

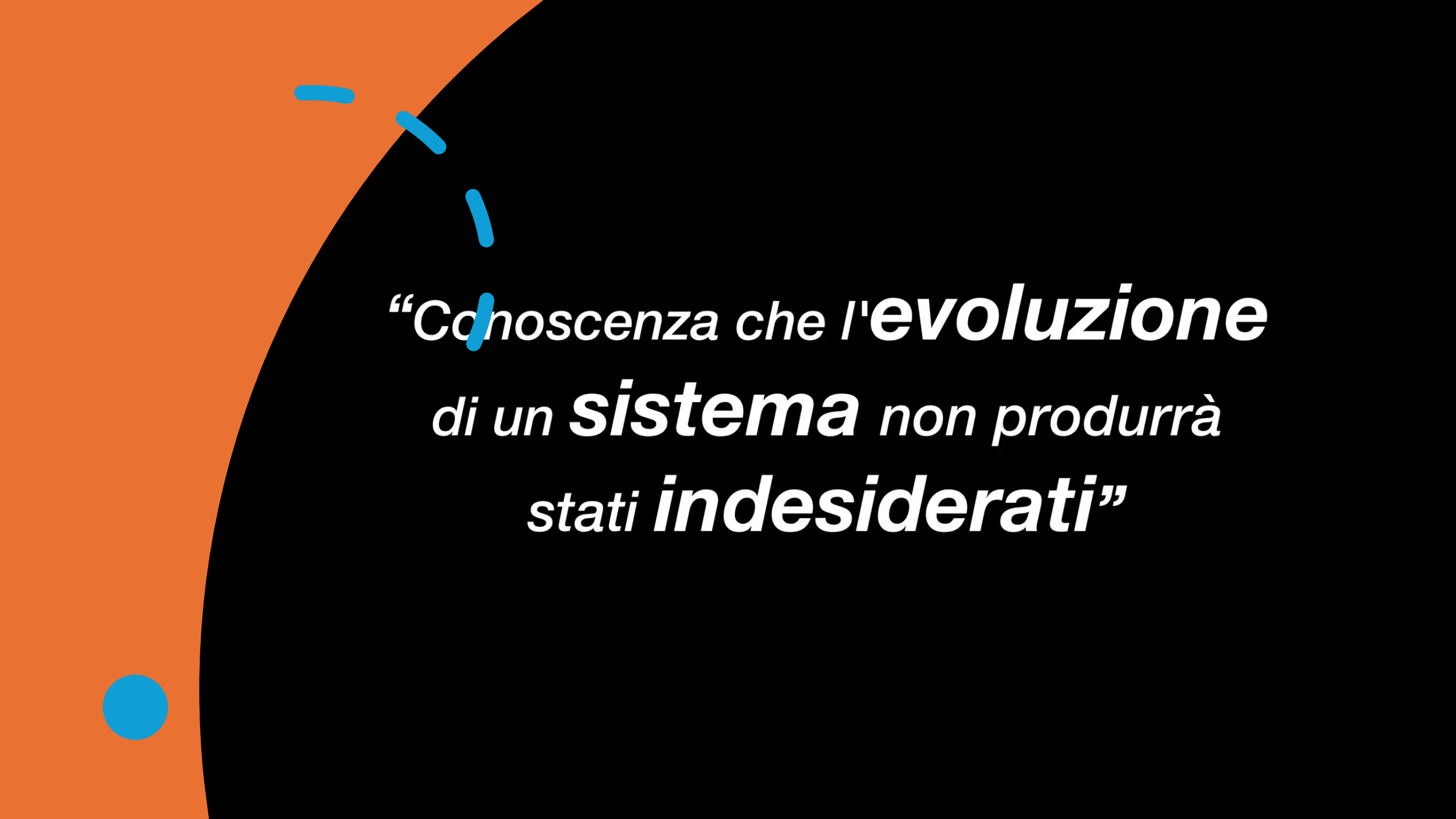
# La sicurezza nell'era del Cloud

Come creare infrastrutture Cloud  
sicure



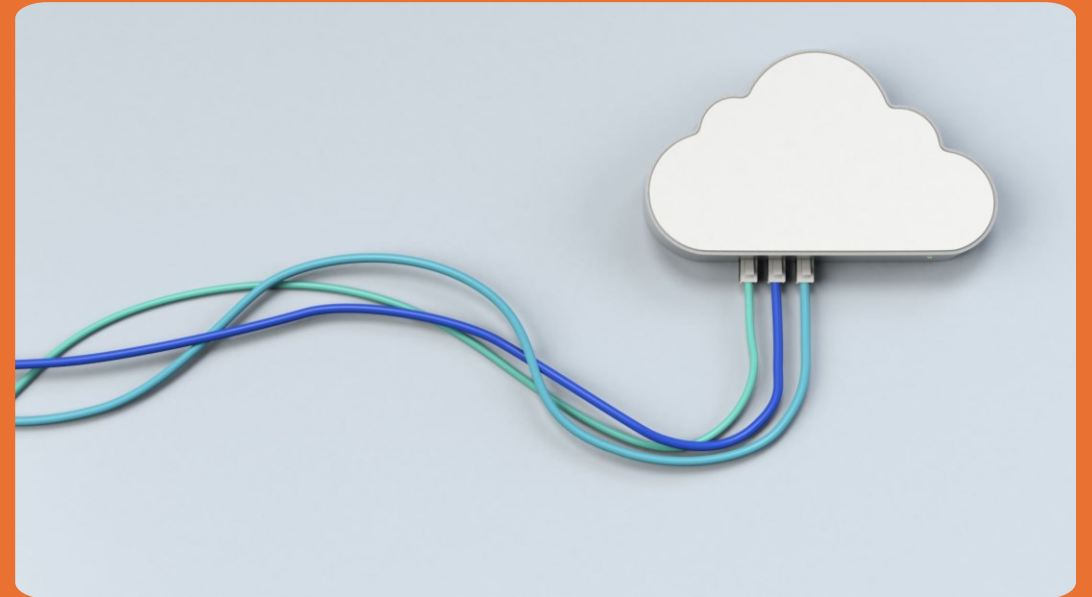
Cose si  
intende per  
sicurezza?





*“Conoscenza che l'**evoluzione**  
di un **sistema** non produrrà  
stati **indesiderati**”*

Come ottenere la  
sicurezza in  
Cloud?





**Sicurezza in Cloud**



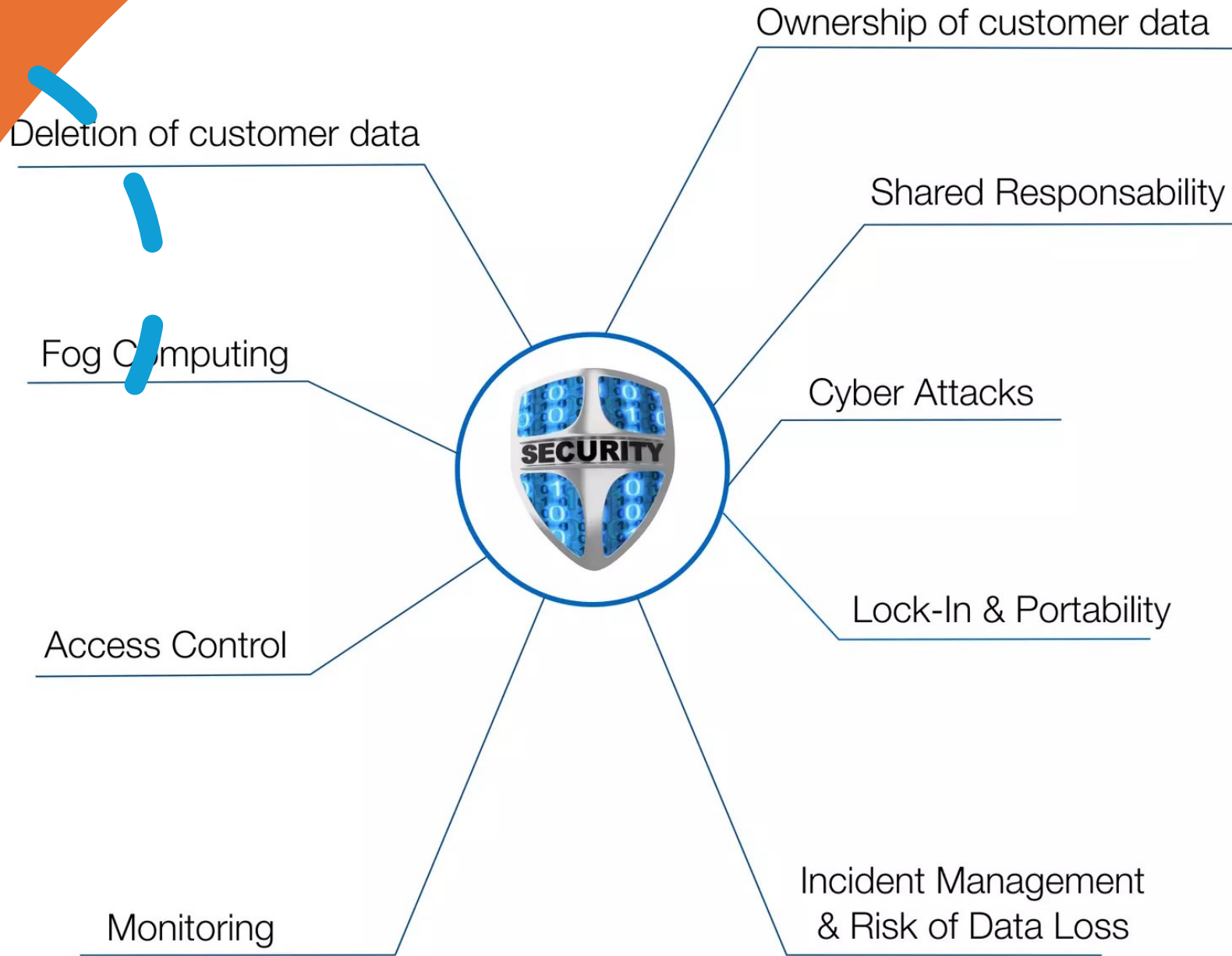
***Aspetti Tecnici***



***Aspetti Legali***



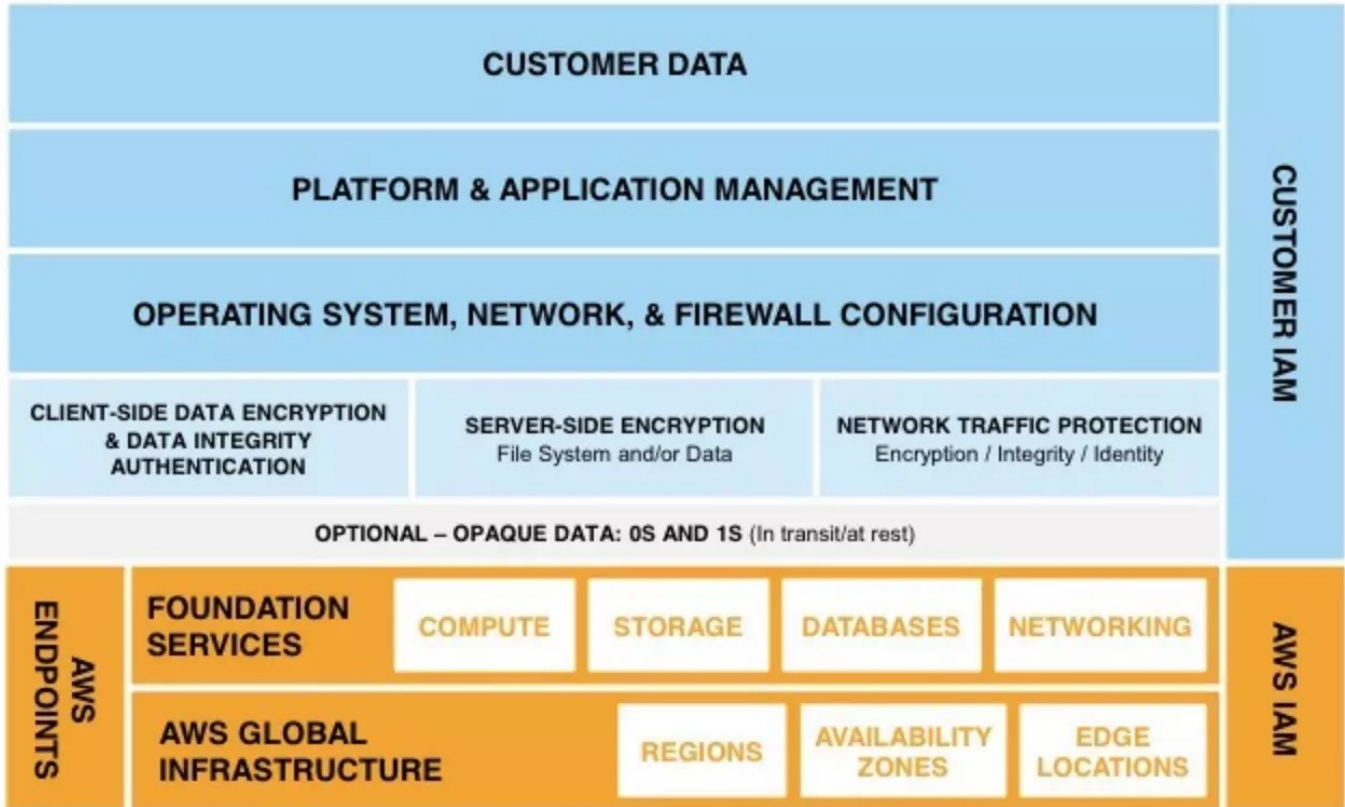
# Tematiche tecniche sicurezza in Cloud





# Shared Responsibility

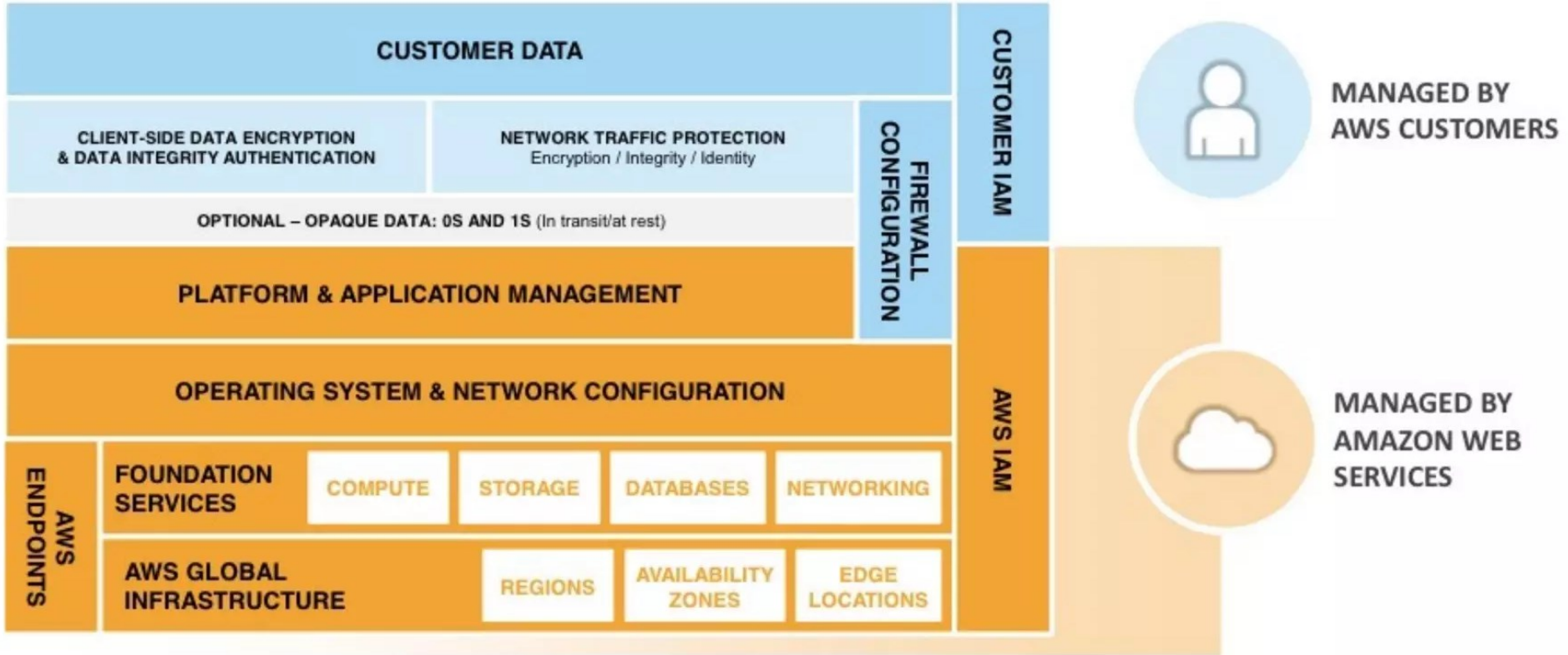




MANAGED BY  
AWS CUSTOMERS



MANAGED BY  
AMAZON WEB SERVICES



# Shared Responsibility



- Infrastruttura fisica
- Sicurezza fisica
- Storage
- Infrastruttura di rete
- Strato di virtualizzazione
- Gestione dei servizi

+



- Configurazione VPC e Sicurezza
- Firewall di Sistema
- Sistemi operativi
- Sicurezza Applicativa
- Configurazione dei servizi

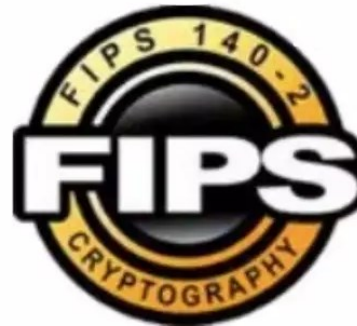
=



**Si ottiene un'architettura molto più sicura e affidabile rispetto ad una soluzione**



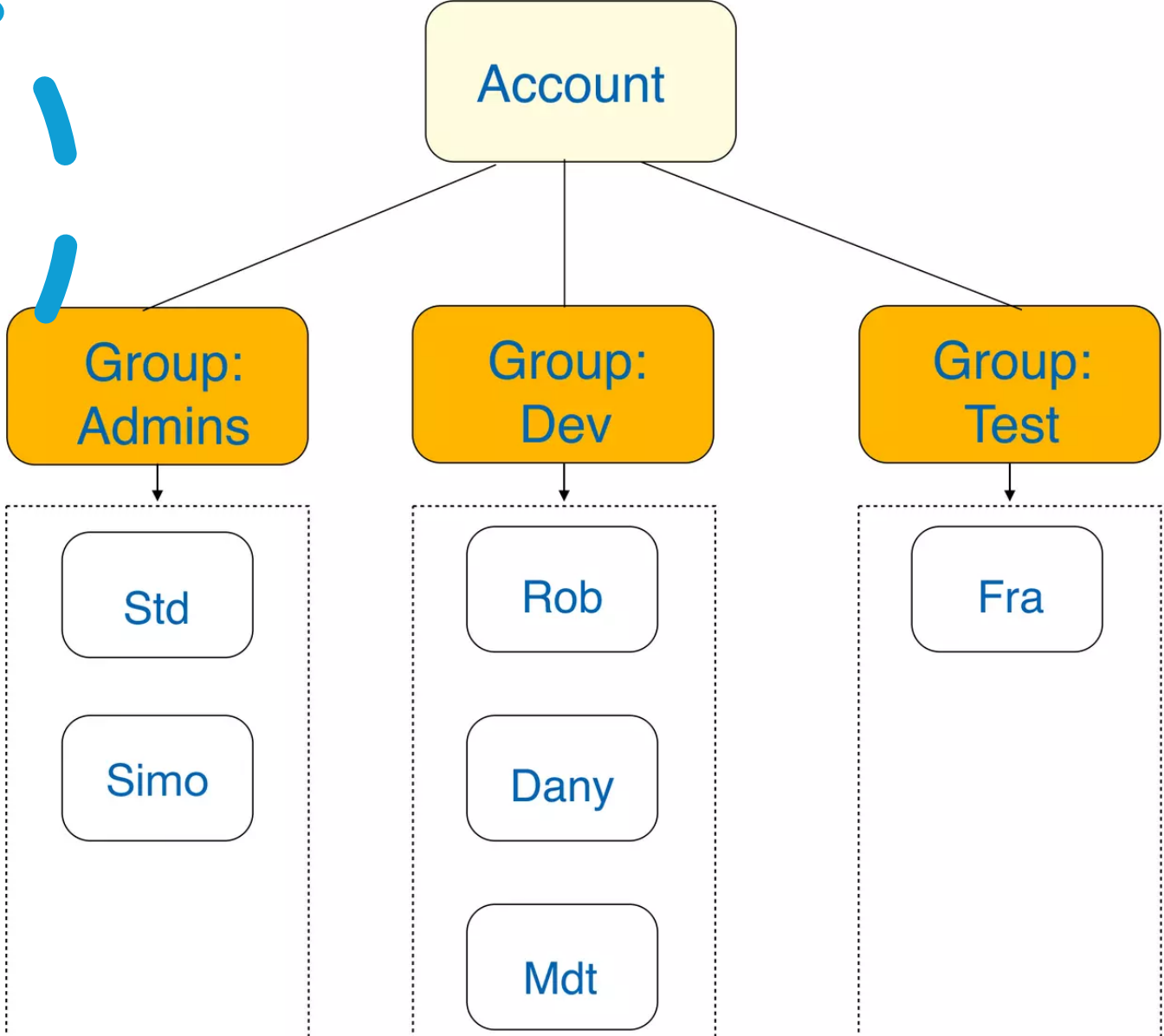
FISMA





# Access Control

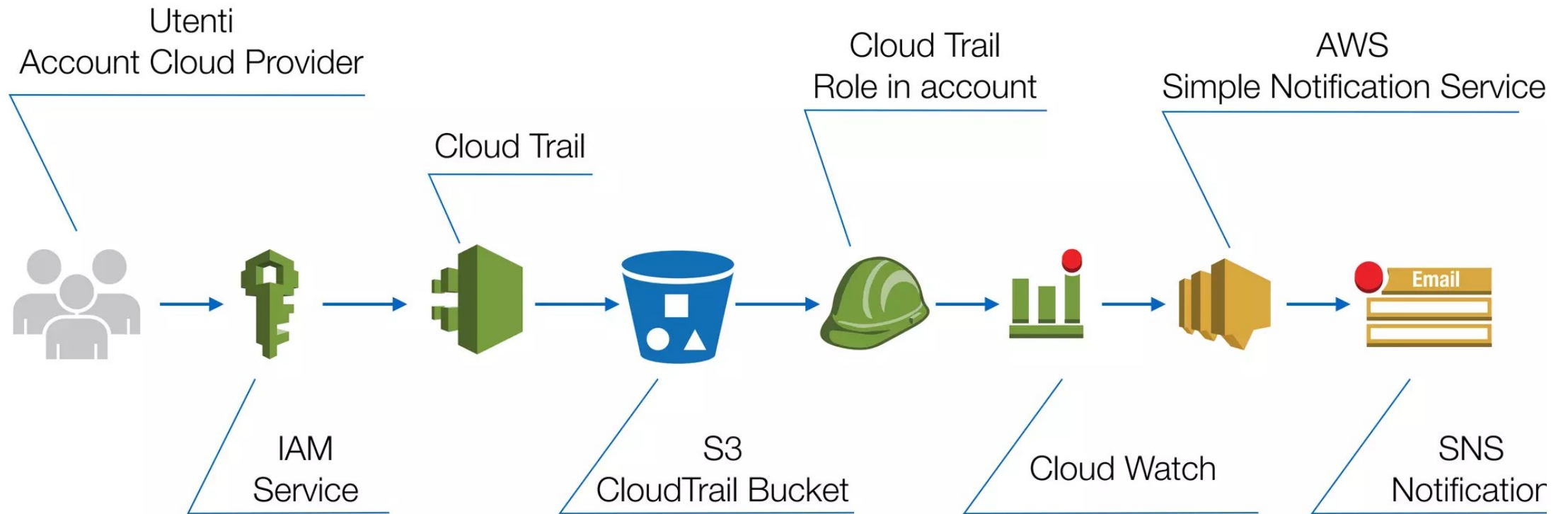
# Identity Access Management



Sign In

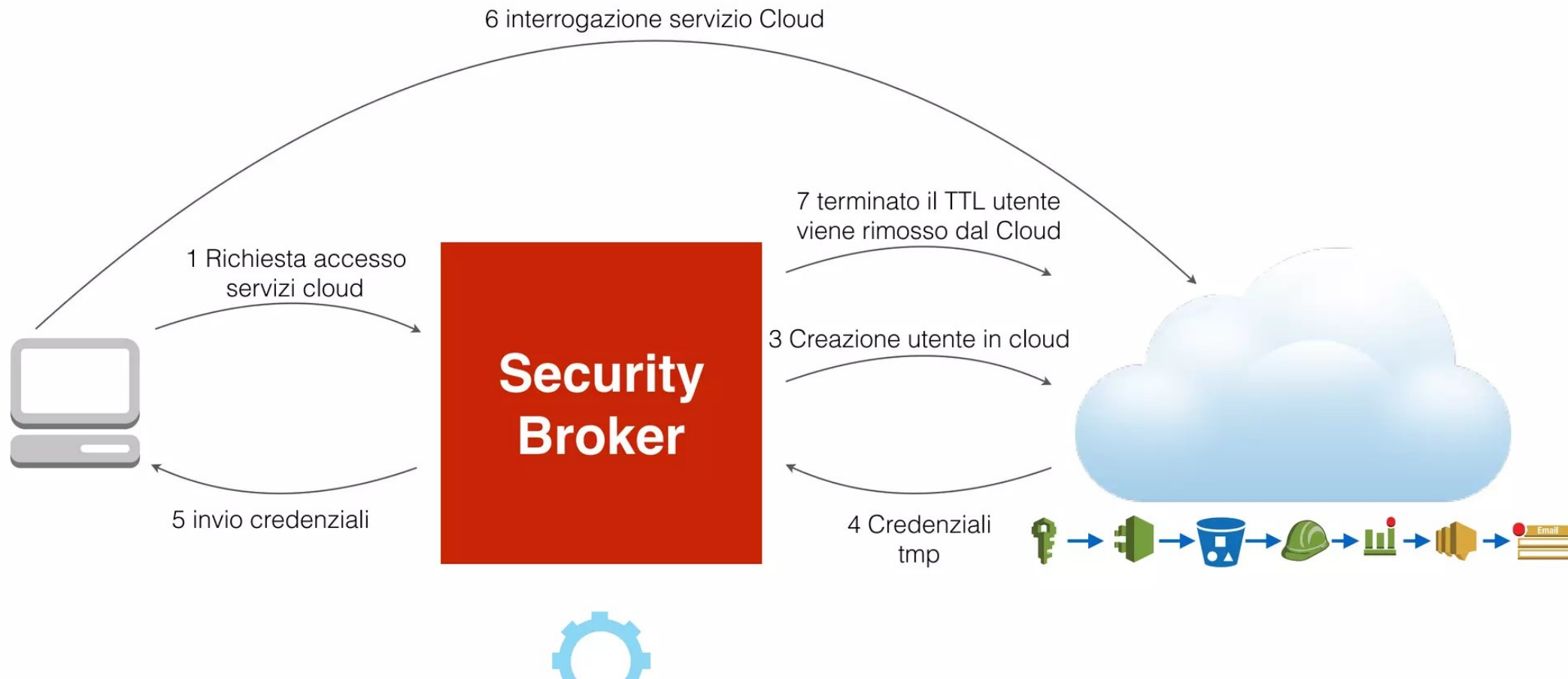
[Sign-in using root account credentials](#)







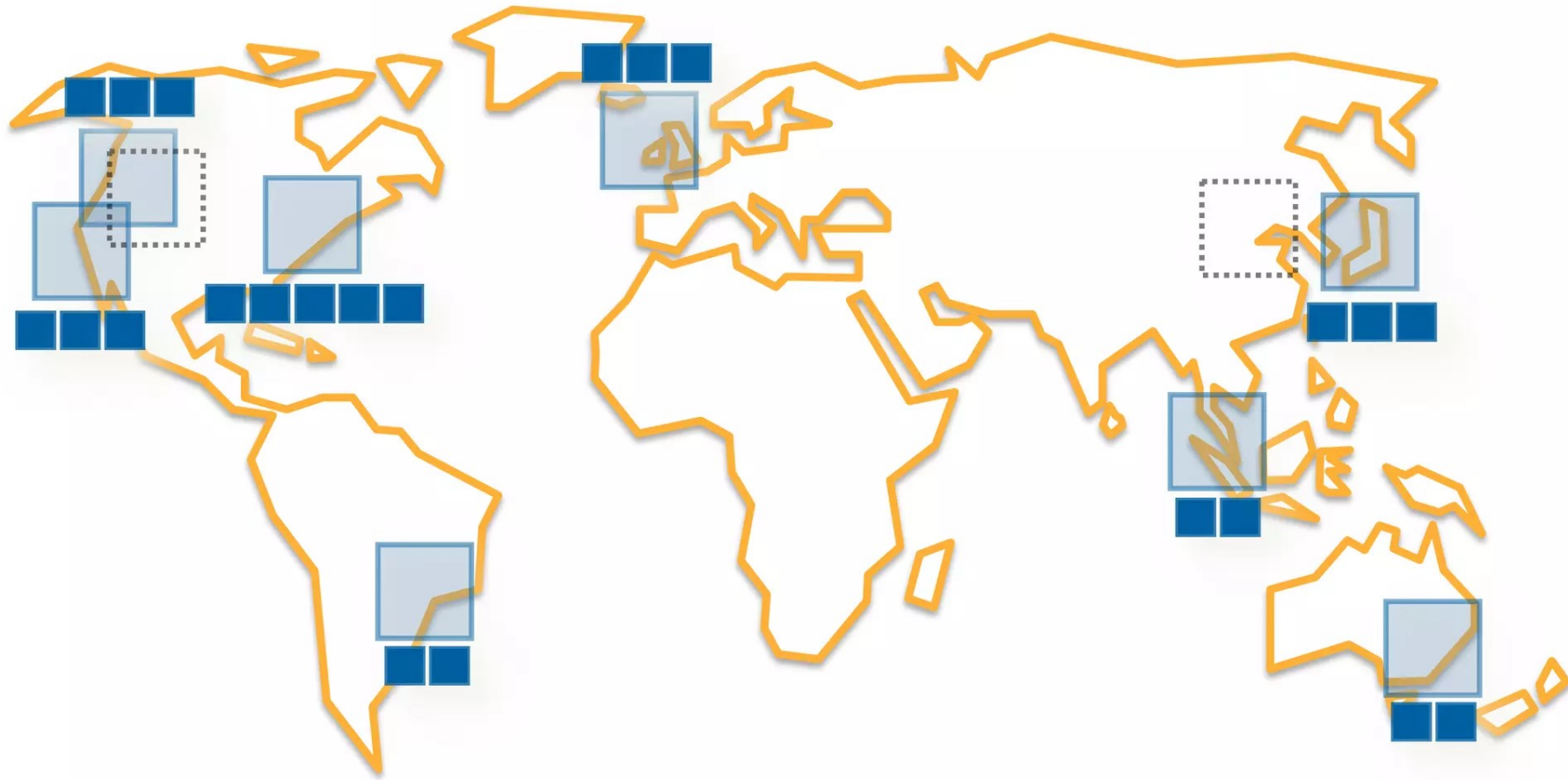
# Security Broker



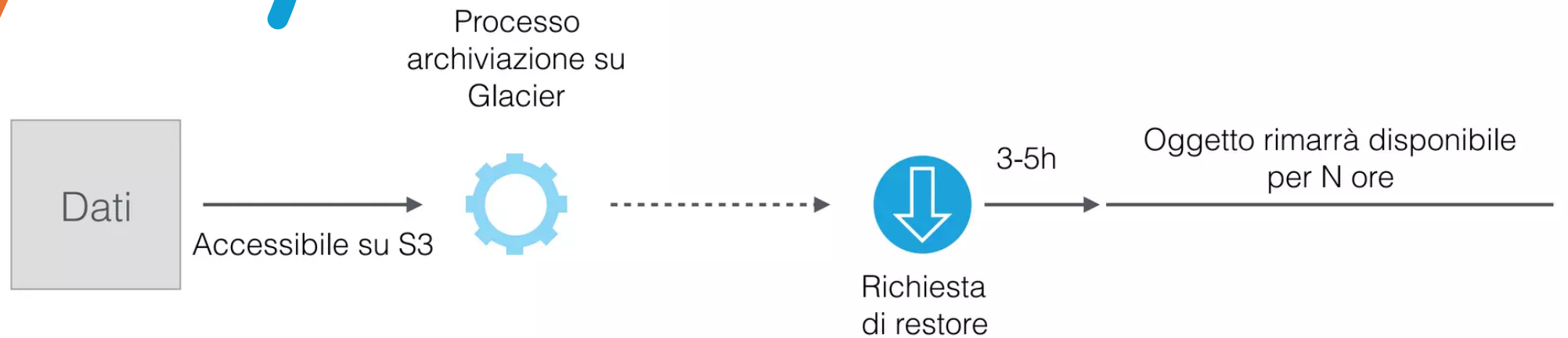


# Incident Management & Risk of Data Loss

# *Distribuzione geografica*



# Risk of data loss





# Lock-In & Portability

# DEVELOPER

lab

Politiche di migrazione

Sviluppare a Moduli

Solo Componenti "Standard"

TTL dei progetti



# Architettura & Cyber Attack

# DDoS Trends in 2014

Infrastructure Attack

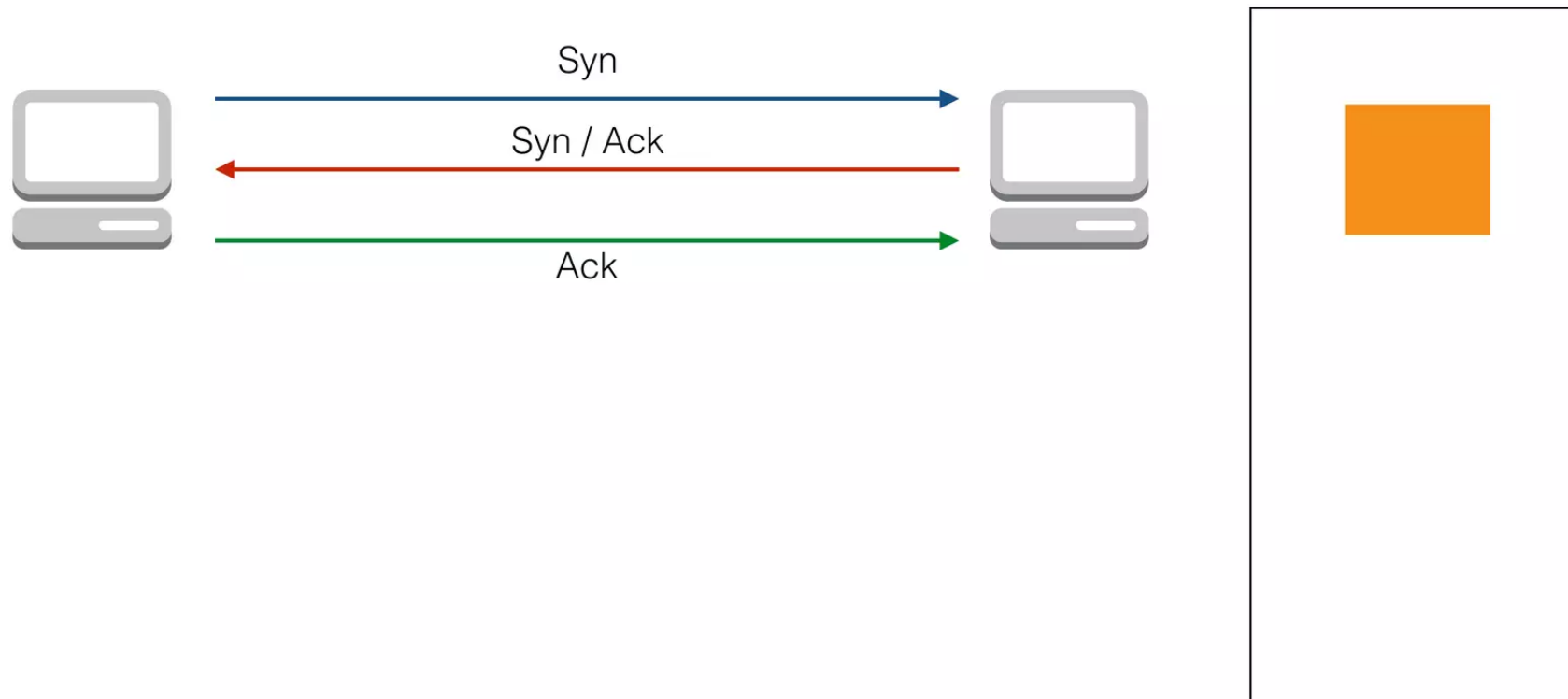
**78%**

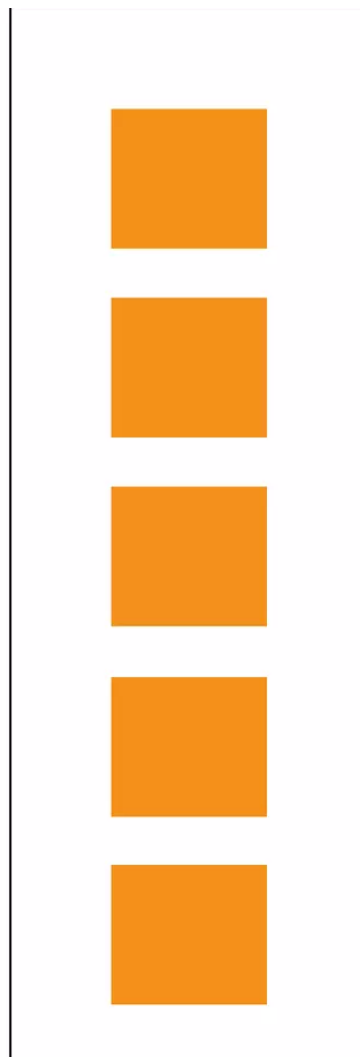
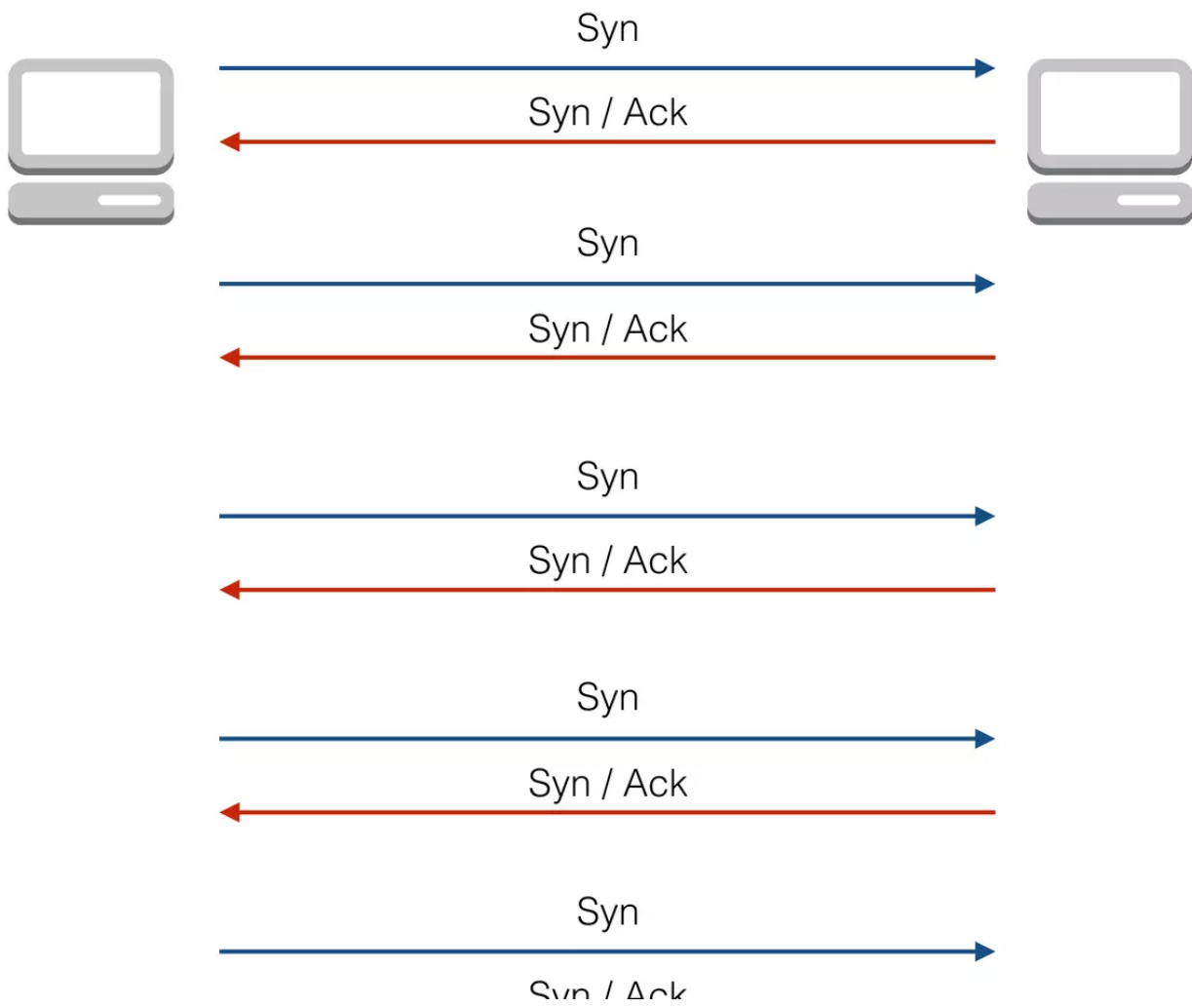
Application Attack

**22%**

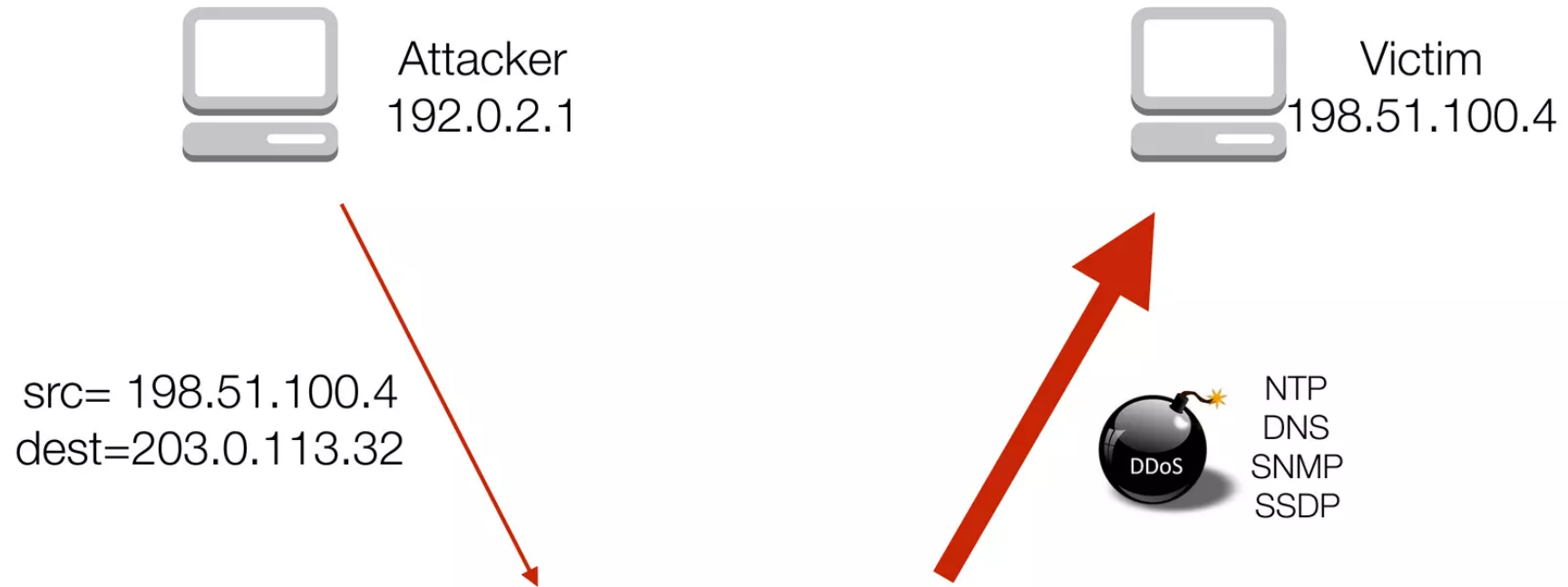


# Syn Flood Attack





# Distributed Reflection Denial of Service



A stethoscope is positioned in the upper half of the image, and a fountain pen is in the lower right. The background is a white surface with a dark grey diagonal line.

# Come Mitigare i DDoS ?

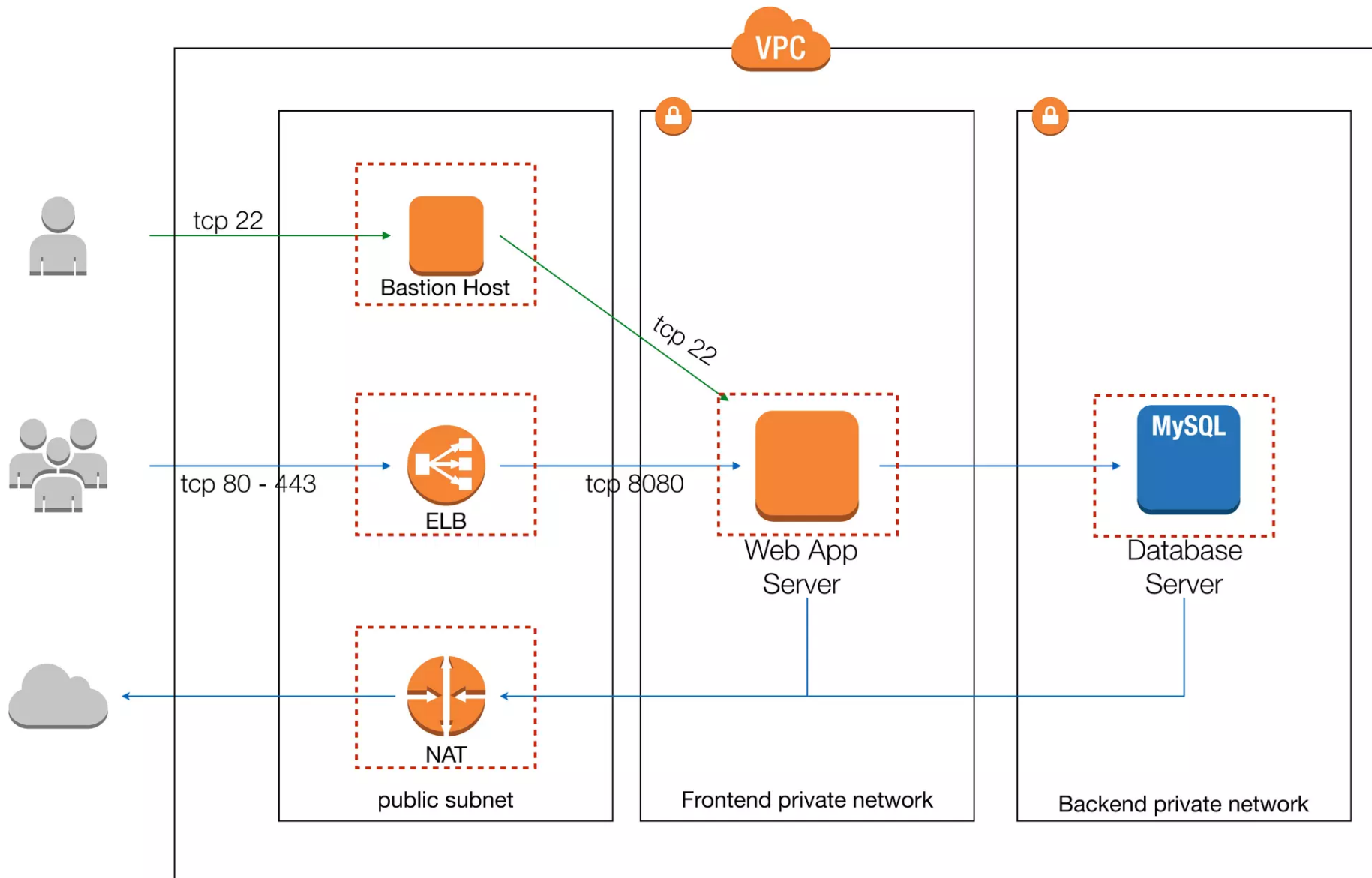
Creare architetture resiliente

Minimizzare aree di attacco

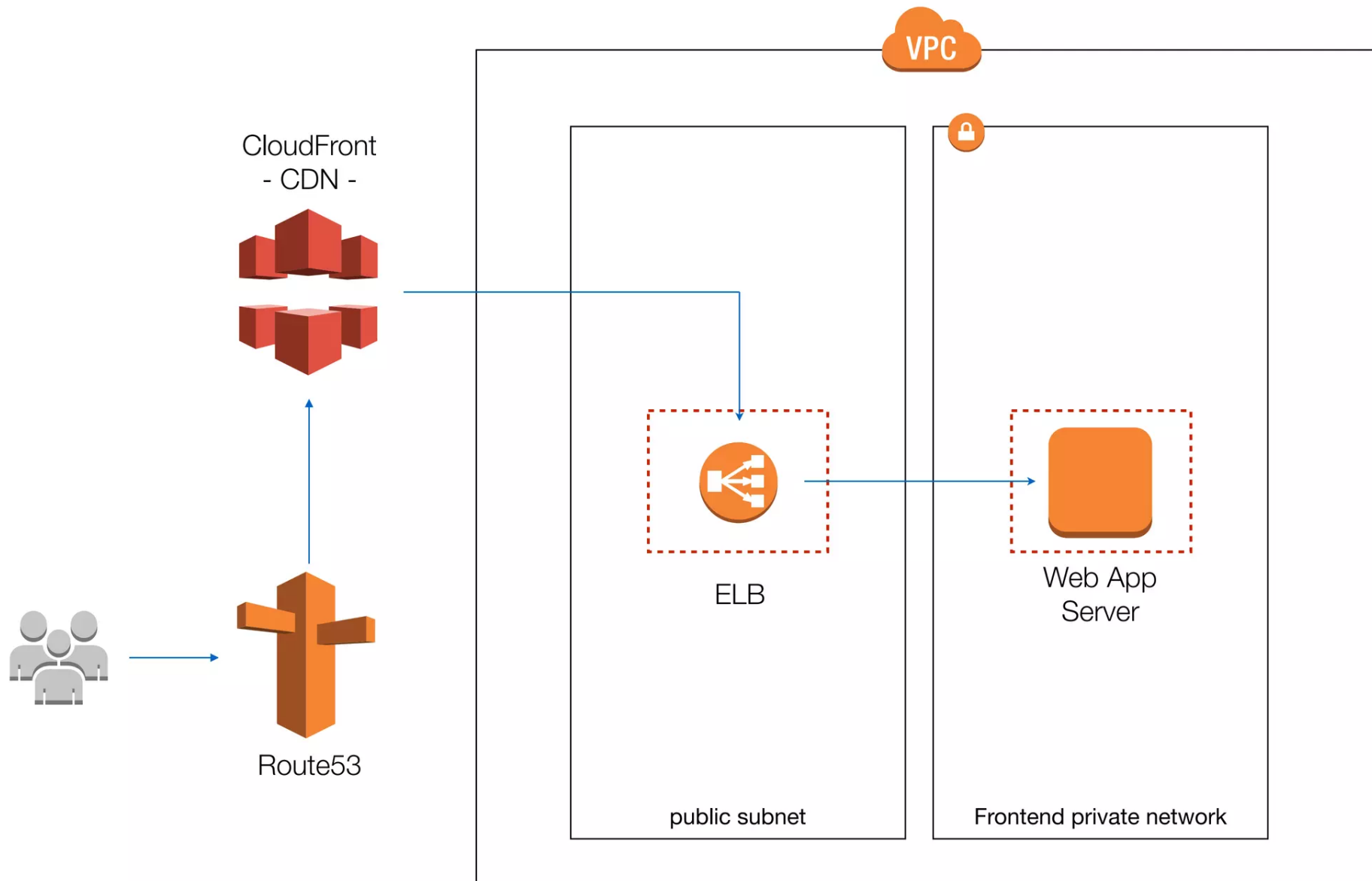
Rendere architettura scalabile

Identificare il normale comportamento

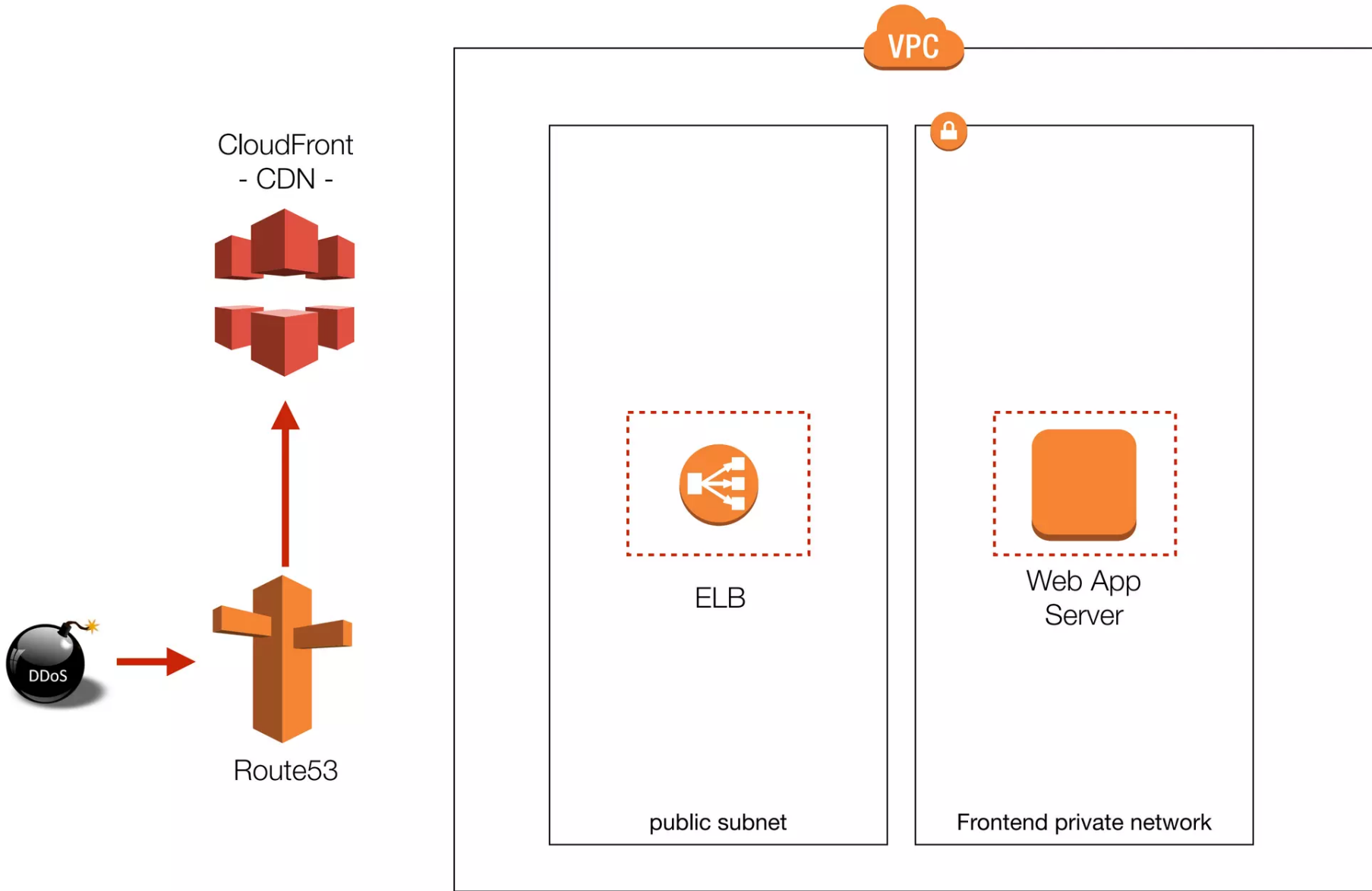
# Minimizzare area di attacco



# Minimizzare area di attacco



# Minimizzare area di attacco



# Conoscere il proprio traffico ...



identificare comportamenti anomali

Anticipare l'uso di picchi di risorse

Permette di limitare sul nascere le anomalie

Definire delle soglie per la segnalazione di allarmi



**Pronti a Scalare ...**

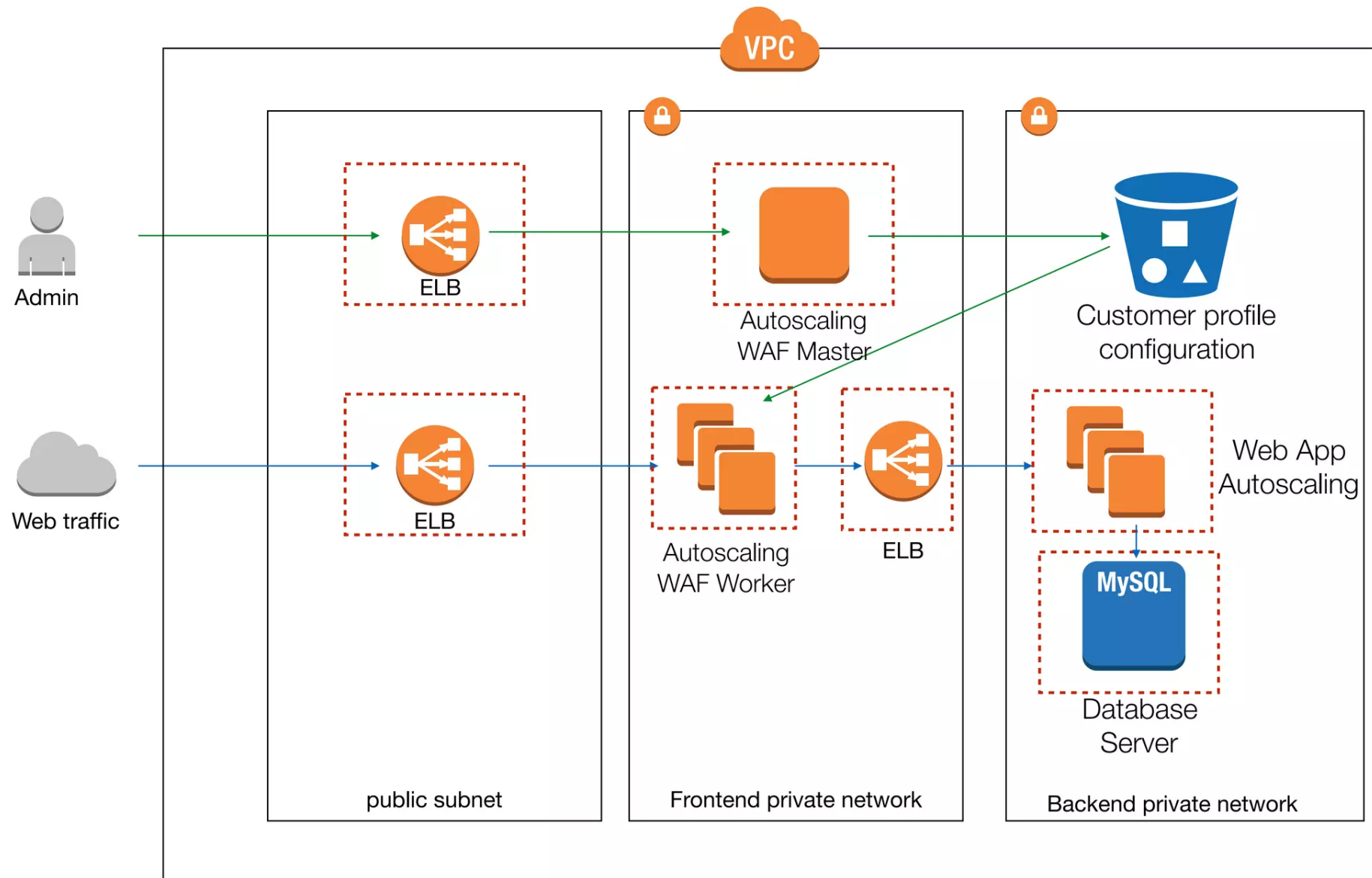
The background features a 3D maze-like structure composed of white rectangular blocks with dark grey top surfaces. Several black silhouettes of people are shown in various climbing poses: some are standing on platforms with arms raised in triumph, while others are actively climbing ladders. The ladders are white and extend vertically from the platforms. The overall scene is set against a light teal background, suggesting a complex and challenging environment.

**Rendere difficile la vita agli “attaccanti”**

**Avere il tempo di pensare ed reagire all’attacco**

**Aumentare + / - risorse in base alle condizioni**

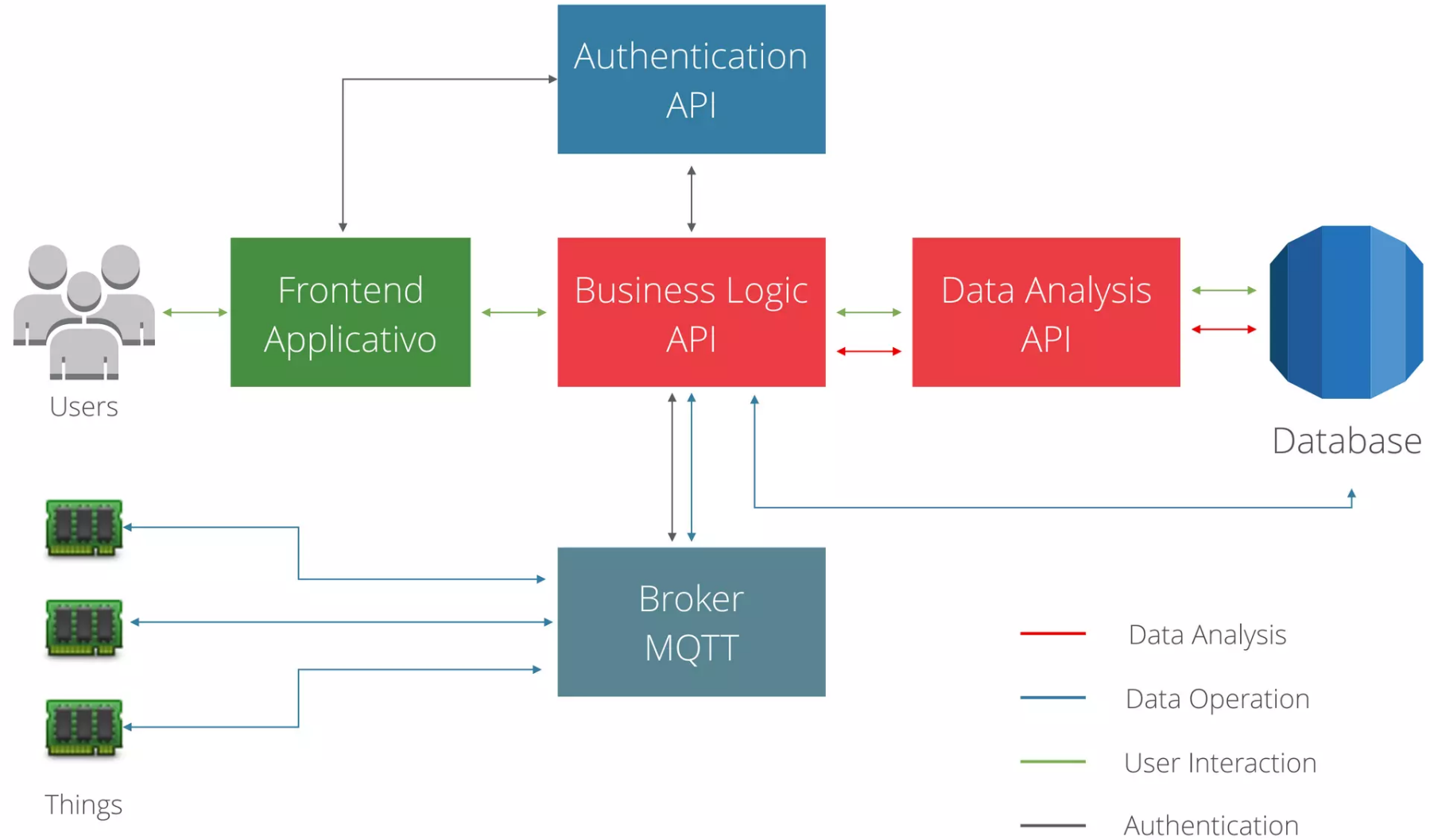
# Web Application Firewall





# Sicurezza in ambito IoT

# Ipotesi architettura IoT



# La sicurezza in ambito IoT

## Things

- Sistemi di autenticazione basati su token
- Crittografia lato oggetto
- Comunicazione tramite canali sicuri
- Gestione delle politiche di accesso alle risorse e funzioni dei servizi IoT
- Identificativo universale del device

## Cloud

- Shared responsabilità
- Architettura a livelli
- Identity Access Management
- Lock-in
- Cyber Attack
- Aspetti classici di sicurezza



# Domande?

[www.vincenzocalabro.it](http://www.vincenzocalabro.it)