BlackBerry Secure Communications

Sovereign Protection for Mission-Critical Communications

For governments and critical infrastructure, secure communication is essential to mission success. Yet conventional platforms often leave communications vulnerable to espionage, security breach, and operational failure. BlackBerry® Secure Communications delivers government-grade protection, validated by the world's most demanding security standards. Trusted for over 40 years by governments and high-stakes organizations worldwide, BlackBerry provides secure communications without compromise.

Challenges

State-Sponsored Espionage and Infrastructure Exploitation	Campaigns like Salt Typhoon reveal how adversaries exploit telecom infrastructure to intercept communications, gather intelligence, and compromise long-term operational security.
Foreign-Controlled Systems	Reliance on external infrastructure surrenders control over encryption keys, data flow, and access governance.
AI Impersonation and Deepfakes	AI-generated impersonation allows for fake messages and false identities, eroding trust at the highest levels of leadership.
Incomplete and Uncontrolled Consumer Applications	Consumer tools lack certified protections, identity assurance, and full communication capabilities required for secure operations.
Escalating Global Turbulence	Crises, conflicts, and disasters disrupt continuity and demand secure coordination under pressure.

Solution Overview

BlackBerry Secure Communications provides a sovereign system built to meet the demands of high-stakes environments. Comprehensive capabilities protect sensitive information, ensure operational continuity, and give organizations full control over their communications. More than end-to-end encryption, BlackBerry Secure Communications provides full protection for the most sensitive conversations—securing the people, devices, and data at every exchange.

Why Choose BlackBerry Secure Communications?

- **Complete Sovereign Infrastructure:** Deploy BlackBerry Secure Communications on-premises, in hybrid environments, or within air-gapped dark sites. Eliminate reliance on foreign-controlled systems and maintain full control over your data and infrastructure.

- **Seamless Coordination at Scale**: Organizations can broadcast urgent alerts, coordinate rapid responses, and maintain operational awareness, even in disconnected or high-risk environments.

- **Certified for Classified and Mission-Critical Operations**: Built to meet the highest security standards, accredited by leading global certifications including NSA CSfC, NATO Security Accreditation, Common Criteria, and Canada Secret certifications.

- **Communication Protection and Identity Verification:** Encrypts all voice, messaging, file, and metadata content—at rest, in transit, and on-device—while enforcing verified identity and hardened device integrity at every point in the communication chain.

Use Cases

- **Securing Mission-Critical Communications:** In the face of increasing threats against communication security, BlackBerry Secure Communications provides end-to-end encryption and robust identity management for operational continuity and trusted communication.

- **Enabling Rapid Incident Response:** BlackBerry Secure Communications means uninterrupted communication for swift action, minimized impact, and quick restoration of services.

- **Strengthening Cross-Agency Collaboration:** Improve secure collaboration, operational efficiency, and real-time joint decision-making within a fully encrypted, certified, and compliant solution.

Control your Communications – Control your Outcomes

BlackBerry provides governments and enterprises with secure, sovereign communications to safeguard sensitive data, enable scalable operations, and maintain mission continuity in an escalating threat landscape.

Talk to an expert

Contact us today to learn more about BlackBerry Secure Communications or visit blackberry.com/securecomms