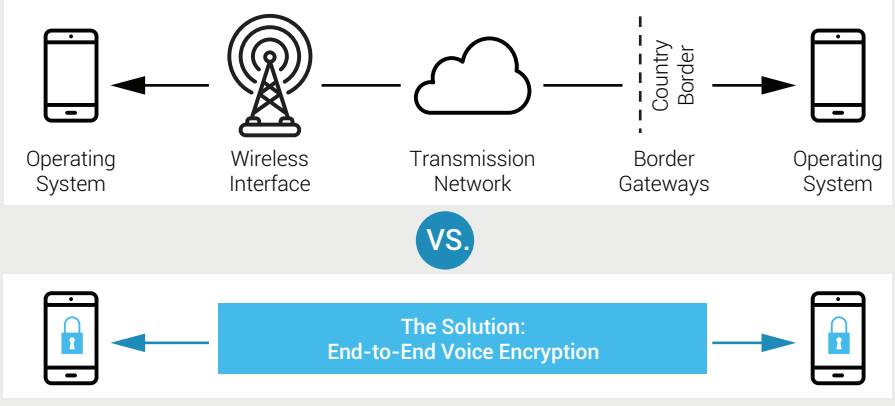
Think of SecuSUITE as a private, highly secure, end-to-end communications network. Only authorized members of the network can use the SecuSUITE app to communicate with each other. Behind the scenes, an administrator controls membership in the network and determines who can access and use the application.

You Always Know Who You're Talking To

SecuSUITE takes security to a new level by protecting against identity spoofing. The solution employs security best practices to ensure that all users are positively identified so you know who you're talking to on every call. And when you get a text message, you always know who it's coming from — and from what device.

End-to-End Encryption

SecuSUITE encrypts calls at every point in their journey



Reduced Long-Distance Costs

Fees for roaming and long-distance calls can get very high, very fast. With SecuSUITE, calls can be made securely over readily available Wi-Fi connections, reducing or eliminating long distance and roaming fees.

No Adware, Robocalls, or Spam

It's estimated that nearly half of all calls people receive are spam or robocalls. Because SecuSUITE is a closed network, however, you will never be bothered by adware or receive annoying spam or robocalls on the SecuSUITE client.

SecuSUITE in Action

SecuSUITE transforms how people communicate anywhere in the world. It provides hypersecure protections for government staff working in sensitive or dangerous locations — or any place where conversations can be intercepted by bad actors. Employees should never assume their government-supplied phones provide sufficient security for phone and text communications. The same applies to corporate executives traveling internationally. A few real-life examples:

International

The threat of cyberattacks and eavesdropping is high when people are out of the country — where it's a reasonable assumption that all cross-border calls are being monitored or recorded. SecuSUITE provides an end-to-end secure system for communicating with co-workers in the home office and with others whose locations may not even be known.

Meeting the Strictest Global Standards

BlackBerry is committed to — and invests heavily in — making SecuSUITE the most secure and reliable government communications platform in the world. The solution has earned the following certifications and approvals from key governmental organizations.

- **Common Criteria Certification.** The SecuSUITE app for iOS, Android, and BlackBerry devices has been certified according to the National Information Assurance Partnership (NIAP) Protection Profiles (PP) for SIP server and network devices.
- **NIAP Certification.** SecuSUITE is an NIAP-certified voice solution that supports iOS and Android devices.
- **Approved by the CSfC Program under NSA specifications.** SecuSUITE is designed to meet the requirements of the National Security Agency's (NSA) Commercial Solutions for Classified program.
- **Approved by the Canadian government for secret communications.** Under the Spectrum Policy Framework for Canada (SPFC) program, SecuSUITE has successfully completed Technical Proof-of-Service (T-PoS) with Shared Services Canada (SSC).
- **Compliant with the Federal Information Processing Standard (FIPS).** SecuSUITE meets the U.S. government's computer security standard for cryptographic modules.

Trusted by NATO

The NATO Communications and Information Agency (NCIA) has chosen SecuSUITE to encrypt conversations of its technology and cyber leaders wherever they communicate — in the workplace, at home, or traveling abroad.

Communicating with Out-of-Network Officials

Government employees traveling or stationed overseas frequently need to communicate over a secure channel with officials and executives from other nations. SecuSUITE enables these employees to securely discuss sensitive topics with foreign officials.

Military Personnel Calling Headquarters

SecuSUITE is an ideal system for enabling military staff posted in overseas locations to securely communicate with headquarters using a regular mobile device.

Communicating with Contractors and Business Partners in Foreign Countries

Government staff working in foreign countries frequently need to communicate with non-government contractors and other business partners. These partners can be issued temporary credentials to communicate with government employees without joining the government telephony network.

Corporate Executives on the Move

High-level business executives can be exposed to hackers and cyberthieves when traveling out of country. With SecuSUITE, communications are encrypted and secured back to their corporate home offices.

A Full Range of Communication Options

Mobile to Mobile

In this scenario, two people who are members of the same SecuSUITE secure private network communicate with each other from anywhere in the world over a secure network. Callers use SecuSUITE's end-to-end secure communication channel managed on premises or in the cloud.

From a SecuSUITE-enabled mobile device to SecuSUITE-enabled mobile device

Protecting World Leaders

Trusted by world leaders, SecuSUITE technology is regularly used by heads of state, cabinet ministers, and top government officials.

Secure Landing

A person using the SecuSUITE mobile app can connect with a greater number of people by tying the call into a secure landline inside an agency or corporate network.

From a SecuSUITE-enabled mobile device to a landline within the agency network

Secure Conferencing

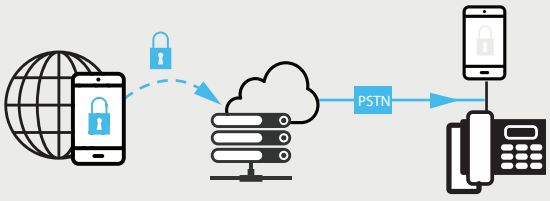
Mobile users of the SecuSUITE app can securely join a conference call over an agency or corporate PBX, allowing multiple individuals to share sensitive or secret information. SecuSUITE software provides encryption and security on both sides.

From a SecuSUITE-enabled mobile device to a secure conference bridge

Break-Out

In this scenario, a mobile user of the SecuSUITE app places a call into an office network, which is then routed via a public network (e.g., AT&T, Verizon) to a number outside the office. Security and encryption are assured from the mobile app to the home office — usually the most "exposed" part of the conversation when the caller is located outside the country.

From a SecuSUITE-enabled mobile device to the user's home network and from there to external mobile or landlines via PSTN extension



Flexible, Predictable Implementations

Governments and enterprises can deploy SecuSUITE in a wide range of environments, including existing datacenters, government clouds, and secure phone systems. They can even be integrated into local tactical systems like military vehicles or police SWAT team vans.

Break-In

This is the opposite scenario from "break-out." It's when someone places a call from an unsecured public network into the user's home government or corporate office network. The call is then securely routed to a user of the SecuSUITE mobile app. While the SecuSUITE mobile user will be protected from surveillance, the person calling in from the public network could be exposed to unwanted eavesdropping and recording by hackers.

From any mobile or landline on the user's home network to a SecuSUITE-enabled mobile device

Security Made Easy

No matter how secure your communications system, it only works when people actually use it. And to ensure adoption, you need to deliver a compelling user experience. SecuSUITE is an easy-to-use, secure communications platform. Calling or texting with the SecuSUITE app is like using your regular iOS or Andriod phone, but with added security.

When employees are on a sensitive mission anywhere in the world, they can leave behind those bulky specialized devices that stand out in a crowd. And there's no longer the need to go to a secure facility to make calls.

Intuitive Interface

The SecuSUITE mobile app interface is simple to navigate, just like commercially available Android or iOS apps. For highly sensitive communications, extra protections such as fingerprints or PIN numbers can be included and managed by the administrator.

Great Voice Quality

When you call people over SecuSUITE's software-defined network, you can expect audio quality that easily meets or exceeds what's available on commercial voice networks, with minimal to no voice latency anywhere in the world.

Streamlined Compliance

SecuSUITE helps organizations comply with a complete range of regulatory requirements around call and message metadata. Using the solution, customers can configure the collection and export of this data to automatically address specific government and industry regulations.

Flexible Implementation and Management

Getting started with SecuSUITE is simple. You can set up the mobile app by downloading it from an iOS or Android app store, or through an MDM push. Users complete the activation by entering an activation code and a URL or by just scanning a QR code. With SecuSUITE, you can do "out-of-band activation" to authenticate devices without having to send a text, avoiding the possibility of "man-in-the-middle" attacks. In most cases, organizations can use their existing mobile device management (MDM) system to provide visibility and easy administration across the user base.

The Future of Secure Communications

With attacks on communications networks escalating worldwide, governments are searching for new ways to safeguard their citizens and advance their missions. Previous security solutions were fundamentally flawed, relying on outmoded technologies that were unreliable, expensive, and inconvenient for users.

SecuSUITE provides a better alternative. Instead of using highly specialized devices and facilities, government employees and contractors can now communicate using standard mobile devices anywhere in the world. The solution is both easy to use — boosting adoption — and vastly more cost effective to own and operate. Crucial for mission integrity, SecuSUITE meets the most demanding certifications and operational requirements of governments worldwide.

Are your communications as secure as they need to be?

Learn More

You can learn more about SecuSUITE at https://www.blackberry.com/us/en/products/messaging/secusuite-government.