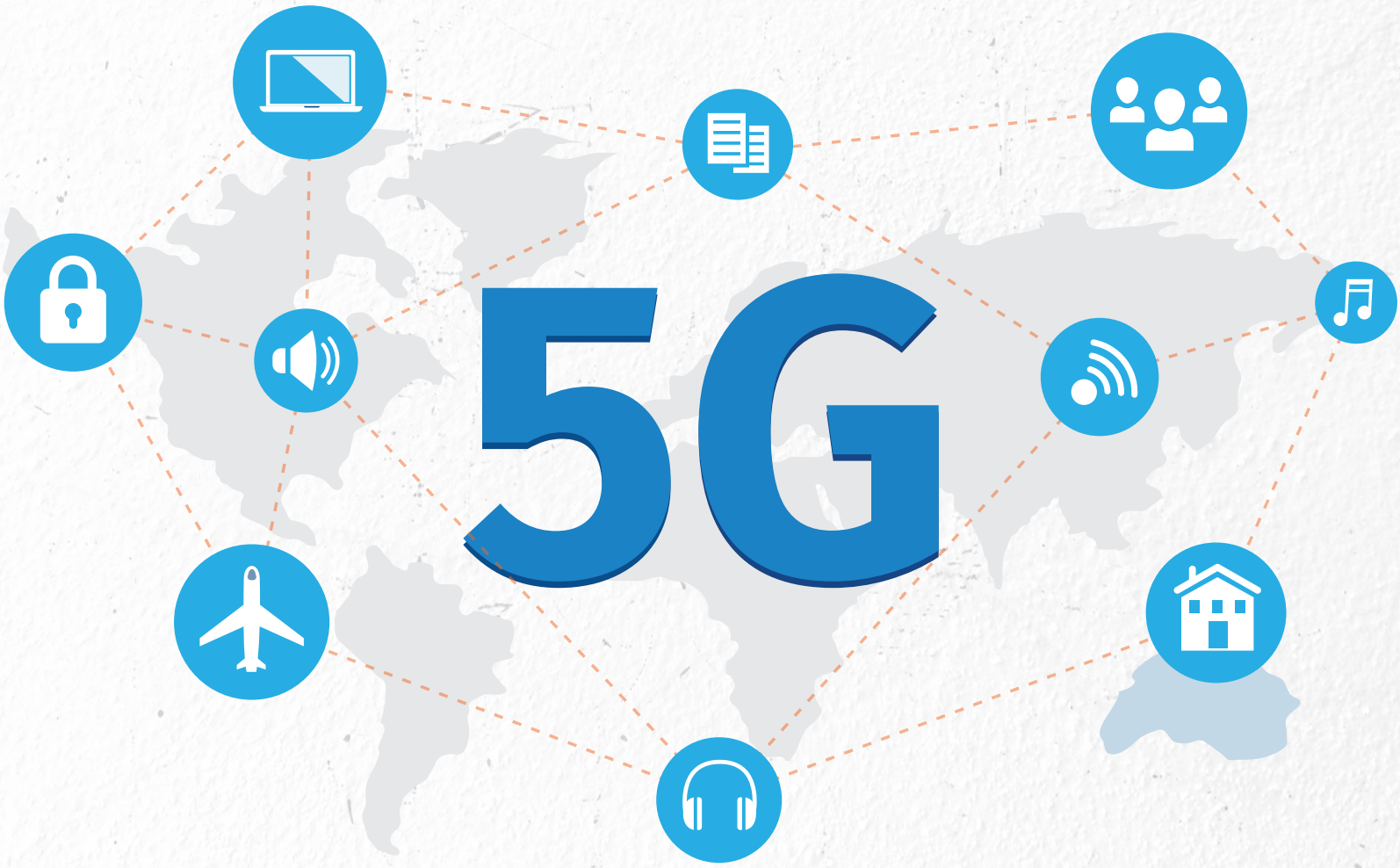
The Promise of Private 5G in Defense and Public Safety

Mitigating Radio Frequency Challenges While Increasing Safety, Security, and Success

Troy M Morley, Principal Analyst

FROST & SULLIVAN WHITEPAPER

CONTENTS

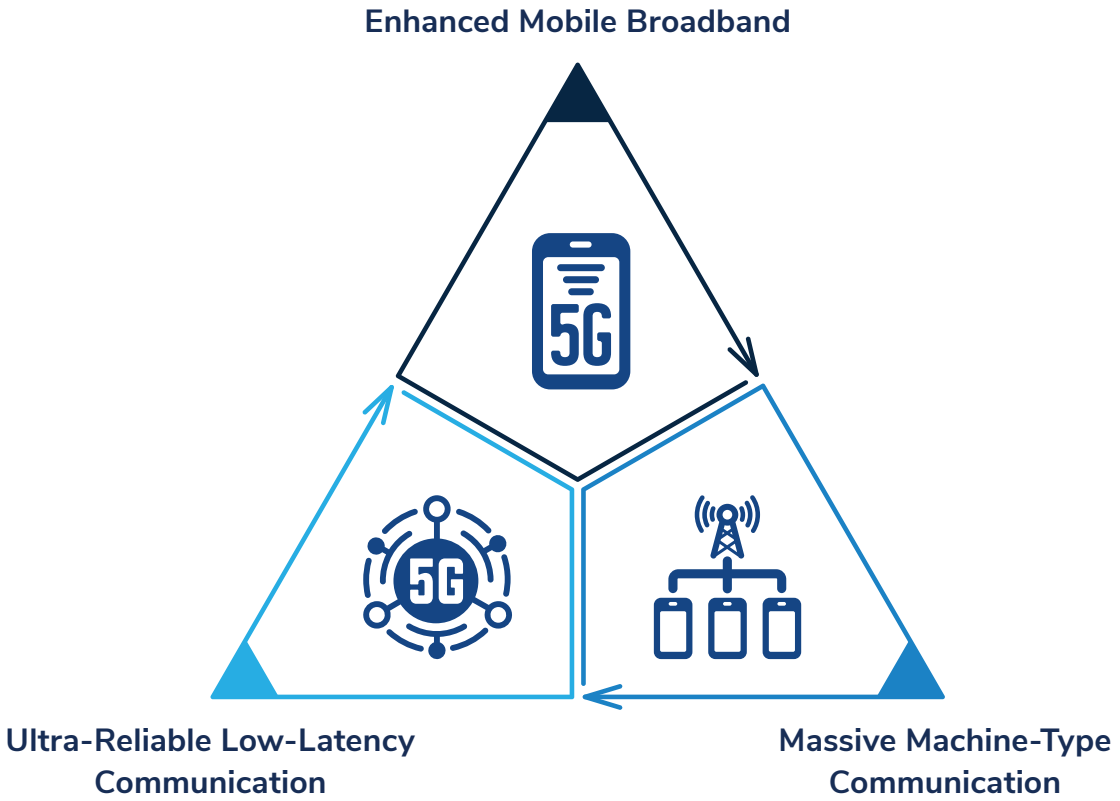


The Opportunities Presented by Private 5G Networks in Defense and Public Safety

Overview of 5G, private cellular networks, and enterprise connectivity needs

Enterprises and agencies related to public safety, first responders, and defense have problems that private networks can help solve. Existing technologies, like Wi-Fi, although here to stay, were not engineered to address the new needs of recent applications like facial recognition that depends on high bandwidth, or the low latency needed for real-time maps and video to manage and train troops.

With the evolution of cellular networks to 5G, the focus has shifted from the consumer to providing new types of capabilities to support the needs of different government agencies or defense-related enterprises as well as enterprises in other vertical markets. The three pillars of 5G are shown below.

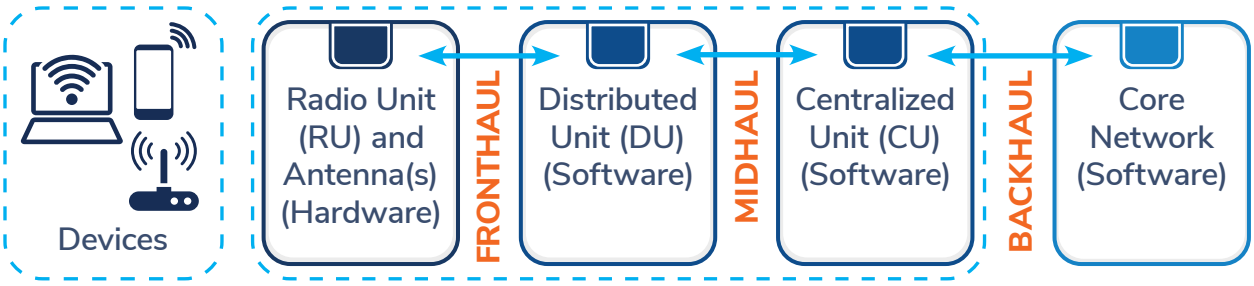


Source: Frost & Sullivan

The public cellular networks provided by mobile network operators (MNOs) are designed to support millions of consumers, and the primary offering is enhanced mobile broadband which increases network speed and capacity.

Private cellular networks have the same components and technologies as public networks, but they are tailored to the specific requirements of *that particular network*. This means each private cellular network is somewhat unique to support a particular application important to the agency or enterprise. Private networks are now likely to use 5G to capitalize on the low-latency or massive communication pillars of the new technology in addition to enhanced mobile broadband.

The Components of a 5G Network (Public or Private)



Source: Frost & Sullivan

The application determines the 5G benefits that are most important to the owner of the private network. For instance, a defense-related manufacturing company using a private 5G network for communication between machines on a production floor will be most concerned with supporting a massive volume of connections to improve productivity and reduce costs. When discussing defense, the first thoughts often involve armed forces; private 5G networks will play a role there as well. On a battlefield, the network may be used between troops or to control machinery such as drones; reliability of the network will help save lives. In all cases, in order to meet the goals of a private cellular network, devices need to access the network when needed and retain that connection as long as necessary.

Why would an agency or enterprise invest in a private 5G network? Simply put, they have problems that cannot be solved efficiently with existing wired or wireless networks. The capabilities of 5G were designed with these requirements of enterprises across verticals in mind. With limited—and expensive—spectrum, a critical factor to any wireless network is to understand the challenges that might be faced while utilizing the available spectrum.

The same is true in the defense vertical: problems must still be solved. The defense vertical shares many needs with other verticals but introduces new requirements that are unique. For instance, there are defense-related manufacturing facilities, warehouses, and bases where private 5G networks could solve problems similar to business enterprises. The security requirements may be more exacting in defense, but many enterprises already treat their intellectual property (IP) as "top secret"; security is a consideration in most private networks.

The stakes become much higher if private 5G networks are used in a conflict. Communication with people and with machines becomes literally about life and death. Interference moves from being somewhat random to intentional, as jamming RF signals becomes a tactical approach. Imagine if a network supporting deployed troops is hit with a jammer. The normal communications radius of several miles would be severely reduced and possibly lost entirely, leaving them isolated and vulnerable.

Opportunities abound

This presents many opportunities around private 5G networks being used by the defense sector:

Defense-related enterprises can solve the challenges they face and increase efficiency, safety, security, and the bottom line.

MNOs—the cellular network experts—can monetize their expertise and their spectrum holdings.

Network infrastructure suppliers have potential new customers, expanding from relatively few MNOs serving each country to a large, well-funded portion of each country's government budget.

System integrators and industry specialists know the needs of their customers and may be best positioned to help with their connectivity needs (working with MNOs and network suppliers.) This is especially true in the defense sector where there is an understandably large need for security.

Defense Use Cases with Private 5G

The Department of Defense (DoD) in the United States has been conducting tests and trials for a number of years with 5G private networks.

The DoD is conducting smart warehouse experiments to utilize advanced technologies powered by private 5G networks to enhance efficiency, automation, and logistics management within warehouses.

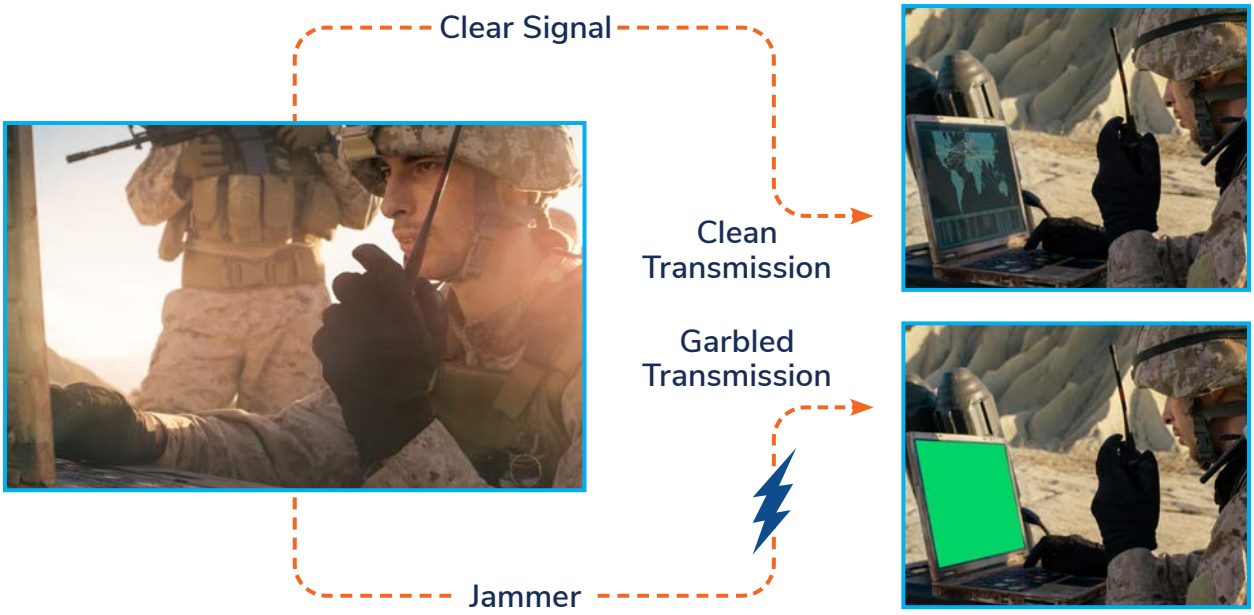
The DoD is also utilizing augmented reality (AR) and virtual reality (VR) with private 5G networks for mission planning and tactical and operational training.

The Navy is experimenting with how private 5G networks can separately manage the security of sensitive data (from ships and planes) and personal device data.

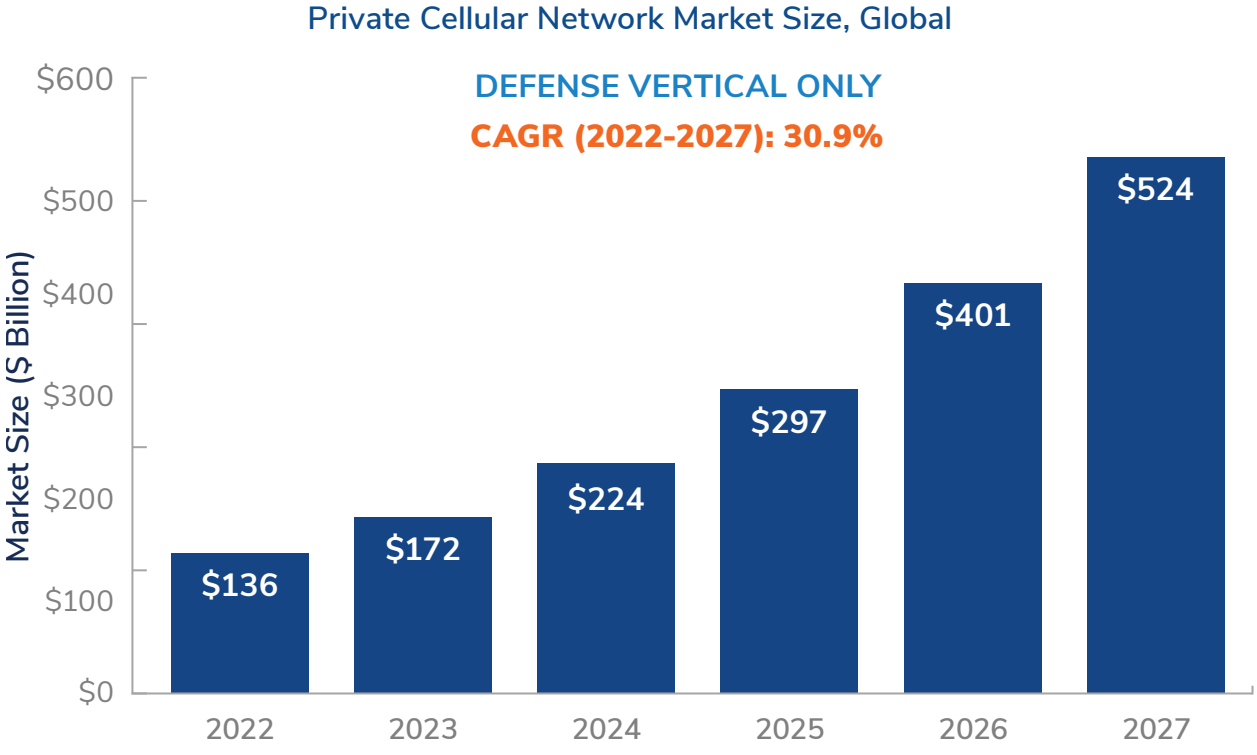
The Navy is also using private 5G networks to provide rapid data transfer from ships to shore.

In addition, the DoD is trialing ways to provide enhanced connectivity and information sharing between different branches of military to allow seamless battlefield decision making.

Jammers are a particular concern to public safety, first responders, and defense. In order to keep wireless networks working as intended, jammers need to be identified and mitigated.



While the public cellular infrastructure market is quite large, it is slow growing, with annual gains in the single digits even in the best years. The private cellular market size for the defense vertical is currently relatively small, though there are many tests and trials ongoing. Frost & Sullivan projects a compound annual growth rate (CAGR) of 30.9% over the next five years and a global market exceeding $500 million in 2027, as shown in the following chart.



Source: Frost & Sullivan

While There Are Opportunities, There Are Also Potential Issues That MUST Be Addressed

Facing RF challenges

If one examines the cables used in a wired network, there is a significant amount of shielding involved. Why? To reduce interference.

In a wireless network, *physical* shielding is not possible, but the challenges in getting the RF signal to the device and back to the RAN can be significant. Interference can reduce the coverage, capacity and reliability of the connection, increase the latency, or disrupt the connection completely, making it difficult to realize the benefits of 5G expected for the application.

The importance of the initial RF design in a private 5G network

Solving these challenges starts with the design of the network, which must be done by experienced RF experts. In addition to the normal planning for capacity, coverage and throughput, networks used for defense, public safety, and first responders need to include resilience against jamming in their design. Maximize coverage and line of site. Minimize blockages. Identify potential jammers. And much, much more.

Even with an expertly designed private 5G network, problems can (and likely will) crop up. The physical layout of the area covered can change, perhaps with a new piece of equipment that may reduce coverage and/or introduce interference. New jammers or other sources of interference may be introduced since the network's initial design.

These issues are not confined to private 5G networks...public cellular networks have the same issues.

A survey of MNOs who own public RANs globally—*that were designed and installed by experts*—reported that **7.5% of cells experienced severe RF interference**.

RF challenges crop up in every wireless network

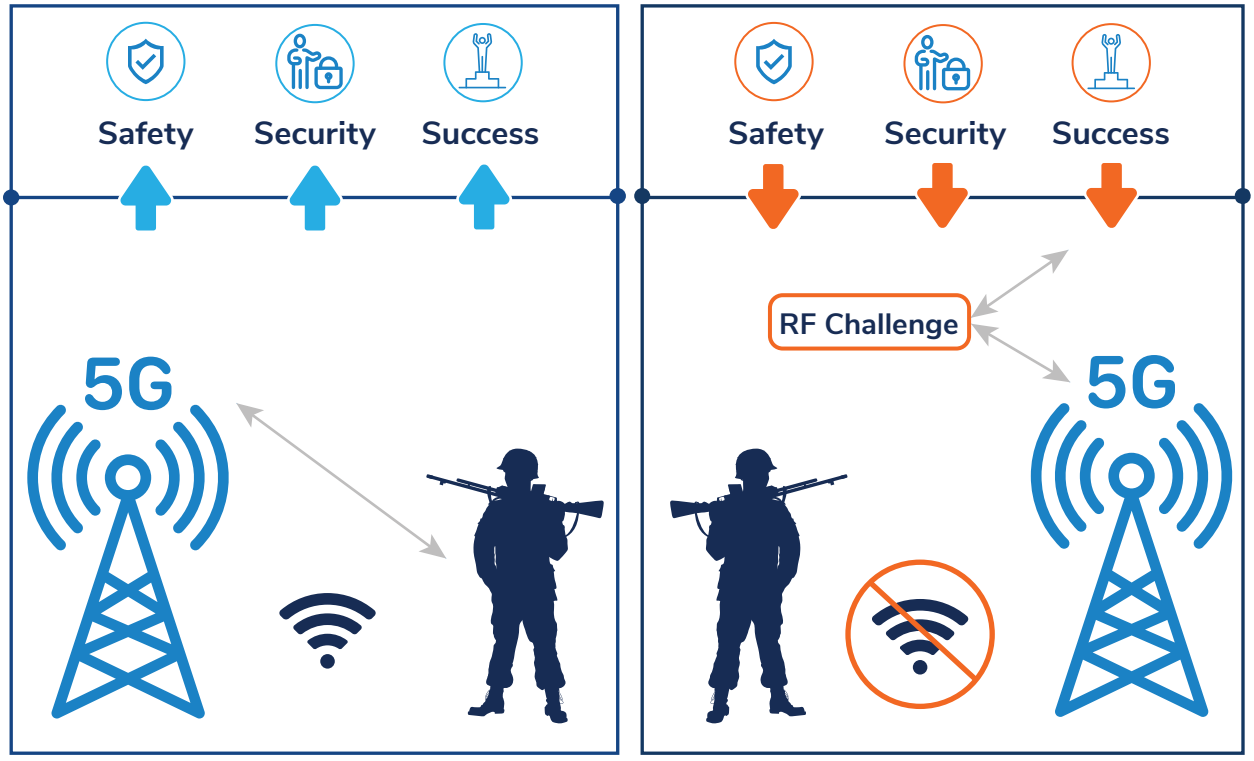
The point is that EVERY wireless network will encounter RF challenges at some point.

For a private 5G network in public safety and defense, what are the implications? If the network is solving problems that are like other industries (such as defense-related manufacturing facilities, warehouses, and bases), the consequences may be *only* financial. It is likely that part of the justification for having the private 5G network in the first place was to enable use cases that involved safety and/or cost savings; RF challenges can impact or even reverse planned cost savings.

The implications for defense, like public safety and first responders, can be much more severe.

Private 5G networks present highly viable opportunities to both the defense and defense-related industries and to MNOs, network infrastructure suppliers, system integrators, and industry experts *IF* the RF challenges are addressed. **The good news is that these issues can be controlled.**

5G Private Network Opportunities Can Be Impacted By RF Challenges



Source: Frost & Sullivan

ISCO International: Reducing RF Challenges and Strengthening Defense Against Jammers

Introducing ISCO International

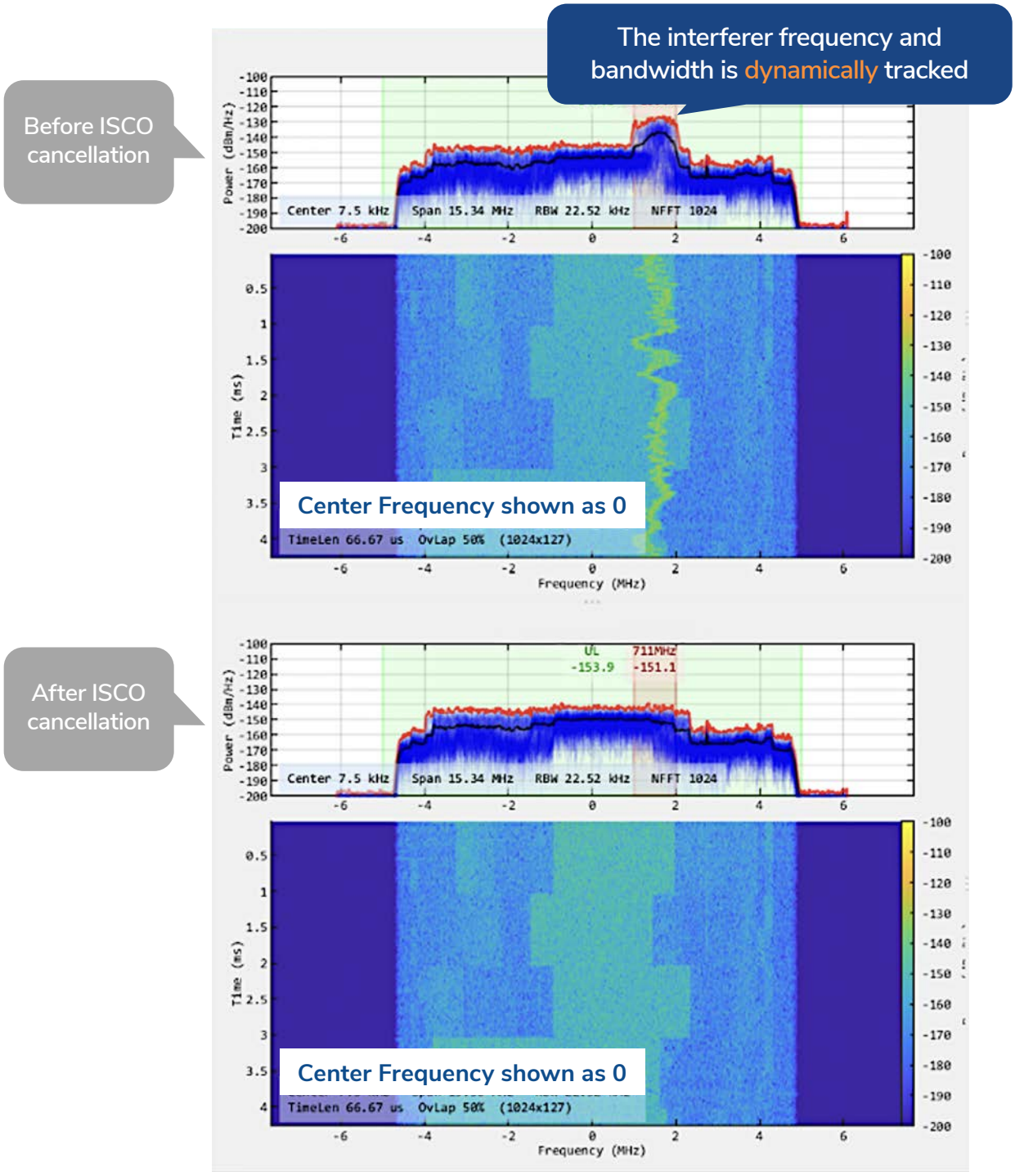
ISCO is a private company that develops and delivers solutions to reduce the impact of RF interference from a wide variety of sources including passive intermodulation (PIM) and jammers. For over 30 years, ISCO has worked with Tier 1 mobile operators to deploy interference management solutions throughout their public networks. This same technology is now being applied for use in private networks to address RF challenges that can prevent these networks from meeting their goals, including in defense and defense-related networks.

Of special interest to public safety, first responders, and defense is the threat posed by jammers. Building on the expertise gained from handling a wide range of interferers found by working with public networks, ISCO has developed the ability to detect, identify, and remediate jammers, offering significant protection at all times along with the increased coverage and capacity that comes from removing or reducing the interference.

A significant challenge for public safety, first responders, and defense is that jammers are always evolving and it's hard to know what specific RF signals to look for in order to protect against them. Due to constant change, an effective solution must very quickly learn, develop, and deploy anti-jammer updates. ISCO has a comprehensive program to provide a strong defense against jammers, made up of four elements:

- **CAPTURE** jammer signatures
- **LEARN** how the jammers operate
- **BUILD** new algorithms to mitigate the interference from each type of jammer
- **REDEPLOY** enhanced software through a quick and easy upload

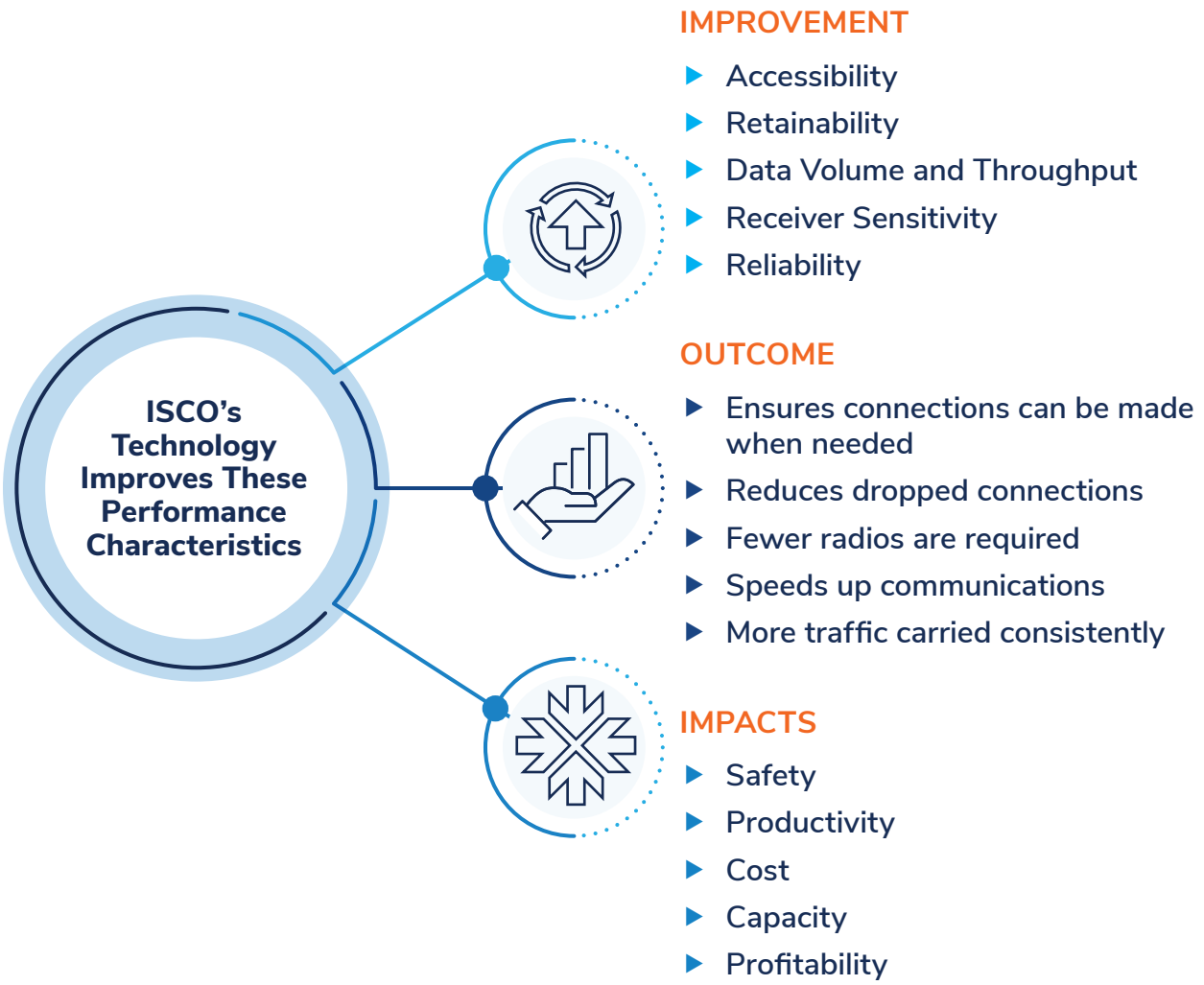
The following figure shows the impact of cancellation on a specific type of interference that was causing harm to a network. The wideband interferer is easy to see in the top half of the figure where the power is elevated in the line graph and the affected physical resource blocks (PRBs) are yellow in the heat map. An important thing to notice in the view after cancellation is that interference is removed and that portion of spectrum is recovered so it can be used to carry traffic and increase accessibility.



Source: ISCO

As mentioned earlier, public safety, first responders, and defense use private wireless networks to facilitate communications across a wide area or on a military base. All of ISCO's solutions improve key performance characteristics in private networks to ensure the goals of the private network are met by ultimately impacting productivity, safety and profitability. These impacts are summarized in the following table.

Private Wireless Network Performance



Source: ISCO

ISCO's Fortis™ Technology

ISCO's new patented Fortis™ technology was recently introduced which specifically capitalizes on polarization properties of radio frequency electromagnetic waves. Fortis complements and enhances other ISCO algorithms and technology – it can be applied to antennas and radio units or to other types of discrete RAN products. Additionally, it can be applied to any device or component that facilitates the transmission and reception of radio frequencies.

The technology can be deployed standalone or embedded in a variety of devices, depending on who is using it and deciding where the interference management will be added. All of these scenarios have already been developed and tested:

1. Fortis IP integrated into an antenna.
2. Fortis IP implemented using digital signal processing in the RAN.
3. Fortis IP embedded in an RF device before the RU.

Fortis IP Integrated into an Antenna

Including Fortis in an antenna reduces and/or eliminates many RF issues as the signal is sent or received. This eliminates the need for complicated antenna positioning and adjustment. For instance, the interference from PIM that can result from antennas located too close together is avoided by the Fortis-enhanced antenna itself.

Fortis IP with Digital Signal Processing

ISCO algorithms perform digital signal processing on the received radio signals. This starts with a segment of the received signal being captured and analyzed using a variety of different patented techniques. The analysis will detect and classify interference if present. This information is then used to compute a set of parameters to condition the signal and reduce or remove the interference.

Fortis IP Embedded in an RF Device

Using its Fortis IP, ISCO has also packaged its technology into a simple-to-install RF product that helps reduce RF challenges, showing that interference management can be included as new devices are developed for private networks.

In addition to the above scenarios that have already been tested, ISCO's Fortis IP can be added directly to silicon chips, expanding the possibilities for use in the various components of private networks.

Protecting the Private 5G Defense Network

Frost & Sullivan projects that the market for private 5G networks specifically within the defense sector will grow very quickly over the next five years. **Why? Because they solve problems for a wide range of defense-related needs that other options cannot solve.**

However, there are many options in providing a private 5G network. Which radios (RUs), which antennas, which DU supplier(s), which CU supplier(s), which transport supplier(s), which core network supplier(s), and more.

Since RF challenges occur in EVERY wireless network, there is another important differentiator: which private 5G network minimizes the inevitable RF issues and interference and protects against jammers? **Answer: the one with ISCO's Fortis technology.**

When ISCO's technology is included, the private network will work better, and risks are minimized because the network can handle more wireless connections. Interference management is critical to public safety, first responders, and defense to not only make sure the network has enough coverage and capacity, but also to remove jammers that can cause serious harm.

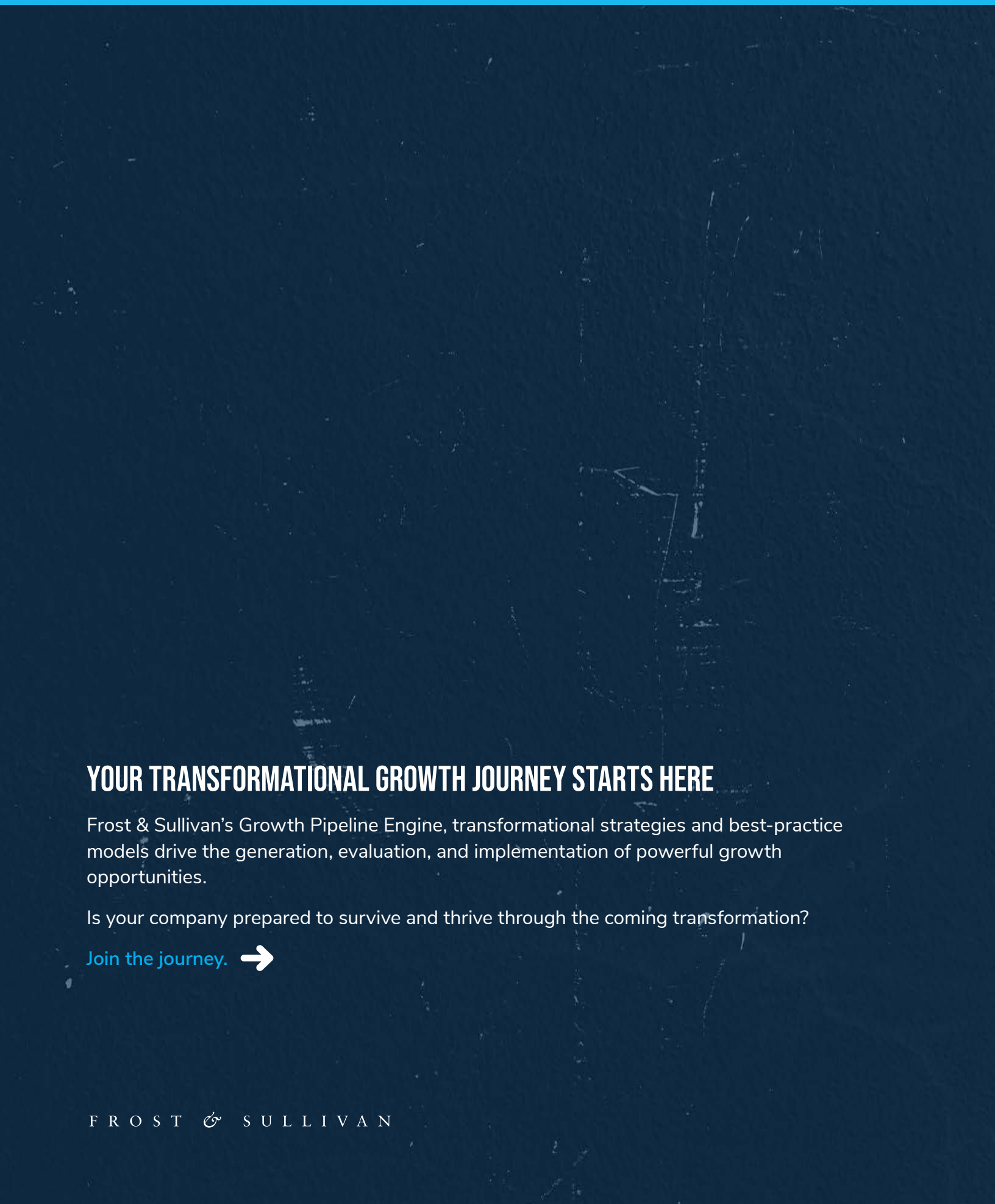
Who is Responsible for Interference Management?

As mentioned previously, there are many ways ISCO's Fortis technology for interference management can be delivered. Therefore, every part of the private 5G network ecosystem can use it to differentiate their offerings.

RU, antenna, and RAN suppliers now have an additional way to differentiate and improve their products by incorporating ISCO's technology to enable their products to eliminate interference, including harmful jammers.

System integrators bring together a set of network suppliers along with defense and public safety expertise to help move in this new direction.

For any of these types of companies, including ISCO's Fortis technology in their offering for 5G private networks for public safety, first responders, and defense helps differentiate them from their competition now and as the needs for safety and security evolve.



YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN