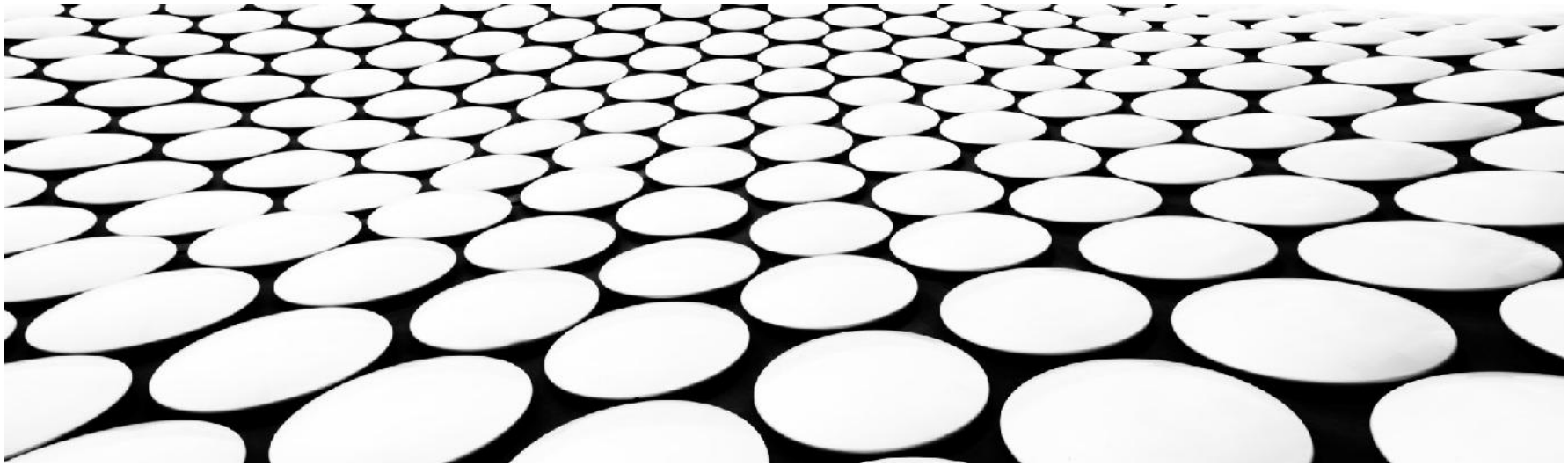
REQUISITI NON-FUNZIONALI DEI SERVIZI CLOUD

VINCENZO CALABRÒ



AGENDA

- Introduzione
- Sicurezza e performance
- Data location e privacy
- Tecniche di protezione dei dati
- Monitoraggio in Cloud

Introduzione

- Migrazione verso la cloud causa perdita di controllo e governance su dati e applicazioni
- Asset di aziende, utenti vengono gestite da terze parti nella cloud (spesso cloud provider)
- Spesso il livello di fiducia (trust) è basato sulla reputation della terza parte
  - Non sempre un buon approccio, ad esempio Yahoo

Introduzione

- Gli utenti della cloud non solo richiedono specifiche funzionalità, ma anche il soddisfacimento di requisiti non funzionali
  - Garanzia sul comportamento della cloud e dei suoi servizi diventa un requisito sempre più critico al successo della cloud

- Necessità di fornire
  - Approcci per la specifica dei requisiti
  - Approcci per la valutazione dei requisiti
  - Evidenza di corretto funzionamento dei meccanismi che soddisfano i requisiti

Problemi del Cloud Computing (recap)

- Problemi di sicurezza causati da
  - Perdita di controllo
  - Mancanza di (meccanismi di) trust
  - Multi-tenancy

- Questi problemi esistono principalmente nei modelli di gestione delle terze parti
  - Self-managed cloud hanno problemi di sicurezza differenti da quelli di cloud pubbliche

Perdita di controllo nella Cloud

- Perdita di controllo dei consumer
  - Dato, applicazioni, risorse sono localizzate presso il provider
  - User identity management è gestito dalla cloud
  - Regole di controllo dell'accesso utente, politiche di sicurezza e loro valutazione sono gestite dal cloud provider
  - Consumer si appoggiano ai provider per assicurare
    - Data security e privacy
    - Resource availability
    - Monitoraggio e adattamento di servizi/risorse

Mancanza di trust nella Cloud

- Fidarsi di una terza parte richiede di prendersi un rischio
- Trust e rischio
  - Diverse facce di una stessa medaglia (J. Camp)
  - People only trust when it pays (Economist's view)
  - Il bisogno di trust emerge solo in situazioni rischiose
- Schemi per la gestione delle terze parti
  - Difficile bilanciare trust e rischio
  - Key Escrow (Clipper chip)
  - La cloud sta prendendo la stessa direzione?

Multi-tenancy nella Cloud

- Conflitti tra tenant con obiettivi opposti
  - Tenant condividono un pool di risorse e hanno obiettivi opposti
- Come la multi-tenancy gestisce i conflitti di interesse?
  - Possono i tenant andare insieme e comportarsi bene?
  - Se no, come possiamo isolarli?
- Come fornire separazione tra tenant?

Problematiche di sicurezza nella Cloud

- Obiettivo, minimizzare le seguenti problematiche
  - Perdita di controllo
    - Riprendersi il controllo
      - Dati e app potrebbero dover rimanere nella cloud…
      - … ma possono essere gestite in qualche modo dai consumer?
  - Mancanza di trust
    - Migliorare il trust (e i suoi meccanismi)
      - Tecnologia
      - Policy, regulation
      - Contratti (incentivi)
      - Compliance e certification
  - Multi-tenancy
    - Private cloud
      - Non utilizzare la cloud in prima battutta
    - Virtual Private Cloud (VPC): non è comunque un sistema separato
    - Separazione forte

Minimizzare la Perdita di controllo nella Cloud

- Monitoraggio
  - Richiede monitoraggio a runtime specifico per l'applicazione e dei tool di gestione per i consumer
- Utilizzare diverse cloud
  - Abbiamo già visto il concetto di 'Don't put all your eggs in one basket'
- Access control management
  - Diversi livelli di controllo dell'accesso
  - Indipendentemente dal modello di deployment, il provider ha bisogno di gestire l'autenticazione utente e le procedure di controlle dell'accesso (alla cloud)

Minimizzare Multi-tenancy nella Cloud

- Non possiamo forzare il provider ad accettare meno tenant
  - Provare a migliorare l'isolamento tra tenant
    - Tecniche di strong isolation (VPC)
      - VM Side channel attacks (T. Ristenpart et al.)
    - Requisiti di QoS devono essere rispettati
    - Specifica di politiche
  - Accrescere il trust tra tenant
    - Chi può essere definite come insider, dov'è il security boundary? Di chi ci si può fidare?
    - Usare SLA per imporre un comportamento fidato

Proprietà non funzionali: sicurezza e performance

Proprietà non funzionali

- Due macro categorie principali
  - Sicurezza
  - Performance
- Diversi meccanismi di valutazione
  - SLAs, audit, certification, compliance, …

Gestione di proprietà non funzionali

- **Trasparenza**. Tecniche che garantiscono accesso a dati di basso livello (back-end) prodotti dall'infrastruttura cloud e a evidenza collezionata sulla base delle proprietà non-funzionali supportati dale applicazioni cloud.

- **Introspection**. Capacità di un cloud provider di esaminare e osservare l suoi processi interni

- **Outrospection**. Capacità degli utenti e service provider della cloud di esaminare e osservare l processi interni della cloud che hanno impatto sulle loro attività, applicazioni e dati

Sicurezza

- Prima di Internet
  - Mondo chiuso
  - Tutti conosciuti a priori
  - Autenticazione, autorizzazione, controllo dell'accesso
- Internet
  - Mondo aperto
  - Utenti sconosciuti
  - Crescita esponenziale degli attacchi
- Cloud
  - Mondo condiviso
  - Multi-tenant
  - Necessità di garantire isolamento

Sicurezza

- Il termine sicurezza ha diversi significati e diversi obiettivi
  - Sicurezza fisica
  - Sicurezza di rete
  - Sicurezza del software
  - Sicurezza dei servizi
  - Sicurezza dei dati

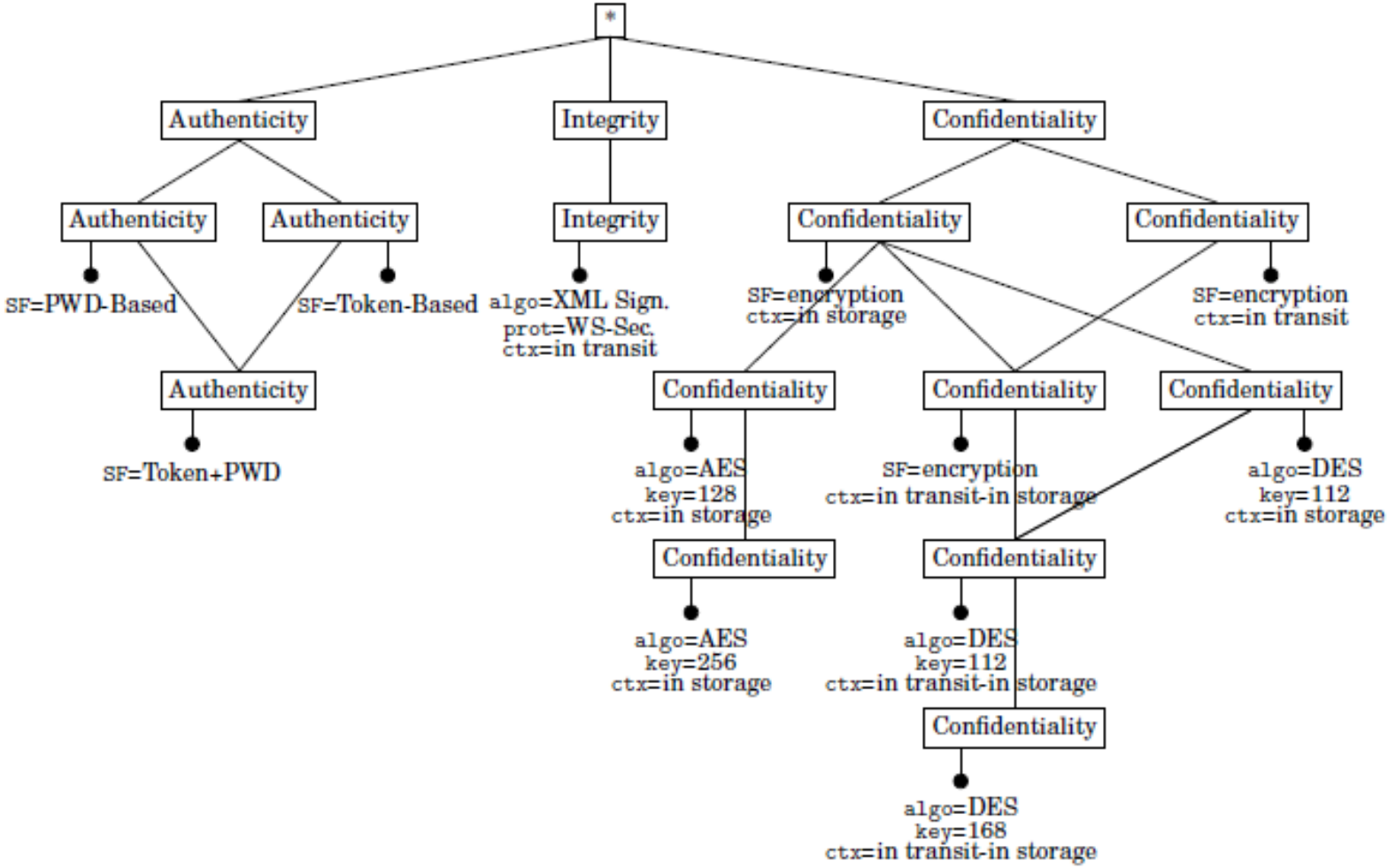
Proprietà di sicurezza

- Garantire sicurezza significa proteggere i dati e le risorse garantendo
  - **Segretezza** (Confidentiality). L'informazione può essere rilasciata – direttamente o indirettamente – solo a utenti autorizzati a conoscerla
  - **Integrità** (Integrity). Le informazioni (e le risorse) non devono essere modificate, cancellate o distrutte in modo non autorizzato o improprio
  - **Disponibilità** (Availability). Non deve essere impedito agli utenti gli accessi propri e per i quali hanno l'autorizzazione necessaria

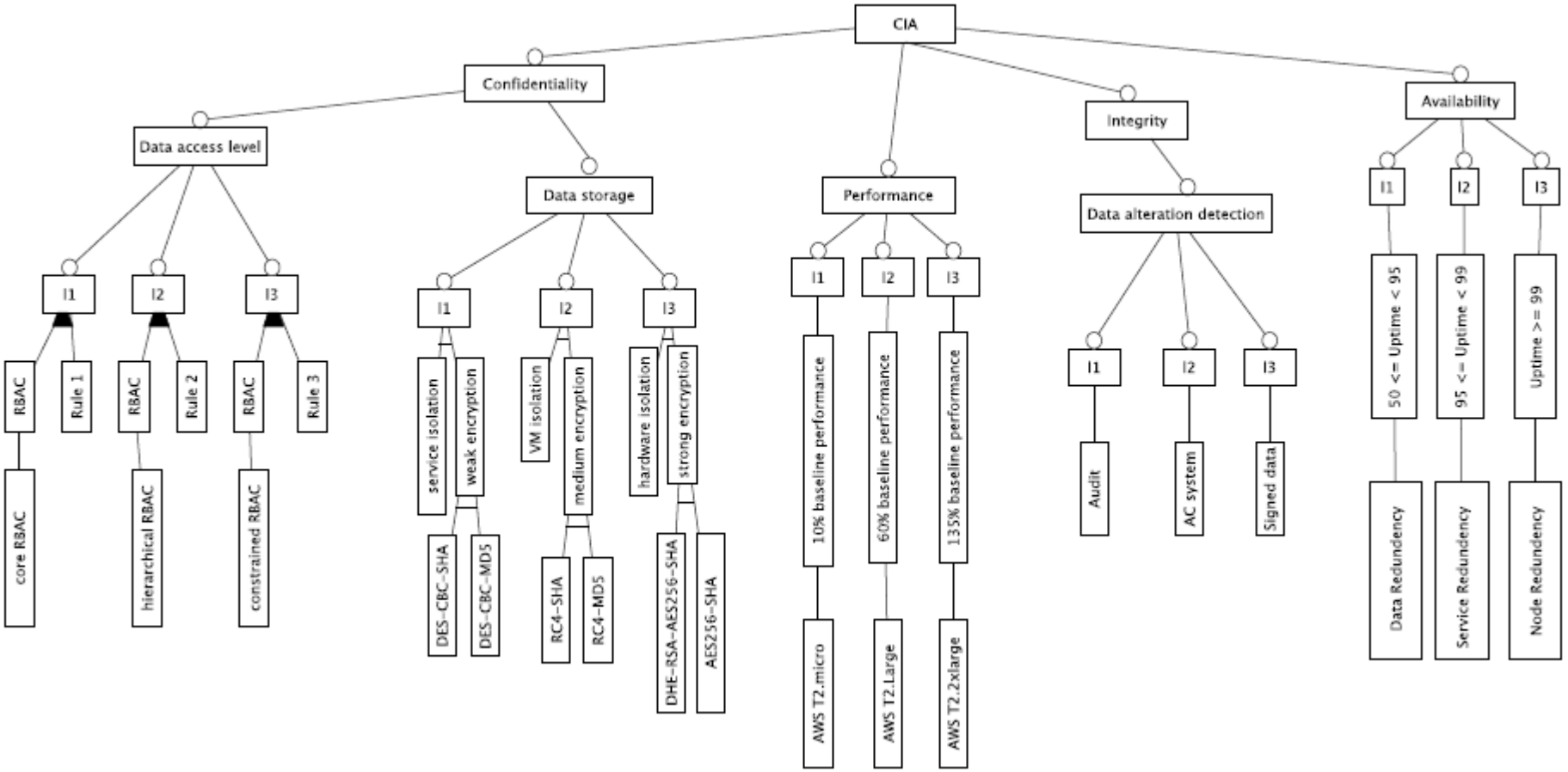
Proprietà di sicurezza

- Garantire sicurezza significa proteggere i dati e le risorse garantendo
  - **Autenticità** (Authenticity): Capacità di provare che un utente o un oggetto sono genuini
  - **Privacy**: Capacità di proteggere le informazioni riguadanti la sfera personale dell'utente
  - **Non-repudiation**: Capacità di verificare e identificare il responsabile di un'attività o un messaggio
  - **Affidabilità** (Reliability): Capacità del sistema di eseguire le sue funzioni anche in caso di fallimenti o errori

Proprietà di sicurezza - Gerarchia



Proprietà di sicurezza – Livelli di robustezza



Meccanismi di sicurezza

- Proprietà di sicurezza vengono garantite attraverso meccanismi di sicurezza
- Meccanismi di sicurezza vengono installati e configurati per supportare una data proprietà a un certo livello
- L'installazione di un meccanismo di sicurezza non garantisce che il sistema/servizio sia sicuro

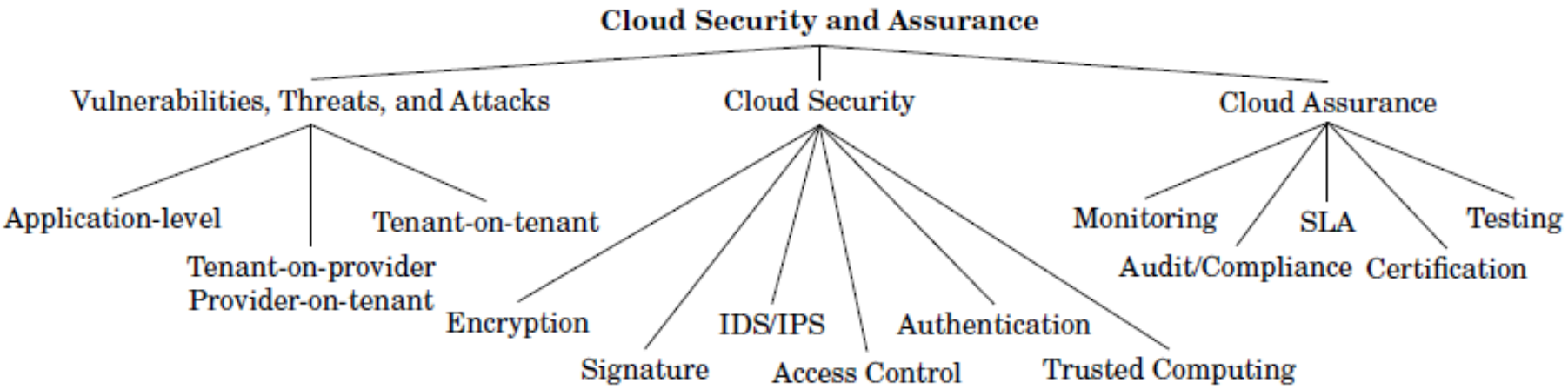
Meccanismi di assurance

- Necessità di verificare che il meccanismo di sicurezza si comporti bene e aderisca a standard (compliance)
  - Ad esempio, criptare i dati usando un meccanismo per cui è noto una debolezza equivale a non criptare i dati

- Security assurance definisce un modo per ottenere evidenza del corretto funzionamento di un sistema
  - Il sistema è in grado di dimostrare il supporto di una o più proprietà indipendetemente da fallimentti e/o attacchi

Meccanismi di assurance

- Cloud security basata su meccanismi che proteggono il sistema da vulnerabilità, minacce, attacchi
- Cloud assurance garantisce il buon comportamente del sistema e dei suoi meccanismi di sicurezza



Performance nella cloud vs on premise

- Performance on premise
  - Bassa capacità di adattarsi a eventi esterni
  - Costi maggiori (non sempre)
  - Maggior stabilità
  - Maggior controllo
- Performance nella cloud
  - Grande capacità di adattarsi a eventi esterni, tramite meccanismi di scalabilità
  - Costi minori (in media)
  - Dipende da utenti sconosciuti (multi tenancy)
  - È tutta nelle mani del cloud provider che fa rispettare le regole di scalabilità

Cloud performance

- L’infrastruttura cloud fornisce una soluzione elastica e scalabile
- Risorse fornite on demand e in tempo reale
- Proprietà di performance sono tra le più importanti in ambiente cloud

Cloud performance

- Cloud provider implementano diversi meccanismi di monitoraggio delle performance e scalabilità automatica
  - Performance sono garantite anche al cambiamento di carico/condizione contestuali
  - Pattern e regole di scalabilità definite e fatte rispettare in maniera automatica
- Scalabilità automatica fornisce l'impressione che un provider stia gestendo risorse fisiche infinite, ma non è così!
  - Ci sono limitazioni tecniche ed economiche
  - Difficile valutare il comportamento di un sistema multi-tenant a priori

Cloud performance

- Nella cloud supporto per scalabilità ed elasticità supportano garanzia delle proprietà di performance tramite tecniche adattative
- Reactivity vs Proactivity
  - Approccio reattivo valuta lo stato della cloud usando metriche e scala in accordo a regole predefinite
  - Un approccio proattivo valuta lo stato della cloud e reagisce prima che il sistema vada in difficoltà e lo stack sia sovraccaricato, sottoutilizzato

Metriche

- Metriche reattive
  - Forniscono un'immagine immediata sullo stato del sistema
  - Permettono di reagire immediatamente in caso di eventi che influiscono sulle performance
  - Esempi: CPU Load, Memory Occupancy, Network Utilization, Response Time
- Metriche proattive
  - Calcolate su una finestra temporale
  - Valutano il trend di performance e l'evoluzione del sistema
  - Permetto di anticipare le mosse riducendo la finestra di decadimento delle performance
  - Esempi: Request Rate, Request Faults, Request Type, CPU Load Trend

Metriche

- Le metriche vengono utilizzate per definire regole di scalabilità e monitorate per causarne l'esecuzione
  - CPU Load valutata attraverso lo script Statistics.CLInfr
  - Una macchina virtuale è aggiunta al cluster di macchine (instancesIncrease) se la CPU load è superiore a 0.75
  - Una macchina virtuale è rimossa dal cluster (decreaseInstance) se la CPU load è inferiore a 0.25
  - CPU Load è valutata ogni 20 secondi (movingTimeRangeInSeconds)

```
service {
  name "tomcat"
  ...
  elastic true
  numInstances 1
  minAllowedInstances 1
  maxAllowedInstances 2
  scaleCooldownInSeconds 20
  samplingPeriodInSeconds 1

  scalingRules ([
    scalingRule {
      serviceStatistics {
        metric "RULE 1"
        movingTimeRangeInSeconds 20
        statistics Statistics.CLInfr
      }
      highThreshold {
        value 0.75
        instancesIncrease 1
      }
      lowThreshold {
        value 0.25
        instancesDecrease 1
      }
    }
  ])
```

Criteri per la gestione di proprietà non funzionali

Service-level category	KPIs	Definition	Unit of measurement
Availability	Service window	Time window within which KPIs are measured	Time range
	Service/System availability	Percentage of time that service or system is available	%
	MTBF	Meantime between failure	Time units
	MTTR	Meantime to repair	Time units
Performance	Response time	Response time for composite or atomic service	Seconds
	Elapsed time	Completion time for a batch or background task	Time units
	Throughput	Number of transactions or requests processed per specified unit of time	Transaction or request count
Capacity	Bandwidth	Bandwidth of the connection that supports a service	bps
	Processor speed	Clock speed of a processor	MHz
	Storage capacity	Capacity of a temporary or persistent storage medium, such as RAM, SAN, disk, or tape	GB
Reliability	Service/System reliability	Probability that service or system is working flawlessly over time	%
Scalability	Service/System scalability	Degree to which the service or system can support a defined growth scenario	Yes/No, or description of scalability upper limit

Interferenza tra requisiti non funzionali

- Requisiti (e proprietà) non funzionali posso interferire tra loro

- A volte il supporto di un requisito porta alla violazione di un altro requisito
  - Ad esempio un algoritmo di criptazione per garantire confidenzialità del dato può diventare molto pesante e influire sulle prestazioni di un servizio

- Grado di interferenza dipende dalla tipologia di proprietà
  - Context-dependent: performance
  - Context- independent: confidenzialità

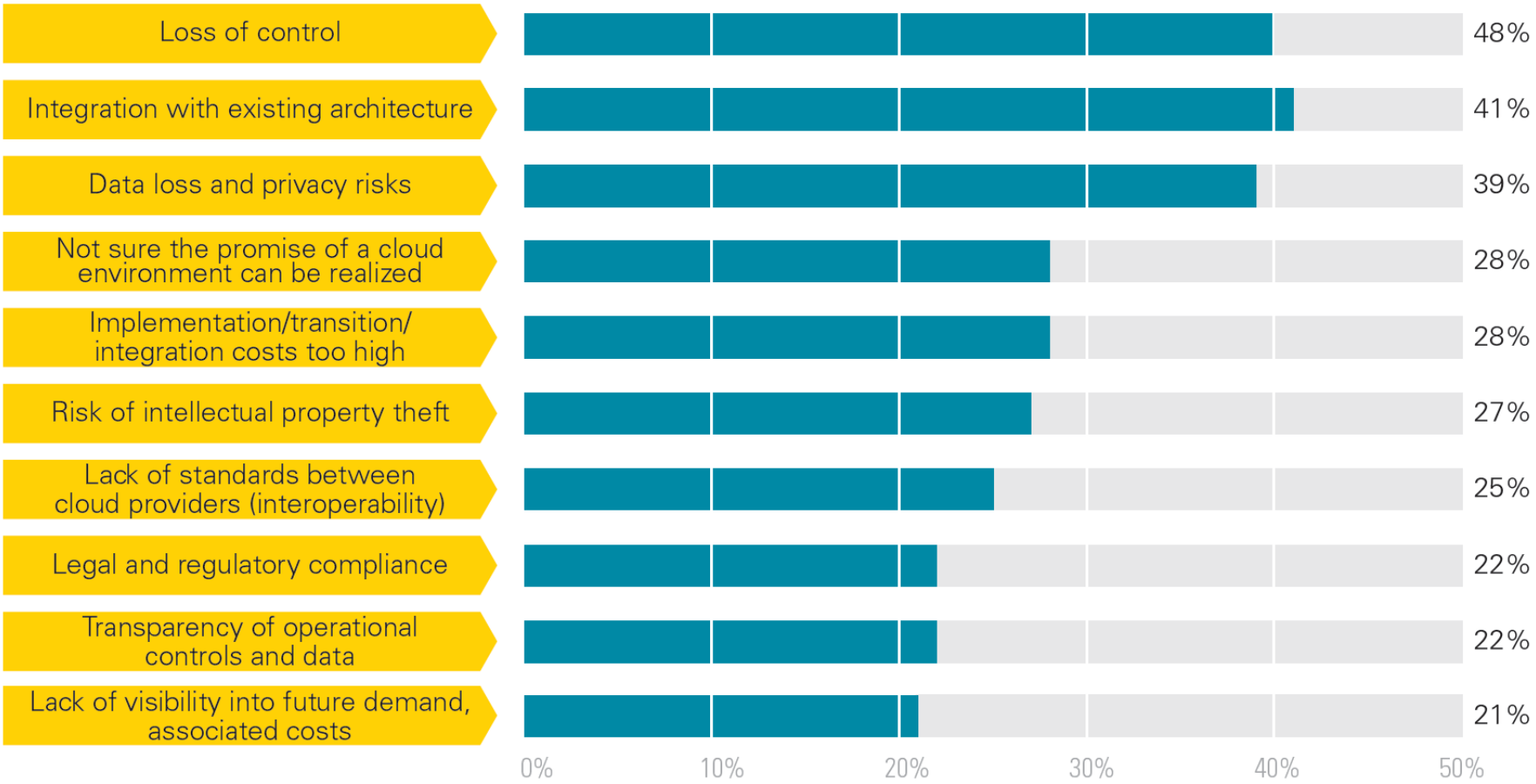
Interferenza tra requisiti non funzionali

- Le problematiche di interferenza crescono esponenzialmente in un sistema virtuale e cloud

- Multi tenancy con separazione logica e isolamento via software apre la strada a interferenze più o meno volute
  - Interferenze possono essere causate da requisiti di diversi tenant
  - Tenant che insistono sulla stessa infrastruttura possono vedere le loro prestazioni decrescere in maniera inaspettata
  - Tenant che insistono sulla stessa infrastruttura possono diventare sorgenti di attacco

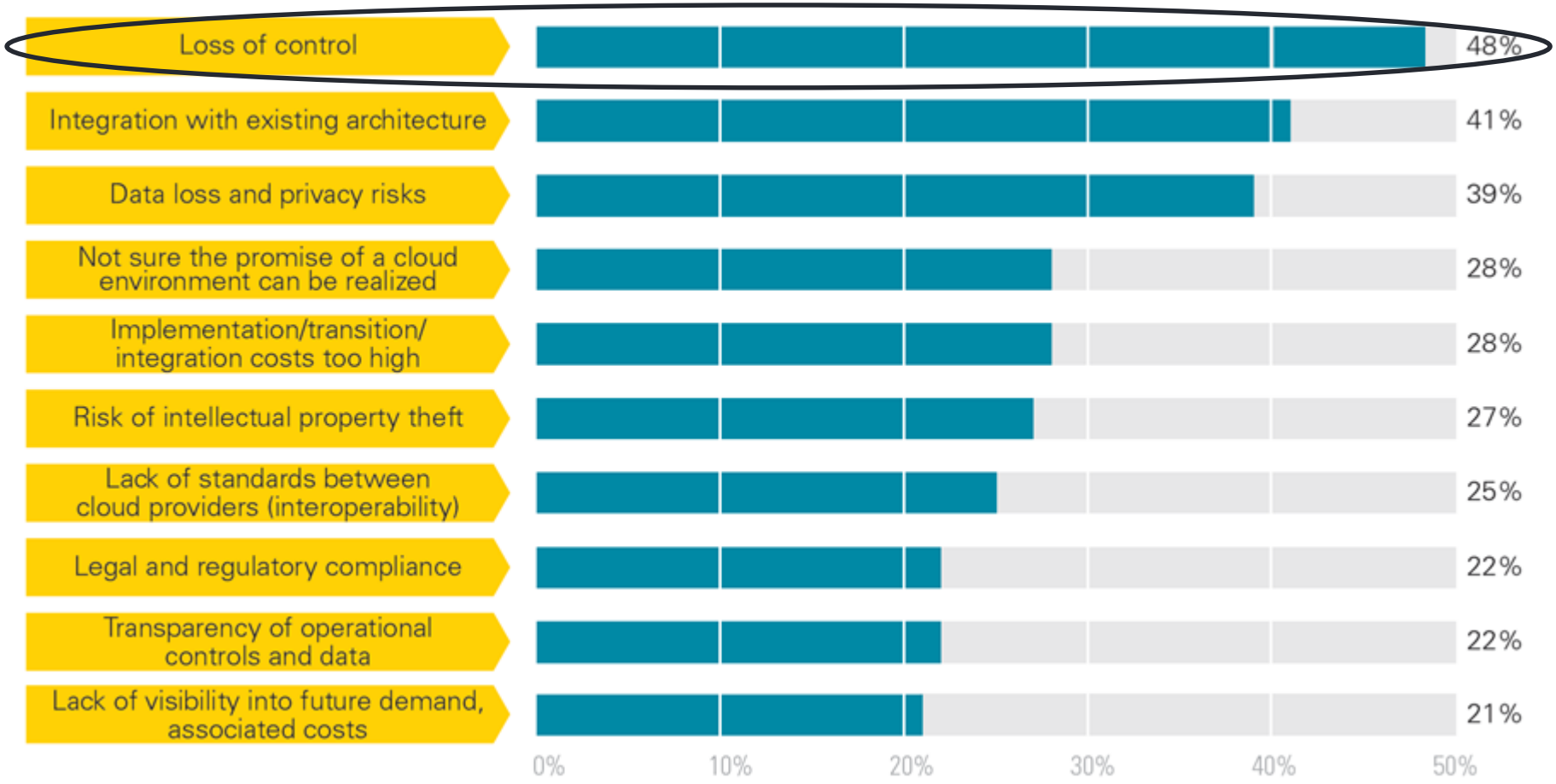
Data Location e Privacy

Maggiori preoccupazioni dei customer



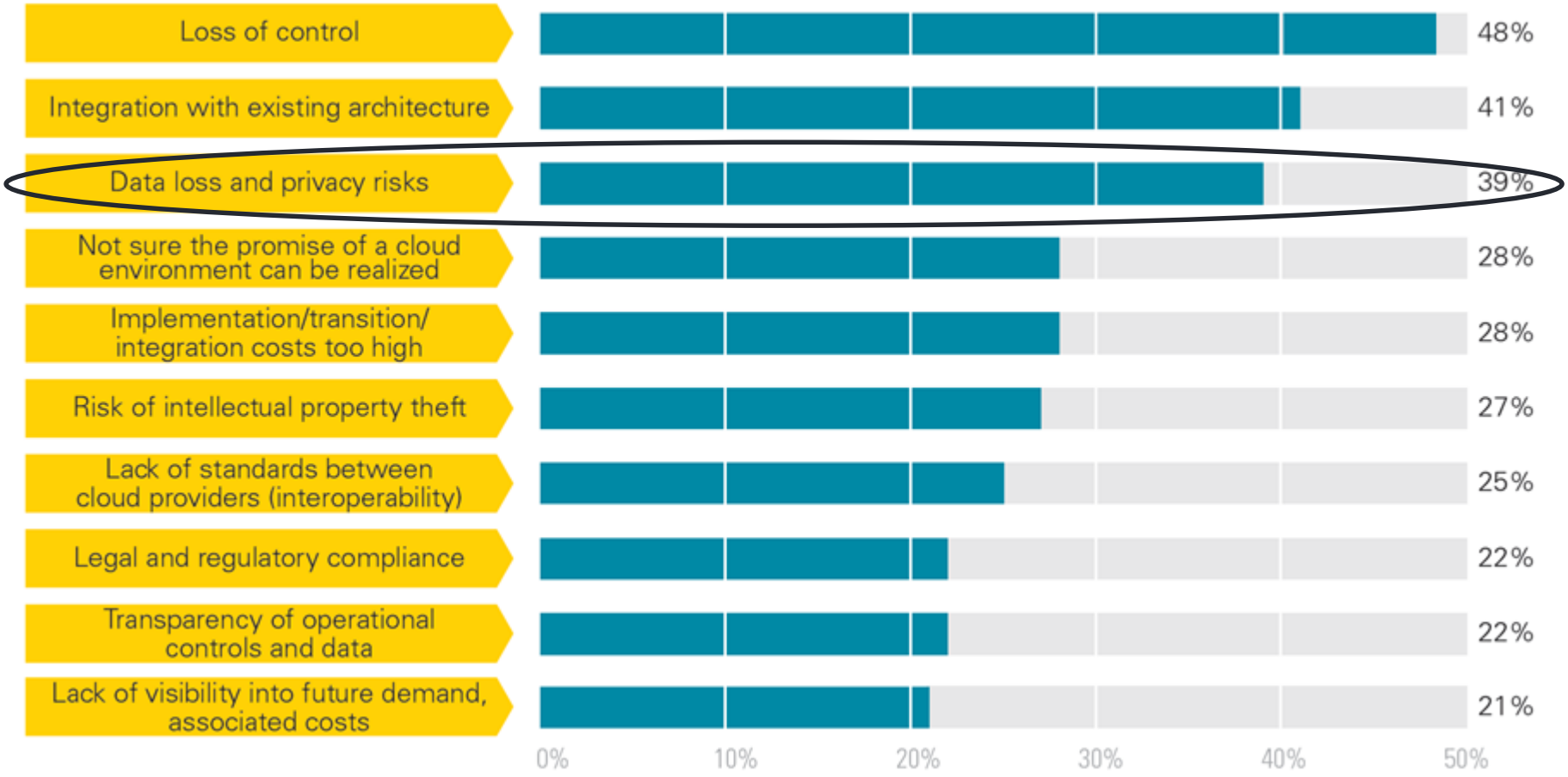
KPMG International's 2012 Global Cloud Provider Survey (n=179)

Maggiori preoccupazioni dei customer



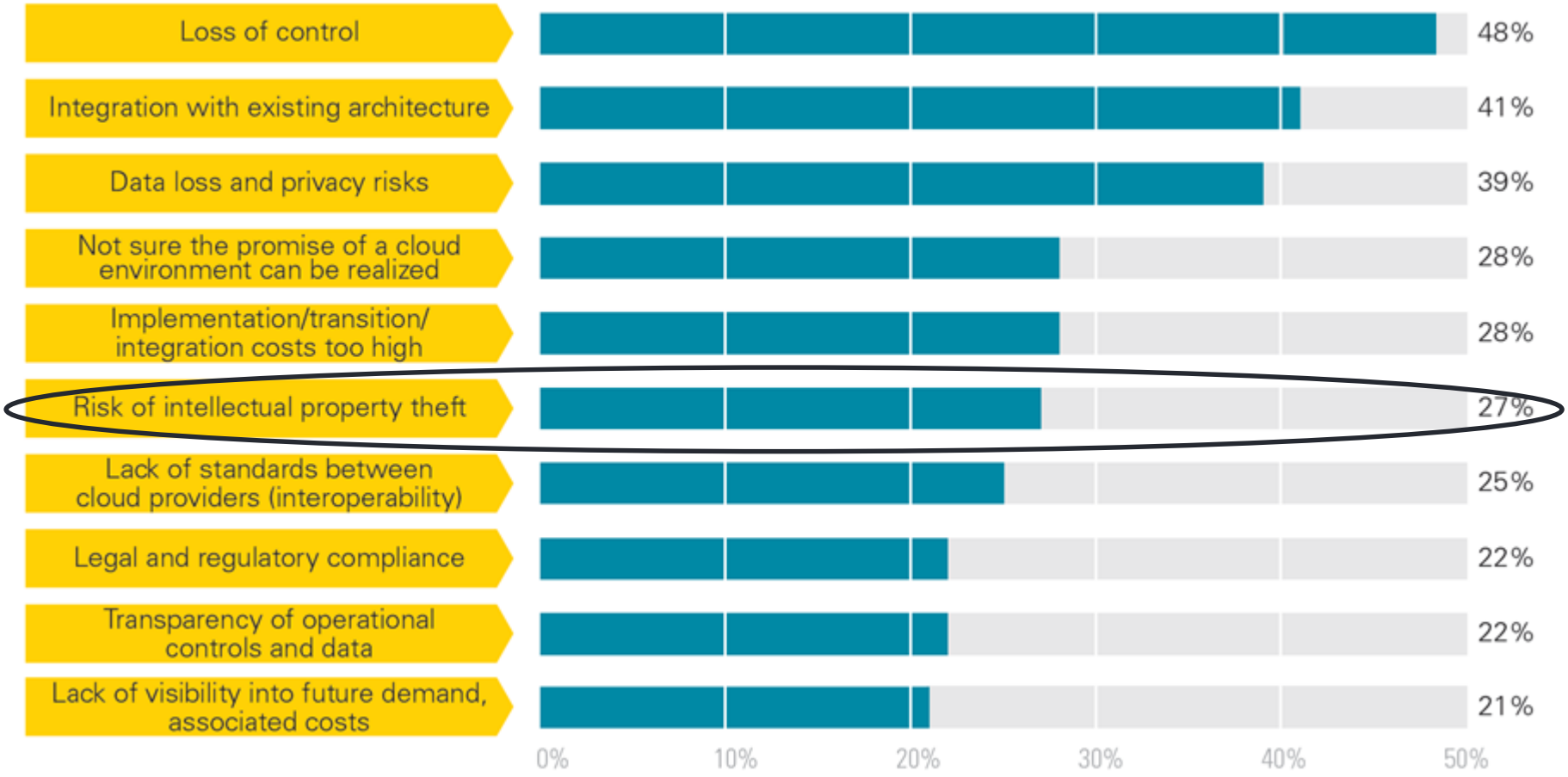
KPMG International's 2012 Global Cloud Provider Survey (n=179)

Maggiori preoccupazioni dei customer



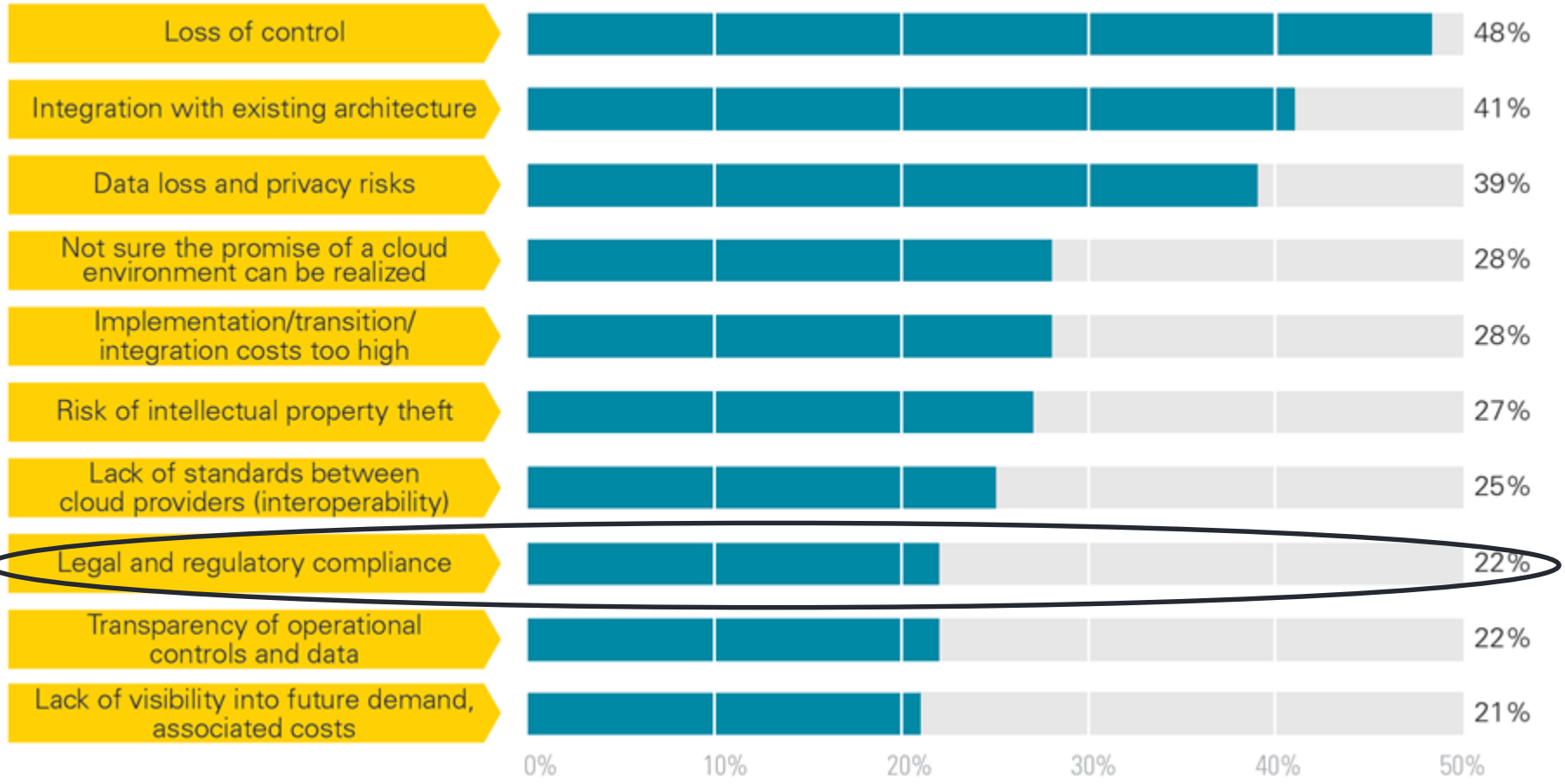
KPMG International's 2012 Global Cloud Provider Survey (n=179)

Maggiori preoccupazioni dei customer



KPMG International's 2012 Global Cloud Provider Survey (n=179)

Maggiori preoccupazioni dei customer



KPMG International's 2012 Global Cloud Provider Survey (n=179)

Data location e privacy

- La cloud cambia radicalmente il concetto di località e di privacy

- La cloud permette di accedere a dati dovunque e in qualsiasi momento
  - Nessuna necessità che i dati risiedano dove risiede l'owner di tali dati
  - Utilissimo per utenti che non hanno le capacità di memorizzazione e le risorse di calcolo per gestire i dati, ma…
  - Crea problematiche aggiuntive (ad esempio, privacy)

Data location e privacy

- Necessità di trovare un bilanciamento tra data privacy e law enforcement access
  - Data location diventa importante in questo contesto
  - Diritto della privacy vs sicurezza nazionale

- Cross-border data flow è importante
  - Le migliori cose si possono ottenere con la libera circolazione dei dati
  - Le leggi sulla privacy lo impediscono o almeno lo regolamentano

Data location e privacy

- Data location diventa uno degli aspetti più critici nella migrazione verso la cloud
  - Dove sono i dati?
- Aziende spesso hanno dei vincoli contrattuali nella gestione dei dati dei loro clienti e dei loro dipendenti
  - Accesso e gestione dei dati
  - Retention
  - Cancellazione
- La posizione fisica dei dati rende applicabile una regolamentazione piuttosto che un'altra
  - Dati memorizzati in USA vs EU

Data location e privacy

- Data Location (Cloud Standards Customer Council)
  - Cloud Service Agreement (CSA) che considera diverse locazioni che seguono diverse giurisdizioni sono complesse
  - Customer devono considerare come CSA specifica dove i dati risiedono, dove sono processati e come questo è in relazione con le diverse regolamentazioni. Customer devono capire dove i dati sono visualizzati o rilasciati, e se questo risulta in un flusso di dati oltre confine con implicazioni di leggi o tasse
  - Ad esempio, può il provider fornire una buona soluzione tecnica se I dati sensibili passano attraverso diverse giurisdizioni con leggi in conflitto? Il provider, nel CSA, si impegna a mantenere i dati in locazioni specifiche?
  - Se il provider aggiunge una nuova locazione o cambia le politiche di scambio dati, avviserà il customer? O meglio, otterrà il suo permesso?
  - Esiste un modo per verificare la locazione corrente di un dataset?

Data location e privacy

- Esempio Microsoft365
  - DATA LOCATION LIMITATIONS. Microsoft stores Office 365 customer data in a number of different countries based on the location of the customer. Moreover, Microsoft can move customer data without notice and will not guarantee exactly where a customer's data will be stored. European Union customer data can be stored in data centers in the US, Ireland and the Netherlands.
  - DATA LOCATION & SECURITY. The location is defined by the company. Data are safely stored within the company perimeter behind the firewall.

Data location e privacy

- Cosa succede a dati di persone europee quando sono memorizzati in altri paesi?
  - Si applicano le leggi Europee?
  - Si applicano le leggi della nazione dove i dati sono memorizzati?
- Ad esempio, EU General Data Protection Regulation (GDPR) propone
  - Increased Territorial Scope (extra-territorial applicability): dati di cittadini europei devono essere processati secondo regole EU indipendentemente dalla locazione

Data location e privacy

- Data privacy (Cloud Standards Customer Council)
  - La data privacy policy del provider dovrebbe essere inclusa nel CSA, e assicurare che il provider condurrà il business in compliance con le leggi sulla data privacy protection
  - Questo include l'dentificazione dei dataset collezionati, le politiche di data retention, come i dati sono comunicati, come I dati personali sono memorizzati e usati
  - Data privacy nella cloud non è solo la protezione delle informazioni circa l'agente del customer che intagisce con il provider, essa include la privacy delle informazioni che potrebbero essere memorizzate circa i customer del customer

Data location e privacy

- Quando i dati sono trasferiti alla cloud, la responsabilità della protezione e sicurezza dei dati rimane con il controller dei dati
  - In alcuni casi può essere condivisa
- Quando il controller dei dati utilizza una terza parte per ospitare o processare i suoi dati, esso rimane responsabile per ogni perdita, danno o misuse dei dati
- L'approccio migliore è che PII controller e processor (il cloud service provider) firmino un accordo scritto (legale) che definisce i ruoli, le attese delle parti, e distribuisca tra loro le responsabilità connesse alla gestione dei dati (at stake)

Key FIPs requirements

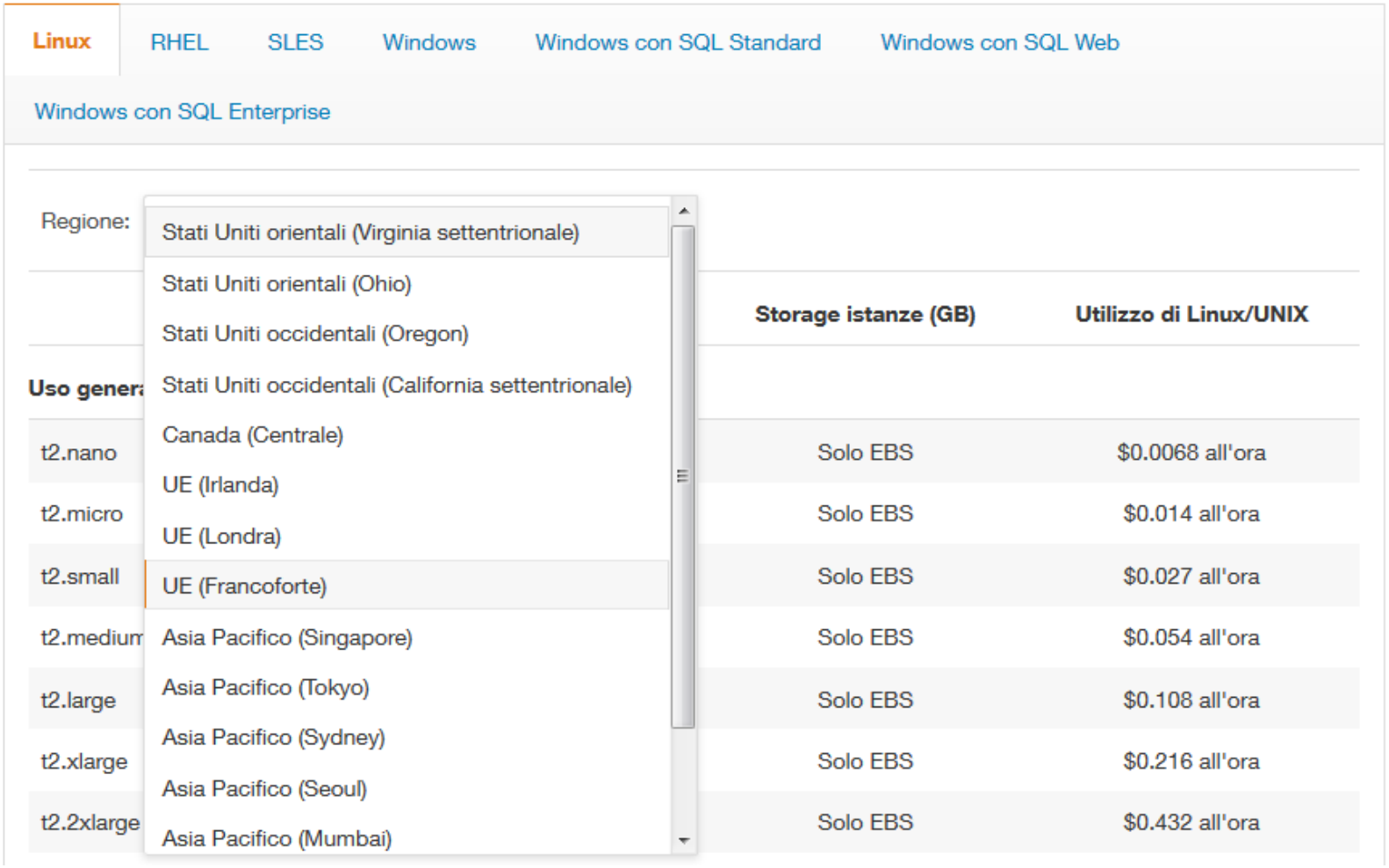
Use limitation	It is easier to combine data from multiple sources in the cloud. How do we ensure data is used for originally specified purposes?
Retention	Is CSP retention period consistent with company needs? Does CSP have proper backup and archival?
Deletion	Does CSP delete data securely and from all storage sources?
Security	Does CSP provide reasonable security for data, e.g., encryption of PII, access control and integrity?
Accountability	Company can transfer liability to CSP, but not accountability. How does company identify privacy breaches and notify its users?
Access	Can company provide access to data on the cloud?

Data location e privacy

- Proteggere PII
- Assicurare compliance a FIPS (Federal Information Processing Standard) principle
- Compliance con legge e regolamentazioni
  - GLBA, HIPAA, PCI-DSS, Patriot Act
- Requisiti multi-giurisdizione
  - EU Directive, EU-US Safe Harbor
- Leggi in diverse nazioni richiede diverse protezioni per la privacy
  - EU Directive più stringente di quella US
  - In US, dati memorizzati su public cloud hanno meno protezione dei personal server
    - Possono essere richieste in processi senza nessuna notifica

Data location e privacy

- Choose your location (Amazon EC2)



Data location e privacy

- Choose your location (Amazon S3)

D: Dove sono archiviati i dati?

Puoi specificare una regione al momento della creazione di un bucket in Amazon S3. All'interno della regione selezionata, gli oggetti sono archiviati in modo ridondante su diversi dispositivi dislocati in varie strutture. Per ulteriori informazioni sulla disponibilità dei servizi di Amazon S3, consulta la sezione relativa a prodotti e servizi per regione.

D: Come si sceglie la regione in cui memorizzare i propri dati?

Vi sono diversi i fattori da considerare a seconda dell'applicazione specifica. È opportuno archiviare i dati in una area geografica:

- Vicina ai tuoi clienti, ai tuoi data center o alle altre tue risorse AWS al fine di ridurre i tempi di latenza nell'accesso ai dati.
- Distante dalle tue altre zone operative per motivi di ridondanza geografica e di disaster recovery.
- Che consenta di soddisfare requisiti legali o normativi specifici.
- Che consenta di ridurre i costi di storage. Per risparmiare, puoi scegliere una regione con tariffe più economiche. Per ulteriori informazioni sulle tariffe di S3, consulta la pagina dei prezzi di S3.

Data location e privacy

- I clienti decidono dove mettere i dati
- Le regioni AWS sono isolate geograficamente by design
- I dati non sono replicati o mossi verso altre regioni a meno che non venga scelto dal padrone dei dati

Data location e privacy

- Possibile soluzione alternative: Hybrid cloud
- Dati e applicazioni sensibili memorizzate on premise
- Dati e applicazioni non sensibili memorizzate sulla cloud
- Necessità di proteggere il flusso di informazioni da e verso la cloud, ad esempio, Elastica Cloud Access Security Brokers (CASB)

Data location e privacy

- Elastica Cloud Access Security Brokers (CASB)

Elastica is a Cloud Access Security Broker (CASB). What's that?

A Cloud Access Security Broker (CASB) is a visibility and control point residing between employees of an organization and the cloud services and SaaS applications they access (e.g., Box, Dropbox, Google Drive, Office 365, Salesforce, Workday, etc.). A Cloud Access Security Broker can potentially be deployed in either of two ways: as an on-premises offering or as a cloud-based gateway or proxy through which traffic enterprise traffic can be siphoned (typically on a per-application basis).

Because of its positioning, a Cloud Access Security Broker not only has (potentially granular) visibility into the traffic going to and from a cloud service or SaaS application, but can be used by IT organizations to actively detect threats and enforce policies.

Data location e privacy

- Possibile soluzione alternative: Selective encryption
- Dati e applicazioni sensibili criptate
- Dati e applicazioni non criptate
- Necessità di soluzioni per la gestione e l'analisi delle informazioni privacy preserving

Data location e privacy

- Requisiti generali
  - Massimizzare il controllo degli utenti
  - Massimizzare la trasperenza nella gestione dei dati
  - Provare la locazione dei dati
  - Selezione dei requisiti di secondary use (pubblicità, miglioramento del servizio)

Tecniche di protezione dei dati

Security management

- Availability
- Access control
- Monitoring
- Vulnerability, patching, configuration
- Incident response

Availability

- Perchè è importante?
  - “Amazon Web Services suffers outage, takes down Vine, Instagram, others,” Aug 26, 2013*
- Ad esempio, AWS feature
  - Protezione contro distributed denial of service (DDoS)
  - Fault-tolerant, independent failure zone

D: Che cosa garantisce il contratto sul livello di servizio di Amazon EC2?

Il contratto sul livello di servizio garantisce per Amazon EC2 e Amazon EBS una percentuale di tempo di attività mensile all'interno di una regione pari ad almeno il 99,95%.

D: Come posso sapere se ho diritto a un credito di assistenza SLA?

Hai diritto a un credito di assistenza SLA per Amazon EC2, per Amazon EBS o per tutti e due i servizi, nel caso in cui entrambi siano risultati non disponibili, se la regione in cui operi ha una percentuale di tempo di attività mensile inferiore al 99,95% durante un ciclo di fatturazione mensile. Per dettagli completi sui termini e le condizioni del contratto sul livello di servizio e per indicazioni sulla presentazione di una richiesta, consulta la pagina http://aws.amazon.com/ec2/sla/

*http://www.zdnet.com/amazon-web-services-suffers-outage-takes-down-vine-instagram-flipboard-with-it-7000019842/

Access control

- Chi deve accedere a cosa?
  - VM, app, servizi…
  - User, admin, business admin, altri?
- Ad esempio, AWS feature
  - Built-in firewall controllano accessi alle istanze
  - Multi-factor authentication (MFA): password + authentication code da un device MFA
  - Monitorare accessi dei dipendenti AWS

Monitoring

- Monitor
  - Availability, attività non autorizzate…
- Ad esempio, AWS feature
  - DoS, MITM, port scan, packet sniffing
  - Password brute-force detection
  - Access log (request type, resource, IP, time ...)

Vulnerability, patching, configuration

- Ad esempio, AWS feature
  - Patching
    - Patching automatico del software per immagini Windows fornite da Amazon
  - Configuration
    - Scadenza della password per i dipendenti AWS
  - Vulnerability
    - Vulnerability scan sugli host operating system, applicazioni web e DB in ambiente AWS

Customer: Responsabilità

- Cloud è un ambiente condiviso

D: Per l'uso di istanze G2 occorrono licenze di terze parti?

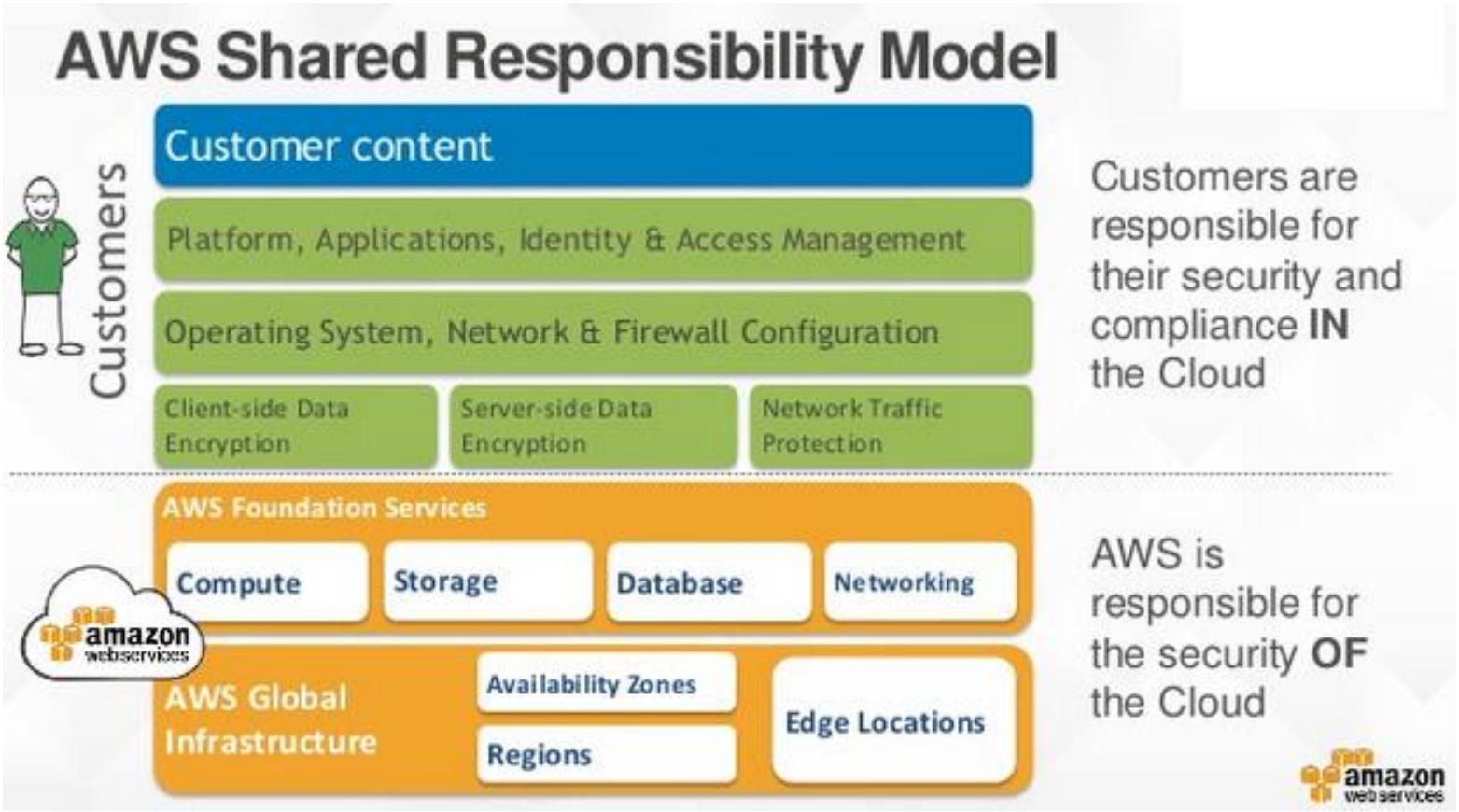
A parte i driver NVIDIA e l'SDK GRID, l'uso di istanze G2 non richiede necessariamente licenze di terze parti. Tuttavia, è tua responsabilità determinare se la tecnologia e i contenuti utilizzati sulle istanze G2 richiedono altre licenze. Ad esempio, se riproduci contenuti in streaming, possono essere necessarie licenze per tutti i contenuti o per almeno parte di essi. Se utilizzi tecnologia di terze parti, ad esempio sistemi operativi, encoder e decoder audio e/o video di Microsoft, Thomson, Fraunhofer IIS, Sisvel S.p.A., MPEG-LA e Coding Technologies, richiedi informazioni sui requisiti di licenza direttamente ai fornitori di queste soluzioni. Ad esempio, se utilizzi l'encoder video h.264 integrato sulla GPU NVIDIA GRID, dovrai richiedere informazioni sulla licenza a MPEG-LA; se invece utilizzi la tecnologia

D: Vi sono altri requisiti per l'importazione di una macchina virtuale in Amazon EC2?

Prima di generare l'immagine VMDK o VHD, la macchina virtuale deve trovarsi in stato di interruzione. La macchina virtuale può essere in stato di pausa o sospensione. Suggeriamo di esportare la macchina virtuale con soltanto il volume di avvio collegato. È possibile importare dischi aggiuntivi utilizzando il comando ImportVolume e collegare quindi tali dischi alla macchina virtuale mediante il comando AttachVolume. I dischi crittografati, ad esempio quelli protetti con Bit Locker, e i file immagine crittografati non sono supportati. È inoltre responsabilità dell'utente disporre di tutti i diritti e le licenze necessari per effettuare importazioni in AWS ed eseguire qualsiasi applicazione software inclusa nell'immagine della macchina virtuale.

Customer: Responsabilità

- Cloud è un ambiente condiviso



Customer: Responsabilità

- AWS richiede ai customer di
  - Patch VM guest operating system
  - Prevenire port scan
  - Cambiare le chiavi periodicamente
  - Fare testing di vulnerabilità delle app
  - Altro…

Data issue: confidentiality

- Dati in transito tra cloud e intranet
  - Ad esempio, usare HTTPS
- Possibile per storage semplice
  - Ad esempio, dati in Amazon S3 criptato con AES-256
- Difficultà per dati processati nella cloud
  - Overhead di ricerca, indexing...
    - Ad esempio, iCloud non cripta I dati sul mail server*
  - Se criptati, dati sono decriptati prima della fase di processing
    - È possibile effetuare computazioni su dati criptati?^

*iCloud: iCloud security and privacy overview, Retrieved Oct 30, 2013, https://support.apple.com/kb/HT4865

^See Fully Homomorphic Encryption Scheme, Wikipedia, http://en.wikipedia.org/wiki/Homomorphic_encryption

Gestione della criptazione

- Algoritmi
  - Proprietari vs. standard
- Dimensione della chiave
- Gestione della chiave
  - Idealmente gestita dai customer
  - Il CSP vede le chiavi di decriptazione?
  - Ad esempio, Apple usa master key per decriptare dati iCloud per controllare contenuto "controverso"*

*Apple holds the master decryption key when it comes to iCloud security, privacy, ArsTechnica, Apr 3, 2012

Data issue: comingled data

- Cloud usa multi-tenancy
  - Dati mescolati con dati di altri utenti
- Application vulnerability potrebbero permettere accesso non autorizzato
  - Ad esempio, Google docs unauthorized sharing, Mar 2009
  - “Identified and fixed a bug which may have caused you to share some of your documents without your knowledge.”

Monitoraggio in Cloud

Monitoraggio in cloud

- Il monitoraggio delle attività in Cloud è fondamentale per comprendere lo stato del sistema
  - Essendo molto complesso diventa una attività onerosa se non automatizzata
- Molte cloud pubbliche offrono strumenti a supporto
- Genericamente possono servire per
  - Calcolare metriche di prestazione
  - Evidenziare problemi di sicurezza
- Genericamente si basano sui log dei vari livelli della cloud

Categorie di logging: AWS

- **AWS Infrastructure logs**
  - AWS CloudTrail
  - Amazon VPC Flow Logs
- **AWS service logs**
  - Amazon S3
  - AWS Elastic Load Balancing
  - Amazon CloudFront
  - AWS Lambda
  - AWS Elastic Beanstalk
  - E tanti altri
- **Host based logs**
  - Messages
  - Security
  - NGINX/Apache/IIS
  - Windows Event Logs
  - E tanti altri

AWS CloudTrail

- AWS CloudTrail è un servizio che consente la governance, la conformità, l'audit operativo e dei rischi del tuo account AWS.
  - registrare, monitorare continuamente e mantenere gli eventi correlati alle chiamate API all'interno dell'infrastruttura AWS.
  - storico delle chiamate API AWS per il tuo account
  - semplifica l'analisi di sicurezza, il monitoraggio delle modifiche delle risorse e la risoluzione dei problemi.

AWS CloudTrail

- Permette di sapere:
  - Chi ha fatto una API call
  - Quando è stata fatta una API call
  - Quale API call
  - Quale risorsa si è comportata male durante una API call
  - Da chi e verso chi è stata fatta una API call

AWS CloudTrail: best practices

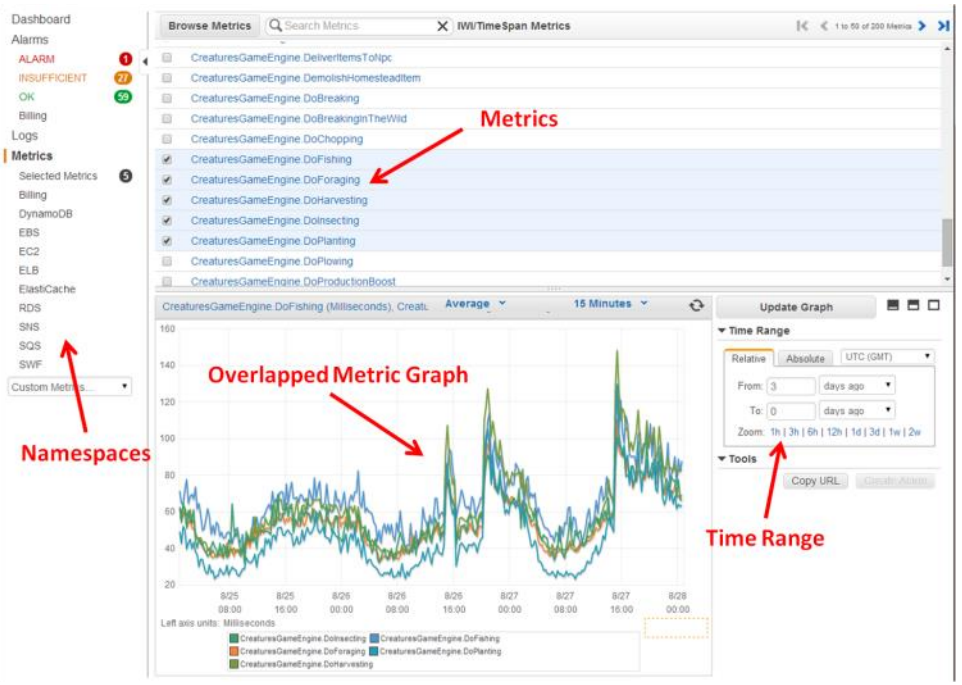
- Abilitarlo per tutte le regioni
  - Tracciare anche regioni non usate
  - Fattibile in un unico passo di configurazione
- Abilitare la validazione dei log
  - Garantire l'integrità dei log
  - Validare i log per security e forensics
  - Basato su standard industriali elevati
  - AWS CloudTrail fornisce log e digest con scheduling orario
  - Digest contiene lo hash dei log e sono firmati

CloudWatch

- Un servizio di monitoraggio per le risorse cloud AWS e le applicazioni in esecuzione su AWS
  - raccogliere e monitorare parametri e file di log
  - impostare allarmi e reagire automaticamente ai cambiamenti nelle risorse AW
- Consente il monitoraggio di
  - EC2, le tabelle Amazon DynamoDB e le istanze Amazon RDS DB, parametri personalizzati generati dalle applicazioni e dai servizi del cliente e i file di log generati dalle applicazioni
- Può essere utilizzato per ottenere visibilità a livello di sistema sull'utilizzo delle risorse, le prestazioni delle applicazioni e lo stato di integrità operativa

CloudWatch: Metriche

- Metriche custom
- Da 5 minuti (default) a 1 minuto di intervallo tra valutazioni
- Si può usare per forensics, tiene traccia per 2 settimane
  - Formato time series
- Dashboard e API per le estrazioni
- Auto-scaling



Managing, Monitoring e Log processing

- CloudWatch Logs
  - Near real-time, aggregazione, monitoraggio, salvataggio e ricerca
- Amazon Elastic search Service Integration (or ELK stack)
  - Analitiche, interfaccia Kibana
- AWS Lambda & Amazon Kinesis
  - Processamento custom
- Export verso S3
  - Batch export e analitiche

AWS Config Rules

- Creare regole per controllare i cambi di configurazione
  - pre-built fornite da AWS
- Regole custom usando Lambda
- Chiamate automatiche per continuous assessment
- Dashboard per visualizzare compliance alle regole e identificare I cambiamenti

AWS Config Rules Repository

- AWS Community repository per regole custom
  - https://github.com/awslabs/aws-config-rules

- Contiene esempi python delle regole AWS Config

CloudWatch Events

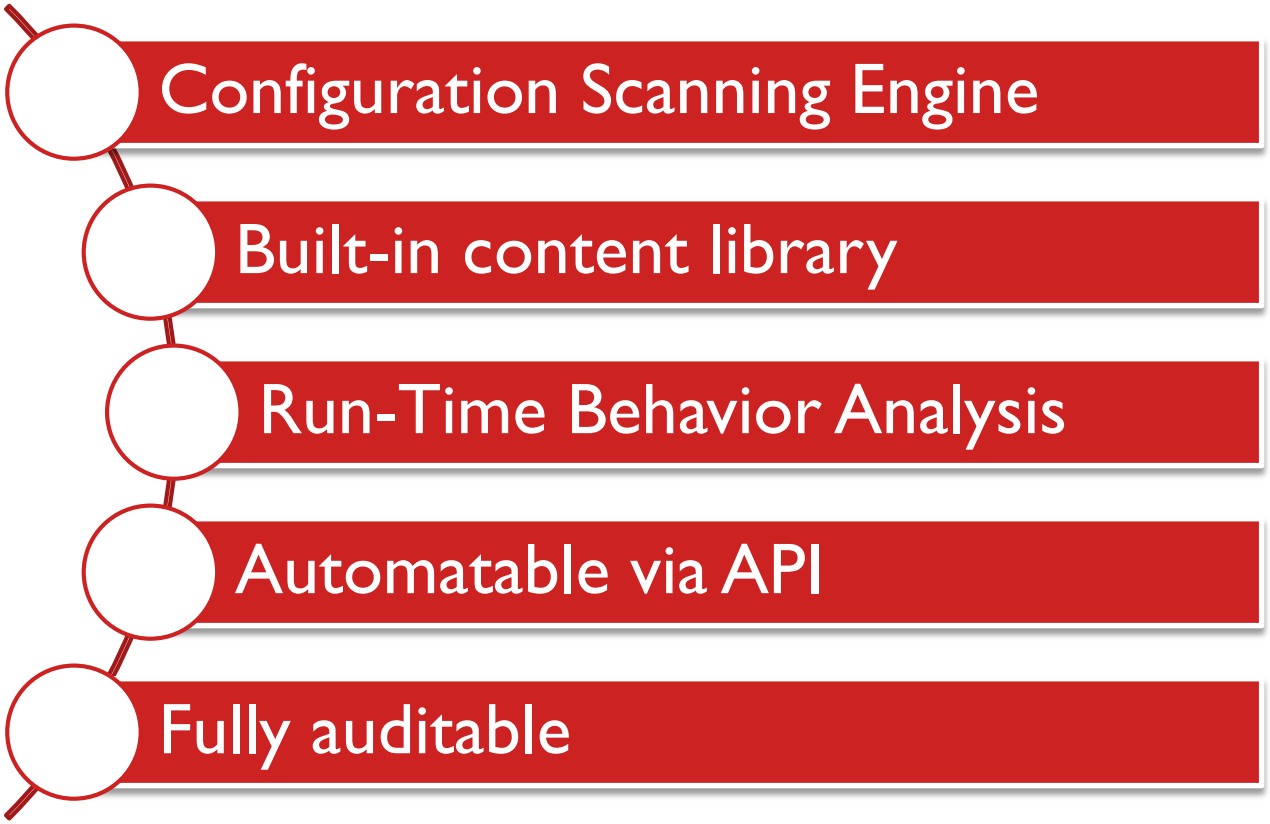
- Trigger on event
  - Notifiche sul cambio di stato di istanze Amazon EC2
  - AWS API call
  - AWS console sign-in
  - Auto Scaling
- Schedule
  - Cron
  - Min 1 min

AWS Inspector

- Servizio di valutazione della sicurezza automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni distribuite in AWS

- Esamina automaticamente le applicazioni in cerca di vulnerabilità o divergenze dalle best practice
  - Elenco dettagliato con i risultati della valutazione, ordinati secondo il livello di gravità
  - Regole aggiornate periodicamente dagli specialisti della sicurezza di AWS

Amazon Inspector: caratteristiche



Amazon Inspector: Regole

AWS Trusted Advisor

- Risorsa online che aiuta a ridurre i costi, potenziare le prestazioni e migliorare la sicurezza ottimizzando l'ambiente AWS
  - Linee guida in tempo reale per aiutarti a effettuare il provisioning delle risorse secondo le best practice di AWS

AWS Security tools

Service	Tipo	Use cases
 AWS CloudTrail	Continuous logging	Registra AWS API calls per uno specific account e fa il delivery dei log
 AWS Config Rules	Continuous evaluations	Codifica le best practices, misconfigurations, vulnerabilità azioni in caso di cambiamenti
 AWS Inspector	On-demand evaluations	Ispezione di security delle applicazioni deployate all'interno di istanze EC2
 AWS Trusted Advisor	Periodic evaluations	Cost, performance, reliability, e security checks
 CloudWach Events	Azioni in risposta a API e cambi di stato	Triggers custom e azioni Lambda

Servizi e tool a supporto della sicurezza nella cloud

AWS Security and Compliance

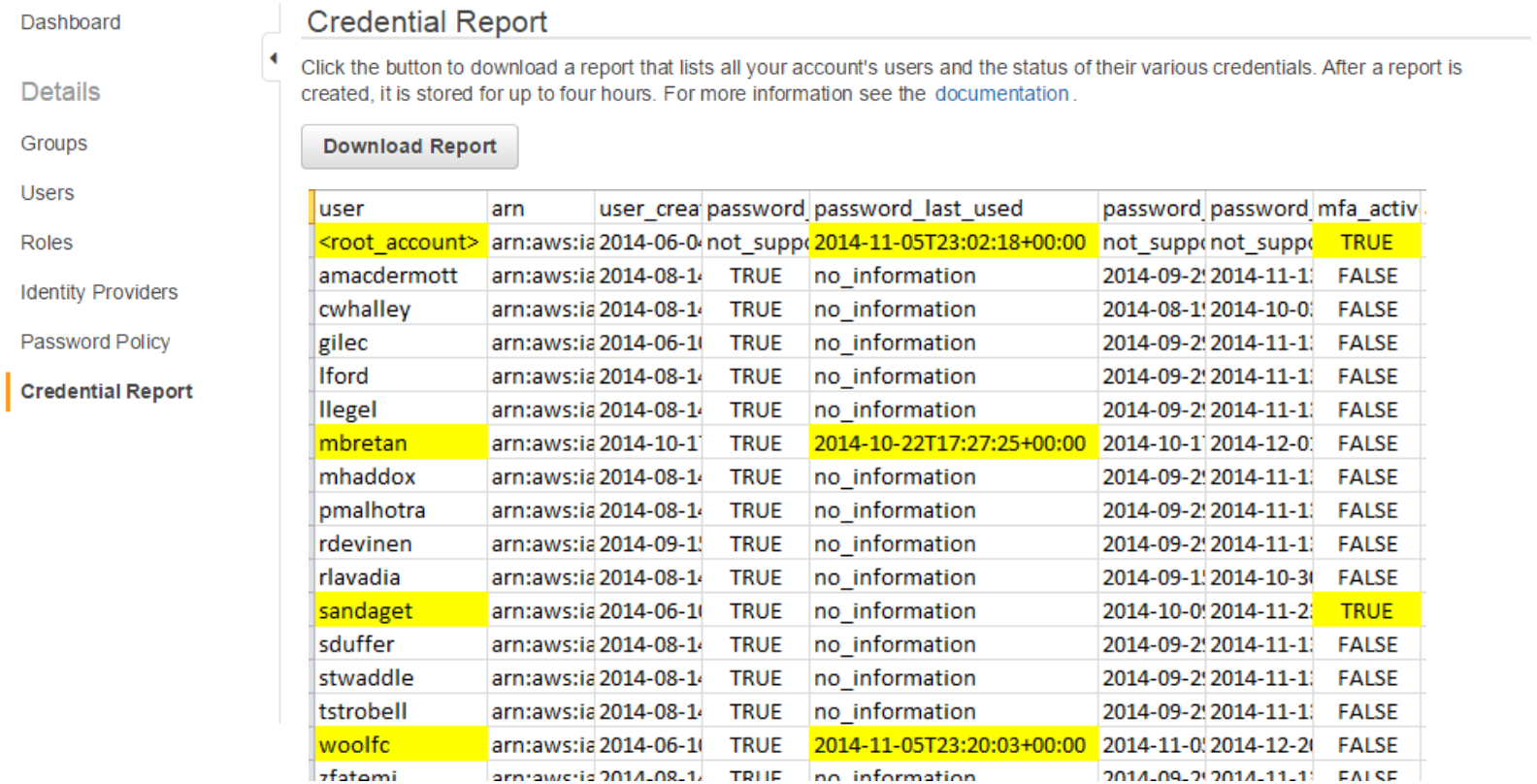
Sicurezza della cloud

Automazione dei controlli

- Autogestiti
  - AWS CloudTrail -> Amazon CloudWatch Logs -> Amazon CloudWatch Alerts
  - AWS CloudTrail -> Amazon SNS -> AWS Lambda
- Compliance validation
  - AWS Config Rules
- Host based Compliance validation
  - AWS Inspector
- Active Change Remediation
  - Amazon CloudWatch Events

IAM Credential Reports

- Tool Amazon interessante a supporto della sicurezza che verifica le credenziali



user	arn	user_crea	password	password_last_used	password	password	mfa_activ
<root_account>	arn:aws:ia	2014-06-0	not_supp	2014-11-05T23:02:18+00:00	not_supp	not_supp	TRUE
amacdermott	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
cwhalley	arn:aws:ia	2014-08-1	TRUE	no_information	2014-08-1	2014-10-0	FALSE
gilec	arn:aws:ia	2014-06-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
lford	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
llegel	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
mbretan	arn:aws:ia	2014-10-1	TRUE	2014-10-22T17:27:25+00:00	2014-10-1	2014-12-0	FALSE
mhaddox	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
pmalhotra	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
rdevinen	arn:aws:ia	2014-09-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
rlavadia	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-1	2014-10-3	FALSE
sandaget	arn:aws:ia	2014-06-1	TRUE	no_information	2014-10-0	2014-11-2	TRUE
sduffer	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
stwaddle	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
tstrobell	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
woolfc	arn:aws:ia	2014-06-1	TRUE	2014-11-05T23:20:03+00:00	2014-11-0	2014-12-2	FALSE
zfatemi	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE

Centro Sicurezza AZURE - Obiettivi

- Identificare lo stato della sicurezza delle risorse di Azure

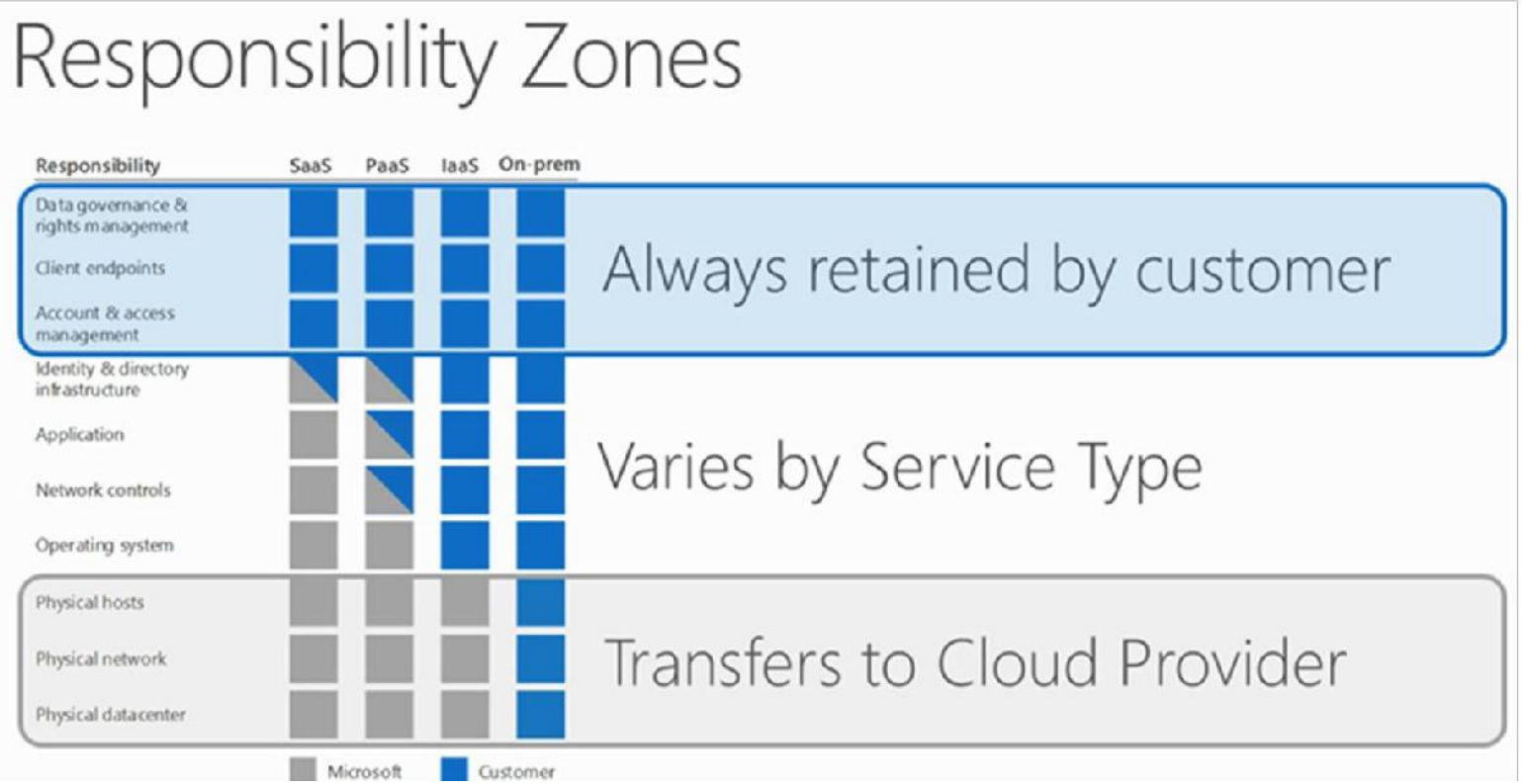
- Acquisire il controllo della sicurezza nel cloud con monitoraggio delle configurazioni di sicurezza basato su criteri

- Semplificare per i responsabili delle operazioni di sviluppo la distribuzione di soluzioni di sicurezza Microsoft e dei partner integrate

- Individuare le minacce con l'analisi del comportamento in base alle conoscenze e all'esperienza di livello globale

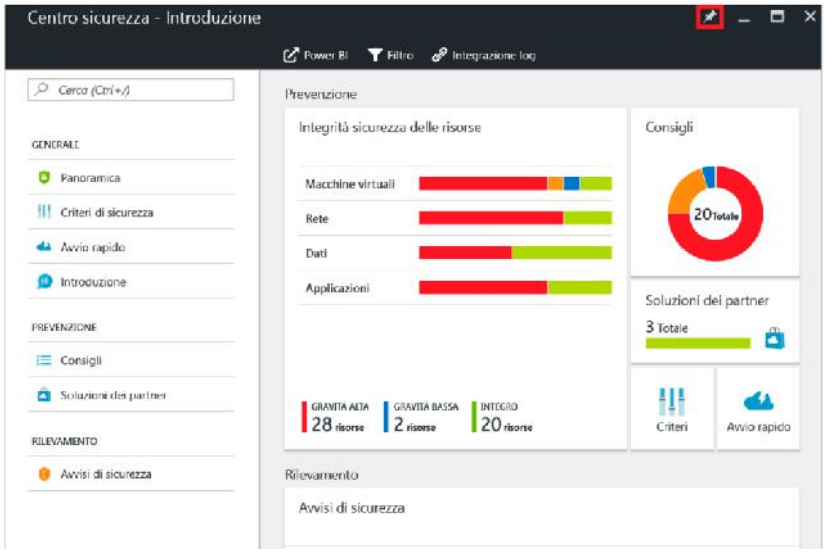
- Rispondere velocemente agli eventi imprevisti con informazioni dettagliate sugli attacchi e suggerimenti per la correzione

Shared Responsibility



Aree di Controllo

- Controlli relativi a servizi di infrastruttura:
  - Coprono configurazione dell'infrastruttura (regole di firewalling, configurazione accessi, immagini deployate, reti, storage, db basic configuration), sistema operativo, patch di sicurezza e aggiornamenti
  - Coprono le minime caratteristiche delle VM



Criteri di Prevenzione

- Il centro di sicurezza è basato su raccomandazioni che vengono mappate sui criteri di sicurezza
  - Impostando Aggiornamenti del sistema su Sì, tutte le macchine virtuali supportate verranno analizzate per rilevare gli aggiornamenti del sistema operativo mancanti
  - Impostando Vulnerabilità del sistema operativo su Sì, tutte le macchine virtuali supportate verranno analizzate per identificare le configurazioni del sistema operativo che possono esporre la macchina virtuale ad attacchi

Controllo Continuo

- Il sistema in automatico, una volta assegnati target e risorse in maniera automatica e continua, controlla lo stato delle raccomandazioni attivate

DESCRIZIONE	RISORSA	STATO	GRAVITÀ	
Installa Endpoint Protection	3 macchine...	Apri	Alto	...
Aggiungi un Web application firewall	2 applicazio...	Apri	Alto	...
Aggiungi un firewall di nuova genera...	5 endpoint	Apri	Alto	...
Finalizza la protezione dell'endpoint...	VM3-RDP-M...	Apri	Alto	...
Abilita i gruppi di sicurezza di rete ne...	subnet1	Apri	Alto	...
Abilita i gruppi di sicurezza di rete ne...	vm1classic	Apri	Alto	...
Indirizza il traffico solo tramite il fire...	vm3	Apri	Alto	...
Abilita controllo e rilevamento delle...	sqlserver1as...	Apri	Alto	...
Correggi le vulnerabilità (di Qualys)	2 macchine...	Apri	Alto	...
Abilita controllo e rilevamento delle...	2 database...	Apri	Alto	...
Abilita Transparent Data Encryption	3 database...	Apri	Alto	...
Applica gli aggiornamenti del sistema	vm1	Apri	Alto	...
Applica la crittografia del disco	Applica la c...	Apri	Alto	...
Aggiorna la versione del sistema ope...	2 ruoli	Apri	Alto	...
Abilita la crittografia per gli account...	9 account di...	Apri	Alto	...
Limita l'accesso tramite un endpoint...	4 macchine...	Apri	Medio	...
Aggiungi una soluzione di valutazione...	4 macchine...	Apri	Medio	...
Riavvia dopo gli aggiornamenti del sis...	vm2	Apri	Medio	...
Specificare i dettagli dei contatti di si...	1 sottoscriz...	Apri	Medio	...
Correggi le vulnerabilità del sistema o...	4 macchine...	Apri	Basso	...

Alert

- Il sistema può essere impostato per avvisare il responsabile della sicurezza di possibili vulnerabilità o misconfiguration del sistema in maniera automatica e tempestiva
- Gli alert spesso suggeriscono quali possono essere le azioni proattive per mitigare o correggere la vulnerabilità

DESCRIZIONE	Centro sicurezza di Azure ha rilevato la mancata corrispondenza di un'immagine in un modulo caricato in memoria durante l'analisi di un dump di arresto anomalo del sistema. Se la presenza di questo modulo non è prevista, il sistema potrebbe essere compromesso.
ORA DI RILEVAMENTO	Sabato 8 ottobre 2016 10:58:48
GRAVITÀ	Alto
STATO	Attiva
RISORSA CHE HA SUBITO ATTACCHI	VM3
SOTTOSCRIZIONE	212f9889-769e-45ae-ab43-6da33674bd26
RILEVATO DA	Microsoft
AZIONE INTRAPRESA	Rilevato
PROCESSNAME	lync.exe
PROCESSVERSION	16.0.6001.1078
MODULENAME1	ntdll
MODULEVERSION1	6.3.9600.18233
PROCEDURA DI CORREZIONE	1) Monitorare le attività di accesso a questo computer, verificando la presenza di exploit noti nel processo indicato su cve.mitre.org. 2) Se si ritiene che il computer sia stato compromesso, individuare gli account utente da cui deriva la compromissione. 3) Ridistribuire il computer da un'immagine vuota con le patch applicate e reimpostare le password degli eventuali account autenticati sul presente computer.

QUESITI?

vincenzocalabro.it