cradlepoint

Trends in Connected Technologies for First Responders

Implications for Mobile Networks, Management & Security

What You'll Get:

- Overview of the evolving public safety technology landscape
- Summary of challenges created by new technology adoption
- Guidelines for creating an Elastic Edge™ enabled mobile network

Overview

Every day, first responders have to be ready to help with someone's worst day or deal with a community's worst nightmare. Increasingly, first responders depend on digital and connected technologies to help quickly provide life-saving assistance, deal with crisis situations, and bring order to chaotic situations.

Digital and connected technologies are transforming first responder organizations by increasing accountability, improving first responder safety, and enhancing triage and treatment. However, these new technologies can create new challenges if they are not implemented correctly, which can consume already limited budgets and precious man-hours.

The modern first responder relies on always-on mobile networks to keep their mission-critical applications and devices up and running. These teams need technology to just work—anytime, anywhere—so they can focus on doing their jobs and trust that the technology will function.

This white paper examines the role connected technologies, including mobile applications, devices, the cloud, and the Internet of Things (IoT), play in the effectiveness and safety of first responders and offer considerations for evaluating mobile network solutions that enable it all to work securely and reliably.

2,000+
POLICE, FIRE & EMS AGENCIES USE CRADLEPOINT SOLUTIONS TO HELP KEEP COMMUNITIES SAFE.

— Cradlepoint collected data

Trends in First Responder Connected Technologies

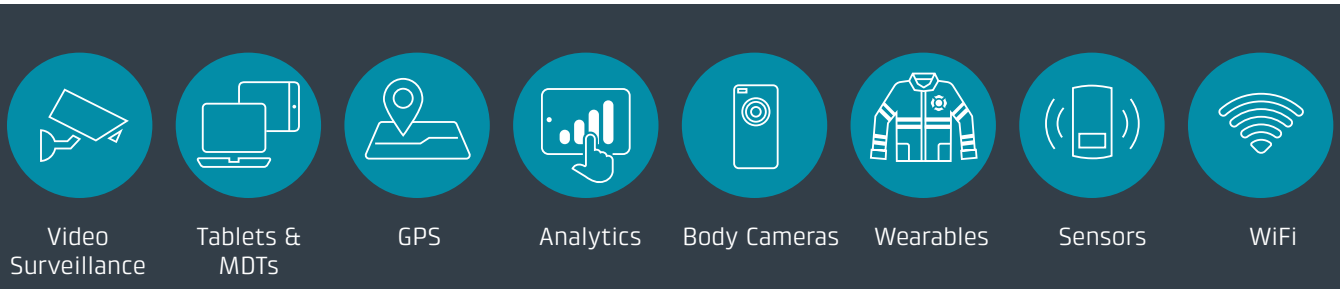
New and innovative connected technologies are helping first responders be more efficient in the performance of their duties, stay safer, collaborate better, and access crucial information faster. The following are some examples of real-world technology use cases and the challenges that first responder IT organizations may encounter in the implementation and management of them.

IoT DEVICES

IoT devices refers to a wide variety of connected devices that provide real-time visibility, situational awareness, or functionality. Typically, IoT devices are task-specific and have limited internal networking or computing power, such as sensors, security cameras, robots, and drones. The adoption of IoT technologies are creating new ways to improve first responder effectiveness, safety, and accountability.

Examples of In-Vehicle & Field-Based IoT Devices in Action

- Dashboard, body-worn, and other video recording devices are becoming commonplace among first responder organizations. Some camera implementations are designed to begin recording based on event triggers, such as removing a firearm or taser from a holster or gun rack.
- In many agencies across the U.S., K-9 officers are utilizing body worn buttons, which are used to remotely trigger the opening of a K-9 cruiser door to release police dogs during critical situations.
- Firefighters can use camera-enabled drones to fly over a structure or wildfire to analyze the situation and plan fire-fighting strategies from a safe distance.
- Onboard sensors on ambulances are used to track the consumption of medications for billing, stocking, and compliance purposes. These sensors can even notify a supervisor whenever a regulated medication is dispensed.
- Police and sheriff agencies are using drones to surveil locations and assess potential threats before sending in officers or deputies to serve warrants—which is one of highest-risk duties that first responders must carry out.
- Bomb squads and SWAT teams can use robots to handle suspicious packages, defuse explosives, and scout out dangerous crime scenes from a safe distance.



IoT CHALLENGES:

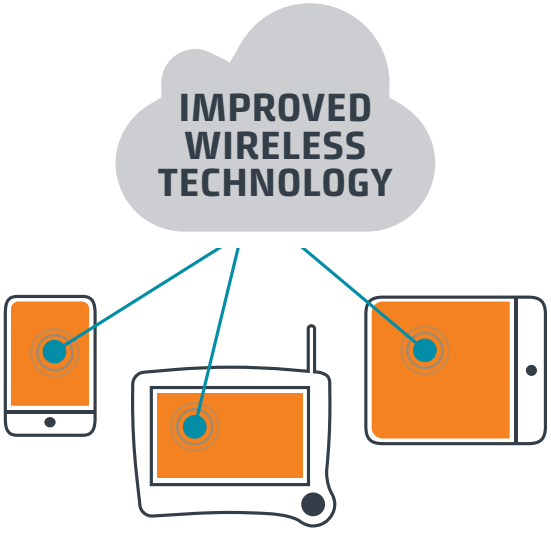
Deploying, securing, and maintaining remote devices isn't without challenges. Here are some IT considerations:

- **Connectivity:** A modern police, fire, and EMS vehicle may have dozens of IoT devices onboard, making connectivity a challenge. The range of IoT devices inside and outside the vehicle requires a variety of connections, including Ethernet, WiFi, Bluetooth, and serial and general purpose I/O (GPIO) ports. Additionally, an OBD-II connector and embedded GPS may be required to enable back-office applications like Computer-Aided Dispatch (CAD) and fleet management.
- **Management:** Many IoT devices are cloud dependent and rely on an always-on 4G LTE and local connections to function. Moreover, they play a critical role in supporting first responders in their daily duties and promote safety. IT teams need to be able to remotely monitor, manage, and maintain these devices and their underlying networks, as well as troubleshoot problems remotely to avoid unnecessary truck-rolls or the need to bring a vehicle off the road to address and troubleshoot network problems.
- **Security:** Every connected device on the network creates a network on-ramp and presents an "attack surface" that a hacker might be able to exploit to gain access to other systems and data on the network. Once these devices are installed in vehicles or deployed in the field, they also risk physical penetration by hackers. A breach of this nature can paralyze a technology-dependent agency and erode public trust.

MOBILE APPLICATIONS

Cloud-connected mobile applications on smartphones, tablets, and Mobile Data Terminals (MDTs) make it easier for first responders to do their jobs in the field. These tools allow them to spend more of their time in the communities they serve instead of behind a desk. Furthermore, reliable connectivity offers first responders the ability to aggregate data from multiple sources to assist in assessments at a particular crisis scene.

The influx of mobile applications in first responder organizations reflects a larger shift across virtually all industries and work-places toward enabling employees to access the information and applications they need to do their jobs whenever and wherever work takes place.



CAN RESULT IN SAVING OVER 10,000 LIVES ANNUALLY.

Source: Federal Communication Commission

Examples of Mobile Applications in First Responder Organizations

- Evidence management apps allow police officers to provide better documentation and chain of custody tracking, stay in the field longer, and reduce mistakes.
- Personnel accountability systems can track the location of firefighters on a scene, so commanders can account for personnel in real time, which is crucial to firefighter's safety.
- Certain mobile applications can aggregate various data sources and present them to first responders in real time. For example, AskRail allows firefighters to access a listing of the contents of any railcar to assess the risk of chemical exposure, explosions, or other hazards in the event of a derailment.

IN LATE 2017, THE DEPARTMENT OF HOMELAND SECURITY ANNOUNCED THAT 32 OF THE 33 POPULAR APPLICATIONS USED BY FIRST RESPONDERS RAISED SECURITY AND PRIVACY CONCERNS.[1]

Mobile Application Challenges

While mobile applications and the devices they run on can bring enormous value, safety benefits, and cost-savings to first responder organizations, they also bring some potential challenges:

- **Accessibility:** Because these mobile applications are most reliant on a cloud backend, they require constant Internet connectivity, which may be difficult to ensure accessibility in remote areas or when an organization's jurisdiction spans a large geographic territory that may not be fully covered by a single cellular provider.
- **Cost:** It is expensive to have multiple 4G LTE connections spread across vehicles, tablets, MDTs, and other devices versus using the vehicle as a connectivity hub.
- **Latency:** The traditional method of providing secure access from a mobile device to a cloud-based application is to have sessions traverse a centralized data center before forwarding application traffic to the cloud. This "backhaul" approach can cause significant application delays for the first responder trying to use them. While providing direct Internet access can significantly reduce these delays, it requires a new security paradigm.
- **Security:** In late 2017, the Department of Homeland Security announced that 32 of the 33 popular applications used by first responders raised security and privacy concerns, while 18 of those applications contained critical flaws. Isolating mobile apps from Internet-borne threats is paramount.

MOBILE COMMUNICATION TECHNOLOGIES

Advancements in a variety of Internet-enabled public safety communications technologies help first responder organizations achieve enormous gains in personnel safety, time-to-response, triage, and remediation or treatment.

Examples of Mobile Communication Technologies Used by First Responders

- Telehealth and videophone systems make it possible for paramedics to be in communication with healthcare providers at hospitals, and for those healthcare providers to see the patient, receive vitals, provide instructions to the EMTs—and even make diagnoses. These systems allow for a seamless and sometimes lifesaving transition from the ambulance to the emergency room by allowing healthcare personnel at the hospital to spring into action immediately, having already gained crucial information before the patient ever arrives on-site.
- Firefighters can use laptops and mobile devices to share photos and video from the field—for example, photos from arson investigations or crime scenes.
- Police officers are using vehicle-mounted and handheld MDTs for a myriad of tasks, including navigation, receiving dispatches and BOLOs, sharing crime-scene photos and video from the field, and running plates and checking driver's licenses. In fact, much of the information exchanged over the radio is now electronically transmitted via MDTs.

WITHIN THE NEXT DECADE, LIVE VIDEO WILL BE STREAMED TO RESPONDERS IN THE FIELD, OFTEN IN REAL TIME, DRIVING THE NEED FOR PUBLIC SAFETY AGENCIES TO CAPTURE AND STORE IMAGES, VIDEO & TEXT IN THE CLOUD.[2]

Top Mobile Communication Challenges:

Communications technologies are core to rapid response and provide a lifeline to first responders. As more of this communication shifts from voice to data, mobile network availability and performance issues can lead to serious and even life-threatening complications. The following are several common challenges:

- **Reliability:** Whenever mobile network connections are disrupted, the constant flow of information stops. For many MDT applications, this results in the session getting disconnected and require restarting before the data can be accessed again. Recovering sessions is both time-consuming and dangerous if it happens in the middle of a traffic stop.
- **Responsiveness:** As experienced during 9/11 and other large-scale emergencies, LTE networks can quickly become congested and impair first responder voice and data communications. Such situations delay the response, make cooperation between first responder teams difficult, and put lives at risk.

- **Coverage:** For first responder organizations that cover large geographic areas, finding solutions that provide seamless connectivity across multiple cellular carriers can be a serious challenge.
- **Interoperability:** Traditional Land Mobile Radios (LMR) communications use many different frequencies that are not compatible between different first responder organizations, as was witnessed in the response to the 9/11 attacks. The same was true for data networks that were not properly designed to interoperate between agencies. The lessons learned were the catalyst behind the creation of new nationwide public safety broadband networks.

Mobile Network Solutions for First Responders & Connected Technologies

Connected technologies are reducing the dependency on outmoded LMR systems and helping to improve the effectiveness, responsiveness, and safety of first responders. However, to support new technology deployments that span vehicles, mobile command centers, buildings, and even field sites, IT organizations are modernizing their mobile networks with advanced 4G LTE, cloud management, and Software-Defined Networking (SDN).

IMPROVEMENTS IN COMMERCIAL 4G LTE NETWORKS

Commercial 4G LTE cellular networks continue to proliferate in coverage and improve in capabilities, thanks to the demands of video-hungry consumers. Except for the most rural of locations, reliable and performant cellular connectivity is available from one or more carriers. When a particular location requires extra capacity—like a sporting event or in the case of a natural disaster—carriers can rapidly deploy COLTs (Cell on Light Truck), COWs (Cell on Wheels), and flying COWs (Cell on Wings that utilize drones) to add surge capability.

NATIONWIDE PUBLIC SAFETY BROADBAND NETWORKS

Post 9/11, the need for dedicated mobile public safety networks that isolate and protect first responders voice and data communications from consumer traffic became clear and the U.S. government created the First Responder Network Authority to plan and deliver a nationwide public safety broadband network. Other carriers have announced or are planning their own mobile public safety network using a dedicated cellular "core." While different in their implementations and capabilities, these networks provide a common ability to prioritize first responder communications and can preempt all other cellular traffic to deliver needed performance.

Success Story

INDIANAPOLIS FIRE DEPARTMENT

With an overall metro area population of more than 2 million, Indianapolis is the largest city in Indiana—and the 12th largest city in the U.S. With its radio modem network set to expire, IFD began using USB-based air cards to keep its laptops and other in-vehicle applications connected on the go.

Fire personnel noticed improved network access with the air cards, but not to the level needed during emergency situations. IFD needed a long-term, ruggedized solution that would support an external antenna. Additionally, IFD required the ability to push out firmware upgrades from a central location.

The department upgraded to Cradlepoint's ruggedized COR Series routers and NetCloud Manager (NCM) solution.Through NCM, the department's IT team has revolutionized the way it monitors, manages, and troubleshoots its network in fleet vehicles.

"Their trouble tickets have dropped to almost nothing since we put Cradlepoints in."

— Battalion Chief. Dale Rolfson, IT manager, Indianapolis Fire Department

CENTRALIZED CLOUD MANAGEMENT

With advancements in cloud management, first responder IT organizations can manage far-flung mobile networks—and the users, devices, and applications that depend on them—from a central location to ensure the everyone and everything stays connected and protected.

The simplicity, orchestration, and automation aspects of modern cloud management systems enable IT administrators to deploy branch, mobile, and IoT networks quickly and manage more endpoints with fewer people. By making use of efficient, over-the-air protocols designed for cellular networks, cloud management enables administrators to configure, deploy, monitor, and manage mobile networks without running up cellular bills, and integrated remote troubleshooting capabilities reduce truck rolls or the need to take vehicles off the road.

SOFTWARE-DEFINED WAN (SD-WAN)

Today's first responder connectivity requirements span people, places, and things leveraging dedicated and commercial 4G LTE services. As a result, the mobile network edge has to be more elastic so it can expand, contract, adapt, move, and evolve as demands dictate. SD-WAN is a new networking paradigm that replaces the traditional hardware-centric approach with software-defined, cloud-centric network solutions that can automatically adapt to disruptions in underlying wireless and wired connectivity and ensure maximum availability and performance for critical applications and connected technologies.

The elasticity and resiliency that SD-WAN affords make it ideal for organizations, like first responders, that have a multitude of fixed locations, mobile sites, and vehicles with the need for secure and reliable connectivity for applications, collaboration, and IoT.

SD-PERIMETER

As the number of connected devices that first responders utilize continues to increase, so does the risk of a dangerous security breach. SD-Perimeter is a new Software-Defined Network technology designed for securing IoT devices and device-to-cloud communications. It provides a perimeter-secured Internet overlay that encrypts and isolates IoT data from the rest of the mobile network.

As a cloud-delivered service, SD-Perimeter makes it simple to deploy and manage a secure overlay network that connects mobile users and IoT devices directly to the resources they need. Each overlay has its own private IP address space, so it remains hidden from the rest of the Internet—and potential hackers. These invitation-only networks offer fine-grain control with firewalling and filtering to regulate communications going in and out.

Success Story

CITY OF TROY, ALABAMA

When the police and fire departments in Troy, Alabama, and the Pike County emergency 911 dispatch began updating their systems with high-impact technologies such as CAD and electronic records, officials knew they would need more reliable, secure connectivity for their first responder vehicles. The MiFi devices they had been using didn't interface with CAD technology or enable active GPS for real-time tracking.

The agencies deployed Cradlepoint's secure, all-in-one in-vehicle solution, which enables the reliable connectivity necessary to keep CAD, GPS, applications, and key information available 24x7. The solution is ruggedized to withstand constant jostling and a wide range of environmental conditions.

The county's IT team uses Cradlepoint's NetCloud Manager to monitor, manage, and trouble-shoot connectivity and security throughout the fleet, saving man-hours and money.

"The COR Series provided the most cost-effective option among devices that met all of the departments' needs. Also, the man-hour savings that come from remote cloud management added a lot of value for us."

– Randall Barr, Troy Chief of Police

Buying & Implementation Considerations

COST & COST MANAGEMENT

The acquisition price is only part of the total cost of ownership that public safety agencies must consider when modernizing their networks. With the number of mission-critical applications and connected technologies continuing to grow, the ongoing cost of managing, securing, and maintaining uptime of distributed branch, mobile, and IoT networks needs critical consideration.

Many software-defined, cloud-delivered solutions are also available as a subscription service. Such solutions can make it possible for first responder organization to afford more robust, enterprise-class capabilities today that require fewer resources to deploy and manage. Additionally, a subscription approach provides superior flexibility, upgradability, and investment protection as needs change over time.

SECURITY

Protecting mission-critical applications, collaboration, and connected technologies across an ever-expanding network attack surface is as essential for IT organizations within public safety agencies as it is for enterprises. A modern mobile network solution needs to provide comprehensive edge security capabilities that protect local users and devices, the WAN, and cloud communications with access control, FIPS-certified data encryption, IoT device isolation, and Internet threat management.

PURPOSE-BUILT HARDWARE

While the enterprise market is shifting towards more general-purpose network solutions, the unique demands and harsh in-vehicle operating environment encountered by first responders demand ruggedized, purpose-built mobile routers. Careful consideration of shock, vibration, humidity, and temperature rating is required to ensure maximum reliability and return on investment.

FEWER BOXES

Every piece of hardware deployed as part of the mobile network solution brings with it a cost of ownership and another point of failure. Consider a converged in-vehicle router solution that acts as an integrated communications hub with multiple 4G LTE modems and extensive network connectivity capabilities, including Ethernet and WiFi LANs and serial, Bluetooth, and GPIO ports, integrated GPS, and vehicle diagnostic connections. This approach eliminates multiple “boxes” and reduces acquisition, installation time, while also sparing costs as well as points of failure.

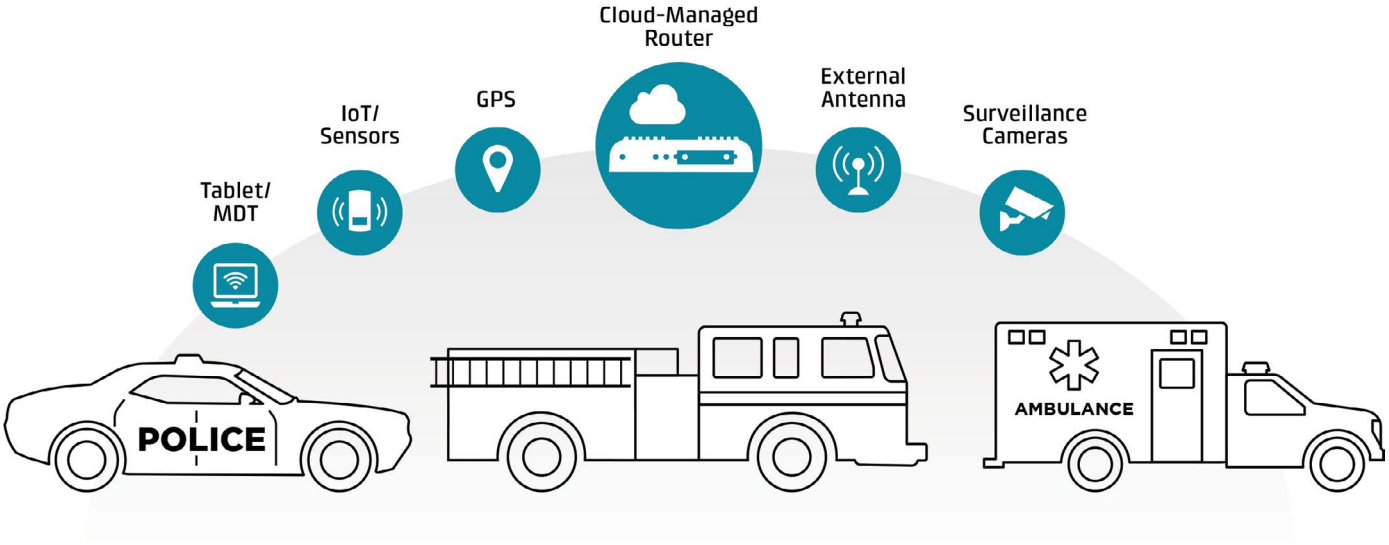
RELIABILITY & RESILIENCY

When it comes to ensuring maximum communications reliability, two links are better than one. Consider mobile network solutions that can support at least two 4G LTE modems, each with multiple selectable carrier networks. When combined with SD-WAN functionality, the router can automatically direct network traffic to the optimal link or links based on a wide-range of real-time performance characteristics. For fixed location deployments, a complement of wired and wireless connections can be used to achieve maximum reliability.

For maximum application resiliency, agencies should consider deploying SD-Perimeter overlay technology that keeps applications and IoT devices always-connected when underlying 4G LTE connections get temporarily disrupted due to poor cell towers hand-offs, switching carriers on a modem, or signal disruptions.

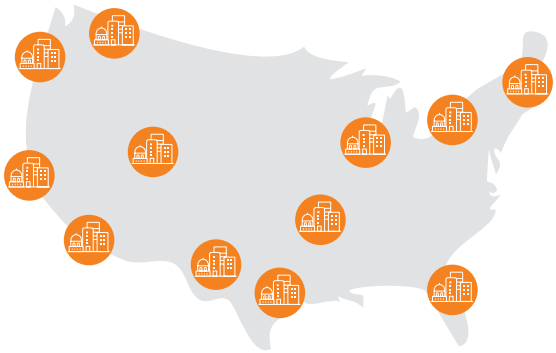
Cradlepoint Advantages

- **Multiple wireless connections:** Cradlepoint branch and mobile solutions support multiple 4G LTE and WiFi-as-WAN network connections to maximize uptime and avoid potentially disastrous service interruptions. By supporting load balancing across multiple wireless connections and even carriers, first responders get the reliable connectivity they need in remote locations, at events, or when disaster strikes.
- **Centralized cloud management:** Cradlepoint's NetCloud Manager cuts the time and cost to deploy and manage networks, both of which are valued assets to any first responder agency. Cloud management enables IT administrators to deploy branch (headquarters), mobile (vehicle fleets), and IoT networks (body worn cameras, etc.) quickly and manage more endpoints with fewer people.
- **4G LTE solutions with mobile SD-WAN:** Cradlepoint's SD-WAN provides first responder applications the highest levels of network resiliency and elasticity with benefits such as intelligent path selection based on LTE signal characteristics and controlling data plan costs.
- **Dual-modem, dual-SIM functionality:** For the most efficient and effective WAN diversity, Cradlepoint offers dual-modem, dual-SIM routers. Dual-SIM means there are two SIM ports inside one modem and the ability to connect to only one carrier at a time and not incur the costs of utilizing two cellular data plans. Or with dual-modem, it may be necessary to utilize two modems at once, where the router is constantly connected to two carriers, allowing for wireless-to-wireless failover and WAN redundancy. Each method can provide agencies the opportunity for cost savings and always-on connectivity, keeping mission-critical applications and devices up and running.
- **Smart WAN selection and advanced analytics:** Cradlepoint offers agencies the ability to understand how their network is being used, pinpoint all applications per network, monitor and analyze traffic patterns and usage, and then optimize network performance based on these fine-grain management capabilities. Being able to see closely into a network helps agency's IT departments save money and achieve a lower total cost of ownership and removes any chances of error that could cause a network interruption at a critical moment.



+ **Software-Defined Perimeter:** Edge security capabilities protect first responders and their devices. With Cradlepoint's NetCloud Perimeter, agencies can spin up perimeter-secured overlay networks with a private IP address space, completely invisible to outside networks, that can be deployed quickly via the cloud.

+ **Comprehensive edge security:** More connected devices means a higher risk of a dangerous security breach. Cradlepoint solutions provide Unified Threat Management (UTM) abilities with a comprehensive intrusion protection system (IPS) and intrusion detection system (IDS), which protects sensitive data. Also, secure web filtering and cloud-based threat intelligence protects first responders whether at headquarters or in their vehicles.



100% of the 10 most populated cities

use Cradlepoint solutions.

About Cradlepoint

With more than 2,000 agency customers, Cradlepoint has public safety and first responder deployments in every U.S. state, including 25 of the largest cities, providing mission-critical data networks for vehicles, mobile command centers, surveillance cameras, and incident response teams, as well as secure connectivity for in-vehicle, on-scene, and body-worn devices.

Cradlepoint is the global leader in cloud-delivered wireless edge solutions for branch, mobile, and IoT networks. Cradlepoint's Elastic Edge™ vision—powered by NetCloud services—provides a blueprint for agile, pervasive and software-driven wireless WANs that leverage 4G and 5G services to connect people, places, and things everywhere with resiliency, security, and control. More than 20,000 enterprise and government organizations around the world, including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and first responders in 10 of the largest U.S. cities, rely on Cradlepoint to keep critical branches, points of commerce, field forces, vehicles, and IoT devices always connected and protected. Major service providers use Cradlepoint wireless solutions as the foundation for innovative managed network services. Founded in 2006, Cradlepoint is a privately held company headquartered in Boise, Idaho, with a development center in Silicon Valley and international offices in the UK and Australia.

To learn more, go to **cradlepoint.com/first-responders**

Sources

https://www.firechief.com/2017/07/03/whats-new-with-firefighter-accountability-and-tracking-technology/

https://www.dhs.gov/sites/default/files/publications/Securing%20Mobile%20Apps%20for%20First%20Responders%20v13_Approved_Final_508.pdf

https://appcomm.org/

http://www.govtech.com/em/next-gen-911/Unlocking-Interoperability-What-It-Means-for-Next-Generation-Public-Safety-Communications.html

http://thehill.com/policy/cybersecurity/365427-homeland-security-project-catches-18-first-responder-apps-with-critical

1 http://thehill.com/policy/cybersecurity/365427-homeland-security-project-catches-18-first-responder-apps-with-critical

2 http://www.govtech.com/em/next-gen-911/Unlocking-Interoperability-What-It-Means-for-Next-Generation-Public-Safety-Communications.html