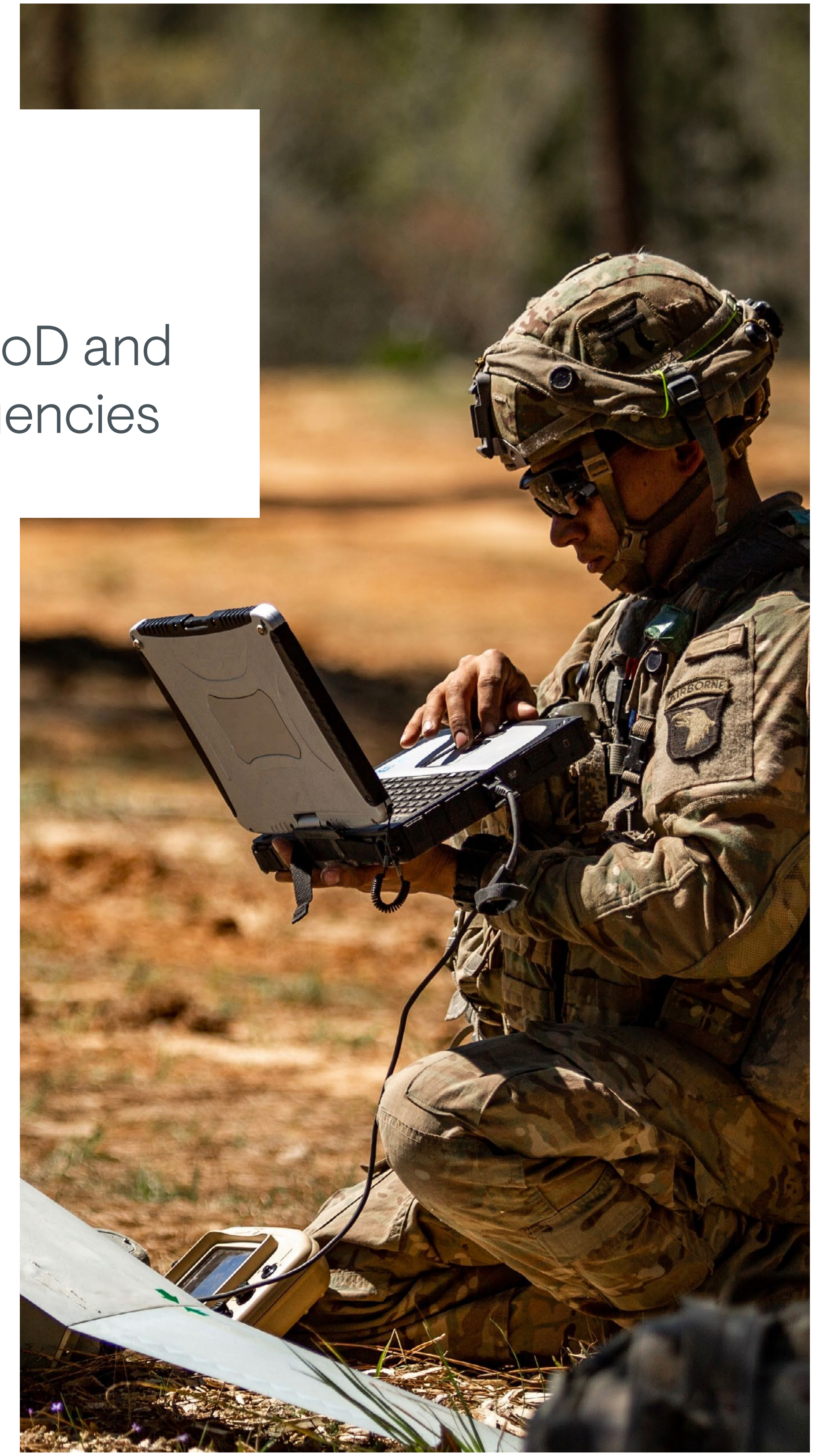
WHITE PAPER | NOVEMBER 2022

How Private 5G enhances the DoD and other federal agencies



A Cisco and GDIT briefing on private networking for mission-critical activities

Executive summary

Industry and enterprise across both private and public sectors are gravitating towards private 5G networks to enhance their existing systems and capabilities. Private 5G can solve current business challenges by supporting new network applications for higher levels of efficiency and productivity, improving worker safety, and contributing to mission effectiveness.

5G delivers comparative improvements in wireless, underscoring a generational shift in technology where greater bandwidth, lower latency, and higher efficiencies will be keys to enabling new functional roles of digital devices in a growing set of use cases. However, designing, building, and managing a private cellular network has never been easy. Cellular networks have traditionally stood apart from private networks, with complex barriers to entry such as regulatory spectrum licensing and the differing technological standards of 3GPP versus IEEE. And with the current ubiquity of Wi-Fi, an IEEE standard, it's important that private cellular networks are designed to both technologically and operationally integrate with existing systems. Both private and public sectors are wanting 5G to augment their current capabilities and become a highly resilient and secure foundation for their future endeavors.

The foundation for any network or business is trust. Two companies you've come to trust – Cisco and GDIT – have partnered to bring private 5G to industries including civil and federal agencies, defense, health, and state and local governments while eliminating most of the complexities and hurdles that normally accompany new technology.

Introduction

Networks have always been complicated, and with the evolution of technology they've become even more so. There's always been a price for the complexity of networks, and the fundamental challenge has become balancing the value of new technology with any increases to network costs and complexity. Because the world is increasingly digital and wireless, today's customers are looking towards private 5G to improve coverage while maintaining control of their operations/systems. In addition, 5G use cases demand better network performance, high reliability, and the flexibility to adapt to evolving needs.

There aren't too many private 4G LTE networks today because the technology is complex which presented large barriers to entry, and they haven't historically aligned well with enterprise systems. Cisco and GDIT have designed private 5G for the enterprise, supporting both 4G and 5G devices and integrating with existing systems such as Wi-Fi because we understand that a private 5G network shouldn't be a technology island unto itself.

Previous private mobile networks were purpose built as rigid systems requiring expertise in 3rd Generation Partnership Program (3GPP), a group of standards organizations that develop mobile telecommunications protocols. Then there's been the challenge of licensing spectrum. Unlike the unlicensed spectrum that Wi-Fi uses, private cellular networks have traditionally needed to buy or lease spectrum. So, what about spectrum availability and regulatory bodies that might stand in the way? How about security-first thinking and the importance of visibility, analytics, and automation?

Below are a few other points to consider about private networks:

- Private wireless networks continue to be complex undertakings, but the major barriers to entry have changed.
- The barriers are less about access to things like spectrum and technology and more centered around operations, applications, and use cases.

Integrating with existing systems is crucial for success and layering new technologies on top of complexity isn't helpful.

There are many questions about private 5G networks. In this paper we'll answer some of them and take a closer look at what 5G as a technology offers such as lower latency, improved capacity, broader coverage, and greater reliability. Technology is moving in parallel with 5G to make it much more accessible than in the past. 5G brings increasingly accessible private network implementations, which means it's not so much a solution unto itself, but rather marks the beginning of digital transformation, ushering in revolutionary internet of things (IoT) applications, new business process and models, and new functional relationships between humans and machines and machines to machines (m2m).

However, implementing private 5G can be complex, so we'll also talk a bit more about the traditional difficulties inherent in deploying private wireless networks. We'll also examine how IT departments aren't necessarily equipped to tackle 3GPP. Because existing systems are already complex, adding more can be a recipe for disaster.

Throughout the public sector there's a diverse array of needs and requirements ready to benefit from private 5G network solutions that combine simplicity with resiliency and security. Our focus is on use cases germane to the public sector, with emphasis on the needs of the Department of Defense (DoD, alternately referred to as "Defense") with the understanding that other government agencies and departments like the Federal Emergency Management Agency (FEMA), Customs and Border Protection (CBP), Veterans Affairs (VA), and the United States Postal Service (USPS) share similar mission-critical delivery requirements.

Private 5G use cases

PLATFORM CONNECTIVITY

Connecting internet of things (IoT) devices to the enterprise

COMMAND AND CONTROL

Taking an action quickly with low-latency data processing

LOGISTICS & MAINTENANCE

Managing supply chain processes

IMPROVED NETWORK

Providing faster connectivity with much lower latency

TRAINING AND SIMULATION

Realistic training and simulation activities using augmented reality (AR) and virtual reality (VR)

SMART INFRASTRUCTURE

Enabling intelligent decisions at the edge, including smart cities and smart warehouses

HEALTH

Telemedicine, including telehealth visits, enhanced contact tracing, and remote surgical procedures

EDUCATION

Broadcasting and improved online learning

Public sector agencies spanning federal, civilian, health, and intelligence, along with state and local governments, have great need for high-speed connectivity across ubiquitous devices. The public sector views 5G as a technological leap forward and the emerging connectivity backbone for our connected world, unlocking powerful new use cases empowered by the potential of IoT, and presenting a viable alternative to the reliability of wired networks.

In the case of the DoD, with thousands of sites spread throughout the world, reliable connectivity, and the ability to quickly deploy a network are important for readiness. Private 5G has multiple use cases for public sector applicationstoday, such as: LOGISTICS AND WAREHOUSING – ensuring people and resources are provided for, on time and as needed, around the world through real-time tracking and enhanced visibility of assets, inventories, and packages. 5G also enables secure digital connectivity for an increasing number of sensors, monitors, and other devices that help enable information sharing, agility, visibility, and tracking of the military supply chain, which enhances planning, control, and coordination.

- FLEET MANAGEMENT AND REMOTE MAINTENANCE – Keeping remote- and forward-operating base infrastructure functional at all times. 5G enables the connection of sensors to monitor the health of a vehicle's operating system so that if anomalies are detected it can either be removed from service or potentially connected to maintenance experts for advice or remote maintenance leveraging augmented and virtual reality (AR/VR) across great distances.
- LARGE BASES FOR BOTH INDOOR AND OUTDOOR NEEDS – Providing connectivity across large bases or within buildings and transforming the Air Force's "Flight Line of the Future" which encompasses all communications across the Air Force base, including on the runways, in the hangars, in remote areas, and within buildings. 5G enables secure communications across these large, typically remote locations.
- HEALTHCARE AND REMOTE TELEHEALTH – Providing medical expertise regardless of where the patient is in relation to the medical expert. By connecting monitoring sensors to soldiers, 5G can alert medical staff if a health issue is detected. 5G, through AR/VR and extremely low latency, can connect medical expertise to the remote soldier to help diagnose a potential problem. It can also remotely instruct medical staff through complicated procedures or even leverage 5G-connected devices to perform surgery from around the world.
- EDUCATION, TRAINING, AND SIMULATION – To keep personnel skills razor sharp and at the ready when needed. With low latency, high bandwidth, and support for many edge devices, 5G enables realistic training and simulation activities using edge sensors and devices as well as AR/VR to immerse soldiers into lifelike simulations.
- ENVIRONMENTAL MONITORING WITH RESOURCE AND SENSOR CONNECTIVITY – Ensuring that not only are intelligent sensors able to analyze edge data and connect with other mission-critical sensors and resources, but also take specific actions related to the information that comes from the data.
- JOINT ALL-DOMAIN COMMAND AND CONTROL (JADC2) – With the goal of gathering all the edge sensor information and connecting all soldiers across all commands and across all services (Army, Navy, Marines, Air Force, and Space Force), the Department of Defense views 5G as a critical enabling capability to its JADC2 initiative helping to connect U.S. military resources across the world.

Connecting everything, everywhere

Secure and reliable connectivity are the underpinnings for many private 5G use cases with the technological capabilities for providing seamless operations in denied, degraded, intermittent, or limited bandwidth (DDIL) environments. Whether applications of private 5G be at home or abroad, 5G will deliver the reliable low latency and high bandwidth necessary for a tactical edge.

5G is considered a mission- and edge-enabling technology set to transform operations. By standardizing and validating architectures, Cisco and GDIT can deliver private 5G solutions that unite network elements in even the most austere environments.

Designed to enhance existing systems

A private 5G network can operate as its own independent network, however integrating 5G technology with existing systems presents the greatest value. Given that most facilities already have some form of networking, be it Wi-Fi and or wired connectivity, adding private 5G into the mix requires thoughtful planning and the right technology partners for integrating with existing systems.

Especially with enhancements to Wi-Fi technology, it's expected that use cases will require both 5G and Wi-Fi to be deployed together. A private 5G network that is designed and built to integrate with existing networks offers fundamental advantages such as establishing common identity and policy profiles that will simplify and unify network operations.

Trusted to work

Since Private 5G is meant to support mission critical operations it must be designed with a zero-trust architecture. GDIT has developed an efficient zero trust implementation process. GDIT leverages the Zero Trust Accelerator and associated frameworks as well as Cisco's robust security product and service capabilities to ensure the private 5G solution is secure and integrates seamlessly with existing security measures. Zero trust is promoted by many cybersecurity experts and standards groups such as the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), International Organization of Standards (ISO), Gartner, Forrester, and

ATTRIBUTE	5G	WIFI 6
PERFORMANCE ENHANCEMENTS OVERPREDECESSOR	10x speed, 10x less latency, 1000x more capacity	4x faster, 75% lower latency, 4x more capacity than wifi 5
OPTIMAL SPEED (Typically, some overhead will prevent achieving maximum)	~ 10 gbps (Depends on spectrum, with mm Wave being fastest. Note that currentspeed achievements fall between 1gbps and 10 gbps)	600Mbps to a max 9.6gbps (Depends on # of devices and other neighbors sharing spectrum)
OPTIMAL LATENCY (Typically, some overhead will prevent achieving maximum)	~ 1 ms	~ 1 ms (Greatly impacted by # of devices and others sharing spectrum)
RANGE	Can provide service within building/space and across campus or larger field area	Optimal use within a building or space
TRAFFIC FLOW	Enables device-to-device communications which provides additional capabilities (vehicle collision avoidance, et.) as well as not requiring the backhaul /trunk to support 100% of traffic	Requires a Wi-Fi 6 AP to communicate with router
HANDOFFS BETWEEN PRIVATE/COMMERCIAL	Enabled through dual SIMs (including eSIMs)	N/A
DEDICATE PURPOSEFUL SLICE(S) FOR DIFFERENT TRAFFIC	Yes	Yes, but limited
SECURITY	Smaller attack surface/Leverages eSIM	Partially due to its intended purpose, Wi-Fi 6 leverages unprotected unlicensed spectrum which has a larger attack surface and a lesssecure WPA3
COST	Higher cost and complexity	Overall lower cost compared to 5G
SPECTRUM	Licensed and Unlicensed - licensed require subscription such as for 5G cell service. Unlicensed space aslo includes protections from being impacted by others	Unlicensed
APPLICATION	Mobile connections covering larger areas and cases with a large # ofsensors such as manufacturing. Potentially used as alternative to wire to provide connectivity to home and business. Typically used for mission critical applications and those requiring low latency.	Home and businesses within a single building Typically used for non-mission critical applicationsor general access within a home or building

other organizations. It has evolved into the preferred approach to cybersecurity.

Much the way 4G transformed how people get from place to place, 5G's performance enhancements will help enable a transformation of defense capabilities. With high reliability and low latency, 5G enables sensor-to-sensor communications, allowing AI-enhanced applications to process data at the edge, and this information can then be shared with other entities or sensors. For example, in a tactical training or live exercise, AR/VR-equipped 5G helmets can potentially interact directly with drones, vehicles, and other persons. Connecting large numbers and disparate edge devices while facilitating the device-to-device communications isn't possible with legacy 4G technology.

Presently, Wi-Fi and 4G devices are more prevalent than 5G devices. While the 5G device ecosystem is rapidly emerging, backwards compatibility with 4G devices and interoperability with Wi-Fi devices is important. Not all 5G implementations are designed for backwards compatibility. A standalone 5G network may not support 4G devices since it doesn't rely on any LTE EPC to operate. While existing devices ranging from cell phones to specialized sensors get phased out over time, they still have a purpose, so it's important that a private 5G network supports both 4G and 5G devices. Additionally, Wi-Fi in its newest iterations (Wi-Fi 6/6E) have applicability moving forward, especially considering the lower cost and ease of administration. The variability of wireless devices makes it important to link wireless technology options to provide unified connectivity.

Beyond wired and controlled environments, a private 5G network affords greater control across broader coverage areas, with tools for traffic segmentation using access point names/data network names (APNs/DNNs) and IP pooling for user types (e.g., contractors on the base vs. mission-critical devices or guest access at VA medical centers). In the future you'll also be able to dedicate resources for specific services using intelligent node selection (e.g., dedicated user plane) algorithms. Securing the traffic and ensuring proper macro- and micro-segmentation of the data reduces the threat surface and minimizes potential downtime.

5G addresses many of the security and privacy concerns present in 4G. For example, devices that connect to a cellular network are issued a unique identifier, which up through 4G has been known as an international mobile subscriber identity (IMSI). While the IMSI is useful for network authentication and device management, it can be exploited by a sophisticated player with knowledge of network. That is, devices connecting to a cellular network can be vulnerable to a man-in-the-middle attack and forced to transmit their IMSI, thus exposing these devices to eavesdropping and tracking. To better secure privacy, 5G changed how IMSI authentication works by implementing mutual authentication, where both the sender and the receiver have to establish trust to make the end-to-end relationship secure. For 5G, IMSI is no longer transmitted as plain text, the IMSI is now known as the Subscription Permanent Identifier (SUPI) and uses the new Subscription Concealed Identifier (SUCI) to encrypt the subscriber identity, enhancing privacy protections with the use of public and/or private key pairs.

Now that we've discussed some of the advantages of private 5G and its security advantages, it's easy to see how the varied use cases can be applied in other government segments beyond Defense:

- FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA) – 5G can greatly enhance disaster response capabilities by providing reliable communications on the ground and leveraging digital insights by connecting sensors, drones, and other edge devices. Real time information, especially concerning warehousing and logistics capabilities, can make a dramatic difference in the way FEMA responds to emergencies.
- CUSTOMS AND BORDER PROTECTION (CBP) – Connecting intelligent sensors, sophisticated surveillance equipment, and customs agents within a shipyard to identify, track, and clear cargo containers arriving in the U.S.
- VETERANS AFFAIRS (VA) – The ability to better treat patients by improving the quality of care, increasing accessibility of doctors with telehealth, and using analytics and insights to improve outcomes.
- FEDERAL AVIATION ADMINISTRATION (FAA) – Leveraging 5G to enhance sensor-to-pilot-to-ground communications to improve overall safety and enhance connectivity in an increasingly mobile environment while also leveraging remote experts to assist in maintenance.

Standardizing on the right architecture

Not all 5G networks are built the same. Private 5G networks can be deployed via three basic models: (1) fully on-premises, (2) cloud-based, and (3) a hybrid-cloud model. The fully on-premises model is straight forward, with all hardware and software residing on-premises and nothing in the cloud or in a third-party edge environment. Meanwhile, the fully -cloud-based model is the opposite, whereby the entire private network resides in the cloud with only the physical radio components located onsite. Each of these has its benefits and drawbacks, but hybrid-cloud deployments can best optimize scalability, resiliency, and security objectives more effectively and cost efficiently than on-premises or fully cloud based.

The hybrid-cloud model is a well measured combination of the other two models, and while all three have their merits, a hybrid-cloud approach might be most optimal for public and private applications, including the DoD and other agencies. With a hybrid-cloud, the components installed on the premises are limited to the radio and the core user plane (or data plane) functions, including user data. The on-premises footprint is very small for the hybrid model. A typical implementation requires a single rack unit (RU) switch and a single RU server, along with the radio access points. A fully redundant system involves two switches and the addition of up to two other servers depending on scale and configuration, which is still much less than typical on-premises solutions. The control and management planes for a hybrid-cloud private 5G implementation are cloud-based.

The benefits of a hybrid-cloud model include a very small footprint and associated low demand on real estate, power, and cooling. Also, data sovereignty is preserved since all relevant customer data is kept onsite. Additionally, end users can enjoy ultra-low latency since the core user plane functionalities are on-premises while the control and management planes are in the secure Cisco cloud. The on-premises private network and the management user interface (UX) are connected via transport layer security (TLS), which encrypts data and protects the network from outside interference like hacking. All security/network function updates are included in the usage costs. So, the hybrid model offers the best of both the on-premises and the cloud-based models for use cases that can leverage it.

Solution management

One thing setting private 5G apart is that it seamlessly integrates with existing operations. It intuitively integrates with existing enterprise and industry systems and processes. Most environments will include a mix of wireless technologies, so private 5G is expected to augment existing capabilities and become part of legacy systems and workflows. It's ready to integrate with identity and access management (IdAM) and identity, credential, and access management (ICAM). It also integrates with Cisco Identity Services Engine (ISE), with role-based access control (RBAC) for empowering more with IT tools, such as lifecycle management, automated updates/upgrades as part of the service offering, and other tools providing network visibility, analytics, and automation.

But it's not a one size fits all solution. It needs to meet the demands of its intended use cases, which is why Cisco Private 5G offers support for visibility across sites and integrates with existing systems and processes. It also offers the ability to customize the solution based on specific supported use cases and customer requirements to ensure the service delivers the optimal outcomes as efficiently as possible at the highest levels of end-user experience.

Cisco Private 5G service is secure, reliable, and resilient. It's designed, built, and managed by GDIT and can be integrated with GDIT's Zero Trust Accelerator and associated frameworks to ensure network services remain functioning for all scenarios.

Intuitively integrated and operated

A major challenge for implementing a private 5G network is managing the complexity of 3GPP-based cellular technology and fitting it into a private environment. Commercial cellular technologies were developed for purposes different than that of industry or enterprise applications. Where existing cellular networks have teams of people dedicated to servicing millions of subscribers, using basic service profiles, a private 5G network also has the potential for servicing millions of devices while offering much more insight and control, with refined configurations and designs to align specifically with customer and use case requirements. The key difference between a private and public network in this regard is that private networks will probably not have a dedicated team of experts for managing daily operations.

In addition, a private 5G network is likely to involve more than basic service profiles, becoming finely tuned to address the needs of its use cases. While private networks will start off with a relatively lower number of subscribers/devices, the service profiles will become more complex and managed by an IT staff that is not an expert in 3GPP. This is what makes Cisco Private 5G "as-a-Service" offering a good choice. The complexity is removed so that network owners can focus on what they do best.

Lifecycle management of services

The lifecycle management (LCM) of a private 5G network involves a new host of considerations for industry and enterprise applications. The technologies that 5G has introduced to mobile networks—from RAN to core to the data center and edge – change the strategies for lifecycle management.

A private 5G network is more than the sum of components such as the RAN or packet core. It becomes a persistent service with automated software updates and upgrades with more emphasis on the lifecycle of the device identity. A fundamental purpose for operating a private network is control. Customers manage the service and not individual network functions or capabilities. Lifecycle management of the identity ensures an experience that will extend beyond the 3GPP networks but also seamlessly provision the identity and policy across wired and wireless services.

Leveraging cloud management for all capabilities, including software LCM for the service, device on-boarding, SIM configuration, and policy management makes it easier for IT/OT to manage services across multiple sites and site-to-site variations with role-based access control.

Services resiliency

While any network design accounts for resilient hardware nodes, and alternate routing capabilities, when possible, it's important to acknowledge that unforeseen situations could create a scenario where the local edge nodes and

network are isolated for a short period of time, such as in the DDIL scenario described earlier. While recovery of the connectivity is being addressed, the Cisco-GDIT solution can help ensure existing devices stay connected without interruption and in some cases new devices are able to connect to the network with appropriate policies and security applied.

The Cisco Private 5G service delivers high available edge appliance as part of the solution with both hardware and software resiliency principles applied so that we can meet the mission critical nature of the use cases discussed throughout this paper. However, understand that some scenarios may not always have the high resiliency requirements. In some cases, a faster time to deployment with minimum footprint is more critical. Our tailorable solution supports both variations – a multi-server node option to ensure higher hardware resiliency and a single server node option with software-only resiliency.

The high availability solution covers multiple software entities which have been hardened to ensure any unintended failure of software components or services would automatically recover using multiple Kubernetes pods or through the ability to spin up additional microservices and recover configuration seamlessly. With our cloud managed solution, one of the critical advantages is that any failures on the local edge nodes can be recovered by pushing the configuration from the cloud to a warm standby node to ensure faster recovery.

While high resiliency scenarios require multiple top of rack (ToR) switch connections and redundancy in transport connectivity towards the authentication services in the cloud, to avoid any interruption during temporary outages of cloud connectivity, the local edge node can maintain the sessions for a configured amount of time while the cloud connectivity is restored. With future enhancements in standards and software, it's also possible to have full local authentication if the use case requires it.

The resiliency aspects of the solution cover full hardware failure, software failure of one network function or some microservices within a network function, hard disk failures, networking failures, etc., and all scenarios are being addressed to ensure minimal impact to user plane connectivity for the devices. The solution leverages a combination of standards-defined capabilities and custom-built resiliency mechanisms to address specific private 5G deployment scenarios.

Designing and planning for today and tomorrow

Together, Cisco and GDIT have been supporting the public sector for more than 30 years and our teams understand that 5G and edge solutions are part of a larger ecosystem of tools/capabilities that must work together securely and seamlessly to deliver outcomes critical to our customers' ability to meet mission objectives.

Since private 5G is not a one-size-fits-all solution, it must be designed for the specific demands of the use case and customer. Here's what to expect when adopting the joint Cisco and GDIT Private 5G solution:

- Security first thinking with Zero Trust architecture – GDIT is well practiced and has a process in place with Zero Touch Accelerator to ensure speedy design through implementation
- Establishing a secure foundation for today and into the future
- Securing the network foundation for a future with 6G
- Removing the complexity by delivering private 5G as a service
- Cloud managed and customer controlled
- It remains the customers' network so you're in control of the processes and operations while the hardware and software are maintained and managed by us
- A solution that evolves with your needs and that's right sized to fit applications and use cases of today and extensibility to grow, ramping up services as needed using a pay-as-you-use subscription model
- Designed and built to integrate with existing systems (not on top of, or just alongside)
- Ability to unify digital assets across networks – networks are more valuable when they're brought together
- Validated and tested by both Cisco and GDIT

Conclusion

We live in a world where firsts matter and a private 5G network is an important first step when moving into a digital future. Reliable communications are essential, especially when they're mission critical. Private 5G offers mobile coverage and connectivity across complex environments, and by simplifying it we're unlocking potential.

GENERAL DYNAMICS
Information Technology

About General Dynamics Information Technology

As a trusted systems integrator for more than 50 years, General Dynamics Information Technology is a leader in 5G and advanced wireless communications, spanning all use cases in defense, intelligence, and civilian agencies from the enterprise to the edge. GDIT supports the most sensitive missions applying 5G, cyber, artificial intelligence, cloud, and high performance computing, to solve technical challenges. GDIT collaborates and co-creates with industry leaders and emerging-technology companies to design and deliver tomorrow's innovative and transformative solutions and services.
For more information, visit: www.gdit.com/5G.

CONTACT

GENERAL INQUIRIES
Christopher Aiello
Senior Marketing Manager
GDIT
Email: christopher.aiello@gdit.com

MEDIA INQUIRIES
Jay Srinivasan
Senior Public Relations Manager
GDIT
Email: jayendran.srinivasan@gdit.com

About Cisco

Cisco is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future.

To learn more on how Cisco Private 5G simplifies both 5G and IoT operations for enterprise digital transformation, please visit www.cisco.com/go/private5G