sysdig

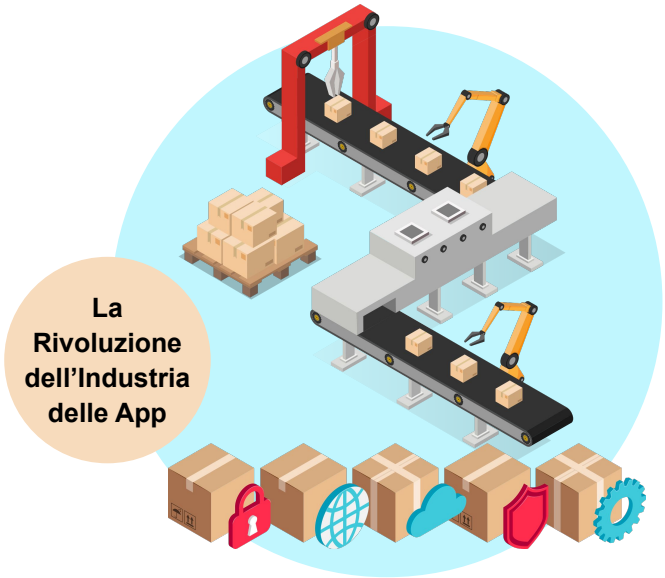
La Protezione dei Container

Anche le nuove frontiere applicative sono attaccabili

Giulio Puri

Solutions Engineer

Il cloud sta cambiando la creazione delle Applicazioni



I 3 Megatrends:

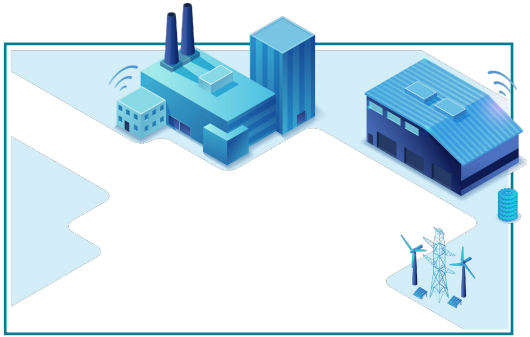
1. Rilascio su **Cloud Pubblico**
2. Struttura a **Microservizi**
3. Processi **DevOps**

Rilascio su Cloud Pubblico

Sfruttando Infrastructure-as-a-Service (IaaS) e Platform-as-a-Service (PaaS)

IaaS

"Affitto della Fabbrica"



Gestito dal team IT/Infrastruttura

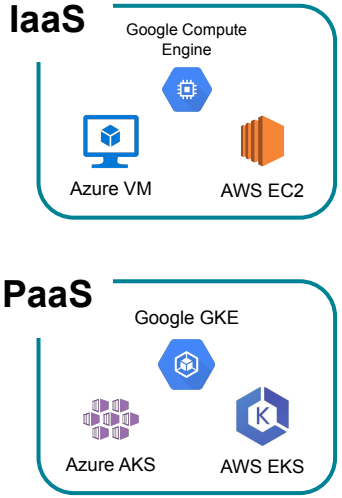
- Servers
- Storage
- Networking

PaaS

"Affitto della Fabbrica e dei Servizi"

Gestito dal team Sviluppo

- Servers
- Storage
- Networking
- Operating Systems
- Middleware
- Runtime



Struttura a Microservizi

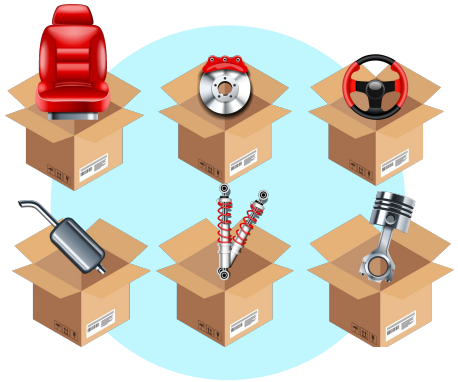
L'approccio Legacy

Auto "Monolitica"

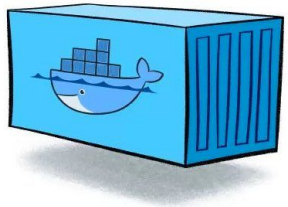
- Lunghe tempistiche di produzione
- Progettata per lunghi cicli di produzione
- Difficilmente modificabile se non impattando l'intero progetto

Il Nuovo Approccio

Componenti Intercambiabili



- Create individualmente
- Facilmente aggiornabili
- Sostituibili senza impattare le altre parti

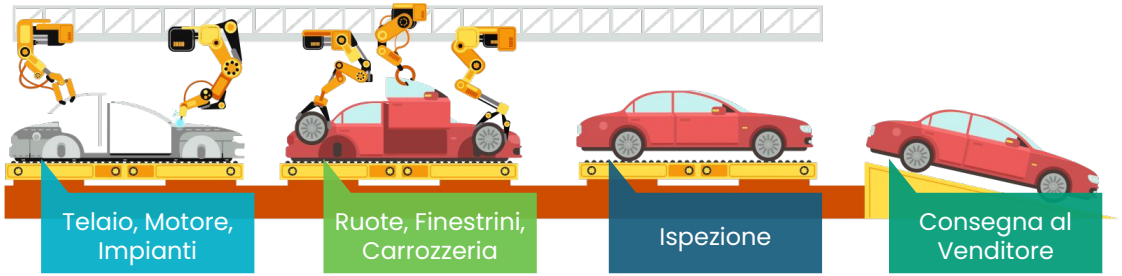


Containers

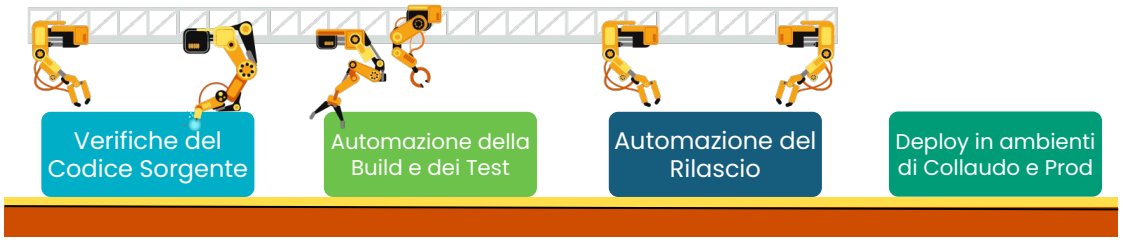
Kubernetes

Processi Development Operations (DevOps)

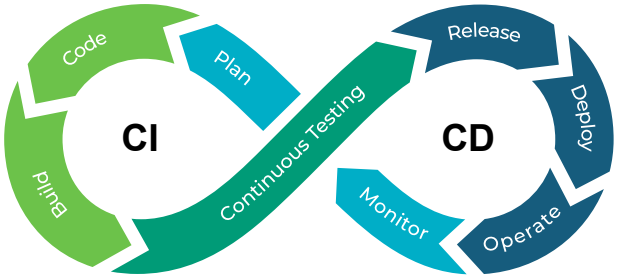
Catena di Assemblaggio



DevOps Pipeline



Efficientare e **velocizzare** il processo di sviluppo e rilascio di Applicazioni



Continuous Integration
Continuous Delivery

La Transizione al Cloud

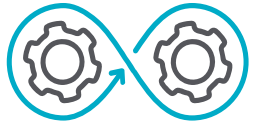
STAGE 1
Flessibilitá
(Rehosting)

STAGE 2
Modernizzazione
(Refactoring)

STAGE 3
Velocitá e Scalabilitá
(Cloud-Native)

Cloud IaaS/PaaS

Containers/K8s



DevOps:CI/CD

Cloud Security Posture Management

Workload Protection

DevSecOps

Cloud Security Posture Management

Statica

- Verifica delle Configurazioni Cloud
- Valutazione rispetto Best Practices e Requisiti Normativi
- Verifica dei Permessi e Ruoli Utente
- Inventario delle Risorse Cloud

Valutazione della Postura e dei Rischi

Real-Time

- Monitoraggio delle Attivitá Utente
- Individuazione delle Minacce
- Controllo dello Stato delle Risorse Cloud

Identificazioni di Attivitá Sospette

Cloud Security Posture Management - CSPM

CSPM - Best Practices

1. Proteggere il "Cloud Control Plane"
Il pannello di amministrazione Cloud deve essere sotto controllo (e.g. logging, MFA), e configurato correttamente (e.g. disabilitando regions e risorse non necessarie)

2. Applicazione del Principio "Least privileges"
Permessi e ruoli delle utenze aventi accesso ai servizi cloud devono essere costantemente monitorati e ridotti al minimo indispensabile

3. Verificare come Vengono Condivisi i Dati
Per mezzo di controlli dedicati a individuare configurazioni errate dei datastore e alla corretta gestione dei meccanismi di cifratura e rotazione delle chiavi

4. Monitorare Continuamente le Attivitá
Tracciando attivitá utente e gli eventi legati alle risorse cloud, al fine di individuare comportamenti sospetti

5. Condurre Cloud Risk Assessments Periodici
Per garantire l'applicazione delle policies di sicurezza e valutare la riduzione del livello di rischio

6. Formazione sulla Cloud Security Awareness
L'adozione di nuove tecnologie richiede una formazione dal punto di vista della sicurezza, per chiarire impatti e rischi che si possono correre

Cloud Security Posture Management - CSPM

Workload Protection

Visibilitá runtime mediante un monitoraggio continuo

Identificazione di attivitá e comportamenti sospetti

Notifiche immediate e automazioni per intervenire

Cloud Workload Protection Platform - CWPP

Workload Protection - Best Practices

1. Applicare una "Security Baseline"
Mediante un insieme di controlli che permettano una prima messa in sicurezza del workload in accordo a framework di sicurezza (e.g. MITRE ATT&CK)

2. Automatizzare la Risoluzione
Integrando strumenti esistenti (e.g. SIEM) ed implementando meccanismi di notifica e collezionamento delle evidenze automatizzati

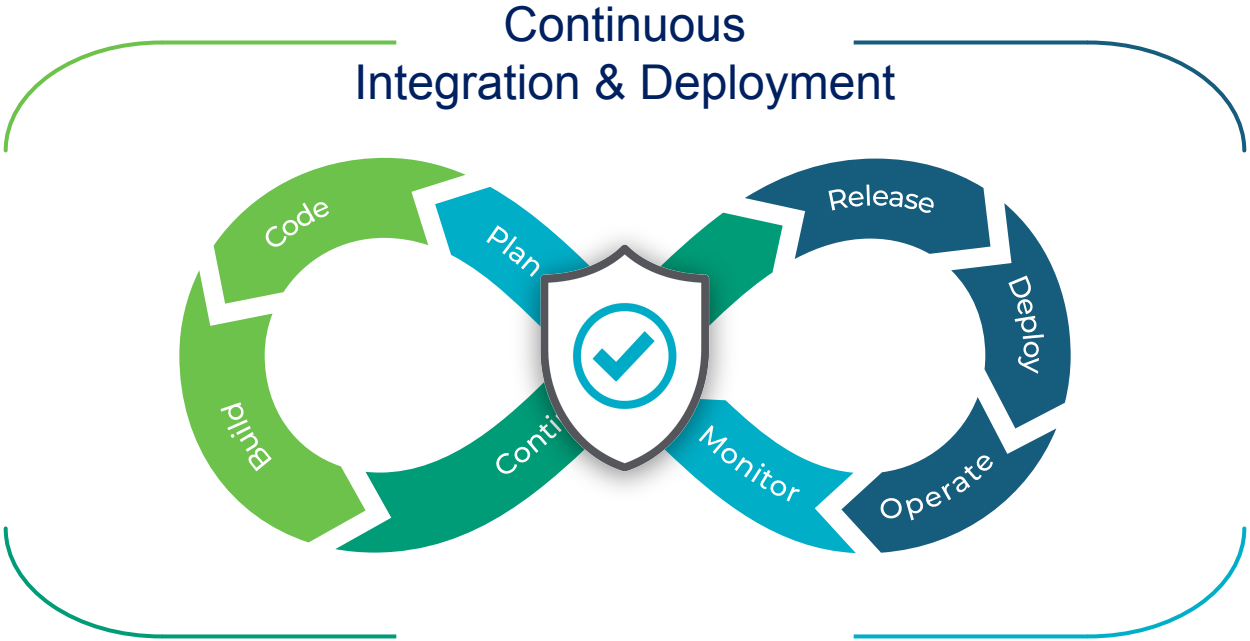
3. Integrare sorgenti di Intelligence e IoCs
Per estendere l'individuazione di minacce e anomalie anche per mezzo di threat intelligence e IoCs

4. Estendere la copertura ad Host/VMs
Garantendo opportuni livelli di controllo anche ai servizi ed istanze che ospitano i microservizi ed i containers

5. Implementare Controlli Ad-Hoc
Che rispettino le priorità di sicurezza individuate e che permettano di soddisfare i requisiti di compliance.

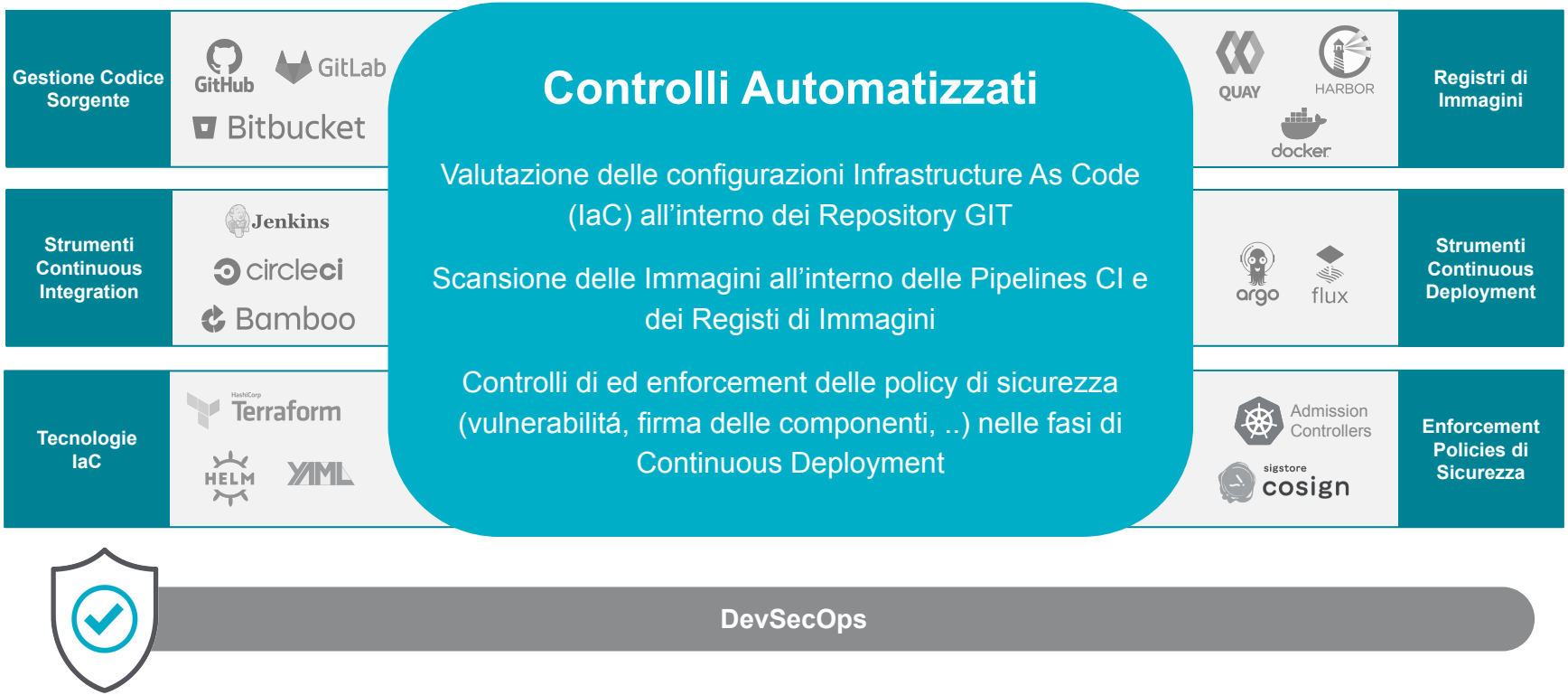
Cloud Workload Protection Platform - CWPP

DevSecOps

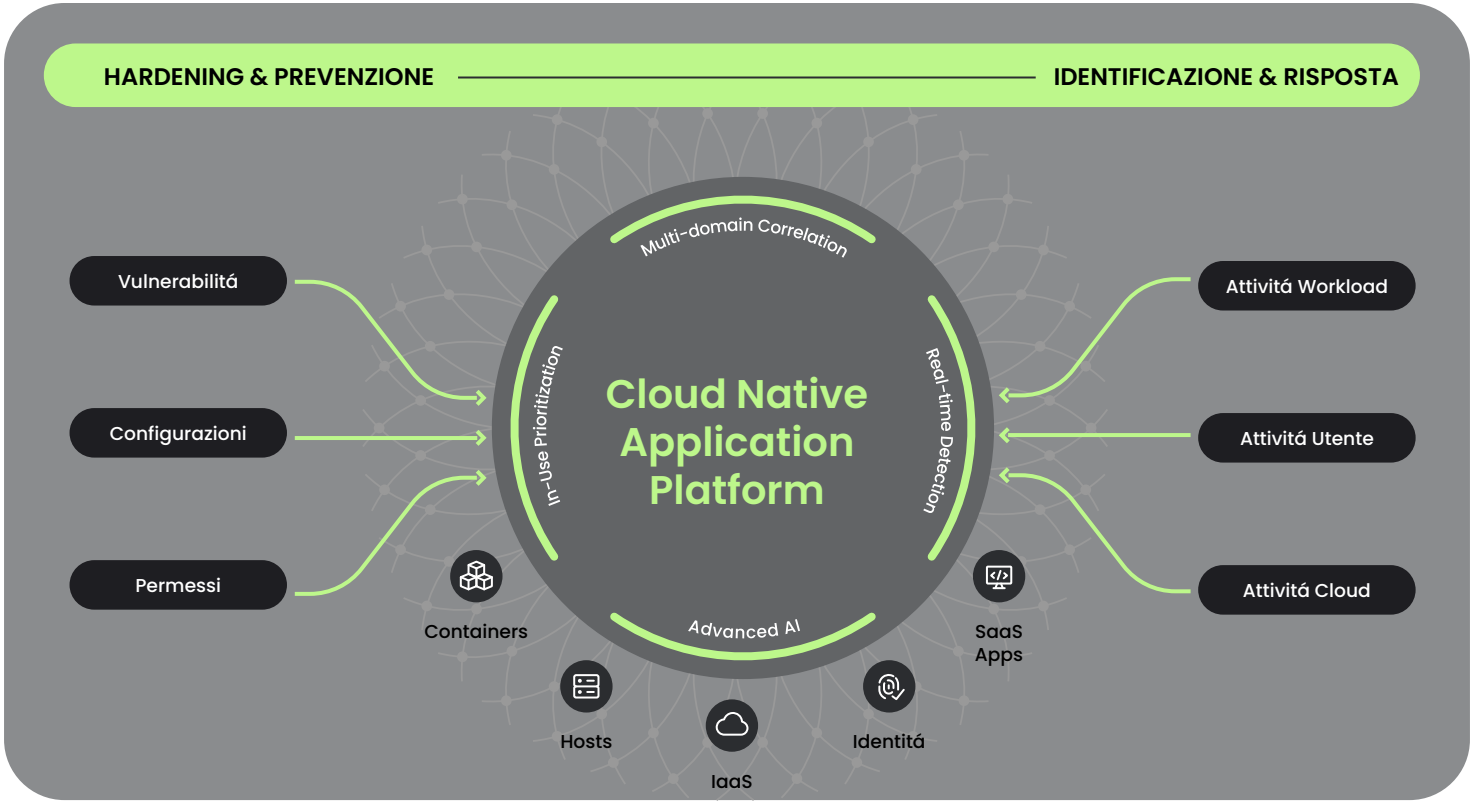


DevSecOps

DevSecOps


Gestione Codice Sorgente
GitHub
GitLab
Bitbucket
Controlli Automatizzati
Valutazione delle configurazioni Infrastructure As Code (IaC) all'interno dei Repository GIT
Scansione delle Immagini all'interno delle Pipelines CI e dei Registi di Immagini
Controlli di ed enforcement delle policy di sicurezza (vulnerabilitá, firma delle componenti, ..) nelle fasi di Continuous Deployment
QUAY
HARBOR
docker
Registri di Immagini
Strumenti Continuous Integration
Jenkins
circleci
Bamboo
argo
flux
Strumenti Continuous Deployment
Tecnologie IaC
HashiCorp
Terraform
HELM
YAML
Admission Controllers
sigstore
cosign
Enforcement Policies di Sicurezza
DevSecOps

Proteggere Applicazioni nel Cloud




sysdig
SECURE
EVERY
SECOND