blueforce DEVELOPMENT

5 DELIVERY WORKER SAFETY

Essential capabilities, enabled by BlueforceBEACON

Why Delivery Worker Safety Software?

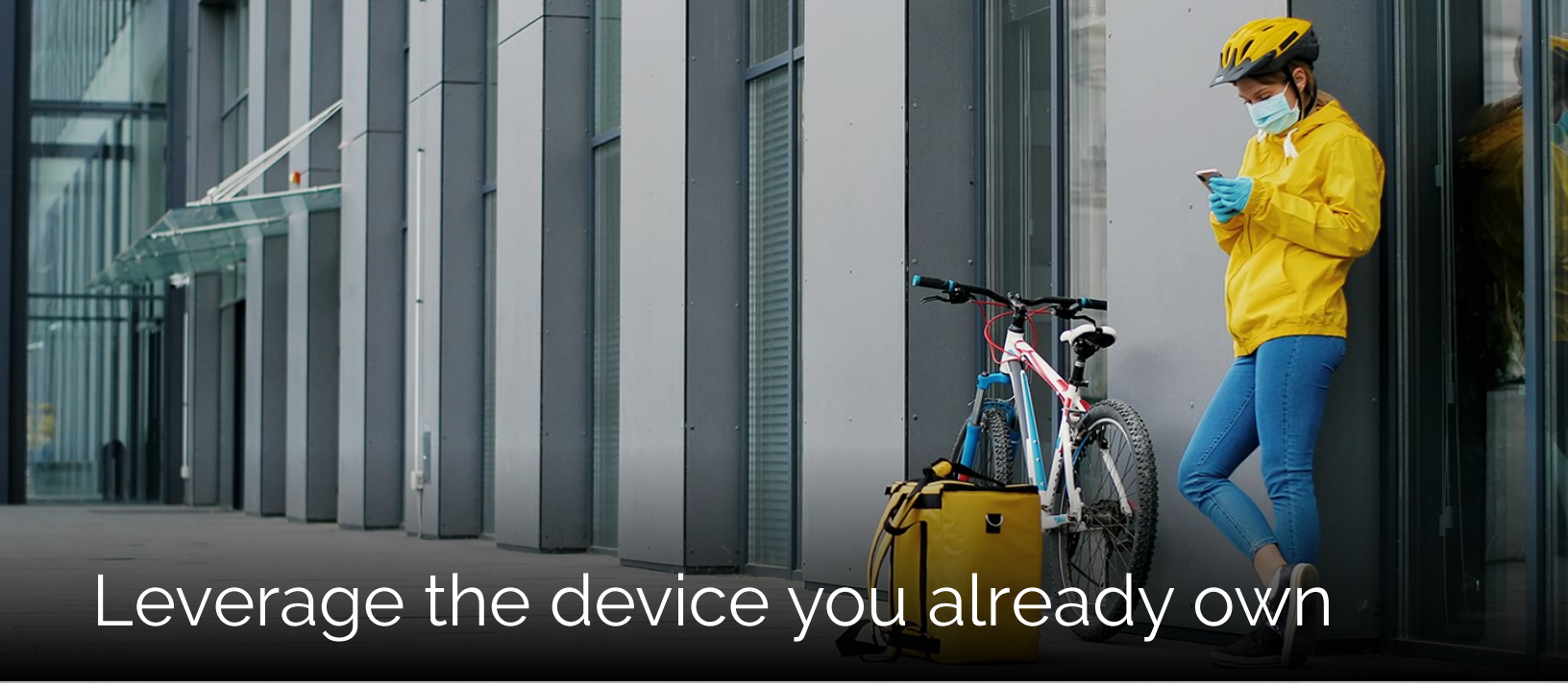
It is most assuredly not our parent's world. We suddenly find ourselves in a new world where the pandemic and serius spikes in crime has implications to our critical infrastructure, our schools, our businesses, and our people. Cybersecurity remains a concern, but physical security in our personal and professional lives is now front and center. Recent attacks and attempted attacks internationally present a diverse and non-predictable threat environment.

Sadly, violent acts have become a significant risk in our work lives and many catastrophic incidents have been reported by headline news. Recent events have shaken the sense of serenity and security that has characterized our work environments, fixed or mobile. While the risk of serious violence remains somewhat low, particularly in its most extreme forms, the potential consequences to people and businesses can be devastating and long-lasting.

Mobile delivery workers face increasing and significant risk of job-related violence. Pick up any newspaper and one can find reports of personal attacks and in a few cases, loss of life of workers that venture into our neighborhoods and homes to deliver goods, provide in-home health care, and support and protect those at risk.

If you are considering solutions to protect your workers, this eBook is for you. The marketplace is rife with "I've fallen and can't get up" big red button hardware solutions, but none of them provide the environmental intelligence and ground truth intelligence needed to properly mitigate and deal with life threatening situations. Muddying the waters further, the total cost of ownership (TCO) between solutions varies dramatically.

Knowledge is power, and this eBook will make the case for software based life safety solution for Delivery Workers. For a number of reasons to be illustrated a software solution is superior for keeping people safe, be it in a school, in an office, or for mobile delivery workers.



Leverage the device you already own

Essential #1:

Personal Security Software Leverages the Devices and Data Plans You Already Own

Let's cut to the chase: telecommunications companies are dying to sell you another device and activation. Activations and "yet another data plan" represent the very metrics by which Wall Street measures carrier growth, hence it is difficult to blame the carriers for pushing hardware solutions. The fact of the matter is that personal security does not require another device, another red button, or another data plan. If your personnel carry an Android or Apple iOS device, they have everything they need for personal security notification. Just about every smartphone and tablet with an existing data plan is capable of being an exceptional personal security tool using less than 60MB of data per month.

An additional benefit of leveraging the smart phone is that in general, no one leaves home without it. We ask you to think about your own behaviors. What is the one thing you carried to lunch today? What is the one thing you carry and hold close for a night out on the town? What is the one thing most of us keep close to our beds at night because we have families and children? We no longer care as much about wallets or purses: We carry and look after our smartphones. Smartphones are what keep us connected to our world and they can be our lifelines as well.

Almost all of us have a data plan that provides at least 10GB of data per month. Personal security software on a mobile device generally uses less than 60MB of data per month. This equates to .006% of an average 10GB data plan. From an economic and cost of ownership perspective, with data usage at less than .006% of one's plan, why would anyone want to pay another $9 a month for a machine to machine (M2M) data plan to enable a big red hardware button? Why would we expect that anyone would want to maintain, carry, and charge yet another device? It is completely duplicative, unnecessary, inconvenient, and significantly more expensive.

Essential #2:

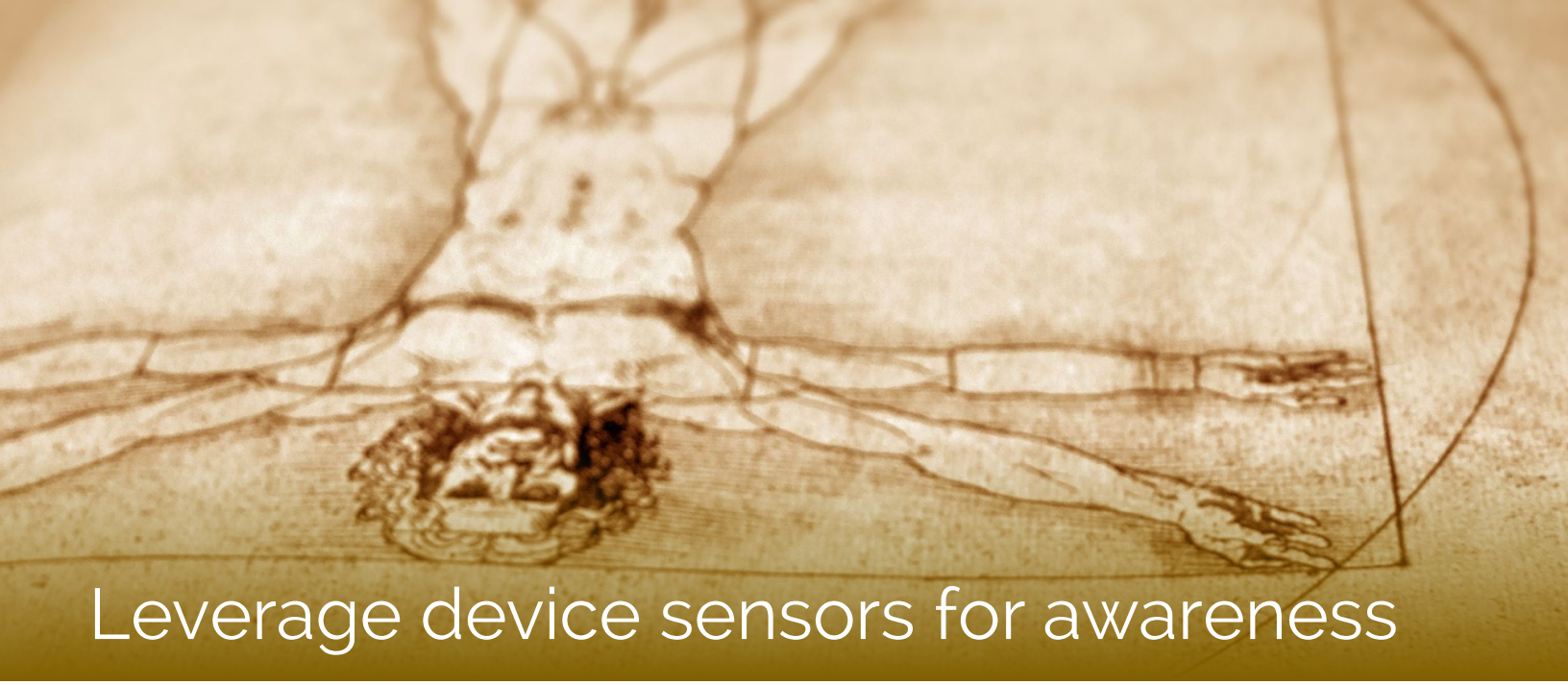
Overt and covert SOS triggers, and a means to signal the nature of the delivery worker emergency

There is a place in the world for the "big red button" hardware solutions and that is for medical emergencies, particularly for the elderly. The big red button hanging around one's neck is an easy target to hit in a medical emergency, but most emergency situations require clarity in the nature of the issue so that the appropriate responders are dispatched. For example, teachers in the classroom environment dealing with a medical emergency requires a very different kind of response versus an active shooter scenario. Hardware-only solutions allow for only ONE call for help: send the "SWAT" team. All emergencies are the same to a hardware solution. Emergencies come in different forms and require different responses.

The BlueforceBEACON software-based solution allows for enterprise definable SOS scenarios, with overt and discrete options. Overt panic signaling is easy to do: explicitly swipe the UI and help is on the way. This is the equivalent of hitting a big red button. Importantly, the modern mobile device allows for a number of additional and non-overt ways to signal that help is needed. These methods are enabled by sensors in the devices themselves, sensors that dedicated panic hardware solutions do not provide.

- "Rip Cord" Signaling: Blueforce's patented approach to capturing hardware sensors allows for an act as simple as pulling one's headphones from the smartphone to signal a panic event. This "ripcord" function allows the user to focus on escape and calling for help via a covertly executed action.
- Button Mashing: Blueforce's patent pending approach to personal security includes a means to mash (i.e., push intently on hardware buttons) various buttons on the device itself to signal a need for help. Blueforce provides native support for device buttons on Zebra handheld products.

Blueforce has supported specialized extensions to wearable and other "Bluetooth-connected" devices for overt triggering of an SOS to include proximity, loiter, and a complete lack of motion leveraging the device accelerometer, gyroscope, and internal GPS.

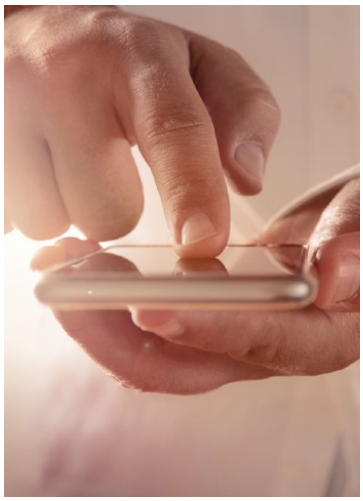


Leverage device sensors for awareness

Essential #3:

Awareness of smart device position, motion, trajectory, and other "ground truth" data

Mobile smart devices are in a constant state of innovation through improvements and diversification of onboard sensor packages. Only software-based solutions can rapidly evolve as manufacturers update hardware and native capabilities. As well, new operating system features (Android, iOS, Linux) features that power smart devices will evolve faster than proprietary dongle/hardware solutions. The multitude of native sensors in the phone provide valuable ground truth as to what is going on with, and around, a user. Consider the following:



- Accelerometer sensors: The accelerometer sensors in even the least expensive of devices have the ability to detect minute elements of movement. While simple ambient air pressure can cause accelerometers to fire, the meta-data from these innate sensors provides great awareness that can be leveraged to discern true endpoint health.
- Gyroscope sensors provide real time information on range of movement. It's not just flutter and detection of movement, it is range of movement and includes awareness of vertical movement, or sub-optimal horizontal movement.
- Device magnetometers provide not only real-time direction of travel, but also provide historical data allowing for the reconstruction of an event. These data points are critical for deriving reliable historical data that can be key in mitigating an emergency.

These same sensors also provide an opportunity for sensor fusion, where software-based solutions can "look across" disparate device sensors and derive meaning. For instance, accelerometer data correlated with GPS data, can indicate a device may be motionless, but only because it is on the dashboard of a moving vehicle indicating that the human is not experiencing a life safety issue.

Essential #4:

Eyes & Ears on the "X"

"X" marks the spot where personal assault or an attack takes place. It's the spot where an adversary is focused, and has planned his or her criminal action. Getting off the X means moving to cover, moving to create distance, or moving to make oneself a more difficult to exploit.

Yet, in many cases, it may not be possible to move off the X, or, moving may further inflame a situation. When movement isn't possible, for whatever reason, an ability to remotely understand "who" and "how many" are around the X, becomes truly important intelligence when coordinating the response.

Seeing is believing, but an ability to "listen" in real time is often just as good. Blueforce software based solutions leverage operating system APIs to control, trap, fire, and transfer imagery as well as audio-based information.

Receiving a PANIC signal from an end-user is most assuredly disturbing, but having an ability to listen live or remotely order the capture of imagery from on-board cameras enhances responders' ability to address the emergency in an appropriate manner. These abilities allow responders to understand "who", "what", and the "intensity" in the environment around the person in trouble.

An ability to remotely turn on the microphone of the troubled endpoint allows responders to hear what is going on and potentially collect information that could also be useful in a response. Furthermore, these audio streams can be persisted maintaining full chain of custody, for evidentiary use.

Blueforce software-based personal security solutions enable this capability with full control over workplace policies specific to privacy, and it is being delivered today.

Atmospherics when GPS Denied

Essential #5:

Leverage and report signal intelligence when in GPS denied situations

What if an employee or loved one finds themself thrown into the trunk of a car? Those tasked with finding and deploying a personal security solution need to consider scenarios that are GPS denied. Denied environments can include locations inside of buildings, or inside the trunk of a motor vehicle. In these situations, a means to extrapolate and report approximate location based on atmospherics becomes critical.

Atmospherics can be thought of as "signal" detection and intelligence. As we go through our day, we are surrounded by signals that are emitted from WIFI access points, cell towers, and Bluetooth Low Energy (BLE) beacons. Software-based personal security solutions riding on smart devices provide an ability to listen for and report these signals even when the user is moving. Furthermore, signal intelligence can be used for evidentiary purposes tying an attacker to a specific location at a give date/time. Consider the following:

- BLE atmospherics can be leveraged for interior proximity detection. Given that BLE beacons have a range of 30 feet or so, they provide an inexpensive means to "tag" a room in a house or a school. When the user is in an emergency state, the software reports the BLE beacons heard by the Smartphone as well as the proximity of the beacon to the Smartphone.
- Similarly, WIFI access points can be detected and reported. If one were to imagine an emergency occurring in a mall. The smartphone can detect proximity to the Starbucks. Your grandmother's panic button certainly cannot do this and this awareness can be the difference between life and death.
- Cellular atmospherics can also be leveraged for situations where the user in trouble is moving, but cannot report GPS coordinates due to a lack of access to the sky. BlueforceBEACON on a smart device can report and update, in real-time, cellular towers the device is connected to and.or proximate to.

About BlueforceBEACON

BlueforceBEACON is a highly secure and privacy aware software based emergency notification system that provides a safety net to mobile workers. The product delivers location services, secure text communications, covert emergency camera triggering, “listen live” capability, and provides situational awareness of end-user movement and position. Built on Blueforce’s patented location and sensor fusion platform, BlueforceBEACON endpoints can be autonomously monitored where no personnel are required and panic notifications are done with email, SMS, and/or automated workflows. When BlueforceBEACON is used with Blueforce Web Command Center (WEBCC), users can be monitored by dispatchers in real-time on the WEBCC map with visual and audible alerts when a user triggers a "panic” event.

Solution Areas

- Lone Delivery and Supply Chain Workers
- K-12 & College Campus Safety
- Executive Protection
- Visiting Social/DCF Workers
- Emergency Management
- Lone Visiting Nurses

www.blueforcedev.com | +1.866.960.0204