BlackBerry | Secure Communications

WHITE PAPER

WHY STANDARD SECURITY FAILS MISSION-CRITICAL OPERATIONS

The Case for Mission-Certified Communications

Supplemented with data from **The State of Secure Communications Study 2026**

RESEARCH BASE
700 Security Decision-Makers

SECTORS
Government and Critical Infrastructure

MARKETS
Canada, US, UK, Singapore

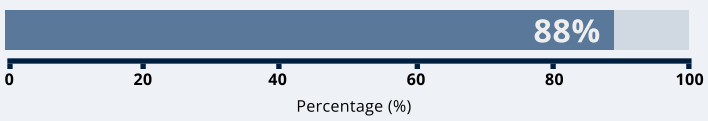
When the Stakes Are the Highest

The core problem facing security teams in government and critical infrastructure today is not a shortage of tools. Rather, it is a fundamental mismatch between what the tools were designed to do and what adversaries can actually target.

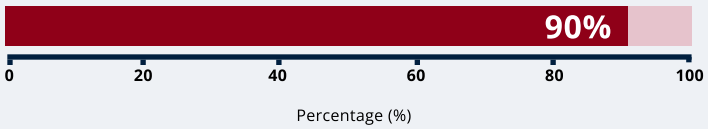
Primarily, the communications platforms deployed across many federal agencies, defense organizations, and critical infrastructure operators were designed to secure business communications. They were not designed to operate under nation-state threat conditions, where metadata is a target, identity is a weapon, and a fragmented response picture during a critical event is an operational failure.

The organizations most exposed to this gap are often the ones that look most secure on paper. They have deployed end-to-end encrypted messaging. They have implemented critical alerting systems. They have met every regulatory compliance threshold applicable to their sector. By every conventional industry measure, they are secure.

However, organizational confidence is not the same as organizational security. Marketing claims often confuse the meaning of end-to-end encryption and what is truly protected. It's not as comprehensive as organizations think.



Security leaders who express confidence in their messaging app security



The percentage of those leaders who hold misconceptions about what that encryption actually protects

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

The data A 2026 study of 700 security decision-makers across government and critical infrastructure sectors confirms what adversaries already know: organizations feel that their communications architecture is secure enough when in reality, that same architecture was never designed to fully protect against vulnerabilities. This confidence gap is systemic, not individual. It is the product of an industry that has treated encryption as a synonym for security for long enough that the distinction has become invisible.

The standard approach to modern security is building a security posture on a threat model that adversaries stopped using years ago.

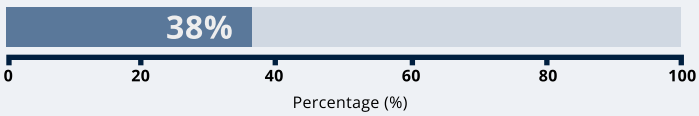
In reality, compliance frameworks measure organizational risk tolerance. Adversaries measure operational exposure. Those are not the same assessment. The gap between them is not a product gap, a budget gap, or a configuration gap. It is an architectural gap. And in mission-critical environments, design gaps are not patched. They are exploited.

The compliance-as-security fallacy is not unique to communications. It runs through federal IT procurement, enterprise risk management, and security certification programs designed to establish floors, not ceilings. In mission-critical environments, the floor is not sufficient. Adversaries do not audit compliance frameworks. They attack operational exposures.

The True Standards for Mission-Critical Operations

Security certification is not a marketing exercise. It is an adversarial validation process conducted by independent authorities whose institutional purpose is to identify failure modes, not approve them. Before examining how standard security fails, it is necessary to understand what the right standard actually requires.

The certifications that govern mission-critical communications represent thousands of hours of technical evaluation against threat models that most commercial security products are never subjected to. These authorities do not issue certifications based on vendor claims. They issue certifications based on demonstrated performance under controlled adversarial conditions. The gap between a product that claims to be secure and a product that has been independently validated as secure is precisely the gap that matters in mission-critical environments.



Security decision-makers who still rely on vendor marketing claims or self-attestations when evaluating security tools

Despite 61% citing government or industry certifications as critical to their selection criteria, more than one in three organizations remain exposed to the consequences of unverified vendor claims — including the E2EE misconceptions documented throughout this research.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

These validations are vital for ensuring mission-critical communications:

FIPS 140

Federal Information Processing Standard 140 validates the cryptographic modules within a communications system. Not just the algorithm. The implementation, the key management, and the operational behavior of the cryptographic boundary are verified under test conditions. A system can use AES-256 and still fail FIPS 140 validation because the implementation introduces exploitable weaknesses the algorithm itself does not.

Common Criteria (ISO/IEC 15408)

Common Criteria evaluates the entire system's security architecture against a defined Protection Profile. This includes the threat model the system was designed to resist, the security functions it implements, and the assurance level at which those functions have been independently verified. Common Criteria certification means an independent laboratory has confirmed the system performs under the specific adversarial conditions its target environment faces.

FedRAMP High

FedRAMP High governs cloud-hosted systems handling the most sensitive unclassified federal data. Systems where compromise would produce severe or catastrophic effects on organizational operations, assets, or individuals. The authorization process requires continuous monitoring, independent assessment, and architectural controls that most commercial platforms are not designed to support.

NATO Restricted

NATO Restricted authorization certifies systems for use in alliance environments where communications compromise could affect multinational operational security and allied interoperability. This certification requires meeting security requirements across the full alliance threat model, not just domestic federal standards.

Certifications not checkboxes. They are proof of design intent. A system that carries these certifications was built, from its architecture through its implementation through its operational deployment model, to function under the threat conditions that mission-critical environments actually face.

Certifications at individual component level are common. Full end-to-end validation against the combined threat model of defense, federal, and critical infrastructure environments is not. That distinction is the design gap.

The following sections explain exactly how consumer- and enterprise-grade security fall short of this standard and why.

How Standard Security Fails the Mission-Critical Threat Model

In high-stakes environments, encrypted communications and critical alerting are treated as separate problems. They are not. Both failures share the same root cause: systems designed for normal operating conditions being pressed into service under adversarial ones. The same threat model that exposes encrypted messaging exposes alerting architecture. An adversary who cannot decrypt your messages can still fragment your operational picture, delay your coordinated response, and exploit the gap between what your command knows and what your field knows. Secure messaging and unified operations management are not two products. They are two surfaces of the same vulnerability.

Failure #1: Encrypted Messaging Is Not Safe Enough

End-to-end encryption is the baseline security promise of virtually every modern communications platform. It is also, in isolation, a profoundly incomplete security posture for mission-critical environments. Understanding why requires separating what encryption does from what security actually requires.

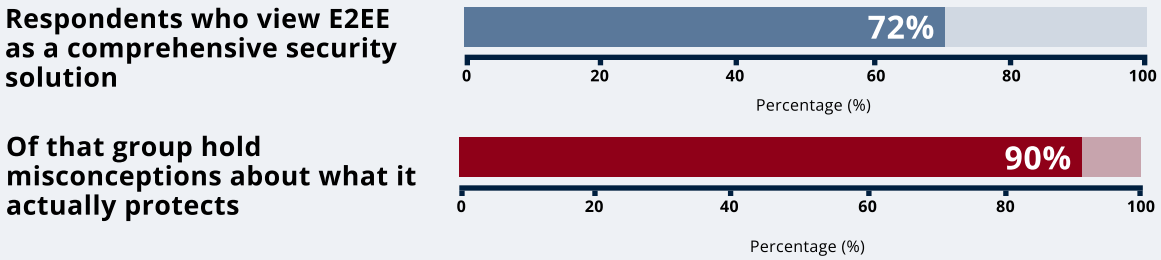
1. Encryption Protects Content. It Does Not Protect Operations.

End-to-end encryption (E2EE) secures the body of a message in transit. It ensures a third party who intercepts a communication cannot read its contents. This is a necessary control. It is not a sufficient one.

Encryption says nothing about who sent the message. It does not verify that the

sender is who they claim to be. It does not confirm that the device used to send it is authorized, uncompromised, or under organizational control. It does not enforce policy on how communications are conducted. It does not protect the data that surrounds every message: the metadata that reveals operational patterns, organizational structures, and behavioral signatures more reliably than message content often does.

In a mission-critical environment, the most dangerous attacks do not decrypt messages. They exploit the infrastructure encryption leaves unprotected.

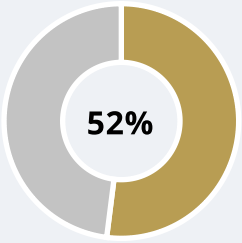


Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

> Consider the operational sequence: an encrypted messaging platform is deployed across a federal law enforcement task force. Every message is protected. Every call is encrypted. The investigation is, by every conventional measure, secure. But the platform is cloud-hosted. The vendor holds metadata. Pattern-of-life analysis of communication frequency between two field offices reveals that activity spikes sharply every 72 hours. The target does not need to read a single message. He needs to know when to move. The encryption was never broken. The operation was.

2. The Metadata Exposure Problem

Every encrypted communication generates metadata: who contacted whom, when, how frequently, from which location, using which device, for how long. This data is not encrypted by standard E2EE implementations. It is exposed — to platform operators, to infrastructure intermediaries, and to any adversary with access to network-layer telemetry.



Security decision-makers who incorrectly believe E2EE protects metadata such as IP addresses, contact lists, and location data

For intelligence purposes, metadata can be as valuable as content. Communication patterns reveal organizational structures, identify key personnel, expose relationships between entities, and signal operational changes. Location metadata tracks physical movements. Timing patterns indicate working hours, travel schedules, and response to events. An adversary with access to metadata can map an organization's structure, identify high-value targets, and monitor operational tempo without reading a single message.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

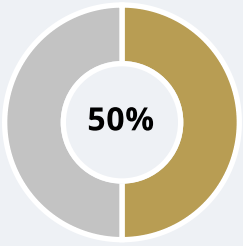
What E2E Encryption Protects	What It Leaves Exposed
Message content in transit	Who communicated with whom
File contents	When and how often contact occurred
Call audio	Device identifiers and locations
Nothing beyond the payload	Network topology and organization structure
Content, not context	Behavioural patterns over time

The metadata exposure problem is compounded by how consumer messaging platforms handle network-layer traffic. More than half of respondents (52%) report being concerned or very concerned about telecom infrastructure being monitored or disrupted by an adversary — yet simultaneously rely on communication platforms that leave metadata fully exposed at that layer.

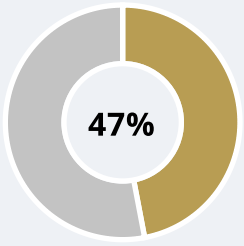
Protecting metadata in mission-critical communications requires architectural controls beyond encryption: identity abstraction, traffic normalization, and sovereign data handling that prevents any third party — including the platform vendor — from accessing communication metadata. This is not a feature most commercial platforms offer. It is a design philosophy most commercial platforms were never built around.

3. The Identity Verification Gap

Standard encrypted messaging platforms authenticate users at enrollment using a phone number or email address. From that point forward, possession of the device is treated as proof of identity. This model is acceptable for consumer applications. It is a serious risk in mission-critical environments.



Security leaders who identify impersonation or deepfakes as a top-3 threat to sensitive communications



The number of those same leaders who incorrectly believe E2EE already protects against the very threat they fear

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

Phone numbers are portable. Devices are stolen, compromised, and cloned. Chipsets are vulnerable to exploits. SIM-swapping attacks have been documented against high-value targets to gain access to secure communications channels with no cryptographic attack required. The encryption was never broken. The identity model was bypassed entirely.

This risk is recognized at the management level: 63% of study respondents express high concern about deepfake voice, video, or impersonation being used to mislead staff. Yet the platforms they rely on verify identity through phone numbers or email — offering no protection against sophisticated impersonation attacks that do not require message decryption.

In a governed operational environment, identity cannot be assumed from device possession. It must be continuously verified against organizational authority. Every user must be explicitly authorized by the organization. Every device must be registered, policy-bound, and continuously attested. Access must be contingent on organizational standing. When an operator is removed from a mission, their access must terminate instantly, completely, and irrecoverably.

4.The Consumer App Problem

Consumer messaging apps have become ubiquitous across government and critical infrastructure sectors. The study found that 98% of respondents are aware that consumer apps are used for sensitive communications in their organizations, and 83% specifically identify WhatsApp as a platform carrying these conversations, messages, and file-sharing.

Three in four security decision-makers report that employees bypass approved communication tools 'sometimes,' 'often,' or 'very often' — for efficiency.

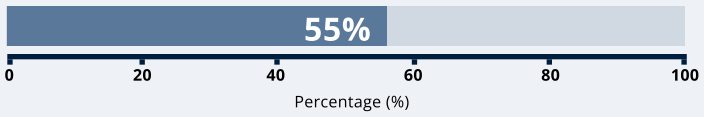
Consumer platforms dominate in practice regardless of policy. Organizations regularly use

83%	54%	50%	46%
WhatsApp	Personal email	Microsoft Teams Free	SMS

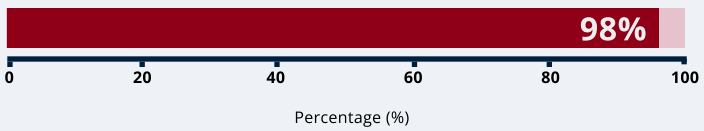
Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

The Sovereignty Problem

Most commercial secure communications platforms are cloud-hosted. The vendor operates the infrastructure. Keys are managed on vendor servers. Data flows through vendor-controlled systems. This architecture is acceptable for enterprise business communications. It is unacceptable for operations that cannot tolerate third-party data access.



Organizations that prioritize full sovereign control over communication systems



Number of those same organizations that use consumer messaging platforms that cannot provide it

This is not a compliance gap that policy updates can close. Consumer messaging platforms are built on centralized, globally distributed infrastructure. Their convenience comes precisely because they do not maintain separate sovereign instances for each country. That design makes them structurally incompatible with sovereignty requirements — not as a configuration failure, but as an architectural reality.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

The kill-switch risk compounds the sovereignty problem. Foreign-hosted platforms can be disabled at the discretion of the host country's government.

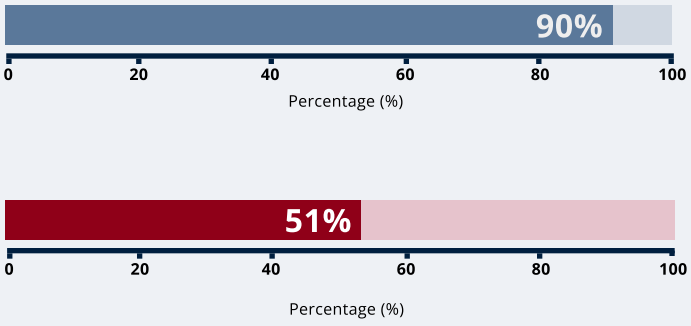
During geopolitical tensions, trade disputes, or international incidents, critical communication infrastructure could become unavailable regardless of encryption strength. For government and critical infrastructure operators, service availability during a crisis is not separable from security. A platform that is encrypted but inaccessible has failed.

Failure #2: Critical Operations Alerts Are Not Smart Enough

The second pillar of standard security posture in mission-critical environments is the critical alerting system. Mass notification platforms, emergency broadcast systems, and incident management tools are deployed across defense, federal, and public safety sectors under the assumption that faster alerts produce better outcomes. The assumption is incomplete.

Speed of delivery is not the binding constraint on critical operations response. Clarity of the operational picture is. And standard alerting systems, almost universally, produce fragmented, low-context signals that force commanders and responders to reconstruct situational awareness from incomplete data — under time pressure, in degraded conditions, during the moments when rapid decisions must be certain.

1. The Crisis Confidence Gap



Security decision-makers who express confidence in their organization's ability to manage major crises effectively

The number of those same organizations that lack a unified crisis management platform — relying instead on email, group chats, and spreadsheets

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

This 90%-vs-51% gap is not a measurement anomaly. It is the defining finding of this research. Organizations that are confident in their crisis preparedness and organizations that have the infrastructure to back that confidence are not the same population. The gap between them becomes visible only during an actual crisis — when it is too late to address.

2. Fragmented Signals Produce Fragmented Understanding

A typical critical operations environment aggregates signals from multiple disconnected systems: physical security platforms, cybersecurity monitoring tools, HR and personnel systems, communication platforms, environmental sensors, external threat intelligence feeds, and field reporting. Each system generates alerts. None of them, by default, speak to each other.

The result is alert fragmentation — a high-volume stream of isolated signals that require manual correlation, contextual interpretation, and cross-system synthesis before they can inform a decision. In a time-sensitive incident, this process is the bottleneck. By the time an operator has correlated alerts from five separate systems and assembled a coherent operational picture, the decision window has often passed.

3. How Organizations Without Unified CEM Actually Coordinate

The State of Secure Communications 2026 Study reported that only 49% have unified Critical Event Management (CEM) platforms that provide critical operations management in an integrated system. According to the study, the 51% of organizations without unified CEM platforms use some combination of the following tools to respond to crises:

Crisis Communication Method	What It Leaves Exposed
Small group chats	56%
Email threads	54%
1-to-1 messaging	41%
Manual conference bridges	31%
Shared spreadsheets	30%
Phone trees	19%

Group chats cannot provide unified situational awareness. Email threads cannot track personnel safety status. Spreadsheets cannot enable federated command across agencies. These tools were designed for normal operating conditions. They fail precisely when coordination demands peak — which is precisely when mission-critical operations need them most.

4. The Visibility Gap

Effective critical operations management requires visibility into three signal categories simultaneously: people, systems, and external conditions. Standard alerting systems are typically designed around one category, with limited integration into the others.

Signal Category	What Standard Systems Miss
People	Personnel location, availability, and acknowledgment status across federated teams
Systems	Cross-platform correlation between physical, cyber, and operational alerts
External Conditions	Real-time integration of weather, public safety feeds, and geospatial intelligence
Combined Picture	Unified view enabling coordinated action across all three dimensions simultaneously

When these signal categories are managed in separate systems, commanders operate with partial information. They know there is a cybersecurity alert. They do not know whether the field team assigned to respond is in position. They know there is a perimeter breach. They do not know whether the access event correlates with a concurrent system intrusion. They issue a notification. They do not know whether it was received, read, or acted upon by every relevant operator.

Each gap is individually manageable. In combination, under pressure, they produce the conditions for cascading operational failure.

5. The Coordination Failure Problem

Critical incidents rarely respect organizational boundaries. A major infrastructure attack implicates the owner-operator, federal agencies, law enforcement, and potentially allied international partners. A cybersecurity incident affecting federal systems may require simultaneous response from agency security teams, CISA, contracted IR firms, and legislative stakeholders.

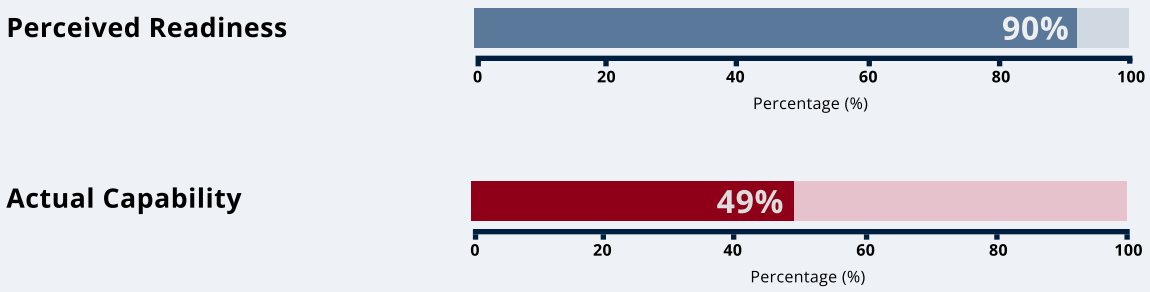
Standard alerting systems are designed for organizational broadcast, not federated coordination. They can push notifications to defined recipient lists. They cannot create a shared operational environment where stakeholders across

agencies, jurisdictions, and security boundaries operate from the same information, understand the same situation, and coordinate action in real time. The practical consequence is that multi-agency incidents default to improvised coordination: phone calls, email threads, improvised chat channels, and liaison officers bridging systems that were never designed to interoperate. This is not a technology failure in the traditional sense. It is an architectural limitation misidentified as a process problem.

6. The Lack of Bidirectional Field Intelligence

Standard mass notification flows in one direction: from command to field. Alerts are issued. Acknowledgments may be requested. But the operational intelligence that field teams generate — position, status, observed conditions, resource needs, emerging threats — rarely flows back to command in a structured, timely, or integrated way.

This unidirectional architecture creates an asymmetric information environment in which commanders make decisions based on the situation they knew about when the incident began, not the situation as it exists. Field teams may be ahead of command's understanding by minutes or hours. In fast-moving incidents, that gap is not a minor inefficiency. It is the difference between an effective response and a reactive one.



90% confidence measured against 49% actual capability represents a dangerous gap. When infrastructure fails and time pressure is acute, email threads and group chats cannot provide the unified command and control that crisis response demands. The gap between confidence and capability may only become visible during an actual crisis, when it is too late to address.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

Secure Enough Simply Isn't Good Enough

Mission-Critical Environments Require Mission-Certified Communications

The organizations that accept standard security as sufficient are operating on a threat model that does not reflect their actual exposure. They have met compliance requirements. They have satisfied audit criteria. They have checked boxes that were designed for enterprise risk management, not for environments where adversaries are state-level actors, where operational compromise has strategic consequences, and where failure is measured in lives, national security outcomes, and critical infrastructure continuity.

Mission-certified communications is not a higher tier of the same product category. It is a different product category entirely, built on different design principles, validated by different authorities, and capable of performing under conditions that would compromise standard commercial alternatives.

Total Communication Integrity

Mission-certified communications help ensure total communication integrity — not just encrypted content, but verified identities, trusted devices, enforced policies, and sovereign infrastructure. It replaces the assumption of security with the assurance of it.

Identity is continuously verified, not assumed from device possession. Every user is explicitly authorized by the organization. Every device is registered, attested, and policy-bound. Access is contingent on current organizational standing. Revocation is immediate and complete.

Metadata is protected, not just message content. Communications behavior — including who talks to whom, when, how often, and from where — is architecturally shielded from third-party access, including the platform vendor.

Sovereign control is available by design. The organization decides where data lives and who holds keys. Fully air-gapped deployment is available for environments where no external network connectivity is acceptable. The architecture is designed to prevent vendor access to communications data or key material.

Mission Orchestration

Mission-certified operations management replaces fragmented alerting architectures with a unified, intelligent platform. Signals from people, systems, and external sources are ingested, correlated, and presented in a single operational view. Commanders see everything — including personnel status,

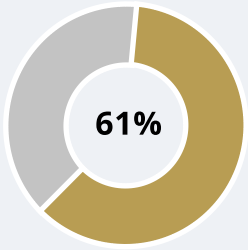
system alerts, geospatial intelligence, and field conditions — without manually correlating data from disconnected tools.

The operational loop is continuous: detection to understanding to coordinated action to recovery. Field intelligence flows back to command in real time. Notifications are bidirectional. Acknowledgment is tracked. Every stakeholder, across agencies, jurisdictions, and security boundaries, operates from the same information simultaneously.

When infrastructure is strained and conditions degrade the systems that normal operations depend on, resilient multi-channel delivery and a high-availability architecture ensure that communications and operations management remain dependable precisely when they are most needed.

BlackBerry Secure Communications is The Mission-Critical Standard

The security authorities that govern mission-critical environments did not arrive at their certification requirements by consulting vendor marketing. They arrived at them by modeling the attacks. FIPS 140, Common Criteria, FedRAMP High, and NATO Restricted exist because the standard was insufficient and the consequences were unacceptable.



Security decision-makers who cite government or industry certifications as critical for selecting security tools

The market is moving toward demanding independent proof. But 38% still rely on vendor self-attestation — a gap that creates exactly the misconceptions this research documents. Organizations that have completed the transition to independent verification report more accurate threat models and more defensible procurement decisions.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

These authorities do not issue certifications based on vendor claims. They issue certifications based on demonstrated performance under controlled adversarial conditions. The gap between a product that claims to be secure and a product that has been independently validated as secure is precisely the gap that matters in mission-critical environments.

Standard commercial communications platforms, regardless of their marketing language, have not been validated end-to-end against the threat models that govern defense, federal, and critical infrastructure environments. Some carry individual component certifications have been certified to perform under high-stakes conditions.

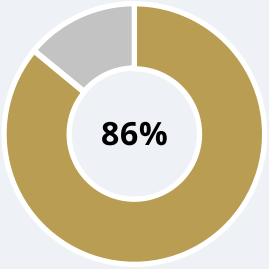
> The world's most demanding security authorities understand the difference between a product designed to pass certification and a product certified because it was designed to perform.

BlackBerry® solutions were built to satisfy those requirements from the architecture out, not the marketing in.

BlackBerry® Secure Communications delivers Total Communication Integrity through continuous identity verification, device attestation, policy enforcement, metadata protection, and sovereign deployment options including full air-gap capability. It delivers Unified Critical Operations through integrated signal intelligence, bidirectional field communication, and real-time federated coordination across organizational boundaries.

The certifications that BlackBerry holds (FIPS 140, Common Criteria, FedRAMP High, and NATO Restricted, etc.) are not peripheral to this claim. They are the validation of it. Independent authorities evaluated BlackBerry solutions against the full scope of threat models that mission-critical environments face. Their certification is not an endorsement. It is proof of performance under adversarial validation conditions.

Organizations that have experienced the cost of the gap between standard security and mission-certified security do not discuss it publicly. The incidents that result from metadata exposure, identity compromise, and fragmented operational response are rarely attributed to the architectural limitations that produced them. The risk persists because the tools used to assess security posture are often the same tools that contain the gaps.



Security decision-makers say they would be 'somewhat' or 'very surprised' if their organization's sensitive communications were compromised tomorrow

Despite the misconceptions documented throughout this research — despite the policy-practice gaps, despite the architectural incompatibilities — organizations do not recognize their own exposure. The confidence is genuine. Whether it is justified is precisely the question mission-certified security is designed to answer.

Source: BlackBerry, The State of Secure Communications Study, 2026 (n=700)

ABOUT BLACKBERRY

BlackBerry® Secure Communications delivers purpose-built solutions for secure communication, collaboration, and robust crisis management. Engineered to protect high-stakes organizations from evolving communications threats, BlackBerry Secure Communications provides operational continuity for critical functions.

ABOUT THE RESEARCH

Study statistics cited throughout this document are drawn from The State of Secure Communications 2026, research conducted on behalf of BlackBerry Secure Communications by OnePoll in December 2025 of 700 security decision-makers in Canada, US, the UK and Singapore. The research examined how government and critical infrastructure organizations perceive and implement secure communications. Questions covered six domains: encryption understanding, device security, infrastructure sovereignty, crisis management capabilities, quantum preparedness, and security procurement criteria. Findings reflect self-reported perceptions and practices among security decision-makers. The research was designed to identify gaps between security confidence and security capability, with particular attention to areas where organizational assumptions may not match technical reality.