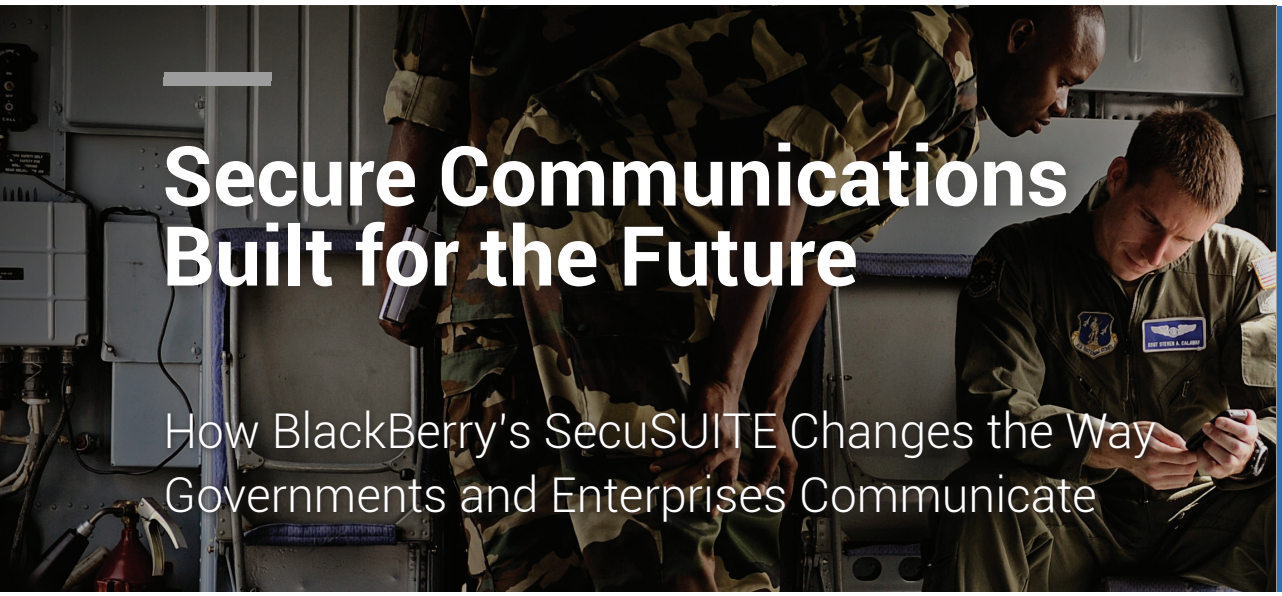

Secure Communications Built for the Future

How BlackBerry's SecuSUITE Changes the Way Governments and Enterprises Communicate

In a Dangerous World, You Never Know Who's Listening In

Today, communications — from phone calls to text messages — are being compromised and intercepted at rates never before seen, putting people and missions at extreme risk. And with the widespread adoption of mobile and wireless communications, the attack surface is broadening. In fact, it's surprisingly easy to eavesdrop on or monitor modern mobile devices, even over the latest LTE and 5G networks. 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.

Governments and enterprises have been trying to fight back, and many have developed sophisticated systems for securing sensitive and classified

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
- **5G GSM (A5/1 A5/3 Crypto) vulnerability** allows bad actors to set up equipment to intercept call connections in a given area and then crack the keys to decrypt the calls

communications. These include specialized bulky "Frankenstein" phones, burner phones, and dedicated secure facilities. Then there's the strategy of simply avoiding conversations about sensitive topics. All of these options are less than ideal and can place severe limitations on critical missions.

Introducing BlackBerry's SecuSUITE

Now there's a better way to protect against cyberattacks and to secure communications in the most sensitive missions and locations worldwide. It's called SecuSUITE® and it's from BlackBerry, a world leader in secure communication services.

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. No other voice communications solution has invested this much in meeting global security standards.

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 out of the picture, vastly improving ease of use and mission flexibility.

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. The solution positively identifies all users, so you always know who you're talking to, eliminating the risk

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 Smart Phone for Classified (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.

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

Simple, Affordable, and Spam-Free
The SecuSUITE mobile app is simple to use: it mimics a traditional phone client, complete with dial pad, call log, and integrated text messaging. For highly sensitive communications, extra protections such as fingerprints or PIN numbers can be included and managed by the administrator.

SecuSUITE also saves money because calls can be made securely over readily available Wi-Fi connections. And remember that SecuSUITE is a closed network, so you'll never be bothered by adware or annoying spam or robocalls.

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.

Flexible Implementation and Management
Getting started with SecuSUITE is easy. 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. In most cases, organizations can use their existing mobile device management (MDM) system to provide visibility and easy administration across the user base.

Empowering Global Travelers

SecuSUITE provides employees, executives, and contractors with a hyper-secure platform for communicating anywhere in the world.

- **Military** staff
- **International** contractors
- **Government** officials
- **Corporate executives** on the move

Are Your Communications as Secure as They Need to Be?

Learn more about BlackBerry's SecuSUITE at blackberry.com/secusuite.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.