

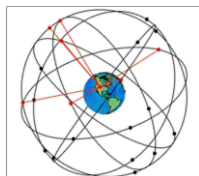


The ubiquitous phrase “critical infrastructure” is often associated with key industrial and government functions and networks. According to the United States Government, [critical infrastructure](#) includes any “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

The primary source of distributed and accurate timing information is from the United States’ Global Positioning System (GPS) satellite constellation. Through GPS signals accurate position, navigation, and timing (PNT) is distributed globally. These PNT signals are a necessary component for multiple critical infrastructure sectors. Precision timing is one feature that is of particular importance. In numerous infrastructure systems, such as the electric grid, law enforcement, transportation, telephony and data communications, as well as financial networks a one microsecond-level or better timing synchronization is required. Generally, GPS timing is used in distributed interconnected systems that require strict timing synchronization for monitoring, control, production, transaction tracking, and other functions. It is these systems, at the heart of a facility, that are the targets for malicious activities. In the United States, a presidential executive order on [Strengthening National Resilience](#) is in place to protect against these activities. By design GPS’ space-based signals are low in power and unencrypted, this makes them susceptible to both intentional and unintentional disruption. The ability to disrupt critical infrastructure operations and deny their processes and services can lead to catastrophic consequences. Both US and Europe are now tracking active jamming events that can disrupt critical infrastructure and report to the government for action such as in [Europe](#) and in the [United States](#). Sometimes it can be too late!



GNSS — Position, Navigation, and Timing



It has become increasingly important that GPS PNT data be both available and reliable. GPS satellites have multiple internal atomic clocks that, in combination, enable very precise and reliable time data. Receivers decode these timing signals, effectively synchronizing their time to the GPS network of atomic clocks that lets time to be determined to within 100 billionth of a second. Jamming attacks have become more commonplace, more dangerous, and more sophisticated. Criminals, terrorists, and other adversaries create havoc and mayhem by jamming GPS signals. Overcoming and ensuring continued operations during jamming disruptions is critical.

The need for global navigation system (GNSS) position, navigation, and timing signals from satellite constellations is growing rapidly in our highly interconnected world. GPS has become an indispensable silent utility that creates significant economic advantages transforming lifestyles and businesses.



infiniDome's full stack solution provides the ability to monitor, detect and protect critical assets real time. Our patented anti-jamming technologies set infiniDome apart. Military and Defense applications have solutions that protect from GPS jamming, however commercial applications like the critical civil applications being described, are still vulnerable. infiniDome brings industry's only commercial GNSS PNT protection solutions. infiniDome's offerings deliver proven [resilient PNT](#) anti-jamming performance for GPS receivers operating and maintaining operations in critical infrastructure environments. Our products offer interference detection and mitigation (IDM) and also a receiver's ability to maintain signal connectivity during a jamming attack. Rejecting RF interference while protecting GNSS signals ensures continuity of operations. Our products are available in small, affordable add-on modules or board options that enhance and protect any GPS receiver. They are secure, lightweight, very affordable and can be configured with all GNSS/GPS receivers interfacing at the RF level.

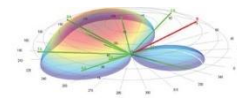
Combining infiniDome's products with our communications module enables real-time data about GPS signal level, disruptions, jamming attempts, etc. to be collected in the cloud and made available as actionable alerts that can protect against real threats. infiniCloud is a SaaS solution collecting real-time and statistical data on GPS jamming attacks and ongoing GNSS signal monitoring for its users as experienced in the field. infiniCloud monitors the health of the GNSS signals in addition to providing instantaneous alerts allowing early detection and immediate response for attacks on critical assets. When a jamming attack is detected, operators can alert authorities with actionable intelligence for appropriate response to the alert. Being cloud-based, infiniCloud can be readily accessed through popular web browsers and supports FCAPS (Fault, Configuration, Accounting, Performance and Security), the 5 major pillars that define network management monitoring systems.



infiniDome technology provides:

Resilient PNT In a Tiny Form Factor

Allows critical infrastructure operators to sprinkle infiniDome's technology across their network due to its small form factor — whether it be power grids, airports or similar critical infrastructure — to monitor, detect and protect GPS disruptions and gain tangible advantages by getting real-time notifications and reports on all their assets. Providing complete resilience!



Intel Gathering, Monitoring and Early Alert

All infiniDome products offer resilient PNT and support IDM to protect and defend GNSS signals. When triggered, an alert is transmitted to both the operator and the operations center. If configured with infiniDome's optional CommModule, the attack data is also sent via a cellular data link to the secure infiniCloud data warehouse which is accessible only to registered users.

About infiniDome, Ltd.

infiniDome provides front-end cyber solutions protecting wireless communications from jamming and spoofing attacks. infiniDome's products protect against attacks of GPS-based systems, which are critical for autonomous vehicles, drones, connected fleets, and critical infrastructure. infiniDome's products have been successfully proven in the field and sold to customers globally.

GET YOUR EVALUATION KIT TODAY! REACH OUT THROUGH OUR [INQUIRY FORM](#) or chat or CALL US: +1-212-729-6052