

# Cloud Computing Forensics

peculiarità e indicazioni metodologiche

Vincenzo Calabrò – Funzionario alla Sicurezza CIS  
(Ministero dell'Interno) e Digital Forensics Analyst



# Cloud Computing Forensics?

- Il Cloud Computing è attualmente il principale modello di deployment di servizi online, applicazioni, risorse e dati
- È adottato da tutte le organizzazioni, indipendentemente dal settore, dalle dimensioni o dalle esigenze di calcolo e/o di storage
- **Si è sviluppato il contenzioso avente ad oggetto il cloud**



**i termini contrattuali  
e/o le condizioni di  
servizio**



**la violazione alla  
sicurezza dei dati o  
dei servizi**



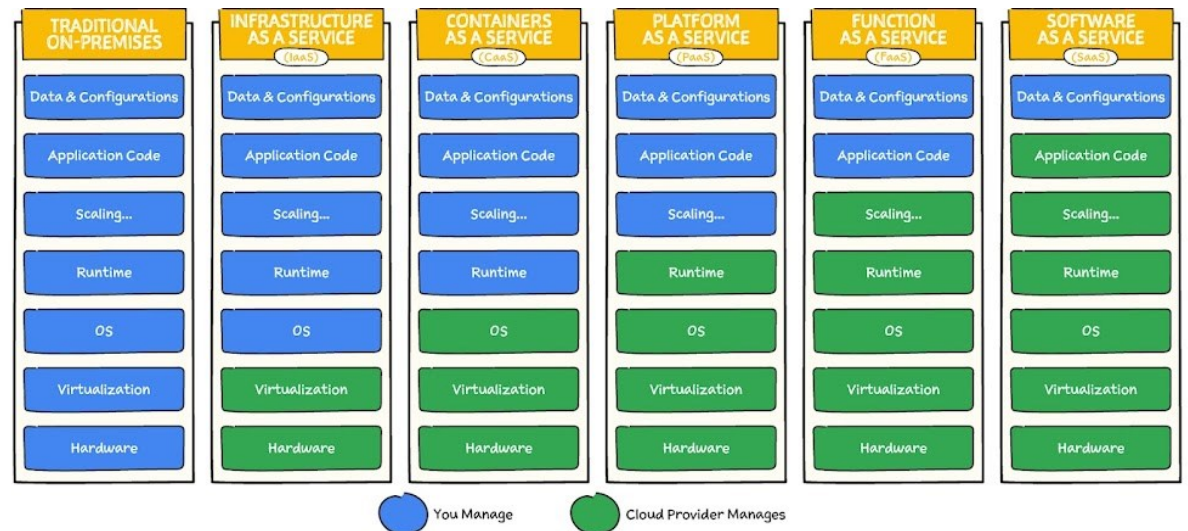
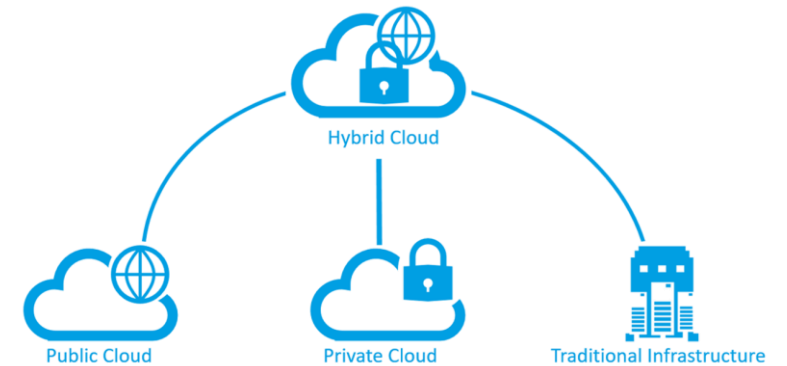
**lo sfruttamento della  
capacità di calcolo  
e/o memorizzazione**



# Cloud computing: peculiarità

Il Cloud Computing si caratterizza dai sistemi on-premise per una serie di proprietà con un impatto significativo sulle investigazioni digitali

- **Modello di deployment** (pubblico, privato, ibrido, multi cloud)
- **Trasferimento della responsabilità**
- **Elasticità, scalabilità e flessibilità**
- **Gestione dinamica delle risorse**
- **Misure di sicurezza e protezione**
- **Distribuzione geografica**
- **Multi-tenancy**



**non è possibile applicare le classiche metodologie di digital forensics**



# Cloud Forensics Process Flow



Identification

Collection - Acquisition

Preservation

Analysis - Presentation

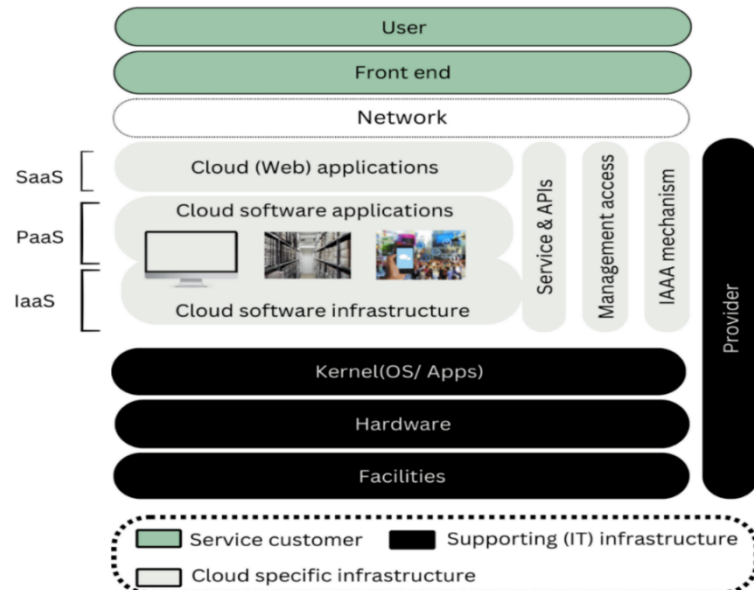


ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence  
ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence

# Identification

## Criticità

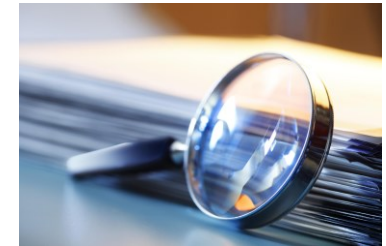
- indeterminazione del posizionamento degli oggetti
- decentramento delle risorse e dei dati
- inaccessibilità fisica del sistema
- cifratura dei dati



ISO/IEC 27037:2012 “the process involving the search for, recognition and documentation of potential digital evidence”

## Cercare / Ottenere

- le specifiche dell’ambiente
- i servizi di supporto abilitati
- le tipologie di servizi oggetto di indagine
- le regioni/zone che ospitano le VM/istanze/dati
- il contratto di fornitura tra utente e provider
- la collaborazione del provider
- le credenziali o i token degli account con privilegi admin
- i log dei servizi d’interesse e dei servizi cloud correlati
- i client per l’accesso alla console dei cloud services



# Collection

ISO/IEC 27037:2012 “the process of gathering items that contain potential digital evidence”

La **collection in cloud** è virtuale e si può realizzare

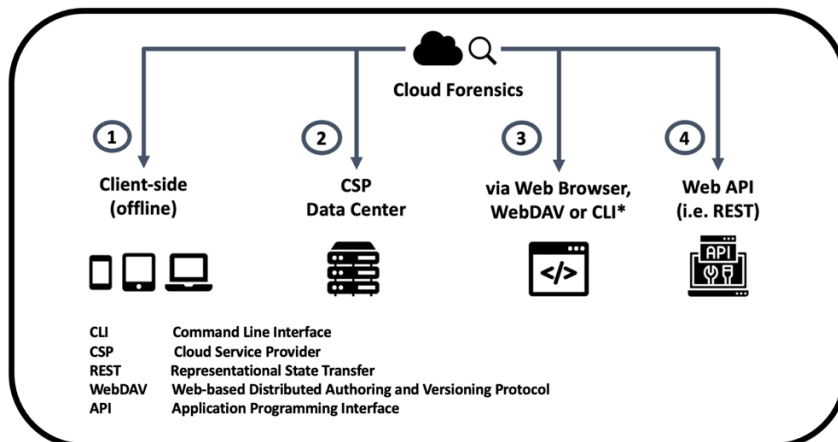
**disabilitando le utenze admin e user** (o cambiando le password)  
**inibendo l’accesso agli utenti** (non per servizi critici)  
**bloccando le VM, le istanze e i servizi** (non per servizi critici)



# Acquisition

ISO/IEC 27037:2012 “the process of creating a copy of data within a defined set”

L’**acquisition in cloud** si caratterizza: **inaccessibilità** fisica delle risorse, **volatilità** delle risorse virtualizzate e uso di meccanismi di **replicazione**. Si procede con l’**acquisizione remota** e il **trasferimento dei dati** con un canale sicuro



## Cosa

- Copia delle macchine virtuali o dei container o dei dati
- Snapshot dello stato delle macchine virtuali/istanze
- Dati di monitoring per la detection & response

## Come

- Interfacce applicative (API)
- Tramite tools di gestione
- Live forensics



# Preservation

ISO/IEC 27037:2012 “the process to maintain and safeguard the integrity and/or original condition of the potential digital evidence”

Si calcola il codice hash crittografico degli oggetti copiati

## Criticità

- Duplicazione
- Volatilità
- Multi-tenancy



**Effettuare una dettagliata documentazione delle fasi di acquisizione e conservazione**



# Analysis - Interpretation

ISO/IEC 27042:2015 “the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability.”

## Criticità

- Integrazioni evidenze provenienti da ambienti eterogenei e diversi
- Aggregazione di logs non omogenei o timestamp disallineati
- Servizi erogati da altri provider
- Cifratura dei dati



**Report intellegibili e autoesplicativi**



# Conclusioni e prospettive future

## Elementi critici di un'indagine digitale in ambiente cloud

- volatilità delle risorse virtualizzate
- inaccessibilità delle risorse fisiche
- cifratura dei dati
- giurisdizione dei provider



## Punti di forza per superare le criticità

- evidenze offerte dalle tecnologie di detection e response attive
- coinvolgimento del provider, a meno che non sia una controparte del contenzioso
- upskilling degli addetti alla cloud security sugli aspetti della digital forensics
- accesso tramite client locali per bypassare il problema della giurisdizione del provider



# Vincenzo Calabrò

**mail** [info@vincenzocalabro.it](mailto:info@vincenzocalabro.it)

**LinkedIn** [/in/vincenzocalabro](https://www.linkedin.com/in/vincenzocalabro)