BUSINESS

# I QUADERNI DI **FASTWEB**

# #10

## LA SICUREZZA DEGLI AMBIENTI MULTICLOUD

### COME CONTROLLARE IL RISCHIO INFORMATICO IN AMBIENTI MULTICLOUD

2019

FASTWEB

# 1 INTRODUZIONE

L'utilizzo di soluzioni e servizi erogati tramite infrastrutture Cloud continua a crescere nelle Imprese italiane. Questa tendenza, già rilevata negli scorsi anni, conferma un'adozione crescente e sempre più consapevole. Secondo i dati dell'Osservatorio Cloud Transformation 2018 del Politecnico di Milano (1) infatti, il mercato Cloud in Italia ha raggiunto quasi i 2,4 Miliardi di euro, in crescita del 19% rispetto all'anno precedente.

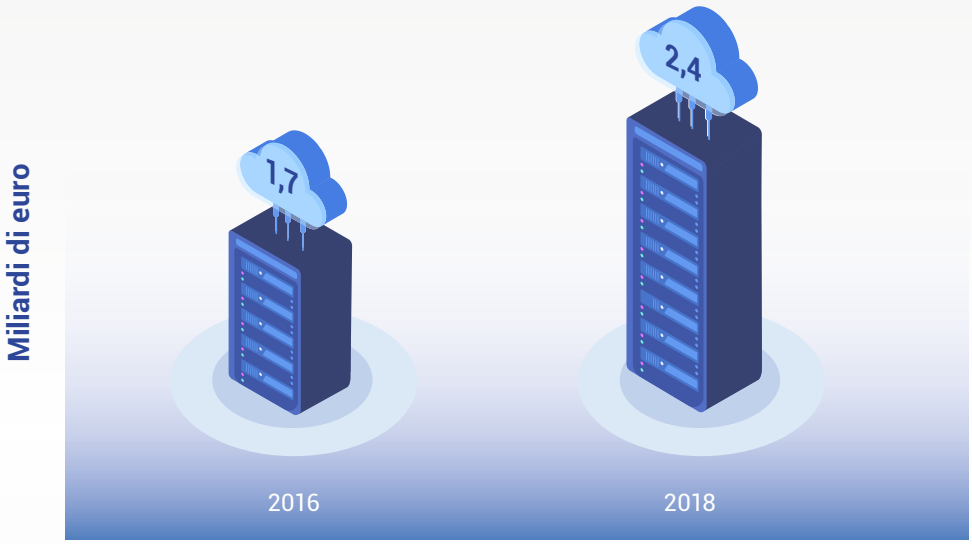
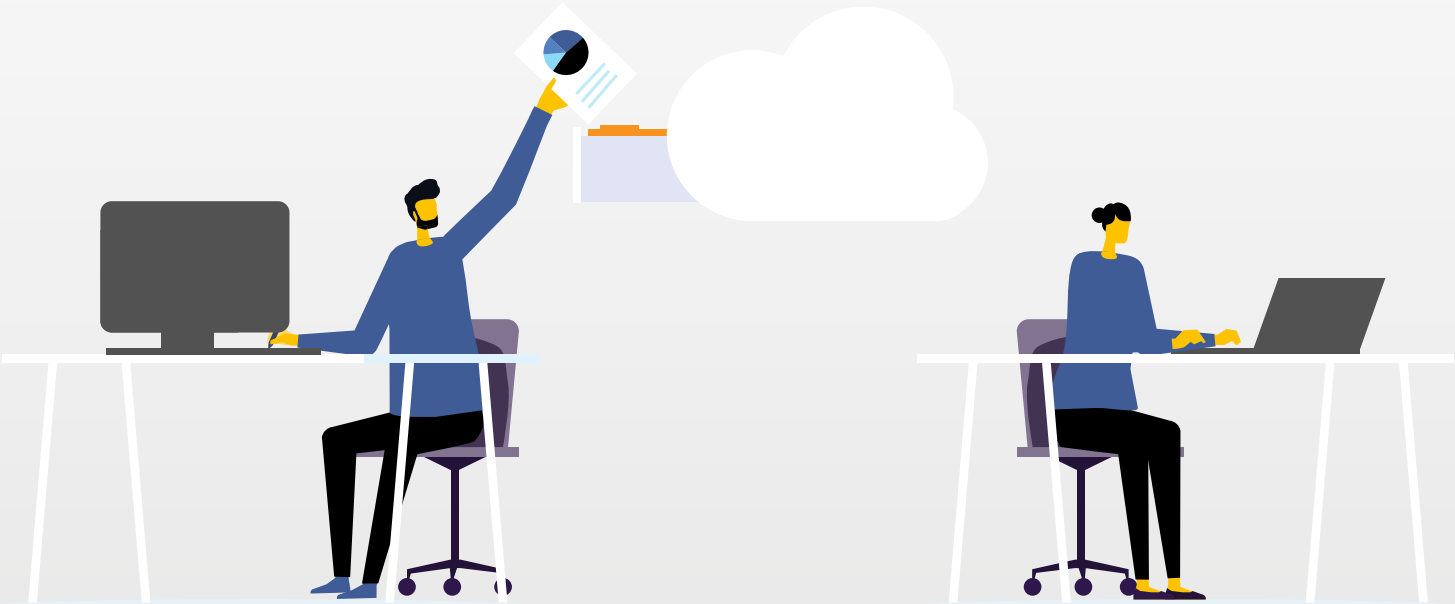
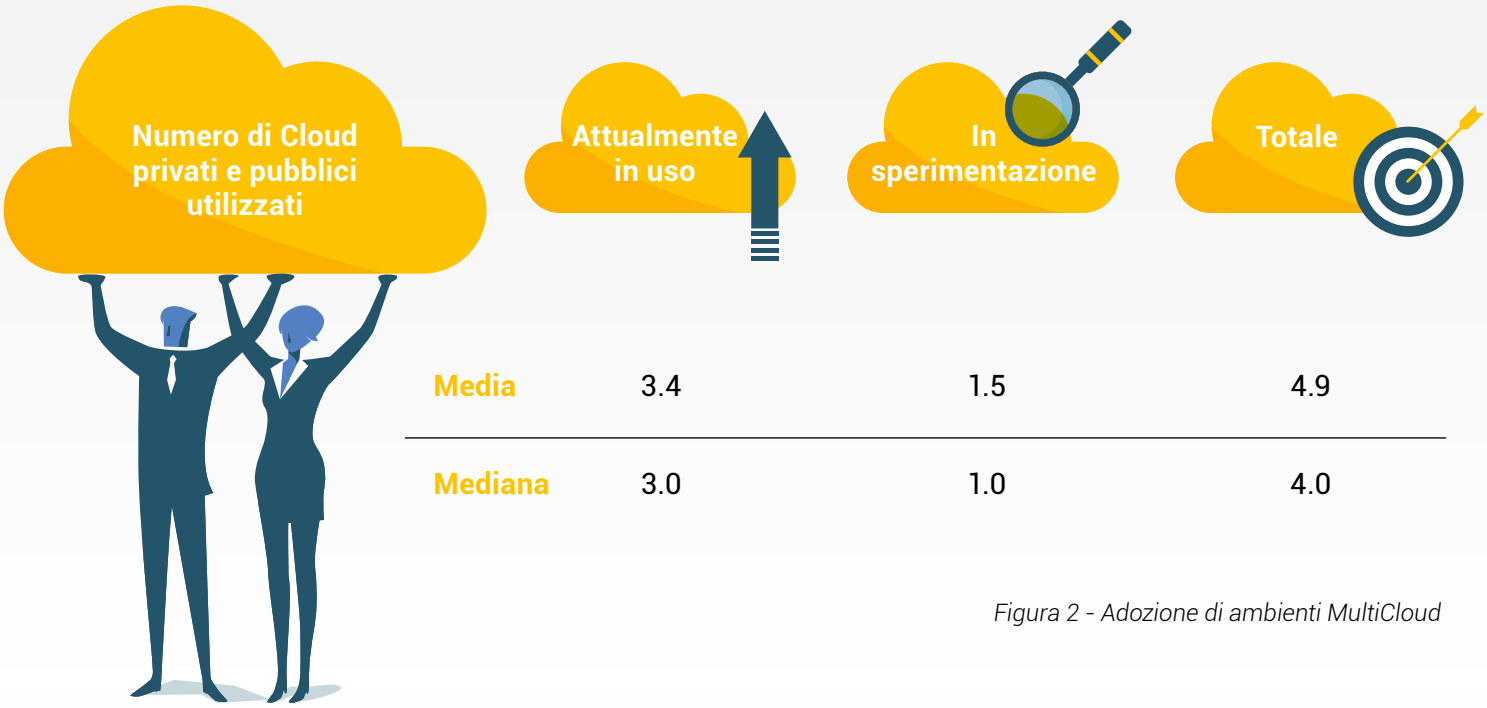



*Figura 1 - Il mercato del Cloud Computing in Italia*

Lo studio rileva che l'**82% delle Imprese medio grandi utilizza almeno un servizio in Public Cloud**, ritenendo tale strategia quella preferenziale per la realizzazione di nuovi sevizi. Il fenomeno non riguarda solo le Aziende medio-grandi, ma impatta anche le PMI italiane; il 74% delle stesse, infatti, riconosce il Cloud come tecnologia abilitante per introdurre innovazione e realizzare più efficacemente i processi di Digital Transformation in Azienda.



In particolare sono molti i vantaggi derivanti dall'uso di infrastrutture Cloud pubbliche e private (MultiCloud) in termini di flessibilità e velocità di implementazione tanto che, a livello globale, le Aziende utilizzano mediamente 4 Cloud differenti (Figura 2).




| | Attualmente in uso | In sperimentazione | Totale |
|---|---|---|---|
| **Media** | 3.4 | 1.5 | 4.9 |
| **Mediana** | 3.0 | 1.0 | 4.0 |

*Figura 2 - Adozione di ambienti MultiCloud*

Accanto ai notevoli vantaggi derivanti dall'utilizzo di servizi erogati in ambienti MultiCloud in termini di flessibilità e rapidità di implementazione, vi sono, tuttavia, anche rischi connessi a tale strategia, per esempio dovuti alla frammentazione dei dati trattati dalle Imprese in differenti ambienti Cloud e nel conseguente ampliamento del perimetro attaccabile da criminali informatici o da concorrenti sleali. Infatti, se prima il ciclo di vita del dato, dalla sua creazione alla sua distruzione, poteva essere confinato all'interno dell'infrastruttura informatica privata della singola Azienda (Figura 3), ora, con il paradigma MultiCloud, tale ciclo di vita deve essere gestito e controllato in ogni ambiente Cloud utilizzato:
**la sicurezza del dato deve cioè essere garantita oltre i confini dell'Azienda.**

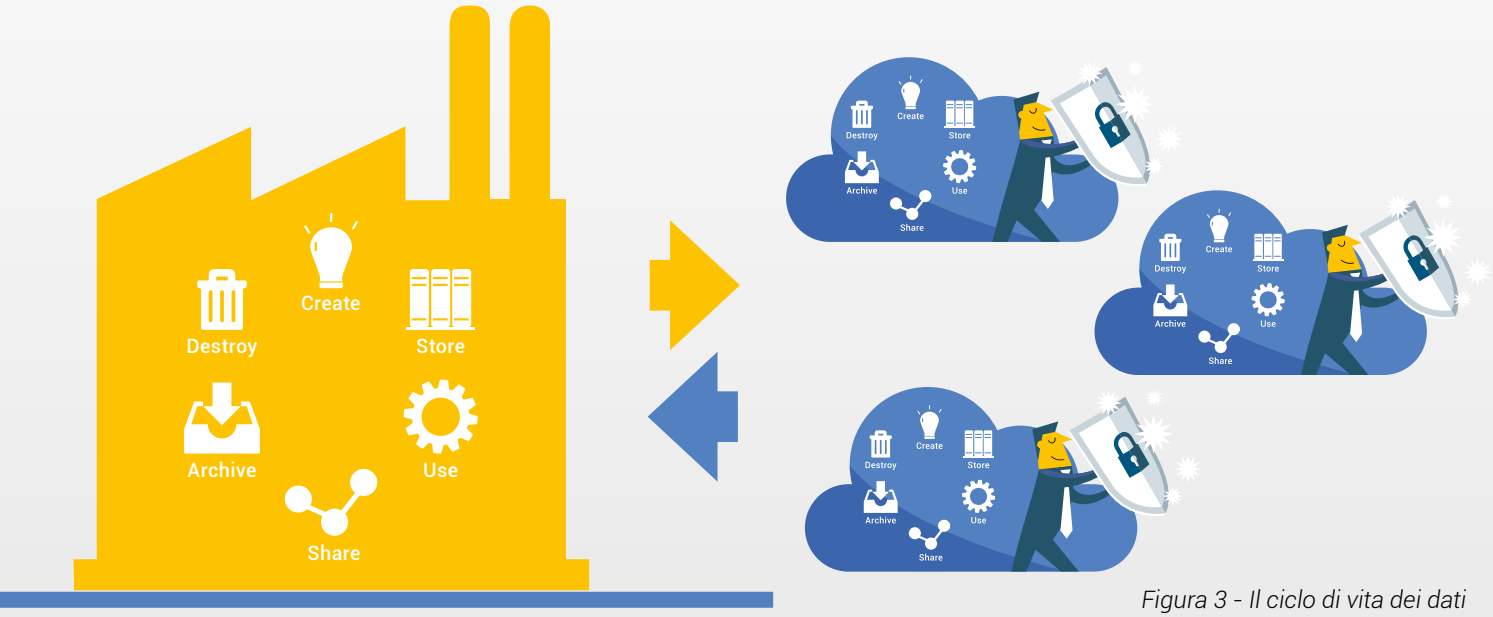
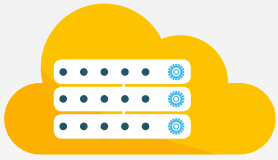



*Figura 3 - Il ciclo di vita dei dati*

# 2 MULTICLOUD

Il mercato Cloud pubblico è dominato da cinque attori primari che operano a livello globale negli ambiti Infrastructure e Platform as a Service (IaaS e PaaS) (Amazon, Google e Microsoft sono i tre player maggiori seguiti da IBM e Oracle) e da molti operatori "locali" nei singoli paesi che hanno un approccio di mercato orientato alla "Customer proximity" e alla fornitura di soluzioni "su misura".
In questo scenario molte Aziende gestiscono le proprie applicazioni IT in più di un Cloud provider perché convinte che l'infrastruttura IT sia più robusta se per ogni specifica applicazione viene scelto il miglior provider Cloud. Anche quando si tratta di sicurezza informatica può essere applicato lo stesso approccio: per mettere in sicurezza gli ambienti di ogni specifico Cloud provider è necessario mettere in campo infrastrutture, servizi e adeguate capacità di gestione specifiche per ogni contesto.

**Si distinguono, in linea di massima, due casistiche principali:**



Utilizzo di **infrastrutture IT erogate in Cloud** (server, virtual private data center, database e/o ambienti di sviluppo) e **layer applicativo "privato"**, ovvero gestito interamente dalle aziende.


**Fruizione diretta delle applicazioni fornite come SaaS (Software as a Service)** dai Cloud provider che ne curano l'erogazione e la manutenzione (tipicamente via browser); l'Azienda cliente non deve cioè preoccuparsi delle infrastrutture IT e della relativa manutenzione.

Nel primo caso tipicamente **gli IaaS e i PaaS Provider applicano un modello di sicurezza basato sul concetto di "responsabilità condivisa" (Shared Responsability Model)**: il Cloud provider mette in sicurezza il servizio venduto (infrastruttura o piattaforma), mentre il Cliente si assume la responsabilità di mettere in sicurezza ciò che decide di installare ed operare sullo stesso (ad es. sistemi operativi, applicazioni..).

Nel secondo caso, a differenza degli IaaS e dei PaaS, il modello di responsabilità, non può essere condiviso: **il provider del SaaS è responsabile dell'infrastruttura su cui l'applicazione è eseguita e dell'applicazione stessa** (il provider è per esempio responsabile di applicare le patch di sicurezza ai sistemi operativi o alle librerie utilizzate dall'applicazione).

Vi sono molte soluzioni di cybersecurity applicabili nei contesti operativi "MultiCloud".
Esse possono spaziare dai Next Generation Firewall, Web Application Firewall, alle tecnologie di Sandboxing e tool di gestione della sicurezza e correlazione degli eventi (SIEM) e si possono applicare indifferentemente a Cloud "pubblici" o "privati".

Dal momento che le esigenze di sicurezza delle applicazioni e dei dati sono comuni e sostanzialmente indipendenti dall'infrastruttura in uso, è importante, nel caso di ambienti "MultiCloud" poter **disporre di tecnologie e competenze omogenee** che possano offrire cioè una capacità di gestione centralizzata della sicurezza, una visione globale e unitaria delle minacce e degli attacchi in corso ad esempio da un unico pannello di amministrazione e monitoraggio che sia agnostico rispetto alla tecnologia in uso.

Relativamente poi al tema della gestione dei dati bisogna tenere in considerazione il fatto che, solitamente, le Aziende utilizzano più di un'applicazione SaaS: ciò ha un impatto significativo sull'operatività delle Aziende stesse poichè devono essere in grado di capire dove risiedano i propri dati, comprendere come essi vengano utilizzati dagli utenti titolati ad accedere e, eventualmente, essere in grado di individuare tentativi di accesso illeciti.

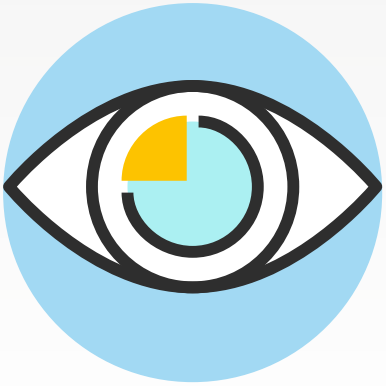
Un notevole supporto in questi casi può essere rappresentato anche dalle **tecnologie CASB** (Cloud Access Security Broker) che sono in grado di fornire visibilità, aderenza alle compliance di settore, sicurezza del dato e protezione dalle minacce per ogni applicazione SaaS in uso dall'Azienda.

# 3 STRATEGIE DI PROTEZIONE IN AMBITO MULTICLOUD

Per poter affrontare in modo efficace, efficiente e a costi sostenibili il tema della sicurezza informatica in un contesto così complesso ed articolato, occorre dare priorità ai seguenti aspetti:

## VISIBILITÀ

La visibilità di quanto avviene sui dati (in Cloud o presso le sedi remote) è fondamentale per identificare e prevenire le minacce informatiche che le Aziende si trovano a fronteggiare. Con il contemporaneo utilizzo di applicazioni in Cloud e "on premise" le sfide che si pongono diventano più complesse da gestire poiché **il coordinamento e la consistenza delle informazioni** divengono un bisogno primario per mantenere in sicurezza i dati Aziendali.



Tali obiettivi si raggiungono attraverso l'uso di consolle centralizzate, capaci di raccogliere informazioni provenienti dai diversi elementi di sicurezza o dai SaaS provider e mostrarle in modo integrato ai team che si occupano della sicurezza nelle Aziende.

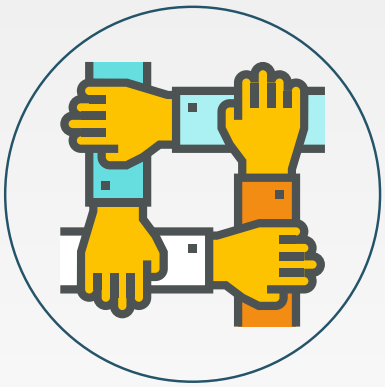
## CONTROLLO END TO END

La gestione centralizzata degli elementi di sicurezza consente di avere visibilità, ma non consente di affrontare le minacce informatiche tempestivamente e possibilmente "in tempo reale".
Le varie funzioni di sicurezza gestite (es. Cloud Firewall, Web Application Firewall, Email Gateway, Sandbox e SIEM), devono poter comunicare l'una con l'altra al fine di identificare velocemente una minaccia e rispondere efficacemente (ovvero in "real time") alla stessa.

Le componenti di sicurezza devono perciò operare armonicamente in modo coordinato: le informazioni raccolte da un componente devono essere messe a fattor comune (notificate) agli altri. In tal modo è possibile ridurre la finestra di rischio che intercorre da quando una minaccia è identificata a quando la stessa viene attivamente bloccata prima che vi sia una compromissione dei sistemi aziendali.
Ci riferiamo, ad esempio, a Mail Gateway o a Web Application Firewall che siano in grado di inviare oggetti da analizzare ad una Sandbox integrata nel Cloud e siano capaci di condividere i risultati dell'analisi degli oggetti sospetti tra loro, consentendo di abbassare significativamente l'esposizione alla minaccia specifica, a prescindere dal vettore di attacco utilizzato dai cyber criminali.

**Solo un approccio integrato ed in real time delle componenti di sicurezza consente una protezione dell'intera superfice di attacco dell'Azienda,** dal Cloud IaaS al Datacenter privato fino alle singole applicazioni SaaS utilizzate.

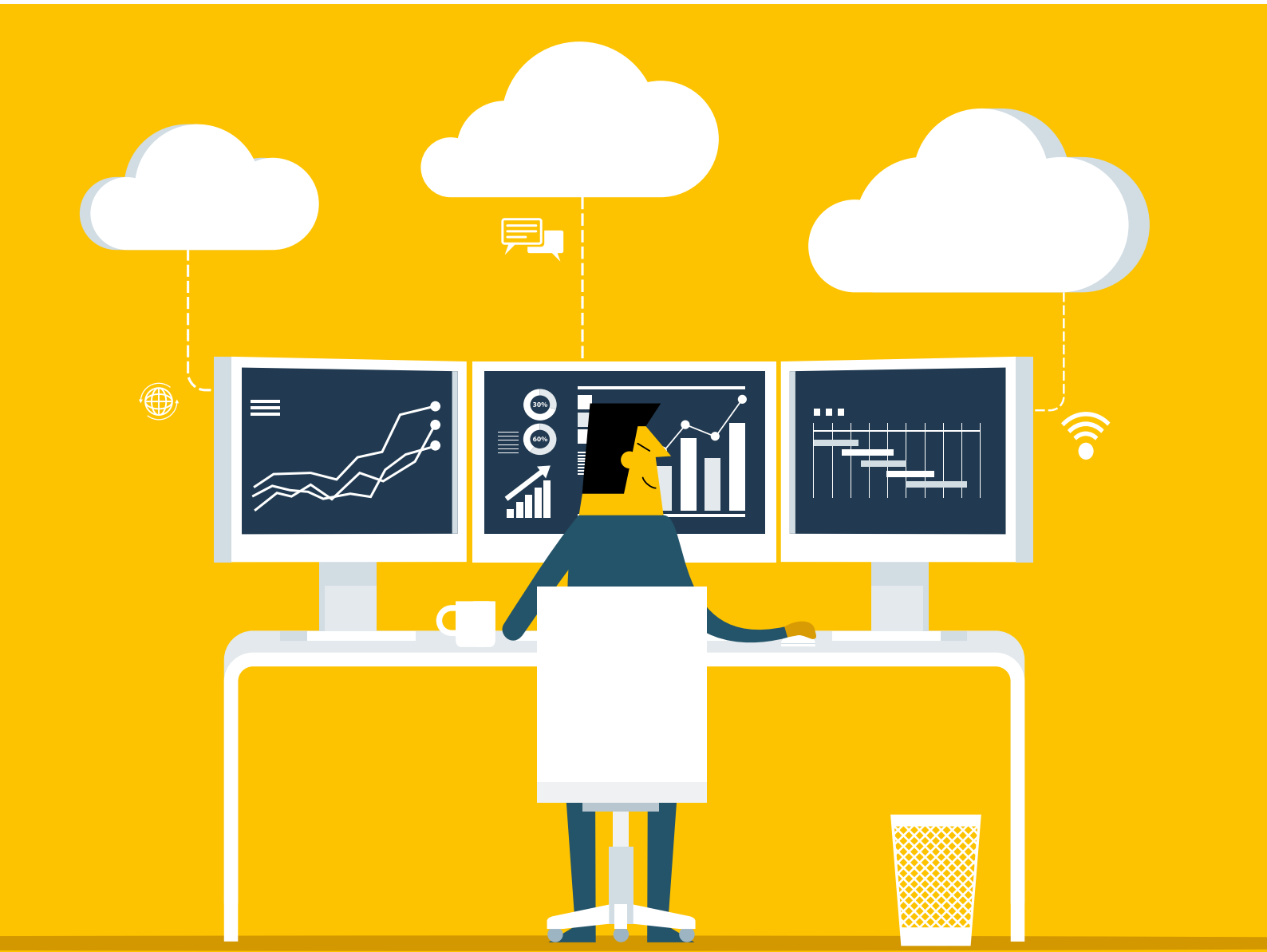
## TEAM DI ESPERTI E COMPETENZE



Per operare efficacemente in un contesto caratterizzato da minacce in così rapida evoluzione diventa fondamentale, oltre all'accesso alle soluzioni tecnologiche più all'avanguardia, poter **contare su un team qualificato e costantemente aggiornato**.

La tempestività nell'indentificazione delle minacce, il dominio delle tecnologie in campo  e la capacità di reazione con adeguate contromisure sono fattori cruciali per evitare che un attacco informatico conduca ad una vera e propria crisi in grado di compromettere l'operatività aziendale con tutte le conseguenze che ne derivano: perdita di fatturato e reputazione o le conseguenze legali derivanti dalle normative  sempre più stringenti, come il GDPR.

In questo contesto **l'utilizzo di servizi erogati da un Managed Security Service Provider (MSSP) può rappresentare un'opzione molto valida:** l'MSSP infatti semplifica enormemente la gestione di tutti gli elementi di sicurezza presenti e applicabili nei vari Cloud mascherandone la complessità all'utente attraverso piattaforme e servizi in grado di integrare e correlare le varie informazioni; l'MSSP è inoltre in grado di intervenire tempestivamente facendo leva su personale altamente specializzato presente nei propri Security Operation Center (SOC).



# 4 RIFERIMENTI


1. Osservatorio Cloud Transformation 2018 – Politecnico di Milano - https://www.zerounoweb.it/cloud-computing/osservatorio-cloud-transformation-2018-politecnico-di-milano-tutti-i-dati-in-anteprima/

2. Business @ Work – Okta (https://www.okta.com/businesses-at-work/2019/)

3. 2019 State of the Cloud Report (https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019)

# FASTWEB

Con 2,6 milioni di clienti su rete fissa e 1,6 milioni su rete mobile, Fastweb è uno dei principali operatori di telecomunicazioni in Italia. L'azienda offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese. Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga. Fastweb ha sviluppato una infrastruttura di rete nazionale in fibra ottica di 50.500 chilometri, con oltre 4 milioni di chilometri di fibra. Grazie all'espansione e al continuo potenziamento della rete ultra broadband, Fastweb raggiunge oggi 22 milioni di abitazioni, di cui 8 con rete proprietaria, con velocità di collegamento fino a 1 Gigabit. La società offre inoltre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G e 4G Plus. Entro il 2020 il servizio mobile verrà potenziato, a partire dalle grandi città, grazie alla realizzazione di una infrastruttura di nuova generazione 5G con tecnologia small cells. Fastweb fornisce servizi di telecomunicazioni ad aziende di tutte le dimensioni, dalle start-up alle piccole e medie imprese, dalle società di grandi dimensioni fino al settore pubblico, alle quali offre connettività e servizi ICT avanzati, come l'housing, il cloud computing, la sicurezza e la comunicazione unificata. La società fa parte del gruppo Swisscom dal settembre 2007.

## Self-Service Cloud Portal


**DISPONIBILITÀ ANNUA**
99,997%

**RISPOSTA AI GUASTI**
automatica senza interruzioni

**100 ORE**
autonomia energetica

**GREEN**
PUE 1,25

**POTENTE**
40 kW/rack

Relativamente ai servizi Data Center e Cloud, Fastweb ha costruito un'infrastruttura dedicata ai clienti Enterprise, basata su un **Data Center di ultima generazione certificato Tier IV da Uptime Institute**. Realizzato secondo gli standard più esigenti in termini di sicurezza e affidabilità esso è in grado di ospitare anche applicazioni e servizi "mission critical" tra i quali vi sono quelli erogati dall'infrastruttura Cloud di Fastweb dedicata alle imprese. Tale infrastruttura è infatti concepita per garantire continuità e performance alle applicazioni di business. In particolare la piattaforma Cloud IaaS (Infrastructure as a service) di Fastweb garantisce la totale segregazione logica e applicativa degli ambienti dedicati ai singoli Clienti in modo da ottenerne il completo isolamento. Grazie ai motori di Orchestration e Automation sviluppati internamente su piattaforma "aperta" Openstack, i sistemi Cloud di Fastweb sono in grado di allocare risorse in maniera scalabile e in tempo reale in funzione del carico e dell'uso applicativo del singolo cliente secondo il modello Software Defined Data Center (le componenti di computing, network, storage e security sono virtualizzate e orchestrate da un'unica piattaforma). Tutta l'infrastruttura Cloud è gestita da team specializzati in centri di competenza e nuclei operativi di gestione dedicati rispettivamente a Data Center, infrastruttura IT e Security, in grado di supportare i Clienti dalla fase di progetto a quella di attivazione ed esercizio.

Per quanto riguarda in particolare i servizi dedicati alla sicurezza, Fastweb rende disponibili alle aziende una serie di servizi e soluzioni di IT Security attraverso il modello di **Managed Security Service Provider**. Tale modello prevede infatti che ciascuna azienda mantenga la totale autonomia nella definizione della Governance dell'IT Security in termini di livelli di rischio e conseguenti priorità di protezione di sistemi e informazioni e demandi invece la gestione operativa dell'IT Security ad un operatore esterno dotato di processi, competenze specifiche e piattaforme tecnologiche adeguate.

Fastweb, oltre a mettere a disposizione un centro di competenza dedicato alla progettazione di soluzioni di IT Security, si è dotata anche di un **Security Operation Center** (SOC Enterprise) dedicato esclusivamente alla gestione dei servizi di sicurezza per le Aziende. Il SOC Enterprise di Fastweb opera in Italia con personale italiano erogando un servizio con copertura H24 7gg/settimana; è dotato di processi conformi alle normative con le certificazioni "ISO 9001 – Quality Management" e "ISO 27001 – Information Security Management", gestisce piattaforme di sicurezza multi-tecnologia sia presso le sedi dei Clienti che centralizzate nell'infrastruttura Cloud di Fastweb, anch'essa con le medesime certificazioni oltre alla conformità alla norma "ISO 27018 – Privacy on Public Cloud". Con il proprio SOC Enterprise Fastweb gestisce direttamente migliaia di apparati e piattaforme di sicurezza operative presso le Aziende Cliente.

**Gestito da personale Fastweb**

**Security Operations Center**

**ISO 27001**

Medie Grandi Aziende Fastweb
fastweb.it