Assurance is the Cornerstone for design, integration, deployment, and operations.

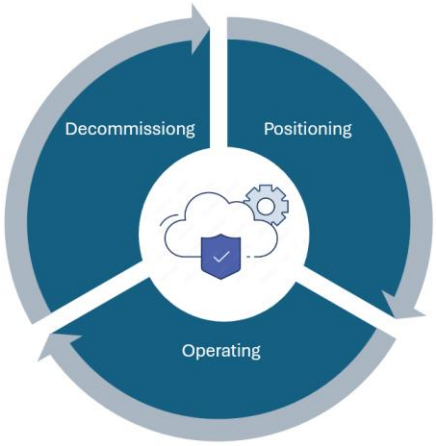
Oct '25 **Keysight** acquired Spirent Communications software-driven lifecycle assurance and automation solutions, creating a holistic 'live-to-lab' ecosystem. This filled a critical gap for Keysight in offering a more comprehensive solution for network testing and assurance to their customers.

- **Lab**
  The role of the lab is shifting—it's no longer an isolated, offline process. Instead, continuous testing is becoming the norm, with lab verification flowing into live operational monitoring. This ensures operational readiness and provides a blueprint for successful, resilient, network operations.
- **Live-to-Lab**
  As cloud-native networks become central to enabling scalable, resilient, and agile infrastructure, traditional testing methods can no longer keep up. Lab-to-Live is a holistic strategy that integrates lab testing, network deployment, and operational monitoring into a unified lifecycle, fostering **continuous** improvement and stronger collaboration across development and operations.

- **CI** – Continuous Integration automates code integration
  Stage 1 Source: software developers write and commit code changes
  Stage 2 Build: the new code is complied, dependencies are noted, and an executable artifact is created
- **CT** – Continuous Testing ensures quality through automated tests
  Stage 3 Test: automated tests, such as unit and integration, run against the Build to verify functionality and catch bugs early
- **CD** – Continuous Deployment automates the release process
  Stage 4 Deploy: the validated artifact is released automatically to different environments, such as staging and production, where it undergoes further User Acceptance Testing

- **Automation** – is the key, as it's impossible to keep pace with the need for constant changes, live monitoring, and testing without it.

- **Lifecycle Assurance** – encompasses the entire process of moving to, managing, and finally decommissioning cloud solutions.

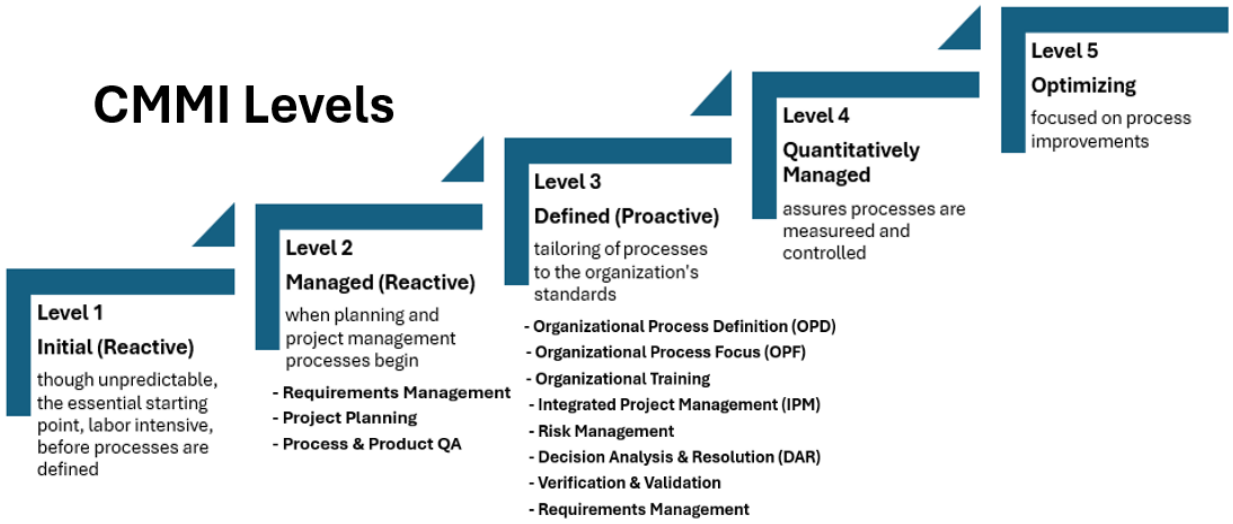


Positioning – NIST 800-145 covers the required practices for cloud networking, including different cloud types – i.e. public cloud and private cloud. The ultimate goal should be '*to provide access to the services the user requires – whenever they need them – with the availability and reliability they expect*'.

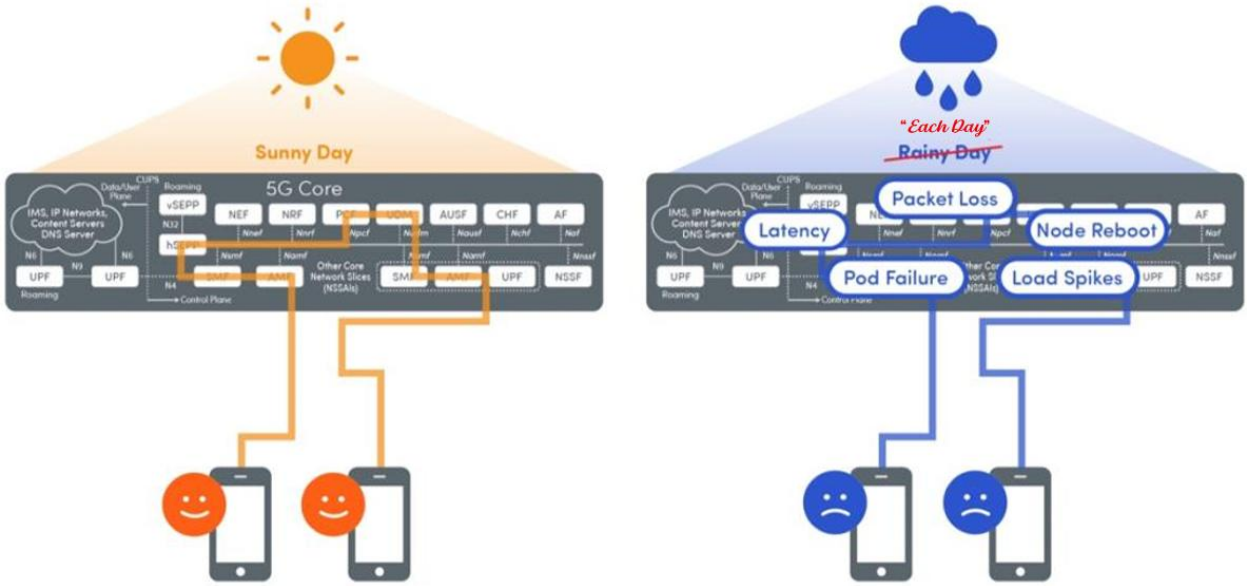
Operating – managing and delivering of a cloud network. Requires consistent application of procedures and uses, automation for test optimization, and ensuring the cloud network meets Service-level Objectives (SLOs). Operations must include strategies to ensure it is – resilient, scalable, repairable, secure and meets all compliance requirements.

Decommissioning – evaluate your current infrastructure and develop a strategy for decommissioning, capture dependencies, obtain '*explicit consent'* from all users and stakeholders, final step – safely retire outdated applications and ensure all data is securely archived and/or deleted.

- **CMMI** – Capability Maturity Model Integration provides guidance for developing or improving processes that meet the business goals of an organization.



- **Each day presents a chance for a “Rainy Day” in the Cloud**
  Function failure is normal in a cloud-native network. Cloud Native networks are fundamentally different than traditional networks. Instead of applications built on highly resilient infrastructure, cloud-native is about building on an infrastructure that is expected to fail. Cloud Native applications are resilient through their ability to rapidly heal a function onto new cloud instances. This drives a need for proactive testing to understand how cloud issues can impact network services. Testing in an environment where every day in the cloud is considered a "rainy day."



Military Use Case for Network Cloud Assurance

Our military leverages cloud computing to enhance their network security and connectivity around the globe, our military requires a highly agile infrastructure that supports the edge for cloud computing (CC) ensuring superior tactical comms, EW, and deployed IoT sensors.

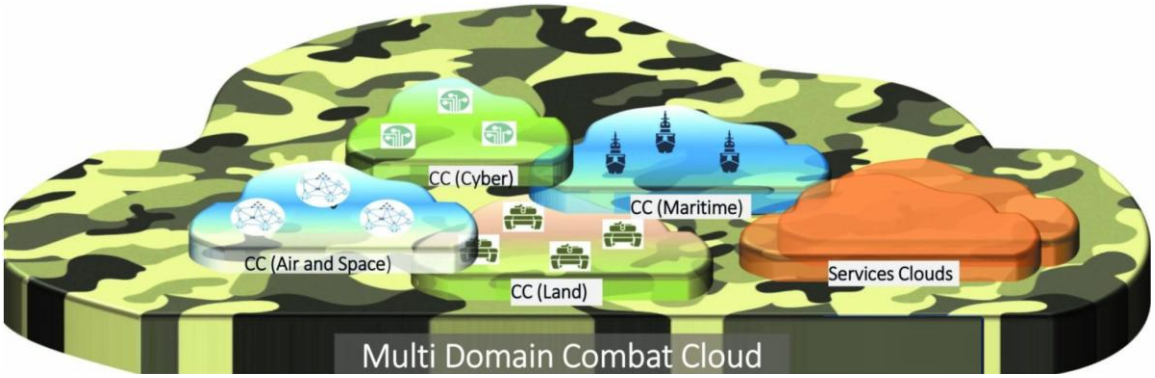


Image source: NATO

- **Global Defense Cloud Connectivity** our military operates all around the globe, including environments where Denied, Disrupted, Intermittent, and Limited (DDIL) network services are experienced. AWS and SES Space & Defense have partnered to leverage SES's multi-orbit, multi-band, global satellite fleet to provide the required **battlefield connectivity** to AWS's deployable Modular Data Center units enabling low-latency, secure, cloud-based services in these DDIL environments.
- **Cloud One** is managed by the USAF, it offers a multi-cloud, multi-vendor ecosystem, delivering speed. scale, and security with cutting-edge technologies.
- **Military Deployable Networks**
    - **Edge Computing** provides data processing closer to the source, thus allowing for real-time data processing, reduced latency, and improved security. Typically, on devices such as local servers, Smartphones, and IoT Sensors
    - **Fog Computing** (is a term attributed to Cisco) acts as an intermediary layer between edge devices and centralized cloud servers. It processes data at local "fog nodes" which are situated close to the edge, allowing for more complex data processing and aggregation from multiple sources
    - **Hybrid Computing** combines private and public cloud-based resources
    - **NEXIUM Defense Cloud** is a private cloud-based solution designed specifically for our military by Thales. It harnesses the power of the latest virtualization, containerization, software-defined networking, and service orchestration technologies
- **AWS Cloud Solutions** offers scalable solutions for our military, including tactical edge. AI/ML, and HPC. AWS also supports the military JADC2
- **Juniper Session Smart SD-WAN** offers agile, secure, and reliable cloud connectivity for military installations worldwide
- **Microsoft Tactical Cloud Platform** offers a suite of cloud-based solutions tailored for military operations

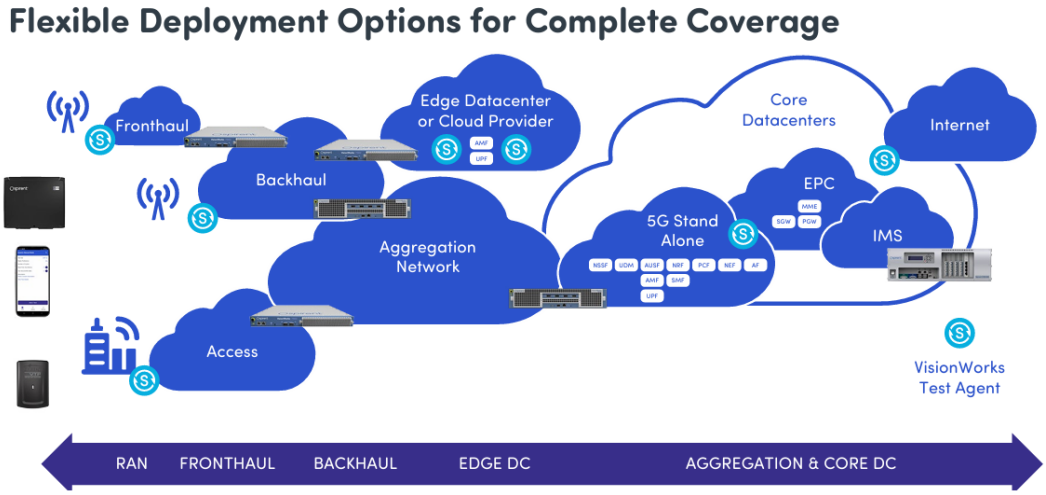
Cloud Security Playbooks

Volume 1
https://dodcio.defense.gov/Portals/0/Documents/Library/CloudSecurityPlaybookVol1.pdf

Volume 2
https://dodcio.defense.gov/Portals/0/Documents/Library/CloudSecurityPlaybookVol2.pdf

Spirent (Keysight) is the leading global provider for Cloud Assurance and Testing solutions.

Spirent's **VisionWorks** Test Platforms support an ever-growing library of active tests that can run on-demand or 24x7 from anywhere, to anywhere.

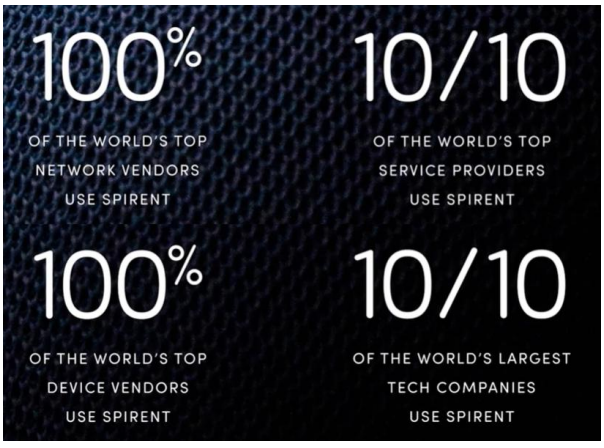


VisionWorks framework

VisionWorks brochure:
https://www.spirent.com/assets/u/spirent-visionworks-brochure

Spirent's **Velocity** Automation Portfolio supports the complete automation of customer lab and testing environments for large enterprises, NEM, and service provider organizations. It is the only fully integrated solution to provide automation and management of lab resources, facilitate automated test suite creation, oversee lab connectivity and topology, and provide professional services for initiative success.

Velocity data sheet:
https://www.spirent.com/assets/u/spirent_velocity_datasheet



Want to learn more and schedule a Demo…

Claude Sweeton, Director of Test & Measurement Solutions
claude.sweeton@dualos.com
630.881.2288 Cell
linkedin.com/in/claudesweeton

- +45yrs in the Test & Measurement industry
- US Navy Veteran 1978-86

Dualos, LLC (Native American, SBA-Certified WOSB, Small Disadvantaged Business)
Founded in 2008
1520 Steele Ave
Sumner, WA 98390

Dualos applies our expertise and products, along with industry-leading partner solutions, to serve the Aerospace and Defense industry. We provide tailored solutions designed to address the complex testing challenges our customers encounter.

253.750.5125

www.dualos.com