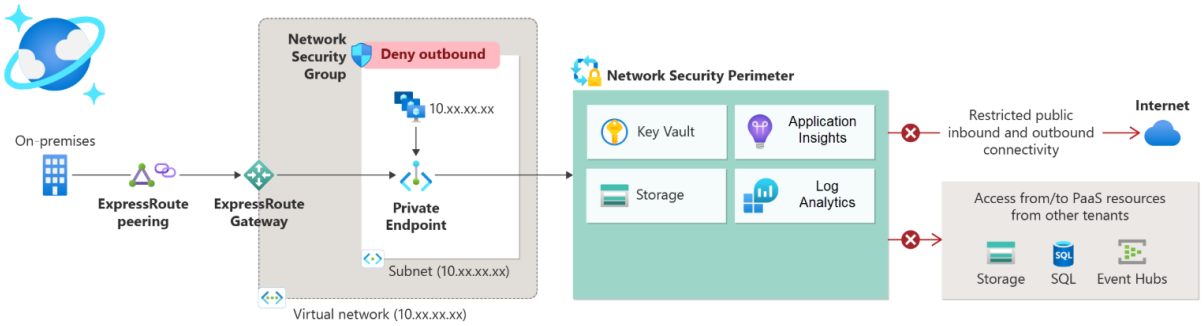
Analisi del Perimetro e della Superficie di Attacco di Microsoft Azure alla luce del modello NIST SP 800-207 (Zero Trust Architecture)

Franco Salvucci - Mario Chiappini

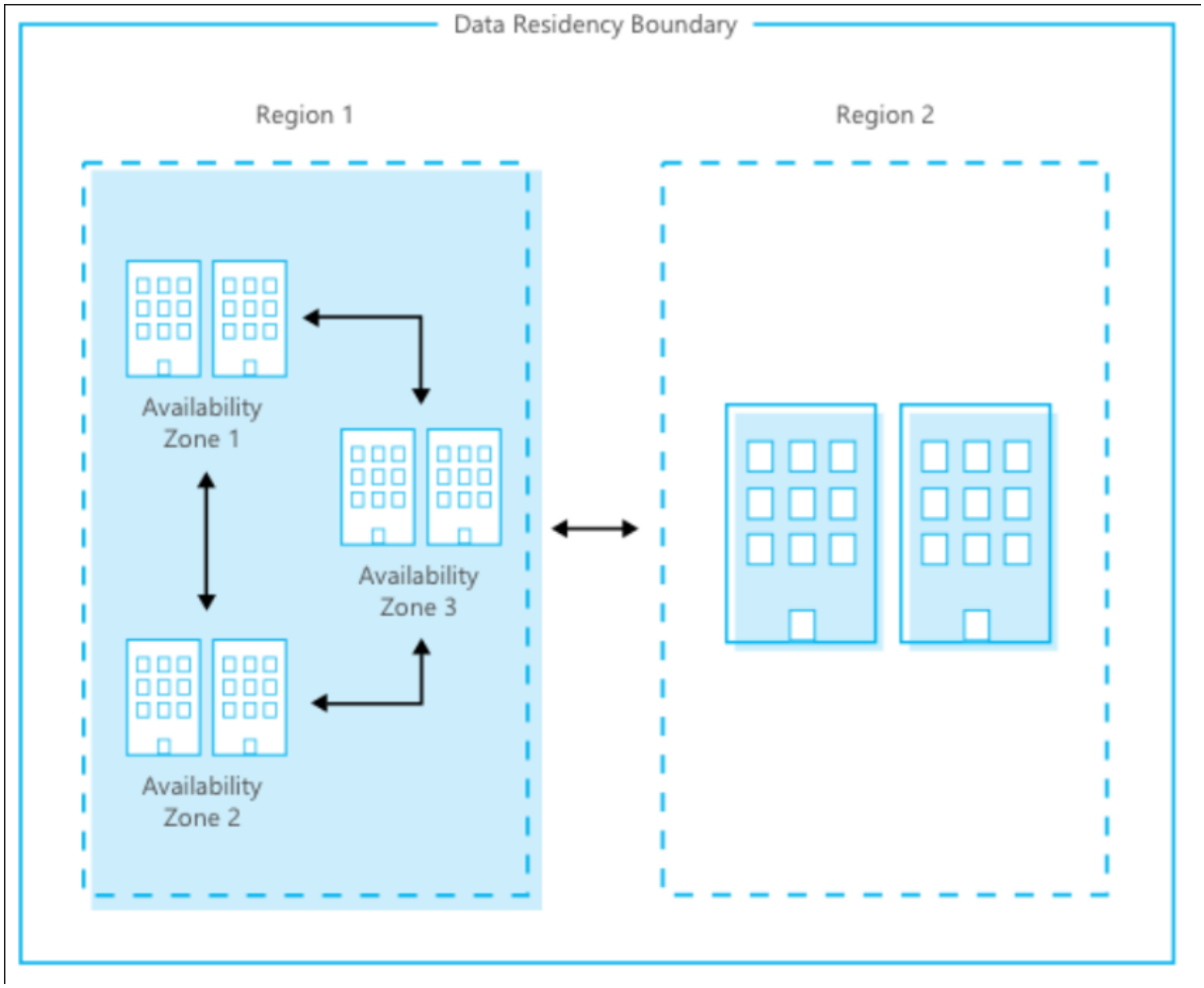
Indice

1 Perimetro dell'architettura (confini di controllo e contesti)

Nel modello architetturale di **Microsoft Azure**, il concetto di perimetro non coincide più con un confine fisico tradizionale, bensì con un *insieme logico e dinamico di contesti di sicurezza*. Seguendo la filosofia della **Zero Trust Architecture (ZTA)**, il perimetro viene ridefinito come un *dominio di controllo distribuito* che si estende attraverso i seguenti livelli.



1.1 Contesto fisico e infrastrutturale



Il primo livello riguarda i **data center globali di Microsoft**, connessi tramite dorsali ad alta capacità e sistemi di interconnessione privata (Azure WAN, ExpressRoute, Microsoft Global Network).

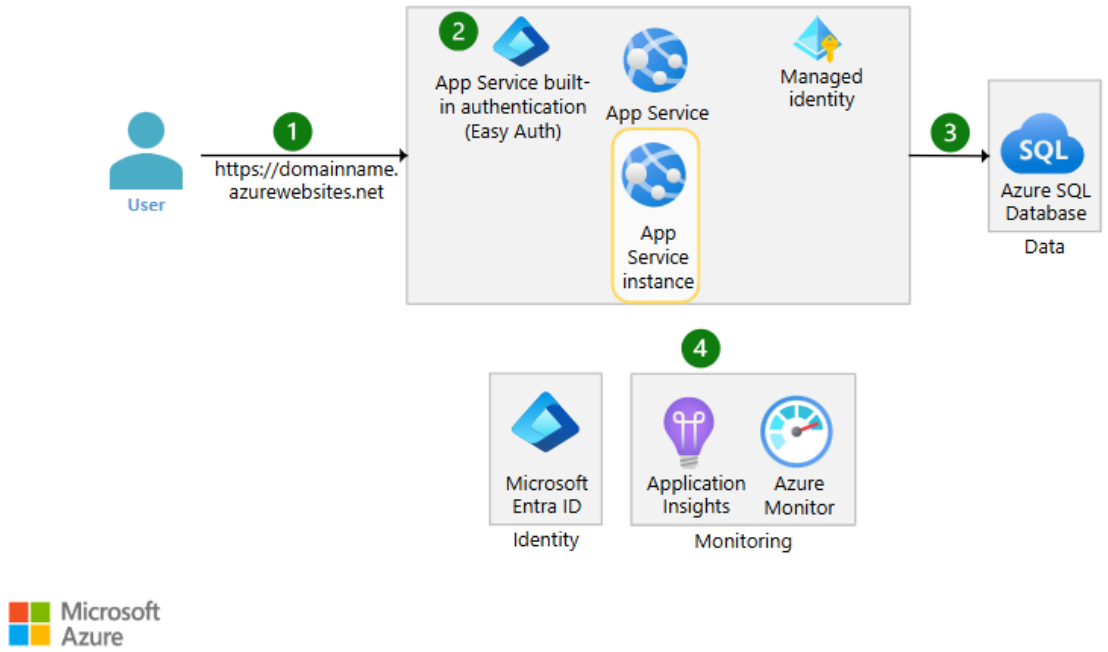
Gli elementi sotto controllo diretto di Microsoft includono:

- Sistemi di protezione fisica multilivello (badge, biometria, videosorveglianza, controllo accessi).
- Infrastruttura di rete proprietaria e sistemi di Network Management isolati.
- Hardware dei server e componenti di virtualizzazione (Hyper-V, Azure Fabric Controller).

Il **perimetro fisico** è quindi delimitato dai data center Microsoft, ma non rappresenta più il confine di sicurezza effettivo: la sicurezza è proiettata verso gli strati logici e applicativi superiori.

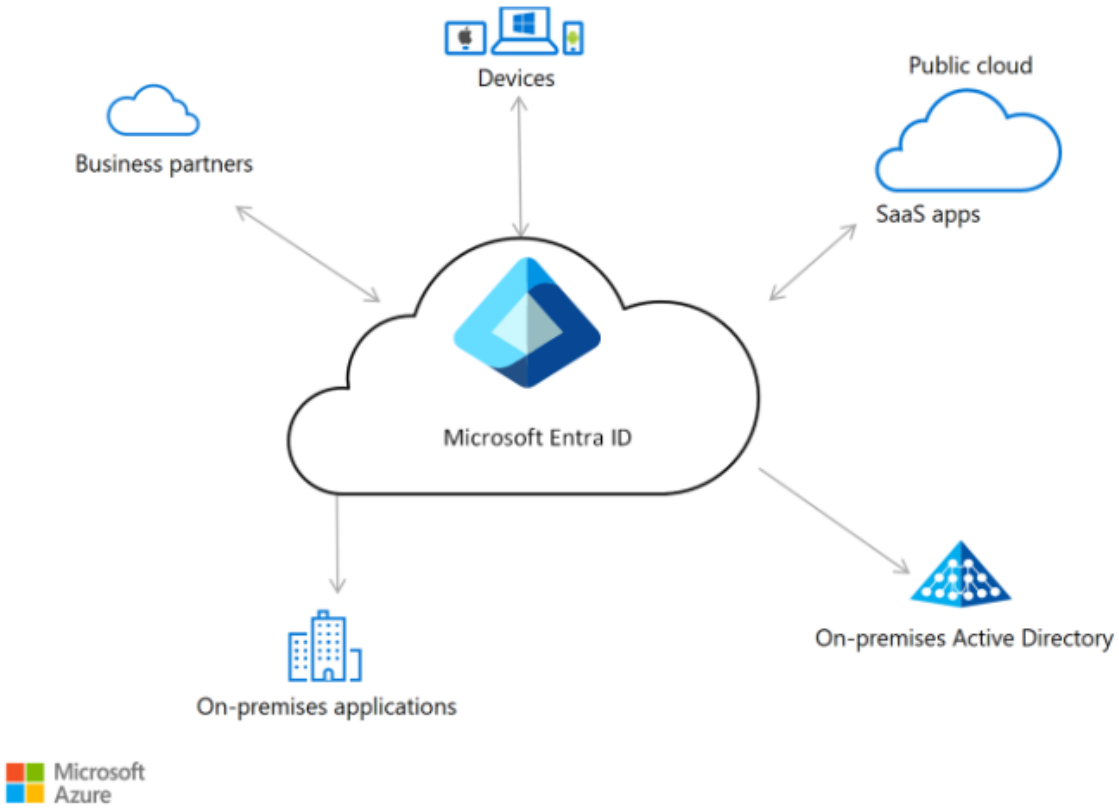
1.2 Contesto logico e di gestione

L'ambiente Azure è organizzato in **tenant**, **subscription** e **resource group**, che definiscono domini amministrativi logici. Il sistema di identità centrale è **Azure Active Directory** (oggi **Entra ID**), che costituisce il principale punto di fiducia.

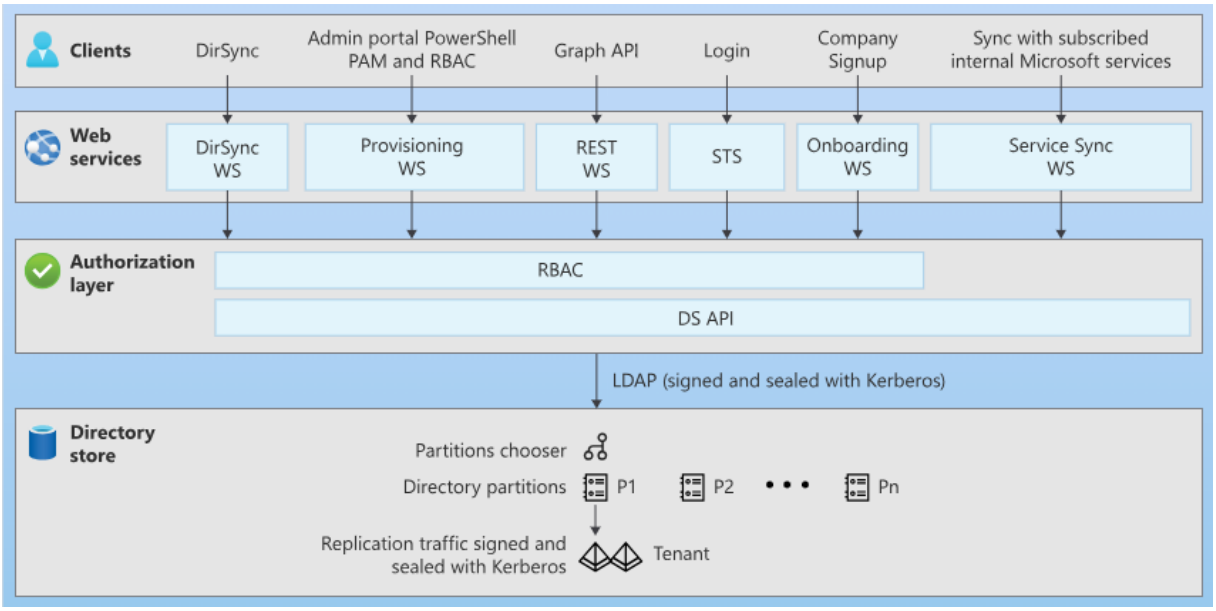


I confini logici di controllo sono stabiliti tramite:

- **Policy di accesso e autenticazione** (Conditional Access, MFA, device compliance).



- **Isolamento dei tenant** tramite separazione delle identità e segregazione delle risorse.

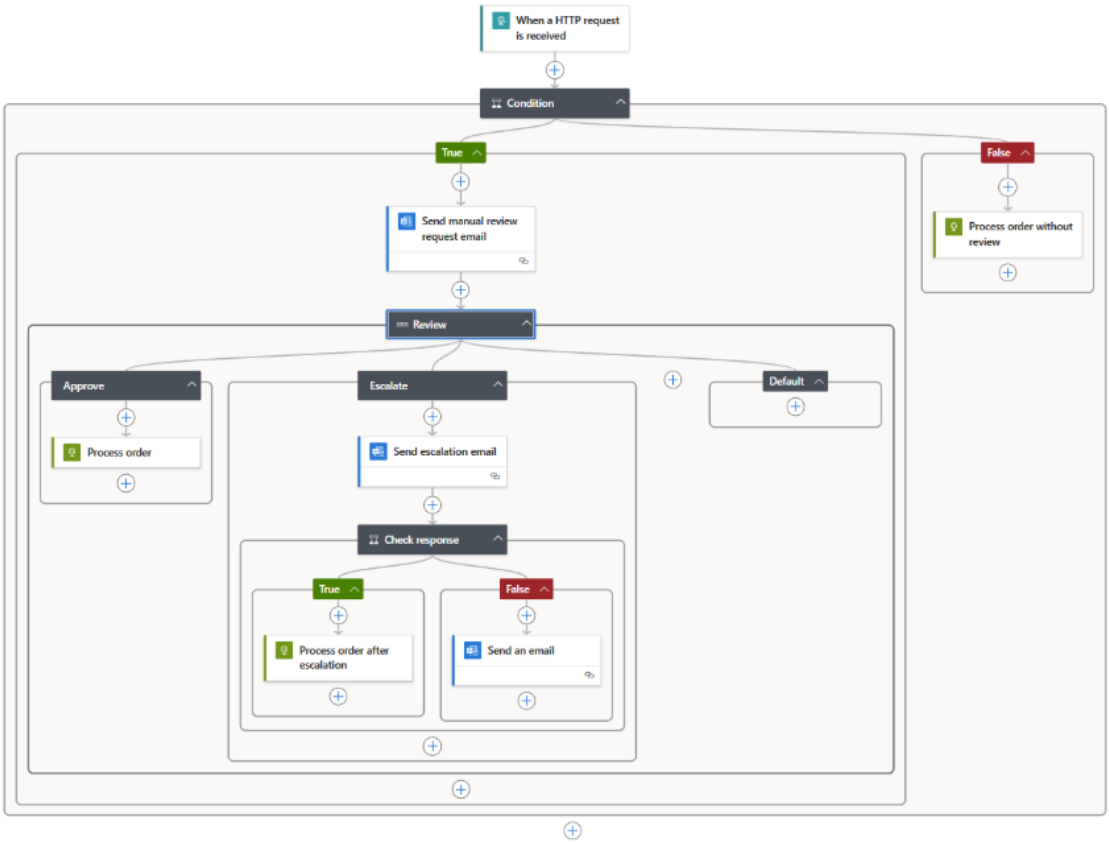


- **Micro-segmentazione di rete** attraverso Network Security Groups (NSG) e Azure Firewall.

Il **perimetro logico** è dunque dinamico e si sposta intorno all'entità autenticata (utente, servizio o dispositivo), piuttosto che intorno alla rete.

1.3 Contesto applicativo e dei servizi

Questo livello include tutte le piattaforme gestite (**PaaS** e **SaaS**) e i componenti virtuali (**VM**, container, microservizi, API) erogati da Azure.

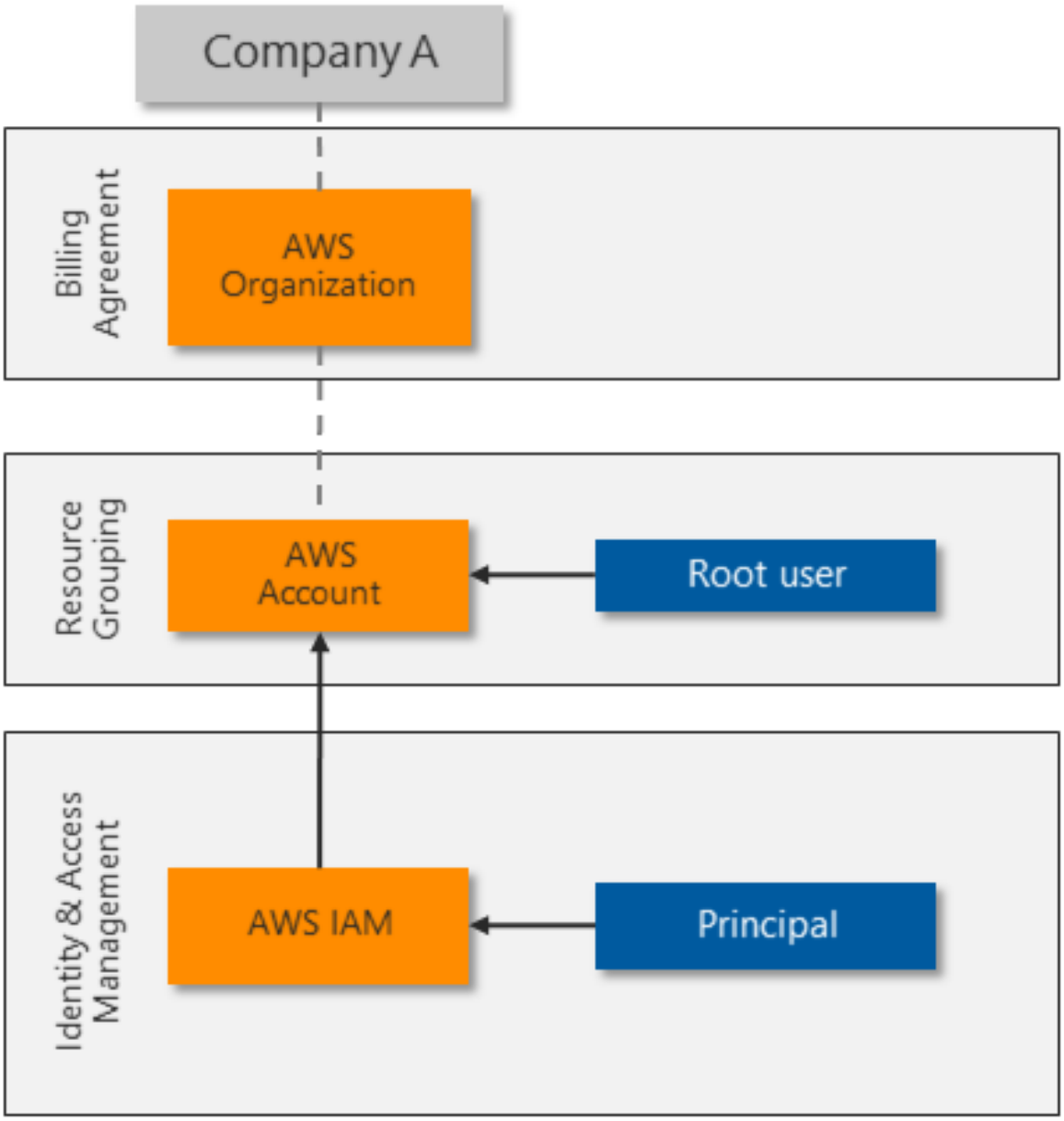


Il perimetro di controllo viene realizzato attraverso:

- **Access token** e **API gateway** che regolano le comunicazioni tra servizi.
- **Azure Policy** per la governance e la conformità.
- **Monitoraggio continuo** mediante Azure Defender e Sentinel.

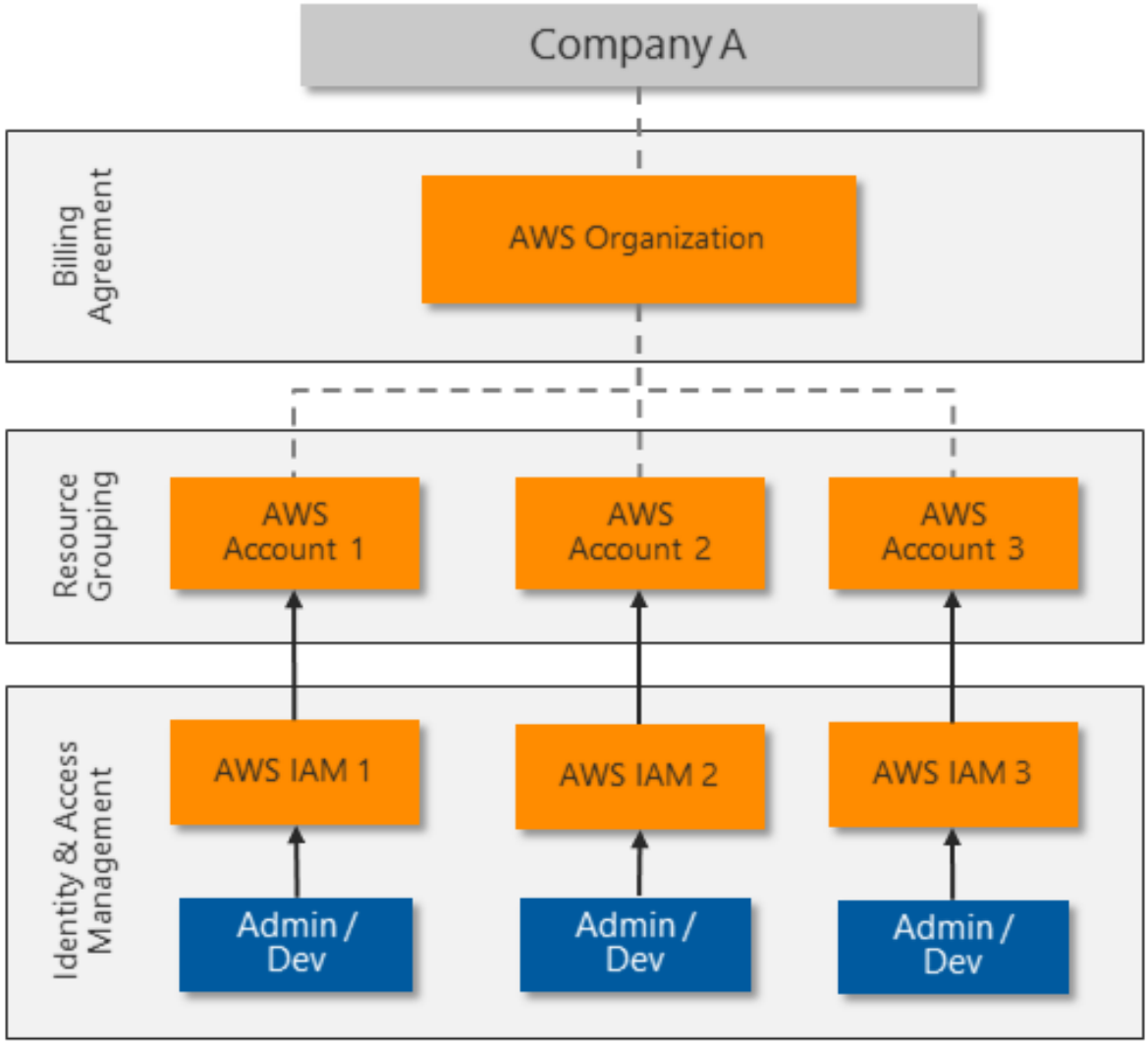
1.3.1 Azure AWS

AWS crea un archivio IAM (Identity and Access Management) separato per ogni account. Il diagramma seguente mostra la configurazione standard per un ambiente AWS con un singolo account AWS:



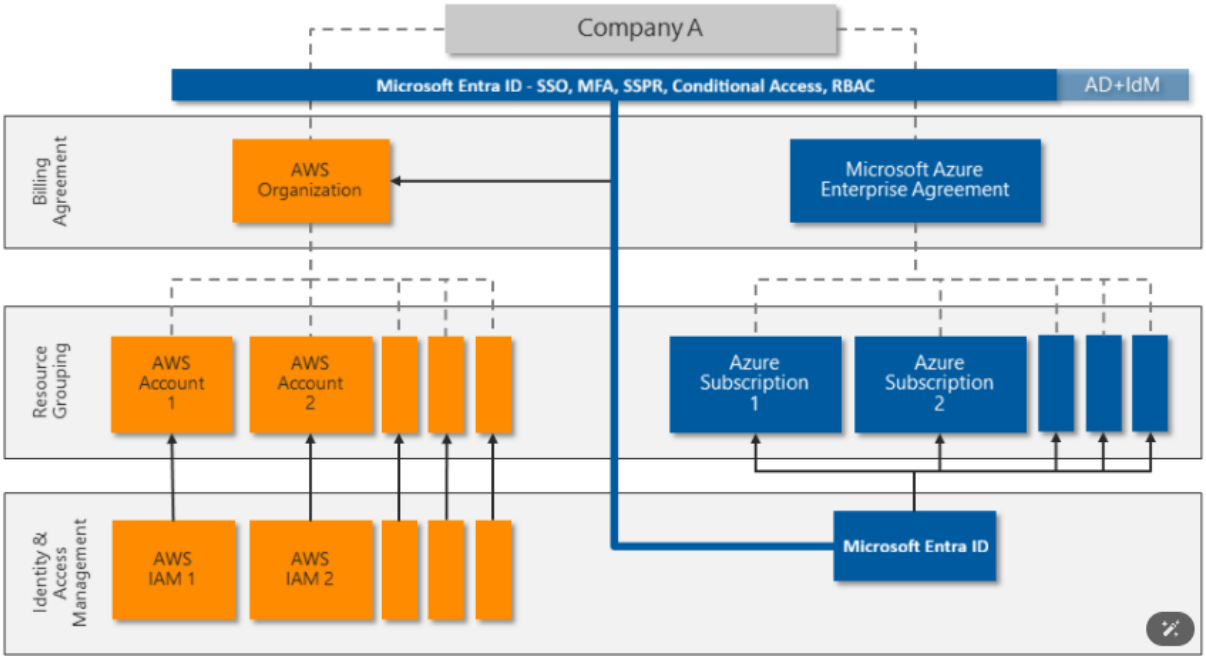
L' utente root controlla completamente l'account AWS e delega l'accesso ad altre identità. Il principal di AWS IAM fornisce un'identità univoca per ogni ruolo e utente che deve accedere all'account AWS. AWS IAM può proteggere ogni account root, principal e utente con una password complessa e un'autenticazione a più fattori di base.

Molte organizzazioni necessitano di più di un account AWS, il che crea compartimenti stagni di identità difficili da gestire:



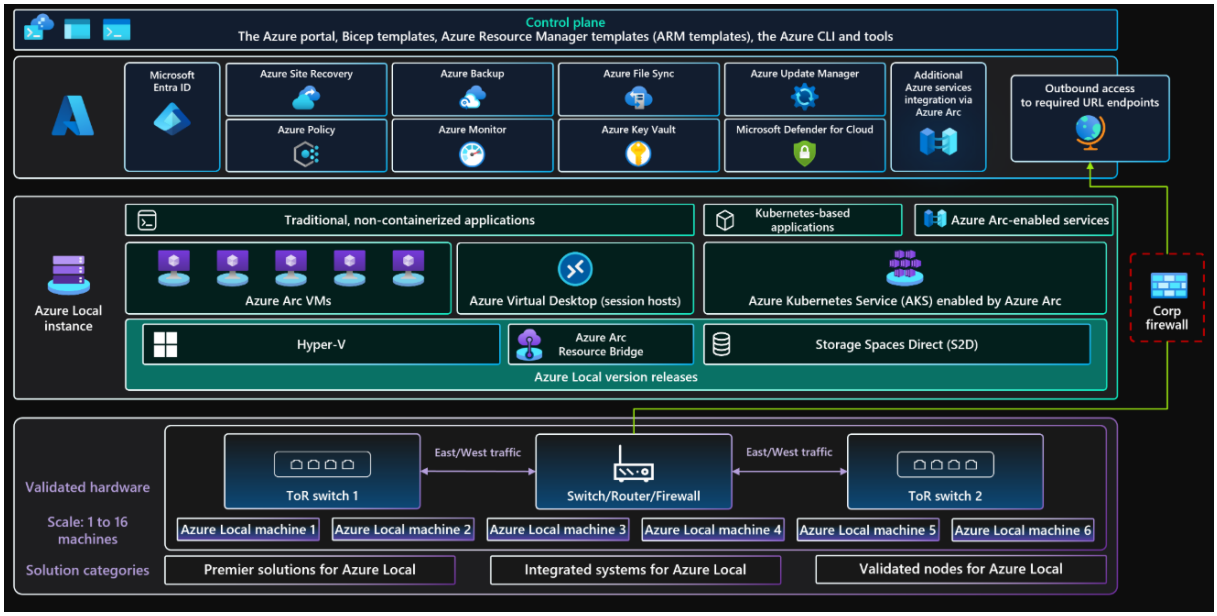
Molte organizzazioni utilizzano già l'ID Microsoft Entra per assegnare e proteggere le identità Microsoft 365 e cloud ibride. I dipendenti utilizzano le proprie identità Microsoft Entra per accedere a e-mail, file, messaggistica istantanea, applicazioni cloud e risorse locali. Integra l'ID Microsoft Entra con i tuoi account AWS per consentire ad amministratori e sviluppatori di accedere ai tuoi ambienti AWS con le loro identità esistenti.

Il diagramma seguente mostra come Microsoft Entra ID può integrarsi con più account AWS per fornire una gestione centralizzata dell'identità e degli accessi:



1.3.2 Azure Local

Questa architettura è costituita da hardware server fisico che è possibile utilizzare per distribuire istanze di Azure Local in sedi locali o periferiche. Per migliorare le funzionalità della piattaforma, Azure Local si integra con Azure Arc e altri servizi di Azure che forniscono risorse di supporto. Azure Local offre una piattaforma resiliente per distribuire, gestire e utilizzare applicazioni utente o sistemi aziendali.



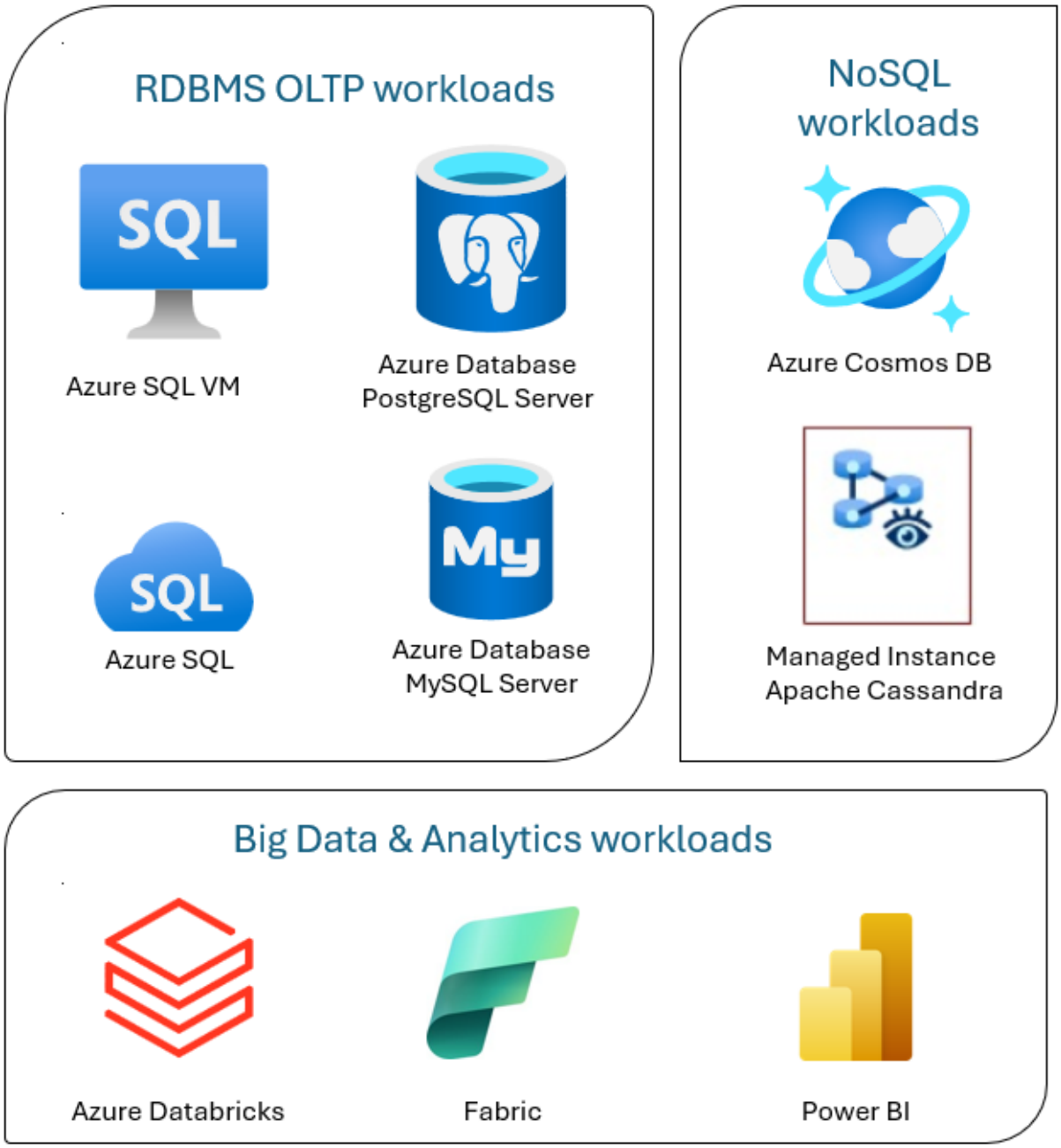
1.3.3 Azure Database

Le soluzioni di database Azure includono sistemi di gestione di database relazionali tradizionali (RDBMS e OLTP), carichi di lavoro di big data e analisi (incluso OLAP) e carichi

di lavoro NoSQL.

I carichi di lavoro RDBMS includono l'elaborazione delle transazioni online (OLTP) e l'elaborazione analitica online (OLAP). I dati provenienti da più origini all'interno dell'organizzazione possono essere consolidati in un data warehouse. È possibile utilizzare un processo di estrazione, trasformazione e caricamento (ETL) o di estrazione, caricamento e trasformazione (ELT) per spostare e trasformare i dati di origine.

Un'architettura Big Data è progettata per gestire l'acquisizione, l'elaborazione e l'analisi di dati di grandi dimensioni o complessi. Le soluzioni Big Data in genere comportano una grande quantità di dati relazionali e non relazionali, che i sistemi RDBMS tradizionali non sono adatti a memorizzare. Queste soluzioni in genere includono Data Lake, Delta Lake e lakehouse.



1.4 Sintesi concettuale del perimetro

Nel paradigma Zero Trust, il perimetro di Azure è **virtualizzato e centrato sull'identità**. Si distinguono tre livelli principali di controllo:

Tabella 1: *
Tabella di Sintesi del Perimetro di Microsoft Azure

Livello	Tipologia di perimetro	Elementi chiave di controllo
Fisico	Data center Microsoft	Accesso fisico, isolamento infrastrutturale
Logico	Tenant, subscription, identità	Policy, IAM, micro-segmentazione
Applicativo	Servizi e API Azure	Controllo di accesso per servizio, telemetria continua

2 Superficie di attacco (punti e vettori di compromissione potenziale)

La **superficie di attacco** di Azure comprende tutti i punti fisici, logici e umani attraverso cui un attore malevolo può tentare di compromettere l'infrastruttura o i servizi cloud.

3 Concetto di Superficie di Attacco Fisica

Il concetto di **"superficie di attacco fisica"** (Physical Attack Surface) si riferisce a tutti i componenti hardware e alle infrastrutture tangibili che un malintenzionato può sfruttare per compromettere un sistema, rubare dati o causare un'interruzione del servizio.

A differenza degli attacchi logici (come malware o phishing), questi attacchi richiedono una prossimità fisica o un'interferenza con l'hardware stesso.

3.1 Accesso non autorizzato ai data center

Questo è lo scenario "Mission: Impossible" della cybersecurity, raro ma con un potenziale impatto devastante. Se un malintenzionato ottiene l'accesso fisico al "cuore" della tua infrastruttura, molte difese digitali diventano inutili.

3.1.1 Come avviene

L'attacco può avvenire tramite ingegneria sociale (convincere un addetto alla sicurezza), **tailgating** (seguire un dipendente autorizzato attraverso una porta), uso di badge clonati, furto di chiavi, o persino un'effrazione forzata.

3.1.2 Impatto

Una volta all'interno, l'attaccante ha il "controllo fisico". Può:

- **Rubare hardware:** Sottrarre server, hard disk o backup tape, con conseguente furto di dati massiccio.
- **Installare hardware malevolo:** Collegare dispositivi come un **keylogger** hardware (per registrare le password digitate), un dispositivo "Rubber Ducky" (una finta chiavetta USB che esegue comandi malevoli) o un piccolo computer (come un Raspberry Pi) connesso alla rete interna per creare una backdoor persistente.
- **Sabotare:** Semplicemente staccare cavi di alimentazione o di rete, tagliare fibre ottiche o distruggere fisicamente i server (Denial of Service fisico).
- **Accedere alle console:** Collegarsi direttamente alle porte di gestione dei server (crash cart) per bypassare i controlli di rete.

3.1.3 Contromisure

Difese a strati come guardie di sicurezza, videosorveglianza (CCTV), **mantrap** (bussole di accesso che intrappolano una persona alla volta), controlli di accesso biometrici (impronte digitali, scansione della retina) e rack dei server chiusi a chiave.

3.2 Compromissione della Supply Chain Hardware

Questo è uno degli attacchi più sofisticati e difficili da rilevare. L'attacco non avviene presso la tua sede, ma molto prima che l'hardware ti venga consegnato.

3.2.1 Come avviene

Un avversario (spesso un attore statale) intercetta i dispositivi durante la produzione o la spedizione. Vengono apportate modifiche hardware non rilevabili a prima vista.

3.2.2 Impatto

- **BIOS/Firmware:** Il codice di avvio fondamentale della macchina (BIOS/UEFI) viene modificato per includere una **backdoor**. Questa backdoor si attiva *prima* che il sistema operativo (Windows, Linux) si carichi, rendendola quasi invisibile ai software antivirus e ai controlli di sicurezza standard.

- **Chip malevoli:** Un piccolo chip extra può essere saldato sulla scheda madre. Questo chip potrebbe essere progettato per intercettare dati (come le chiavi di crittografia direttamente dalla CPU), creare una connessione di rete nascosta o persino consentire uno "spegnimento" (kill switch) da remoto.

3.2.3 Contromisure

Estremamente difficili. Includono l'acquisto solo da fornitori noti e fidati (Trusted Vendors), l'uso di sigilli di garanzia (tamper-evident seals) sulle spedizioni e l'uso di tecnologie come il **Trusted Platform Module (TPM)** e l'avvio sicuro (Secure Boot) che verificano crittograficamente l'integrità del firmware a ogni avvio.

3.3 Attacchi alla Rete Fisica (Tapping)

Questo attacco prende di mira i dati "in transito" (data in transit), intercettando le comunicazioni mentre viaggiano sui cavi al di fuori delle aree protette.

3.3.1 Come avviene

I collegamenti WAN (Wide Area Network) collegano i tuoi data center tra loro o al resto di Internet. Questi cavi (spesso in fibra ottica) viaggiano in condotti sotterranei, pali telefonici o armadi di smistamento in strada. Un attaccante può localizzare questi cavi e:

- **Effettuare un "tap":** Utilizzare uno "splitter" ottico o un "vampire tap" (per cavi in rame) per copiare passivamente tutto il traffico che passa attraverso il cavo.
- **Intercettazione attiva:** Tagliare il cavo e inserire un dispositivo (un "interpositore") che può non solo leggere, ma anche modificare o bloccare il traffico (un attacco Man-in-the-Middle a livello fisico).

3.3.2 Impatto

Spionaggio industriale o governativo, furto di credenziali, intercettazione di dati sensibili (finanziari, personali, segreti commerciali) prima che raggiungano la loro destinazione sicura.

3.3.3 Contromisure

La difesa principale è la **crittografia end-to-end**. Anche se un attaccante "vede" il traffico, la crittografia (come IPsec per le VPN o MACsec a livello di link) lo rende illeggibile. Altre misure includono la sicurezza fisica dei condotti e l'uso di sistemi di monitoraggio (come OTDR per la fibra) che possono rilevare cali di segnale anomali causati da un "tap".

Conclusione

In sintesi, la superficie di attacco fisica ci ricorda che la cybersecurity non riguarda solo il software; l'integrità e la sicurezza dell'hardware sottostante sono fondamentali.

4 Definizione di Superficie di Rete

La **superficie di attacco di rete** (Network Attack Surface) in un ambiente cloud come Azure comprende tutti i punti di ingresso e di uscita di rete che un malintenzionato può scoprire e tentare di sfruttare da Internet.

Si tratta, in essenza, di qualsiasi risorsa che possiede un indirizzo IP pubblico o che è raggiungibile attraverso protocolli di rete. La gestione di questa superficie è un equilibrio tra la necessità di esporre servizi a utenti legittimi e il principio di sicurezza di "minima esposizione".

4.1 Endpoint Pubblici: I Punti di Esposizione

Qualsiasi servizio configurato per "ascoltare" su un indirizzo IP pubblico contribuisce ad allargare la superficie di attacco.

4.1.1 Endpoint dei servizi (API, Web App)

Le applicazioni web e le API (Application Programming Interfaces) esposte pubblicamente sono il bersaglio più comune. Un utente malintenzionato può tentare di sfruttare vulnerabilità nel codice dell'applicazione (es. SQL Injection, XSS) o nell'autenticazione.

4.1.2 Servizi DNS

Sebbene il DNS (Domain Name System) debba essere pubblico per definizione, può essere usato per la ricognizione. Gli aggressori enumerano i record DNS (es. `A`, `CNAME`, `MX`) per mappare l'infrastruttura di un'organizzazione, scoprendo gli indirizzi IP di server web, server di posta e altri servizi critici.

4.1.3 Servizi di Storage (es. Blob Storage)

I servizi di archiviazione di oggetti, come Azure Blob Storage, possono avere endpoint pubblici. Una configurazione errata (es. un container impostato su "accesso anonimo" o "pubblico") può portare a un'esposizione massiccia e involontaria di dati sensibili.

4.1.4 Gateway di Rete (es. Gateway VPN)

I gateway VPN e Application Gateway sono "porte" progettate per consentire l'accesso alla rete privata (VNet). Questi dispositivi sono ad alta criticità: se un aggressore riesce a

compromettere un gateway (sfruttando una vulnerabilità o rubando credenziali), ottiene un punto d'appoggio diretto all'interno della rete privata.

4.2 Vettori di Attacco Tipici

Una volta identificati gli endpoint, gli aggressori utilizzano diverse tecniche per attaccarli.

4.2.1 Attacchi DDoS (Distributed Denial of Service)

Questi attacchi mirano a sovraccaricare un endpoint (come un server web o un gateway VPN) con un volume massiccio di traffico di rete fasullo. L'obiettivo non è rubare dati, ma esaurire le risorse (CPU, larghezza di banda) e rendere il servizio inutilizzabile per gli utenti legittimi (attacco alla disponibilità).

4.2.2 Scanning delle Porte e Ricognizione

L'attaccante utilizza strumenti (come `nmap`) per "scansionare" sistematicamente gli indirizzi IP pubblici alla ricerca di porte aperte. Una porta aperta (es. 22 per SSH, 3389 per RDP) indica un servizio in ascolto, che può essere poi analizzato per debolezze note o password deboli.

4.2.3 Attacchi Man-in-the-Middle (MitM)

In un attacco MitM, l'aggressore si interpone segretamente tra l'utente e il servizio cloud. Questo può avvenire tramite DNS poisoning o compromettendo un punto della rete. Se la comunicazione non è crittografata (o se la crittografia è debole), l'attaccante può intercettare, leggere e persino modificare i dati in transito (es. rubare password o session cookie).

4.3 Strategie di Difesa e Mitigazione in Azure

La difesa in Azure si basa su un approccio "defense-in-depth" (difesa a strati) per proteggere la superficie di rete.

4.3.1 Azure DDoS Protection

Azure fornisce due livelli di protezione. Il livello **Basic**, gratuito, protegge l'intera infrastruttura Azure da attacchi volumetrici su larga scala. Il livello **Standard** è un servizio a pagamento che offre protezione avanzata e adattiva specificamente per le risorse VNet, con telemetria e avvisi, cruciale per applicazioni business-critical.

4.3.2 Crittografia del Transito (TLS)

Il protocollo **TLS (Transport Layer Security)** è la difesa primaria contro gli attacchi MitM. Imponendo l'uso di HTTPS (TLS su HTTP) per tutte le API e le applicazioni web, si garantisce che i dati scambiati tra il client e il server siano crittografati e che la loro integrità sia protetta. È fondamentale applicare configurazioni TLS moderne (disabilitando versioni obsolete come SSLv3 o TLS 1.0/1.1).

4.3.3 Isolamento della VNet (Virtual Network)

Questa è la strategia di difesa più efficace: **ridurre la superficie di attacco**.

- **Network Security Groups (NSG):** Agiscono come un firewall a livello di porta/IP. La best practice è "negare tutto" (deny-all) in entrata da Internet e consentire solo le porte strettamente necessarie (es. la porta 443 per un server web).
- **Principio di "Zero Public IP":** Ove possibile, i servizi non dovrebbero avere affatto un indirizzo IP pubblico. Servizi come Azure SQL Database o Blob Storage possono essere resi accessibili *solo* dall'interno della VNet tramite **Service Endpoints** o **Private Endpoints**. Questo rimuove completamente quel servizio dalla superficie di attacco Internet pubblica.

5 Definizione di Superficie Logica

A differenza delle superfici fisica e di rete, la **superficie di attacco logica** è astratta. Non è composta da cavi o porte di rete, ma da identità, applicazioni, protocolli e, soprattutto, dalle autorizzazioni che legano insieme questi elementi.

Questa superficie rappresenta l'interfaccia di "controllo" del sistema. In un ambiente cloud moderno come Azure, il "controllore" centrale è il sistema di gestione delle identità e degli accessi (IAM).

5.1 Target: Sistemi di Autenticazione e Autorizzazione

L'obiettivo principale della superficie logica è il provider di identità (IdP). Nel mondo Microsoft, questo è **Azure Active Directory (Azure AD)**, ora noto come **Microsoft Entra ID**.

Azure AD è il "sistema nervoso centrale" dell'ecosistema cloud:

- **Autenticazione:** Verifica l'identità dell'utente (username + password + MFA).
- **Autorizzazione:** Decide cosa un utente (o un servizio) autenticato ha il permesso di fare (es. leggere un database, eliminare una VM).

Compromettere Azure AD non significa rubare un singolo file; significa ottenere le "chiavi del regno", con il potenziale di controllare l'intera infrastruttura.

5.2 Vettori di Attacco alla Superficie Logica

Gli attacchi non mirano a un IP, ma a un'identità.

5.2.1 Credential Theft e Phishing

Questo è il metodo più comune per ottenere l'accesso iniziale. Tramite email di phishing, l'attaccante inganna un utente (spesso un amministratore) per indurlo a inserire le proprie credenziali su una pagina di login contraffatta. L'obiettivo è rubare la coppia username/password.

5.2.2 Token Hijacking (Furto di Token)

Questo attacco è più sofisticato e bypassa l'autenticazione. Dopo che un utente ha effettuato l'accesso (e ha completato l'MFA), il suo browser conserva un "token di sessione" (simile a un lasciapassare temporaneo). Se un attaccante, tramite malware sul computer dell'utente o un attacco Man-in-the-Middle, riesce a rubare questo token, può presentarlo ai servizi Azure e impersonare l'utente senza bisogno di password o MFA.

5.2.3 Privilege Escalation (Escalation dei Privilegi)

Spesso un attaccante ottiene l'accesso iniziale con un account a bassi privilegi (es. un dipendente standard). Il suo obiettivo successivo è l'"escalation": muoversi lateralmente all'interno del sistema per trovare un modo di aumentare i propri permessi, fino a diventare Amministratore Globale o Proprietario della Sottoscrizione. Questo può avvenire sfruttando configurazioni errate (es. un account di servizio con troppi permessi) o vulnerabilità nelle applicazioni.

5.3 Rischio Elevato: Accesso a Risorse Distribuite

Il rischio associato alla superficie logica è il più elevato per un motivo fondamentale: **il controllo dell'identità trascende la posizione della risorsa**.

In un attacco di rete, un aggressore potrebbe compromettere una singola Virtual Machine. In un attacco alla superficie logica, un aggressore che compromette un'identità di amministratore ottiene accesso immediato e simultaneo a *tutte* le risorse collegate a quell'identità, indipendentemente da dove si trovino:

- Può accedere a VM in diverse region (Europa, USA, Asia).
- Può leggere dati da database (Azure SQL) e storage (Blob).
- Può accedere alle caselle di posta (Microsoft 365).
- Può eliminare l'intera infrastruttura (backup, VM, account) e cancellare i log per coprire le proprie tracce.

La superficie logica è quindi il vettore che consente a un attaccante di passare da un singolo punto di compromissione al controllo totale dell'ambiente.

5.4 Mitigazione e Difesa

La protezione della superficie logica si concentra sulla protezione dell'identità:

- **Multi-Factor Authentication (MFA):** La difesa più critica contro il furto di credenziali.
- **Azure AD Conditional Access:** Politiche di accesso granulari (es. "richiedi MFA se l'utente si connette da una rete sconosciuta").
- **Principio del Minimo Privilegio (PoLP):** Gli utenti devono avere solo i permessi strettamente necessari per il loro lavoro.
- **Privileged Identity Management (PIM):** Gli amministratori non hanno privilegi elevati permanenti; devono "richiederli" per un tempo limitato (accesso Just-in-Time).

6 Definizione di Superficie Applicativa

La **superficie di attacco applicativa** si riferisce alla totalità del codice eseguibile e delle interfacce (API, form web, endpoint) che un utente malintenzionato può tentare di manipolare. A differenza della superficie di rete (che riguarda porte e protocolli), questa superficie riguarda la *logica* stessa dell'applicazione.

In un'architettura cloud, questa superficie è distribuita e complessa, in quanto non risiede più su un singolo server monolitico.

6.1 Coinvolgimento di PaaS, SaaS e Microservizi

Il modello di servizio determina chi è responsabile della sicurezza del codice.

6.1.1 Servizi PaaS (Platform-as-a-Service)

In un modello PaaS (es. Azure App Service, Azure Functions), il provider (Microsoft) gestisce il sistema operativo e l'infrastruttura sottostante, ma **l'utente è responsabile del codice dell'applicazione** e delle sue dipendenze. È qui che le vulnerabilità classiche del codice prosperano.

6.1.2 Servizi SaaS (Software-as-a-Service)

In un modello SaaS (es. Microsoft 365, Dynamics 365), la superficie di attacco si sposta dal codice (che è gestito dal provider) alla **configurazione**. Rischi comuni includono un controllo degli accessi troppo permissivo, configurazioni errate della condivisione e l'abuso di API esposte dal servizio.

6.1.3 Microservizi

Questa architettura scompone un'applicazione monolitica in molti servizi più piccoli (es. un servizio per i pagamenti, uno per gli utenti, uno per il catalogo). Se da un lato migliora la resilienza, dall'altro **moltiplica la superficie di attacco**:

- Ogni microservizio espone un'API, che diventa un potenziale punto di ingresso.
- La comunicazione "Est-Ovest" (tra i servizi stessi) diventa un nuovo vettore di attacco se non è adeguatamente protetta (es. tramite autenticazione mTLS).

6.2 Possibili Vulnerabilità

Queste sono vulnerabilità che sfruttano una gestione non sicura degli input da parte dell'applicazione.

6.2.1 SQL Injection (SQLi)

L'attaccante "inietta" comandi SQL malevoli all'interno di un campo di input (es. un form di ricerca). Se l'applicazione concatena ingenuamente l'input dell'utente con la query al database, l'attaccante può bypassare l'autenticazione, rubare l'intero contenuto del database (es. `' OR '1'='1`) o persino modificarlo.

6.2.2 Command Injection

Simile a SQLi, ma ancora più pericolosa. L'attaccante inietta comandi della shell del sistema operativo (es. `; rm -rf /`). Se l'applicazione passa l'input dell'utente a uno script di sistema, l'attaccante può ottenere l'esecuzione di codice arbitrario (RCE) sul server che ospita l'applicazione.

6.2.3 Deserializzazione Insicura

Le applicazioni moderne spesso "serializzano" dati (convertono oggetti complessi in un formato stringa o binario per l'archiviazione o la trasmissione). La deserializzazione è il processo inverso. Se un attaccante può fornire un payload serializzato malevolo, e l'applicazione lo deserializza senza validarlo, l'attaccante può istanziare oggetti imprevisti, portando a RCE.

6.3 Rischio di Escalation da Container Compromessi

Questo è uno scenario critico nelle architetture basate su microservizi, che spesso utilizzano orchestratori come **Azure Kubernetes Service (AKS)**.

Il processo di attacco (attack chain) è il seguente:

1. **Compromissione Iniziale:** L'attaccante trova una vulnerabilità applicativa (es. Command Injection) in un microservizio esposto su Internet.

2. **Accesso al Container:** Sfruttando la vulnerabilità, ottiene una shell *all'interno* del container che esegue quel microservizio.

3. **Container Breakout (Fuga dal Container):** L'obiettivo ora è evadere dall'isolamento del container per raggiungere il "Nodo" host sottostante (la VM che esegue il container). Questo è possibile se il container è stato configurato in modo insicuro (es. eseguito come utente `root`, con privilegi `-privileged`, o con volumi sensibili del nodo montati).

4. **Compromissione del Nodo e del Cluster:** Una volta sul nodo host, l'attaccante può rubare le credenziali usate dal nodo per comunicare con il **Kubernetes API Server**. Se ottiene queste credenziali, può tentare un'escalation per diventare **Cluster Admin**, ottenendo di fatto il controllo totale di *tutte* le applicazioni in esecuzione sull'intero cluster.

Questo dimostra come una singola vulnerabilità applicativa possa, attraverso una catena di escalation, portare alla compromissione totale di un'infrastruttura di microservizi.

7 Definizione di Superficie Umana

La **superficie di attacco umana e di gestione** (spesso chiamata "The Human Element") è la più imprevedibile e la più difficile da proteggere. Non è definita da hardware o software, ma dalle **persone**, dai loro privilegi, dalle loro conoscenze e dai loro comportamenti.

Questa superficie rappresenta tutti gli individui che interagiscono con il sistema, dai più privilegiati ai meno privilegiati. In un ambiente cloud, dove il confine tra gestione interna ed esterna è labile, questa superficie include diversi attori.

7.1 Gli Attori: I Punti di Interazione

La superficie umana è composta da cerchi concentrici di fiducia e privilegio.

7.1.1 Amministratori (Alto Privilegio)

Questo gruppo include gli Amministratori Globali di Azure AD, i Proprietari delle Sottoscrizioni e, in un certo senso, gli ingegneri di supporto Microsoft che potrebbero (con autorizzazione) accedere all'infrastruttura di back-end. Una compromissione di questi account è **catastrofica** e porta alla perdita totale di controllo, riservatezza e integrità.

7.1.2 Operatori e Sviluppatori (Medio Privilegio)

Questo gruppo (es. team DevOps, amministratori di database, operatori IT) possiede privilegi elevati ma specifici (es. "Collaboratore VM", "Amministratore del database SQL"). Sono un obiettivo primario perché hanno accesso pratico ai sistemi che contengono dati e logica di business.

7.1.3 Utenti Finali (Basso Privilegio)

Questo è il gruppo più vasto. Include i dipendenti standard che utilizzano servizi SaaS (come Microsoft 365) o applicazioni line-of-business. Hanno privilegi minimi, ma rappresentano la **superficie di attacco più ampia** e sono il bersaglio preferito per gli attacchi di accesso iniziale (es. phishing).

7.2 Minacce e Vettori Principali

Gli attacchi a questa superficie sono di natura psicologica, manipolativa o accidentale.

7.2.1 Errore Umano

Questa è una minaccia involontaria ma estremamente comune.

- **Misconfiguration:** Un operatore applica un Network Security Group (NSG) errato, esponendo una porta RDP a Internet. Un sviluppatore carica accidentalmente chiavi di accesso (access keys) su un repository GitHub pubblico.
- **Scarsa Igiene di Sicurezza:** Riuso della stessa password, mancata applicazione di patch, invio di dati sensibili all'email sbagliata.

L'errore umano non è un attacco in sé, ma *crea* la vulnerabilità che un altro attacco (es. scansione di rete) può sfruttare.

7.2.2 Phishing (e Ingegneria Sociale)

Questo è il vettore di attacco *attivo* più comune contro la superficie umana. L'obiettivo è ingannare l'utente per indurlo a compiere un'azione che comprometta la sicurezza.

- **Credential Theft:** Indurre l'utente (spesso un utente finale) a inserire le proprie credenziali su un falso portale di login di Microsoft 365.

- **Spear Phishing:** Un attacco mirato e altamente personalizzato contro un amministratore o un operatore, utilizzando informazioni specifiche per guadagnare la sua fiducia.
- **MFA Fatigue:** Se l'MFA è attivo, l'attaccante (che ha già la password) invia una raffica di richieste di approvazione MFA, sperando che l'utente, infastidito, ne approvi una per errore.

7.2.3 Insider Threat (Minaccia Interna)

Questa è la minaccia più difficile da rilevare, poiché l'autore possiede già un accesso legittimo.

- **Insider Malizioso:** Un amministratore o un operatore scontento che abusa dei propri privilegi per sabotare l'infrastruttura (es. eliminando i backup) o rubare dati per profitto personale.
- **Insider Compromesso:** Un utente (qualsiasi dei tre attori) la cui identità è stata rubata (es. tramite phishing). L'attaccante esterno ora agisce *come* un insider, rendendo difficile distinguere le sue azioni da quelle legittime.
- **Insider Negligente:** Un utente che, per convenienza, aggira le policy di sicurezza (es. condividendo un account di servizio, usando una rete Wi-Fi pubblica non sicura per accedere a sistemi sensibili).

7.3 Mitigazione della Superficie Umana

Poiché questa superficie non può essere "patchata" come il software, le difese sono un misto di tecnologia, processi e formazione.

- **Tecnologia:** Applicazione rigorosa dell'MFA, uso dell'Accesso Condizionale (Conditional Access) per bloccare accessi rischiosi, implementazione del Principio del Minimo Privilegio (PoLP) e uso di Privileged Identity Management (PIM) per l'accesso just-in-time degli amministratori.
- **Processi e Formazione:** Formazione continua anti-phishing (Security Awareness Training), procedure di "four-eyes" (doppia approvazione) per modifiche critiche, e monitoraggio attivo dei log per comportamenti anomali (UEBA - User and Entity Behavior Analytics).

8 Conclusione

Nel modello Zero Trust adottato da Azure, il perimetro non è più una linea statica, ma la somma di **domini di fiducia continuamente verificati**. La superficie di attacco, ampia

e multidimensionale, richiede una validazione continua dell'identità, una segmentazione rigorosa e un monitoraggio costante di ogni livello dell'infrastruttura.

Tabella 2: *
Tabella di Sintesi della Superficie di Attacco di Microsoft Azure

Livello	Esempi di vettori di attacco	Natura del rischio
Fisico	Accesso ai data center, supply chain	Bassa probabilità, alto impatto
Rete	DDoS, port scanning, MitM	Alta esposizione, mitigabile
Logico	Credential theft, privilege escalation	Critico, punto di ingresso primario
Applicativo	Vulnerabilità software, API abuse	Alta complessità, rischio laterale
Umano	Phishing, errori di configurazione	Costante e trasversale