



Securing critical communications

Use case

Public safety agencies depend on secure communication systems to coordinate operations and respond to emergencies. With the rise of cyberattacks, these critical networks face growing risks from external threats and unauthorized access attempts. Sensitive data, such as law enforcement information, must be protected from breaches, while communication channels themselves need to be safeguarded against disruption. As security demands increase, agencies require solutions that ensure data privacy and protect vital communications, especially during emergencies.

Challenges

Public safety agencies are increasingly vulnerable to cyberattacks that target their critical communications infrastructure. As the nature of threats becomes more sophisticated, there is a growing risk of bad actors compromising these systems during emergencies, when secure, uninterrupted communication is most essential, even during network congestion. Protecting communication channels from tampering or disruption is critical to maintaining operational continuity and ensuring the safety of both responders and the public.

Another pressing challenge is the need to safeguard sensitive data, such as law enforcement records and intelligence, from unauthorized access. The failure to secure this information not only jeopardizes public safety but also undermines the trust in agencies responsible for maintaining order. As cyber threats evolve, so too must the measures taken to protect these communications and the sensitive data they carry.

Solution

Nokia addresses the security challenges facing public safety agencies by combining its Core Enterprise Solution for Public Safety with the advanced capabilities of Nokia CyberSecurity Dome. The dedicated 4G or 5G private wireless network provides secure, high-performance connectivity, enabling agencies to maintain operational continuity during emergencies. This private network is isolated from public networks, ensuring that critical communication channels are protected from unauthorized access and external threats.

Nokia CyberSecurity Dome enhances this network with an integrated cybersecurity framework that actively monitors and protects the entire communication infrastructure. Using advanced encryption, access control methods, and AI-driven threat detection, it helps secure sensitive data and maintain the integrity of the communication channels. Its automated threat scoring and incident response capabilities ensure that any potential cyberattacks are identified and mitigated swiftly, allowing public safety teams to focus on their mission without the distraction of compromised communications.

Nokia's Core Enterprise Solution for Public Safety and Nokia CyberSecurity Dome create a protective shield around your emergency and rescue operations.



Benefits

Public safety agencies gain exceptional operational continuity during emergencies by utilizing a dedicated 4G or 5G private wireless network. This ensures critical communications remain secure and functional, even when public networks are down or overwhelmed. The ability to maintain reliable communications under pressure enables faster, more coordinated responses to unfolding incidents.

The combination of advanced encryption, access controls, and real-time threat detection provides robust protection for communication channels, significantly reducing the risk of cyberattacks and unauthorized access. This proactive defense prevents potential disruptions from external threats, keeping operations running smoothly and safeguarding mission-critical systems.

With real-time monitoring and automated threat responses, any breach attempts are swiftly mitigated, ensuring that sensitive data remains secure. This allows public safety agencies to operate confidently, knowing that their communications and data are fully protected from emerging cyber threats.

Results

With a private 4G or 5G wireless network and Nokia CyberSecurity Dome in place, public safety agencies can operate with an unprecedented level of security and efficiency. Reliable, secure communication channels are maintained even in the most critical moments, ensuring that responders have the tools and information they need to make life-saving decisions without delay. The ability to sustain operations during emergencies allows agencies to respond with speed and precision, improving outcomes for the communities they serve.

By significantly reducing the risk of cyberattacks, these agencies can focus on their mission rather than the vulnerabilities of their systems. Secure, private networks, enhanced with real-time threat detection, ensure that sensitive information remains protected, safeguarding both public safety operations and the data they depend on.

Discover more about how Nokia's solutions can help secure your organization's most critical communications and data.

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2025 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID214390 (January)