**Key Points from Secure Communications Platform** (by slide):

|  |  |
| --- | --- |
| **Slide** | **Key Point** |
| 2 | * Defending business and mission interests is a challenge for any organization, but for some the stakes are unusually high. * The adversaries they face have no conventional limitations when it comes to time, expertise, or financial backing. |
| 3 | * These organizations assume that their personnel’s conversations are being intercepted anytime and cannot rely on commercially available devices and apps * They are contending with AI-equipped adversaries using zero-day vulnerabilities developed to target them. When something goes wrong, human lives are in the balance. |
| 4 | * An adversary could simultaneously cut you off from the internet, attack your critical infrastructure, and monitor and out-maneuver any response you tried to mount. * We only see the surface-level results in the media, from nation-states attacking each other and corporations to clandestine cellular modems hidden in busy port equipment communicating to unknown destinations. |
| 5 | * In the rush to buy a laundry list of technologies, organizations end up with dozens of vendors, partners, integrators, contractors and consultants– all sourced through painful procurement processes. * Organizations lose operational fluidity, and although they may have a lot of tech, they become “combat ineffective”, even introducing more risk given that 62% of system intrusion incidents come through partners. |
| 6 | * BlackBerry is the most comprehensive, highly secure, and extensively certified platform available for critical and secure communication delivered on four key capability pillars across Critical Communications, Mobile Fortification, AI-Driven Cybersecurity and Crisis Management. * Certified and deployed by NATO, the NSA, the governments of Germany, Canada, the United States, and most recently Malaysia, assuring our solutions meet the strictest global standards. |
| 7 | * BlackBerry solutions are deployed extensively with 18 of the G20 governments, all 7 of the G7, nearly half of all Fortune 100 and 8 out of 10 of global banks. |
| 8 | * From a critical communications perspective – BlackBerry provides end-to-end cryptographic protection of digital voice and text conversations, making any incepted signal of zero value to an adversary. * Approved by the NSA for Top Secret Communications it sets us apart from any other commercial solutions like WhatsApp, widely known to have been compromised by zero-click attacks like the NSO Group’s Pegasus surveillance spyware. |
| 9 | * Our mobile fortification creates separate secure space on mobile devices so that even if the device gets compromised, data and applications remain safe, to safely leverage BYO and COTS devices. * BlackBerry’s is the only solution of its type certified for use by NATO in classified and non-classified environments. |
| 10 | * It takes AI to stop AI and BlackBerry stops breaches from ever occurring and can do that better across more types of endpoints than any other vendor. * This is a capability that is field deployable on resource-constrained, intermittently connected environments. |
| 11 | * When organizations inevitably face a crisis cyber, kinetic or a natural event crisis they need to respond instantaneously to mass-alert civilian populations and orchestrate first-responders. * BlackBerry is used by 90% of U.S. federal government employees. |
| 12 | * BlackBerry has a track record of providing foundational talent pipeline and can deliver everything from point-in-time certification and training through ongoing centers of excellence. * Role-based education and hands-on experience programs provide organizations with the specific skills they need for their job roles. |
| 13 | * BlackBerry was part of the centralized crisis response to the US capitol insurrection in January 2021 and there is an official federal warning on the screen of an unlocked computer warning staff of the current situation. * That alert was delivered via BlackBerry, and you can tell just how quickly staffers had to leave because of the threat to their life. |
| 14 | * BlackBerry was used immediately by the department of Homeland Security and the US cost Guard to help orchestrate a response and minimize impact in the recent Baltimore’s bridge collapse. |
| 15 | * BlackBerry partnered with the government of Malaysia, with secure, reliable, real-time access to BlackBerry software and services hosted in a sovereign cloud. * BlackBerry will establish a world-class Cybersecurity Center of Excellence (CCoE) in Kuala Lumpur in 2024, offering specialized training to advance Malaysian cybersecurity capacity and readiness to reduce the country’s shortfall of 12,000 cyber professionals. |