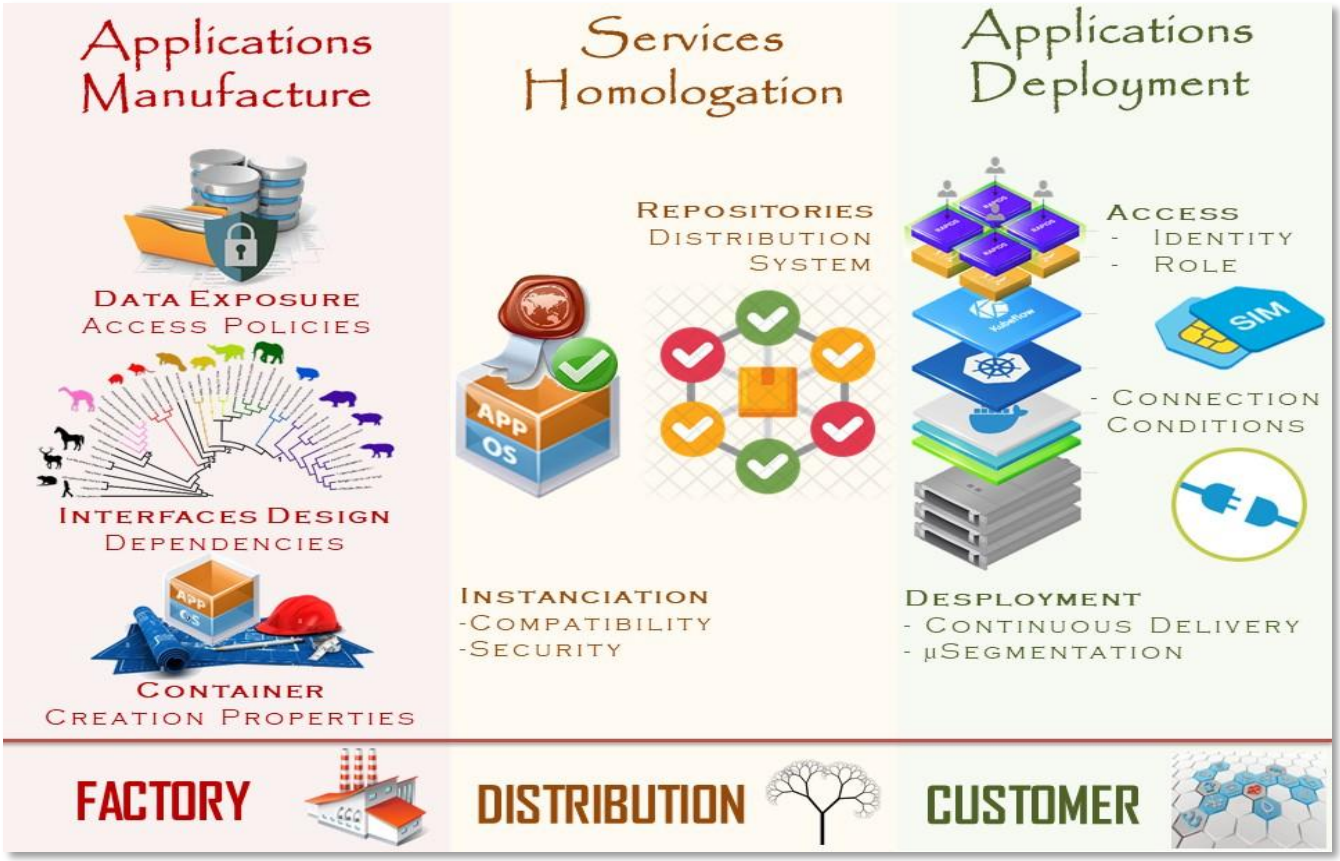


CRITICAL INFRASTRUCTURES Upgrading the Software Production Model

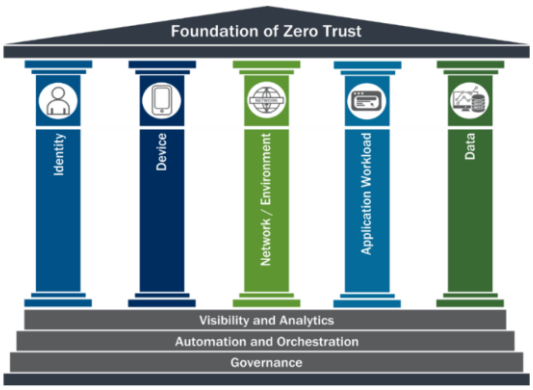
INDEX

1.- MODERNIZATION OF CRITICAL INFRASTRUCTURES.

1.1.- MOTIVATION: CYBERSECURITY ZERO-TRUST MODEL.

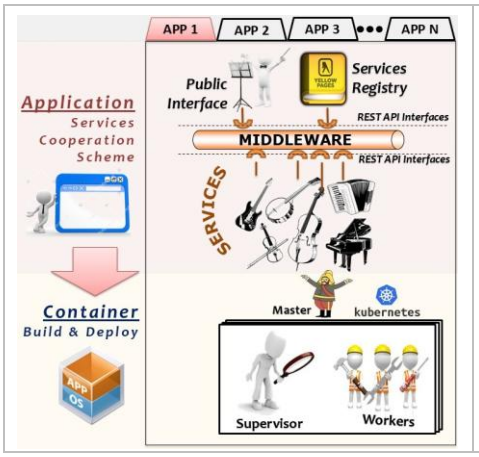
1.1.1.- MODERNIZATION: THE NEW SOFTWARE PRODUCTION MODEL.

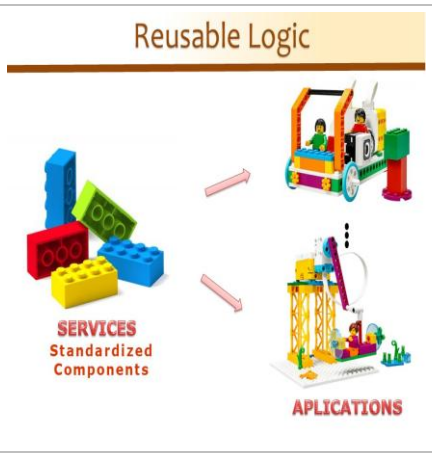
The first security principle is the governance of the environments that you want to protect; a set of highly scattering environments is ungovernable. Therefore, the US National Security Infrastructures maturity plan towards Zero-Trust[1] cybersecurity principles begin with ***unifying and stabilize the application production model over technological evolution through standardization*; both the execution environments (Platform One) and the delivery format of the applications (Iron Bank)**, overcoming all the limitations of previous production models that have been hindering the evolution of the sector... and thus being able to keep up with the times, today and tomorrow. *This implies restructuring the software value chain to achieve both decoupling the evolution of applications from the platform where they run* (thanks to the delivery of the application in a container repository); *and the evolution of the execution platform from the hardware where it is deployed*:

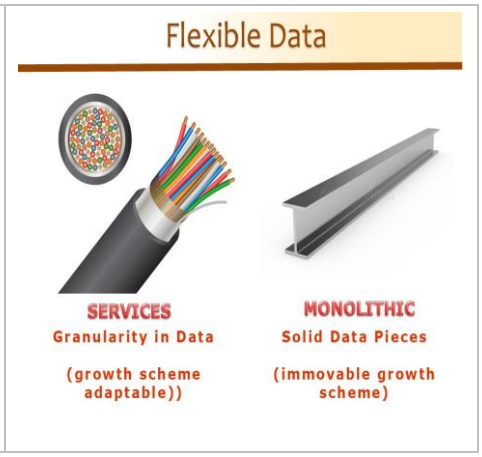


- **Data Center Operator**: standardization of the execution platform isolates its evolution from the hardware where it is deployed. A single control plane for network of environments with an identity system enables centralized, ubiquitous, end-to-end management of all computing resources:

- **Application Factory:** responsible for providing secure out-of-the-box applications; controlling both the data plane design and logic dependencies (SBOM=Software Bill Of Materials). Key is a Services/uServices-oriented[2] design to accelerate deliveries.







[1] ***CISA Zero-Trust Maturity Model***: https://www.cisa.gov/zero-trust-maturity-model
[2] ***How Department of Defense moved to Kubernetes and Istio***: https://youtu.be/YjZ4AZ7hRM0

1.1.2.- THE PROBLEM: SUPPLY OF STANDARDIZED PRODUCTION TOOLS.

Without tools, not even a screw can be unscrewed. The cloud technologies where these applications are designed and executed are evolving rapidly[3] without any standard, without any long-term plan, focused exclusively on renting virtualized machinery, leaving other use cases out of the equation such as critical infrastructure, which requires its own private clouds.

The US National Security strategy is committed to industrialize the production of critical infrastructure applications. By **providing free standardized manufacturing means, they make possible, the impossible...** that National Security infrastructures adopt the path towards Zero-Trust principles which entail a very expensive redesign of the entire software value chain, including **refactoring of applications and environments where they run**. The modernization of National Security infrastructures must be done only once, to a stable DevSecOps execution platform over time, both at factory and at the datacenter operator, in other words, based on standards.

Modernization of Defense infrastructure begins with a deadline of 2027, followed by government agencies. *It is not possible to apply international rules over data without first universalizing quality to all application manufacturing processes, thanks to democratizing access to appropriate tools with baked-in quality*.

1.1.3.- COMMUNITY CREATION OF MANUFACTURES

For the creation of a community of National Security manufacturers, three elements have been established:

- **System of Manufacturing Standards**, structure of production processes that allows to monitor the degree of security of the released applications. Processes described in reference documentation *"DevSecOps Reference Design"* https://p1.dso.mil/resources/platform-one
- **Modernization plan,** gradual incorporation of new methodologies and working tools, with the required personnel training programs. The Catalyst community is responsible for catalyzing the incorporation of new manufacturers into the National Security ecosystem: https://catalystcampus.org/ecosystem-overview/ .
- **Supply of standardized manufacturing means**, to speed up the launch of new factories... a series of vendors commercialize manufacturing means that guarantee compliance with the rigorous United States National Security regulations regarding computer applications: https://catalystcampus.org/platform-one-commercialization/ .

[3] ***Cloud Technologies Landscape:*** https://landscape.cncf.io/

There are consulting services that can be a gateway to this ecosystem of manufacturers linked to US National Security:

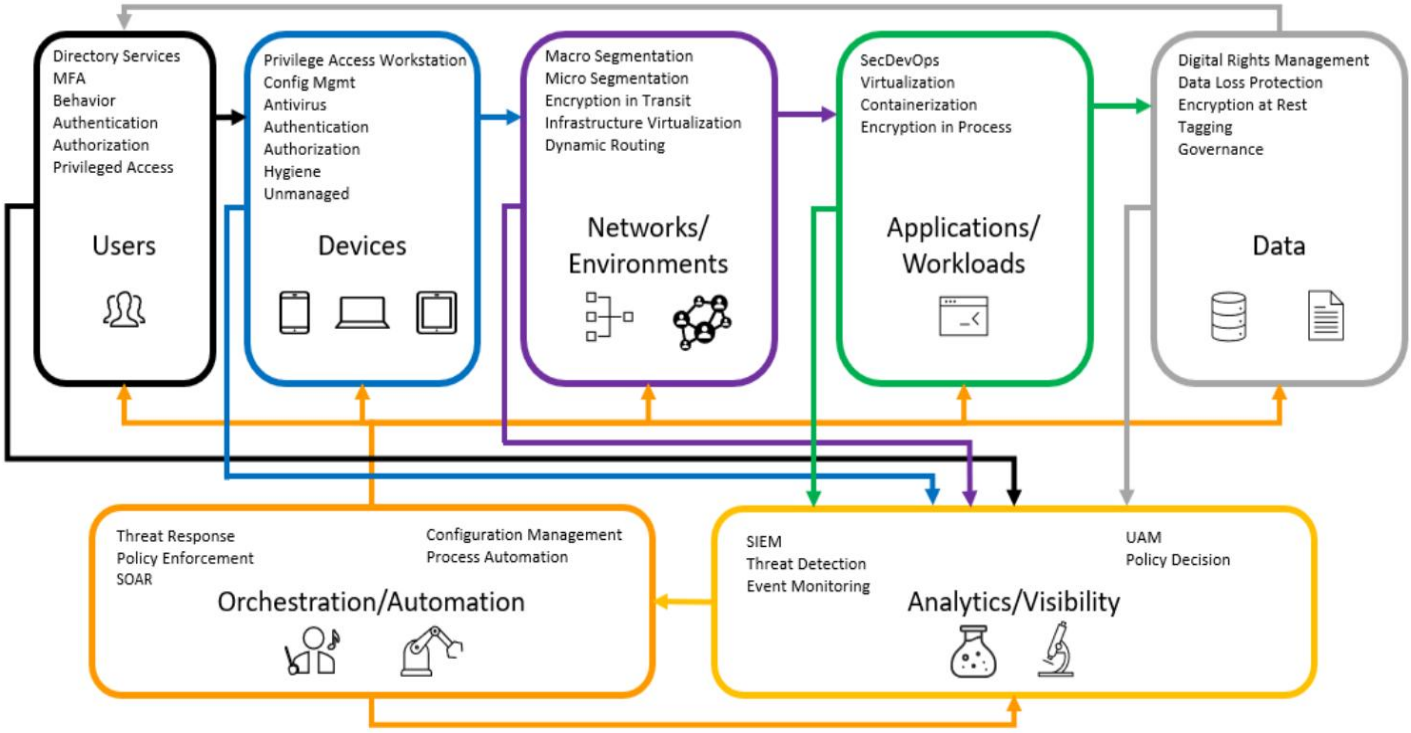
How can I effectively modernize my legacy system, both hardware and software?
By using modern design patterns, modularization, microservices, and translation tools,
Seed designs an effective, efficient plan to move your mission system forward.
https://www.seed-innovations.com

1.1.4.- BRINGING US SOFTWARE PRODUCTION MODEL TO EUROPE

Joint work with other manufacturers that share the very same problem may result in a significant reduction in modernization costs and greater compatibility **with common standards that maintain a stable evolution plan over time**, avoiding the uncontrolled maelstrom of evolution lines that they end up dying. Furthermore, *standardization makes critical infrastructure independent of manufacturers*.

- Technologies tested by a large community of manufacturers.
- Consulting and support services available.

In short, import this new software production model (based on the centralized distribution of containers) from the USA to Europe. The Catalyst community has intensive 6-month[4] training programs in the USA, where you learn this universe of National Security, in addition to establishing connections that will facilitate all manufacturing distribution means processes. In fact, the creation of a community of manufacturers is the reason for the existence of this community, that is, to facilitate contracting.



[4] ***Training Programs, 6 months***: https://p1.dso.mil/residency

1.2.- DATA CENTER ARCHITECTURE.

1.2.1.- CLOUD ONE AND PLATFORM ONE.

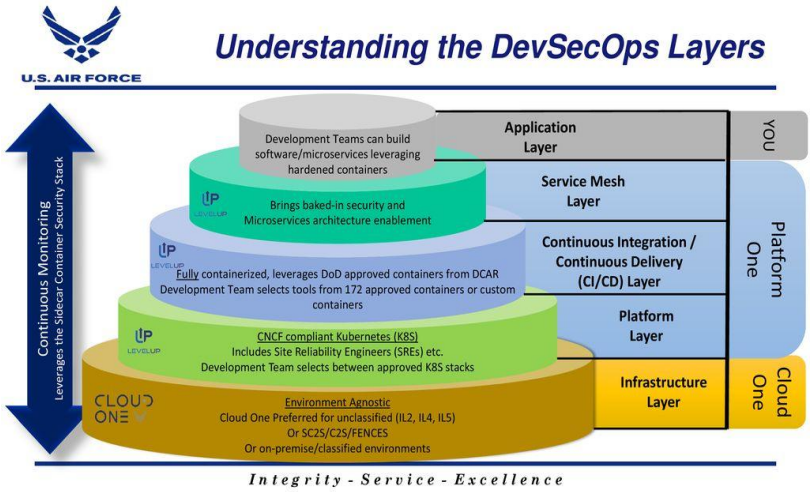
When it comes to managing data center infrastructures, two layers appear, the undercloud (US Defense calls it Cloud One) and the DevSecOps Platform (US Defense calls it Platform One[5]), which is nothing more than a way to initialize the clusters, that is, a Helm Chart[6] that defines the tools that the cluster must have. *This two-tier architecture decouples the DevSecOps software platform from the hardware undercloud, allowing constant evolution of the application execution environment regardless of the hardware where the platform is deployed.*

PLATFORM ONE BIG BANG UNIVERSE

https://p1.dso.mil/services/big-bang

VivSoft ENBUILD

https://www.vivsoft.io/post/big-bang-deployment-simplified-with-enbuild



PLATFORM ONE SMOKEY WATERFALL, ONLY YOU CAN PREVENT

Clusters Initialization

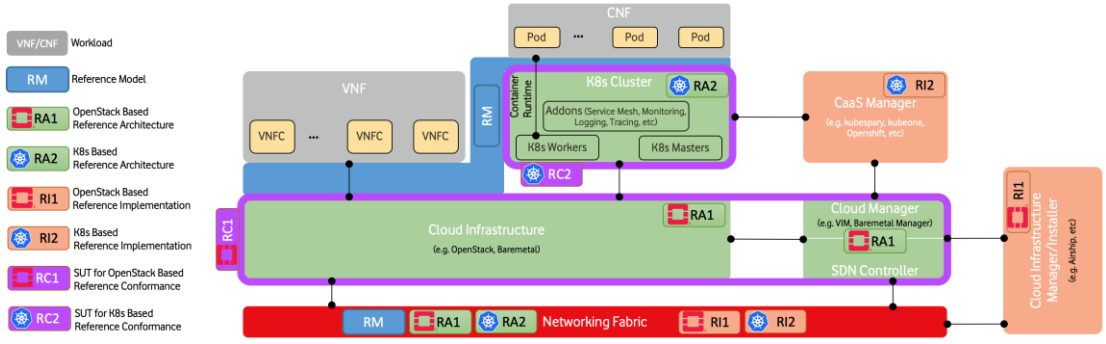
https://p1.dso.mil

(Open Source tools to avoid vendor lock-in)

On Premise: Telco Cloud Standards

Anuket(https://anuket.io/) = CNTT(https://cntt.readthedocs.io) + OPNFV (https://www.opnfv.org/)

Stable standarization over time, with a governance model[7] that establishes testing and delivery cycles[8].



On Cloud: Rules of each Cloud Provider.

CLOUD ONE FAST SECURE STREAMLINED

UnderCloud

https://www.cloud.mil/

[5] ***Platform One layering structure***: https://csrc.nist.gov/csrc/media/Presentations/2022/oscal-mini-workshop-1-P1_DoD%2BNIST/P1%20OSCAL%20PA%20Approved.pdf

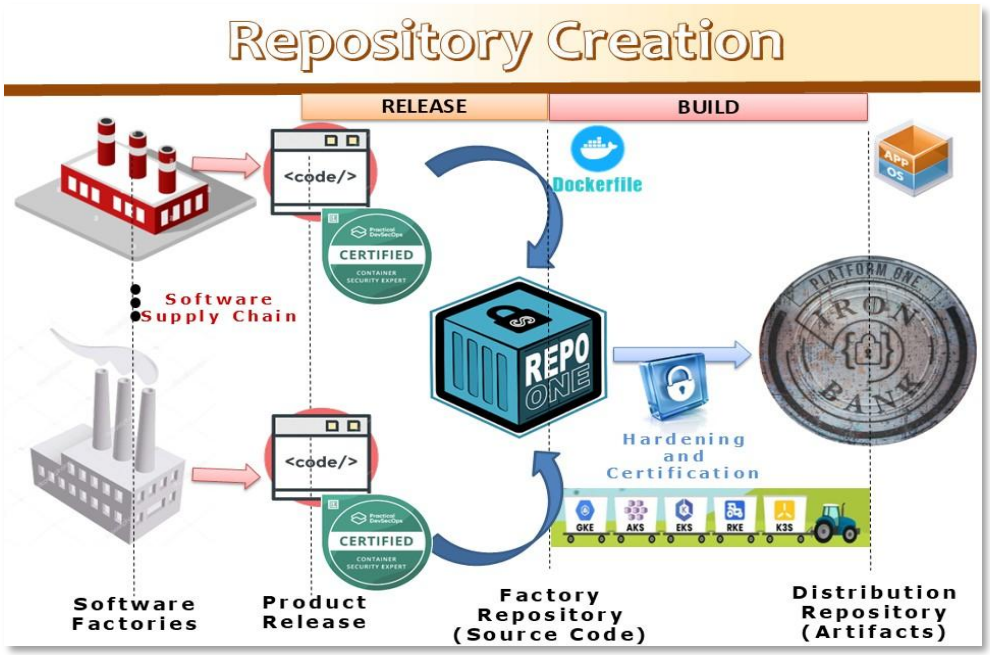
[6] ***Demo BigBang***, *Configurable Helm Chart to deploy different tools on a cluster according to their role within a DevSecOps construction pipeline:* https://www.youtube.com/watch?v=rfufvM3ktYE&t=1047s

[7] ***Telco Cloud Government Model:*** https://osm-download.etsi.org/ftp/osm-7.0-seven/OSM9-hackfest/presentations/OSM%239%20Hackfest%20-%20HD0.0%20Introduction%20to%20NFV%20and%20OSM.pptx.pdf

[8] ***Telefonica Unica,*** *pioneer in Telco Cloud:* https://youtu.be/npYqd_l5YjY?si=XqJC2ElZnnJjqE01

1.3.- DATA CENTER USE CASES

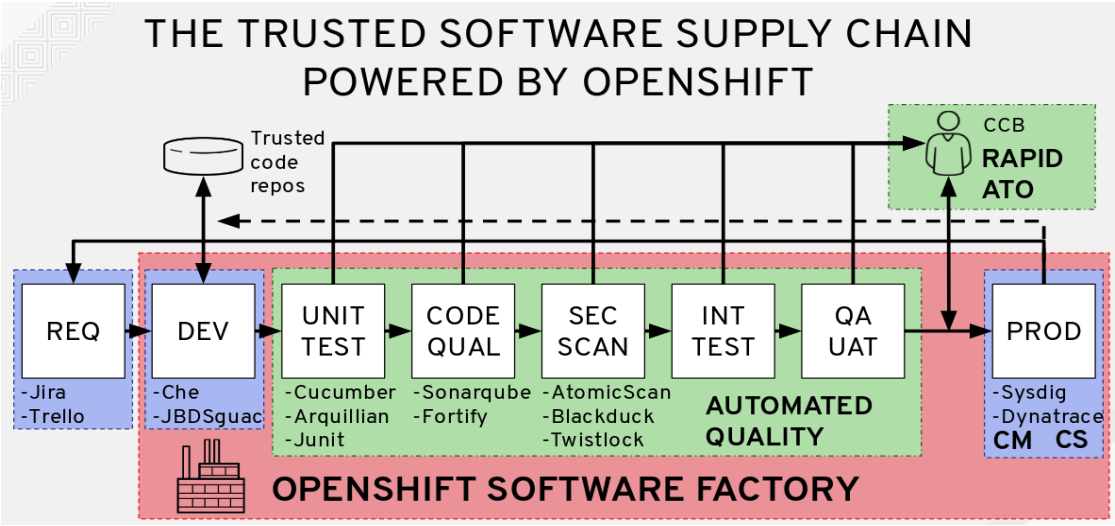
1.3.1.- APPLICATION DISTRIBUTION: THE REPOSITORIES



The software distribution repository[9] plays a critical role within the USA National Security application production model. The container repository[10] shared by all factories with homologation processes for their containers for execution on a standardized platform (comparable to a Linux package distributor) decouples the evolution of application factories from data center operators.

1.3.2.- SOFTWARE FACTORIES: DEVSECOPS METHODOLOGY

1.3.2.1 FACTORY STRUCTURE[11]

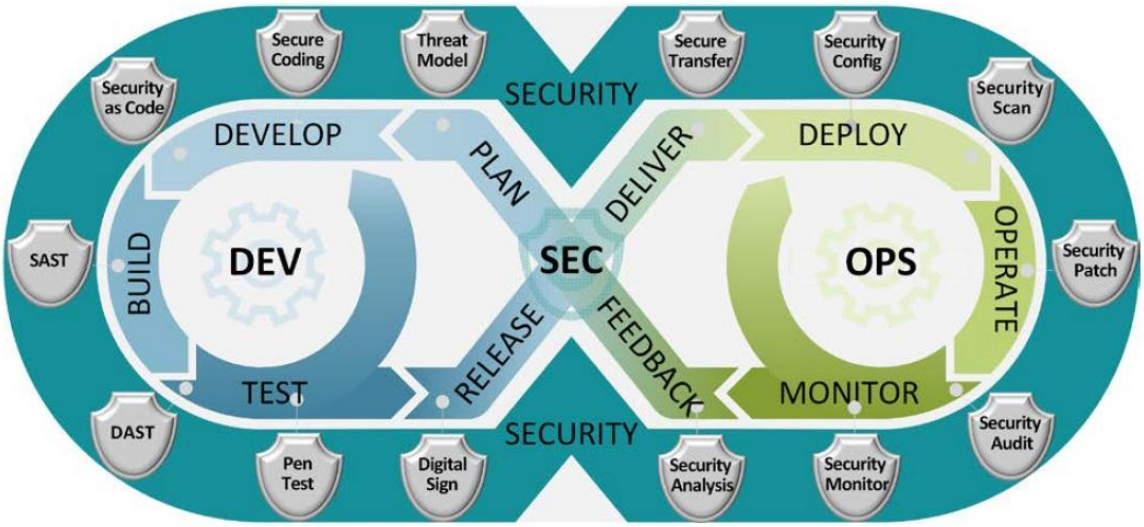


[9] ***Repo One - DCCSCR,*** *DoD Centralized Container Source Code Repository:* https://repo1.dso.mil/dsop/dccscr

[10] ***Iron Bank - DCAR,*** *DoD Centralized Artifacts Repository (DCAR):* https://docs-ironbank.dso.mil/overview/

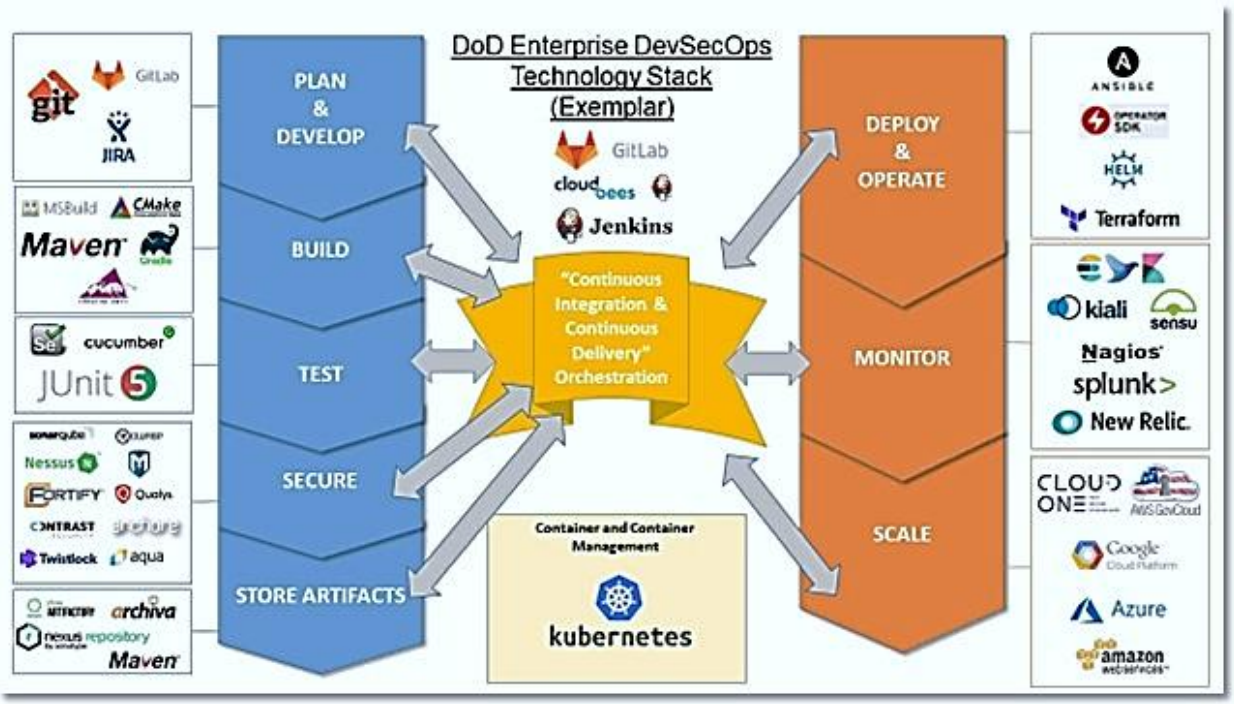
[11] ***IBM RedHat Secure Software Factory:*** http://redhatgov.io/workshops/secure_software_factory/

1.3.2.2 STAGES OF A SOFTWARE PRODUCTION PROCESS



One of the decisive factors to speed up delivery processes is the system of authorization points (gates) distributed in this sequence of manufacturing processes. The end result is called cATO (*Continuous Authorization to Operate*) [12].

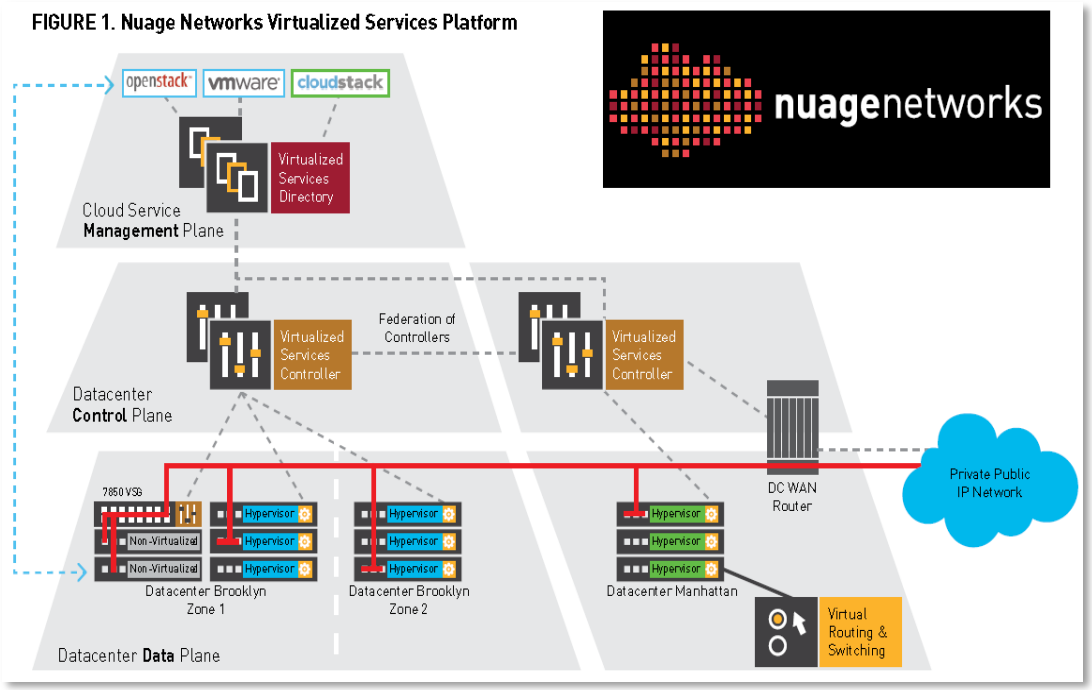
1.3.2.3 TOOLS FOR APPLICATION MANUFACTURING



[12] ***Unites States Department of Defense cATO,*** *"Continuous Authorization to Operate",* ***https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF***

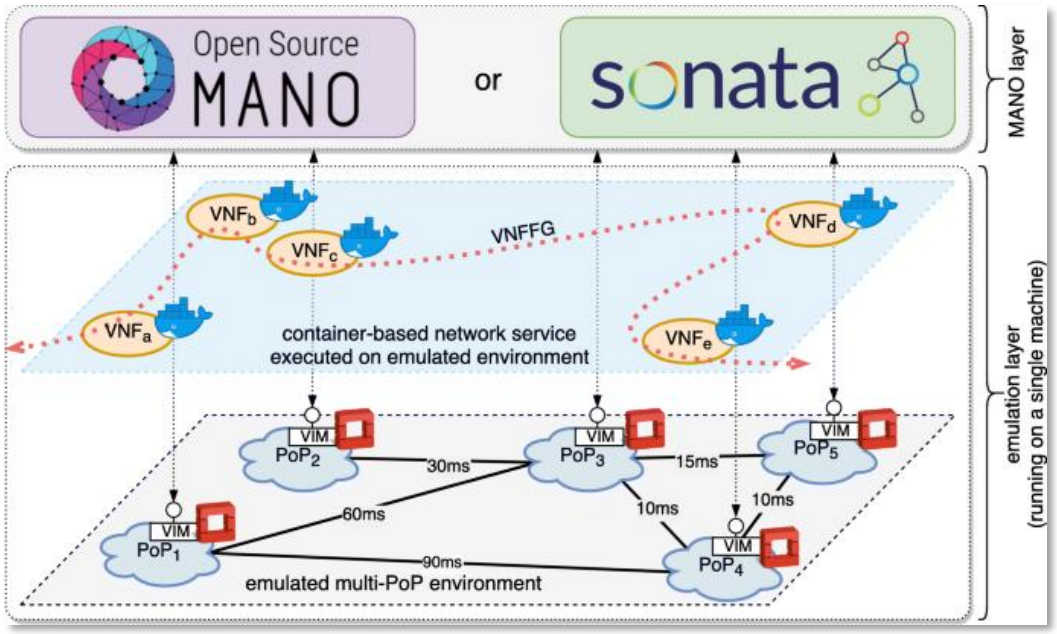
1.3.3.- DATA CENTER OPERATORS: SOFTWARE DEFINED PERIMETER

1.3.3.1 SCALABILITY: SOFTWARE DEFINED NETWORK



Over these lines, the structure that allows centralized control of network policies throughout the entire network of data centers.

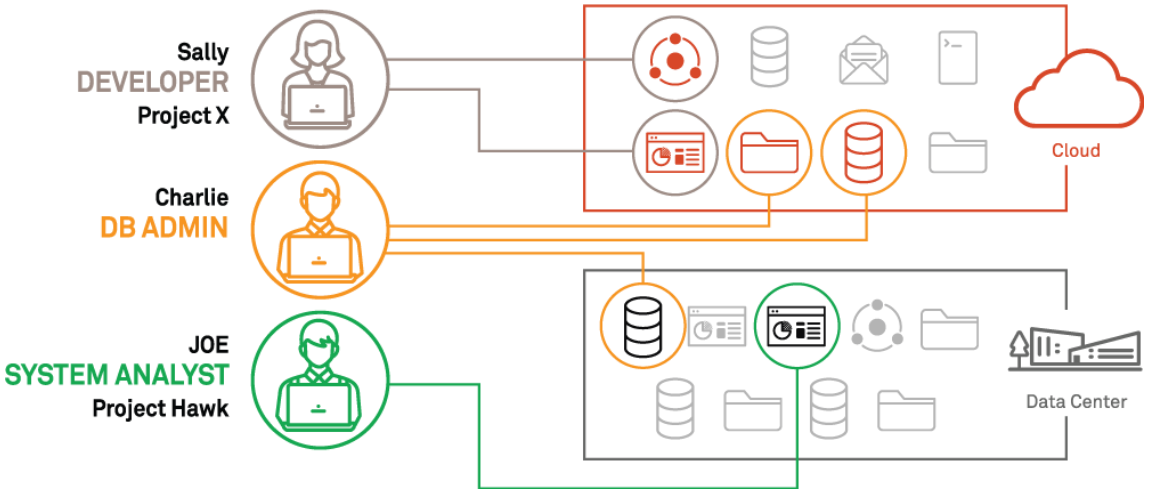
Below these lines, a simulation environment[13] to check scalability.



[13] ***Simulation of NVFs orchestrators*** *in scenarios with multiple points of presence (PoP):* *https://www.researchgate.net/publication/334046310_Automated_testing_of_NFV_orchestrators_against_carrier-grade_multi-PoP_scenarios_using_emulation-based_smoke_testing*

1.3.3.2 SECURITY: CNAP – CLOUD NATIVE ACCESS POINT

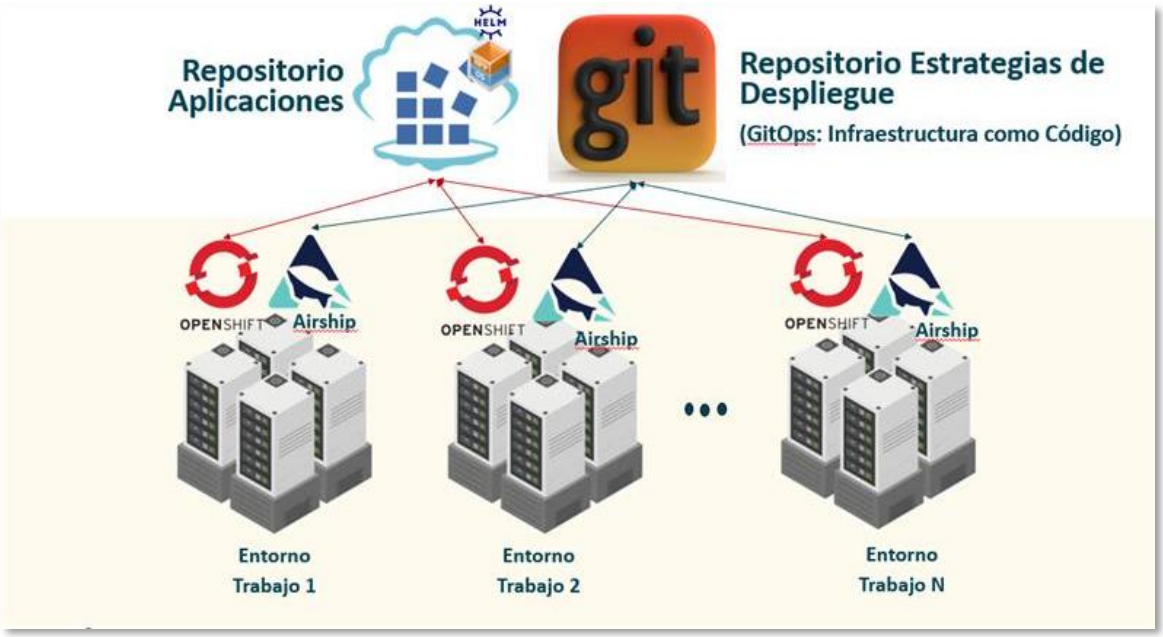
As the image shows, Cloud Native Access Point[14] consists of deploying a software-defined network for each user access (the so called segment of one), which only gives visibility to the resources over which that user has permissions, depending on their role in the system, the device you use to access and your geographic location. A process is in charge of continuously scanning if the access conditions of each connection, to reconfigure the software-defined network of the connections for which their conditions change.



1.4.- R&D TESTING LAB.

1.4.1.- TESTING LAB ARCHITECTURE.

In the R&D facilities, work structures such as those indicated in the image are deployed, serving as an extensive test battery for future production environments.



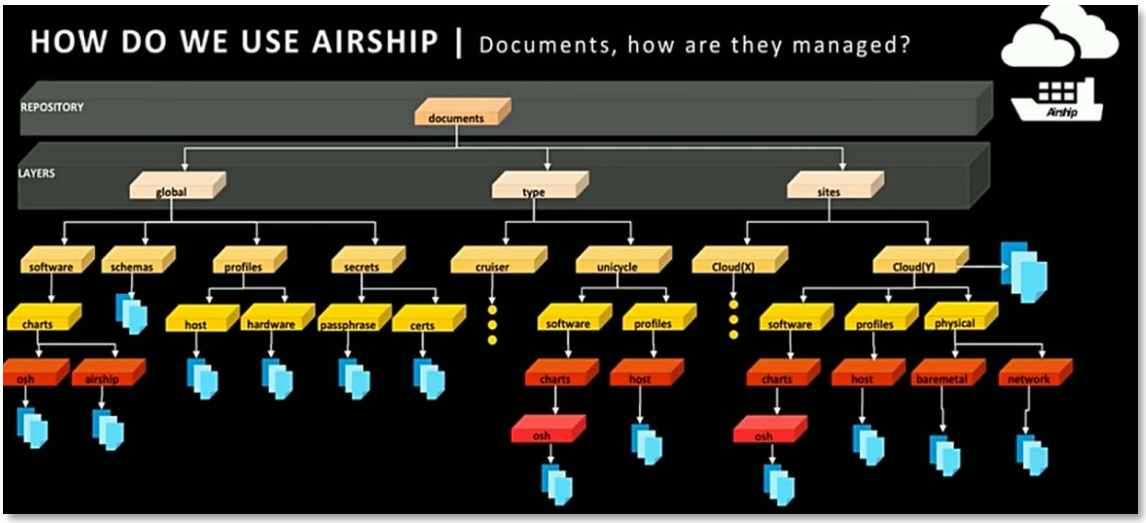
[14] ***Cloud Native Access Point***: https://www.youtube.com/watch?v=15KlsxFxkxo

1.4.2.- APPLICATION: REPOSITORIES, INTERFACES BETWEEN APPLICATIONS AND PLATFORM.

The key of the design is the repository structure that decouples the evolution of the application from the evolution of the platform. Continuous improvement processes can be applied in execution environments towards Zero-Trust principles if the evolution of the platform is isolated from application development through a stable interface: containers and infrastructure as code. Two repositories appear:

- **Application Repository**: applications are stored in the form of containers. Containers are created through a process of homologation[15] and securization[16] from a source code repository. These applications will be deployed on Zero-Trust platforms, which are kubernetes clusters (e.g. RedHat OpenShift) already initialized with continuous monitoring, provisioning, and user identity tools.
- **Deployment Strategies Repository:** collections of YAML documents that define all the configurations necessary to deploy each data center in a fully automated manner. The data center downloads its deployment strategy from the repository and from there it installs itself. These strategies have three elements:
  - *Infrastructure Description*: e.g., sectoring into kuberneter clusters to control the lifecycle of Helm applications, such as Helm OpenStack. The tools to solve this problem are in the world of Telco Cloud[17], such as AirShip[18] from AT&T.
  - *Description of Execution Environments*: e.g., cluster initialization with the necessary tools in each stage of a DevSecOps pipeline. BigBang from US Defense is one of the tools to solve this problem
  - *Configurations of each Execution Environment*: e.g., customizing each work environment of a Software factory.

In the picture, how deployment strategies look like in AirShip:



[15] ***Debian approval*** *for .deb repositories:* https://www.debian.org/doc/manuals/developers-reference/index.en.html

[16] ***NSA & CISA Methodology,*** *"Kubernetes Securing Guide"* https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2716980/nsa-cisa-release-kubernetes-hardening-guidance/

[17] ***CNTT-RI2, Kubernetes Installer Comparison:*** https://lf-networking.atlassian.net/wiki/spaces/LN/pages/15653770/Kubernetes+Installer+Comparison

[18] ***Airship***: https://www.airshipit.org/

1.4.3.- PLATFORM: INDUSTRIALLY PRODUCED FOLLOWING CNTT STANDARDS.

In the Telco sector, data centers are assembled in a factory[19], and then placed in their final location. From there, the data center connects to the region header from which it downloads the configurations that must be applied to that site.

In Brazil, an estimation of 50,000 antenna controllers in remote locations; without this degree of automation, neither the rolling out nor the updating of the entire network of data centers would be possible.

Using this same machinery, under CNTT standardization, means establishing a clear and stable line of evolution over time for the cloud platform. Additionally, the Telco sector has centers specialized in investigating cybersecurity[20] problems, which guarantees continuous improvement of the Zero-Trust platform in cybersecurity issues.

TRANSPORTATION TO THE SITE	AUTOINSTALLATION
	

1.4.4.- CYBERSECURITY: EXECUTION ENVIRONMENTS GOVERNANCE.

The first security principle is the governance of the environments that you want to protect. *This principle applied to computing means to use an application execution platform designed under a single standard*, with continuous improvement processes. A heterogeneous spread of execution environments is ungovernable, regardless of investments in different technological tools for computer security.

The use of a single standardized execution environment *'urbi et orbi'* requires to structure[21] software production[22] based on standardizing both the execution platform[23] and the application delivery repositories. *Abstracting the complex problems of execution environments and their evolution release workforce of software factories, that now are able to focus on the manufacture of better application designs*, incorporating new security aspects, such as data governance structures to avoid data fragmentation thanks to growth schemes.

---

[19] ***Nokia Datacenter Delivery Service***: https://youtu.be/nCKNIYdp7_Y?si=prtsgq8MqZyuTU2z

[20] ***Nokia Berlin Security Centre***, *analysis and continuous improvement of application security*: https://youtu.be/LNR-0Q4FUVY?si=brk9rZeyuVjVKxdc

[21] ***US National Security Software Production Model***: https://media.dau.edu/playlist/details/1_wwqs338p

[22] ***US National Security Refactoring of Applications:*** https://media.dau.edu/playlist/details/1_0kko71p1

[23] ***US National Security DevSecOps Platform:*** https://media.dau.edu/playlist/details/1_iu6ulm7r

2.- INFORMATION SOCIETY.

Everywhere we appreciate how computer applications infiltrate every interstice of our daily lives. In the car they guide our route, on the mobile they keep us connected at all hours, at work preparing reports or organizing our agenda. No space or activity escapes its influence, a phenomenon that we have agreed to call "digital transformation."

Without realizing it, we are increasingly dependent on a virtual world which we know little about. From the largest corporations to each one of us - individually - no one is able to escape this powerful influence... we are all at the mercy of these computer applications, like buoys adrift on ocean currents.

Where are the currents of this digital ocean dragging us? Cinema repeatedly evokes the fear of being dominated by machines that we ourselves have created. We feel that this new reality is pushing us into an uncertain future, sacrificing the treasure of our intimacy along the way.

However, this entire virtual universe that surrounds us is reduced to computer applications: in all its wide spectrum of goals and manufacturing technologies... from flight control systems, through factory robotics, artificial intelligence, big data, to the applications on our personal computers or mobile phones.

In DNA we find encoded the organizational schemes of all the systems that make up a living organism. Information exists to organize and coordinate life, that is, for the order and good rhythm that governs our Cosmos. Human societies do not escape this law, which is why we find ourselves surrounded by all those computer tools that serve to organize ourselves better as a society, in what they label as "information society." It becomes vital, therefore, not to leave the production of those applications that organize all our lives in the hands of short-sighted commercial interests, which trap us in virtual experiences with uncertain intentions and dubious usefulness.

Perhaps it is our inability to organize and govern the production of those applications that control our lives that really gives us that feeling of being at the mercy of those technologies, instead of putting them at our service. Is artificial intelligence the problem, or the data that feeds those algorithms that run on machinery available for very few pockets, causing the problem of digital sovereignty? Our data is concentrated and crammed in an unhygienic manner in clouds over which we have no control, since we are not its owners... with high fragmentation, managed by algorithms with very poor traceability, which do not usually conform to any quality standard. When there is a lot of leaf litter, it is easy for a small spark to start an unstoppable fire. Could this be our true fear, are we simply unable to crystallize it into words?