BlackBerry

SOLUTION BRIEF

Defend Against Telecom Breaches With SecuSUITE

SALT TYPHOON-CLASS TELECOM ATTACKS

The telecommunications landscape is increasingly vulnerable to sophisticated cyber-espionage. In late 2024, the Salt Typhoon cyber-espionage campaign breached numerous major providers including AT&T, Verizon and Lumen Technologies, accessing sensitive communications and user metadata. The campaign targeted high-value communications from:

- Government officials and diplomats
- Military and defense personnel
- Corporate executives
- Intelligence agencies

This exposed critical weaknesses in the global telecom infrastructure. Organizations must now assume traditional telecommunications channels are compromised and take decisive action to protect their most critical communications.

WHY COMMON COMMUNICATION TOOLS FALL SHORT

In the wake of Salt Typhoon's infrastructure-level breaches, organizations should reevaluate their entire communications stack. Standard tools built on traditional telecom infrastructure inherit several fundamental security weaknesses.

PUBLIC NETWORKS AND SMS:

Traditional phone networks prioritize connectivity over security. They lack robust identity verification, use weak encryption, and store data vulnerable to theft.

CONSUMER MESSAGING APPS:

While these apps offer basic encryption, they weren't designed for enterprise or government security requirements. They remain vulnerable to identity spoofing and unauthorized data access.

ENTERPRISE COMMUNICATION TOOLS:

Standard business communication platforms focus on general office use rather than high-security environments. Their integration with corporate networks creates additional attack vectors, and they lack the rigorous protection required for classified communications.

WHY SecuSUITE?

UNMATCHED SECURITY STANDARDS

Protect communications with encryption certified by the NSA, NIAP and NATO for securing classified data

COMPLETE CONTROL

Maintain ownership and sovereignty of your communication infrastructure independent of public networks

GLOBAL TRUST

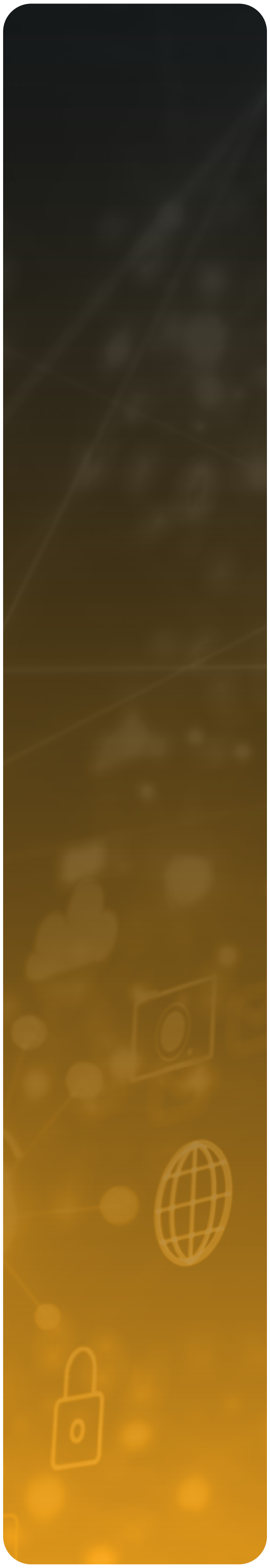
Trusted by NATO members, leading governments, and major enterprises worldwide

SEAMLESS EXPERIENCE

Deploy enterprise-grade security without compromising productivity or user experience

TOP MOBILE COMMUNICATIONS RISKS THAT THREATEN SECURITY

While common communication tools each have their limitations, they share core vulnerabilities that can be exploited through telecom infrastructure attacks. Understanding these specific risks is critical for protecting sensitive communications against sophisticated threats like Salt Typhoon.



EAVESDROPPING:

Attackers can exploit vulnerabilities in mobile networks or unsecured communication apps to intercept phone calls, messages and two-factor authentication codes. This allows them to access private conversations, sensitive data, and critical information, creating opportunities for privilege escalation and compromising security.

FAKE IDENTITIES (ID SPOOFING):

Adversaries can impersonate trusted contacts through sophisticated spoofing techniques, leading to compromised information exchanges and fraudulent communications. This risk is particularly acute when dealing with high-trust communications channels.

TRACKING WHO YOU TALK TO AND WHEN (METADATA EXPLOITATION):

While message content may remain encrypted, adversaries can monitor communication metadata — revealing who communicates with whom, when, and how frequently. This pattern analysis exposes organizational structures, relationships, and activities even without accessing the actual communications.

DEVICE TRACKING:

Through compromised networks and metadata analysis, threat actors can monitor device locations and movement patterns. This capability exposes sensitive operations, compromises physical security protocols, and puts confidential activities at significant risk by revealing personnel locations and organizational patterns.

THE SOLUTION

Organizations must now assume traditional telecommunications channels are compromised and take decisive action to protect their most critical communications. They are adopting end-to-end encrypted communication solutions to protect their most sensitive conversations from gaps that can lead to interception and compromise. SecuSUITE® delivers NSA-certified encryption, sovereign deployment options, and proven reliability trusted by governments and enterprises worldwide.

COMPREHENSIVE SECURITY FOR CRITICAL COMMUNICATIONS

SecuSUITE offers a complete solution for protecting sensitive communications without compromising usability or control. Leveraging BlackBerry's decades of security expertise and advanced encryption technology, it integrates seamlessly with existing infrastructure while ensuring communications remain private and untouchable.

SOVEREIGN DEPLOYMENT

- Own and operate your entire communication infrastructure
- Choose between on-premises or private cloud deployment
- Maintain independence from vulnerable public networks

BEYOND STANDARD ENCRYPTION

- Safeguard all communications with NSA-certified encryption
- Block unauthorized interception and eavesdropping attempts
- Control access through role-based security management

SEAMLESS INTEGRATION

- Deploy rapidly across existing devices and systems
- Empower users with intuitive, minimal-training interfaces
- Connect seamlessly across iOS® and Android™ platforms

PROVEN RELIABILITY

- Join leading organizations that trust SecuSUITE globally
- Meet the highest government security certifications
- Operate confidently in high-stakes environments

DON'T WAIT FOR THE NEXT MAJOR BREACH

Contact BlackBerry today to learn how SecuSUITE can protect your organization's most sensitive communications with proven, certified security trusted by world leaders.

TALK TO AN EXPERT

BlackBerry. Intelligent Security. Everywhere.

ABOUT BLACKBERRY

BlackBerry (NYSE: BB; TSX: BB) provides enterprises and governments the intelligent software and services that power the world around us. Based in Waterloo, Ontario, the company's high-performance foundational software enables major automakers and industrial giants alike to unlock transformative applications, drive new revenue streams and launch innovative business models, all without sacrificing safety, security, and reliability. With a deep heritage in Secure Communications, BlackBerry delivers operational resiliency with a comprehensive, highly secure, and extensively certified portfolio for mobile fortification, mission-critical communications, and critical events management. The company is also a pioneer in leveraging Artificial Intelligence and Machine Learning to deliver advanced cybersecurity solutions to its customers.

For more information, visit BlackBerry.com and follow @BlackBerry.