



BlackBerry SecuSUITE

Communications sécurisées pour les opérations gouvernementales

La sécurité des communications est constamment menacée dans le monde hostile d'aujourd'hui. Les outils de communication traditionnels tels que les réseaux téléphoniques publics, les applications grand public et les suites de productivité d'entreprise ne sont pas à la hauteur de la sécurité critique. BlackBerry® SecuSUITE® est spécialement conçu pour protéger les communications les plus sensibles.

Défis

Écoutes téléphoniques

Les attaquants exploitent les vulnérabilités des réseaux mobiles ou des applications de communication non sécurisées pour intercepter les appels téléphoniques, les messages et les codes d'authentification à deux facteurs. Cela leur permet d'accéder à des conversations privées, à des données sensibles et à des informations critiques, créant ainsi des opportunités d'escalade des privilèges et compromettant la sécurité.

Usurpation d'identité

Les adversaires peuvent se faire passer pour des contacts de confiance grâce à des techniques sophistiquées d'usurpation d'identité, ce qui compromet les échanges d'informations et les communications frauduleuses. Ce risque est particulièrement élevé pour les canaux de communication de haute confiance.

Exploitation des métadonnées

Alors que le contenu des messages peut rester crypté, les adversaires peuvent surveiller les métadonnées des communications - révélant qui communique avec qui, quand et à quelle fréquence. Cette analyse des schémas met en évidence les structures, les relations et les activités de l'organisation sans accéder directement au contenu des communications.

Contrôles insuffisants

L'absence de pistes d'audit pour les messageries grand public ne permet pas de savoir si des informations sont partagées ou copiées, ce qui rend presque impossible le contrôle de la conformité et l'analyse médico-légale après un incident. En outre, la dépendance à l'égard de services en nuage tiers signifie que les utilisateurs sont à la merci des conditions de service commerciales et des lois en vigueur dans leur juridiction.

Aperçu de la solution

BlackBerry SecuSUITE est la référence en matière de sécurisation des communications mobiles. Conçu pour les environnements à fort enjeu, il protège les appels, les messages et les données grâce au chiffrement de bout en bout et à la validation cryptographique de l'identité. Évalué et approuvé de manière indépendante par des organismes tels que l'OTAN et le NIAP, BlackBerry SecuSUITE élimine l'exposition des métadonnées, permet un contrôle complet de chaque couche de communication et s'adapte de manière transparente à tous les environnements. Avec plus d'une décennie d'expertise, SecuSUITE permet aux organisations de communiquer en toute confiance, même dans les environnements les plus difficiles.

Résultats

- **Contrôle souverain** : Prenez le contrôle total de votre infrastructure de communication avec une solution conçue pour répondre à divers besoins de déploiement. Que ce soit sur site, en nuage privé ou hybride, BlackBerry SecuSUITE s'aligne de manière flexible sur vos exigences uniques. En fonctionnant indépendamment des réseaux publics vulnérables, il garantit une communication fiable et véritablement privée.
- **Intégration transparente** : Déployez facilement la solution sur vos appareils et systèmes existants. BlackBerry SecuSUITE offre une interface intuitive, nécessite une formation minimale et l'intégration transparente sur iOS et Android permet à votre équipe de rester connectée sans effort.
- **Fiabilité éprouvée** : Les gouvernements et les organisations du monde entier font confiance à BlackBerry SecuSUITE pour sa fiabilité et ses performances. Soutenu par les certifications de sécurité les plus élevées, il permet des opérations en toute confiance dans les environnements les plus exigeants.
- **Au-delà du cryptage standard** : Protégez vos communications grâce à un cryptage certifié par la NSA, garantissant une protection de premier ordre contre les interceptions et les écoutes non autorisées. Grâce à une gestion de la sécurité basée sur les rôles, vous pouvez maintenir un contrôle d'accès strict pour renforcer votre infrastructure de communication.

Cas d'utilisation

- **Communications critiques** : BlackBerry SecuSUITE protège les communications qui façonnent la sécurité mondiale, la diplomatie et les infrastructures critiques. De l'alliance Five Eyes et de l'OTAN aux gouvernements d'Asie, d'Afrique et d'Europe, notre plateforme sécurise les opérations les plus sensibles.
- **Communications de voyage** : Les dirigeants en déplacement sont confrontés à des risques de surveillance lorsqu'ils utilisent des réseaux non fiables. BlackBerry SecuSUITE protège les appels et les messages par un cryptage de bout en bout, fonctionne indépendamment des systèmes locaux et est simple à utiliser.
- **Protection de la propriété intellectuelle pour les fabricants mondiaux** : Le partage de données sensibles crée des risques. BlackBerry SecuSUITE sécurise les communications et le partage de fichiers, protège les métadonnées et contribue à garantir la conformité aux normes de protection des données.

Lorsque la communication est essentielle et que le contrôle n'est pas négociable, BlackBerry SecuSUITE est le bon choix.

Parler à un expert



Contactez-nous dès aujourd'hui pour en savoir plus sur BlackBerry SecuSUITE ou visitez BlackBerry.com/securecomms.

À propos de BlackBerry

BlackBerry (NYSE : BB ; TSX : BB) fournit aux entreprises et aux gouvernements des logiciels et des services intelligents qui alimentent le monde qui nous entoure. Basé à Waterloo, en Ontario, le logiciel de base haute performance de l'entreprise permet aux grands constructeurs automobiles et aux géants industriels de débloquent des applications transformatrices, de générer de nouvelles sources de revenus et de lancer des modèles commerciaux innovants, tout cela sans sacrifier la sûreté, la sécurité et la fiabilité. Forte de son héritage dans le domaine des communications sécurisées, BlackBerry offre une résilience opérationnelle grâce à un portefeuille complet, hautement sécurisé et largement certifié pour la fortification mobile, les communications critiques et la gestion des événements critiques.

