neacademy

DATAFEST

Microsegmentazione di rete e Zero Trust nei data center

Fabrizio Bruzzese

Head of Network Project Team – **Engineering Group**

3 - 4 GIUGNO 2026

L’Era dello Zero Trust e la Microsegmentazione

Navigare il cambio di paradigma: dalla sicurezza perimetrale alla protezione avanzata dei workload.

Il Fondamento Teorico: L’Architettura Zero Trust

“Mai fidarsi, verificare sempre. Ogni carico di lavoro (workload), processo e microservizio è responsabile della propria sicurezza.”

Assunzione di Violazione

Operare con la certezza matematica che la rete interna sia già ostile. Nessun indirizzo IP garantisce l’affidabilità.

Accesso Least-Privilege

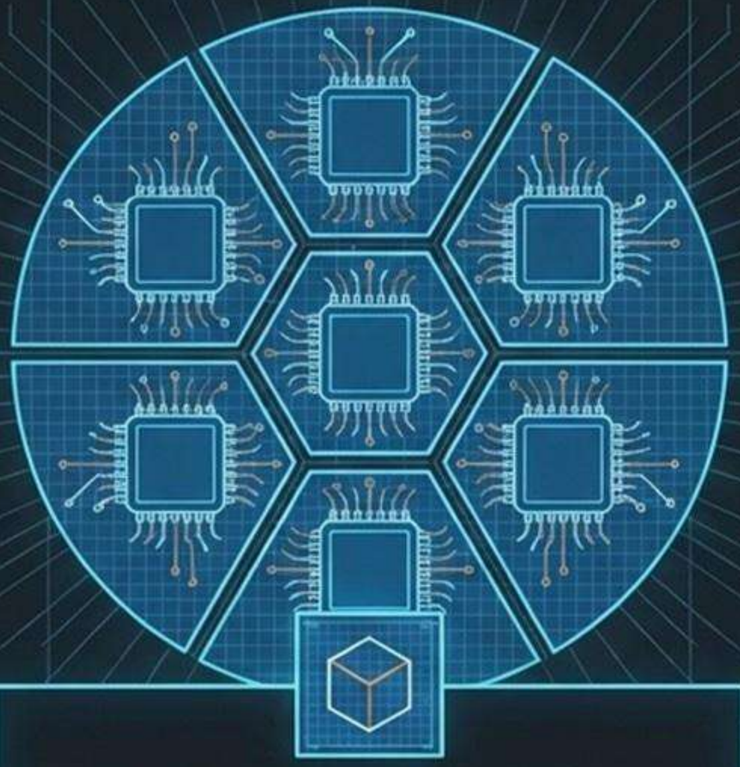
Concedere esclusivamente le autorizzazioni di rete strettamente necessarie, bloccando tutto il resto (Default Deny).

Validazione Continua

Le regole non si basano su IP statici, ma su identità crittografiche, etichette (Ruolo, Ambiente) e contesto applicativo.

Cos'è la Microsegmentazione?

La divisione della rete in segmenti iper-granulari e isolati a livello di singolo workload, applicando policy di sicurezza basate sul principio del privilegio minimo.



Zero Trust

Nessuna fiducia implicita, ispezione continua e validazione di ogni connessione

Isolamento Granulare

Campi di forza software attorno a ogni singola applicazione o processo

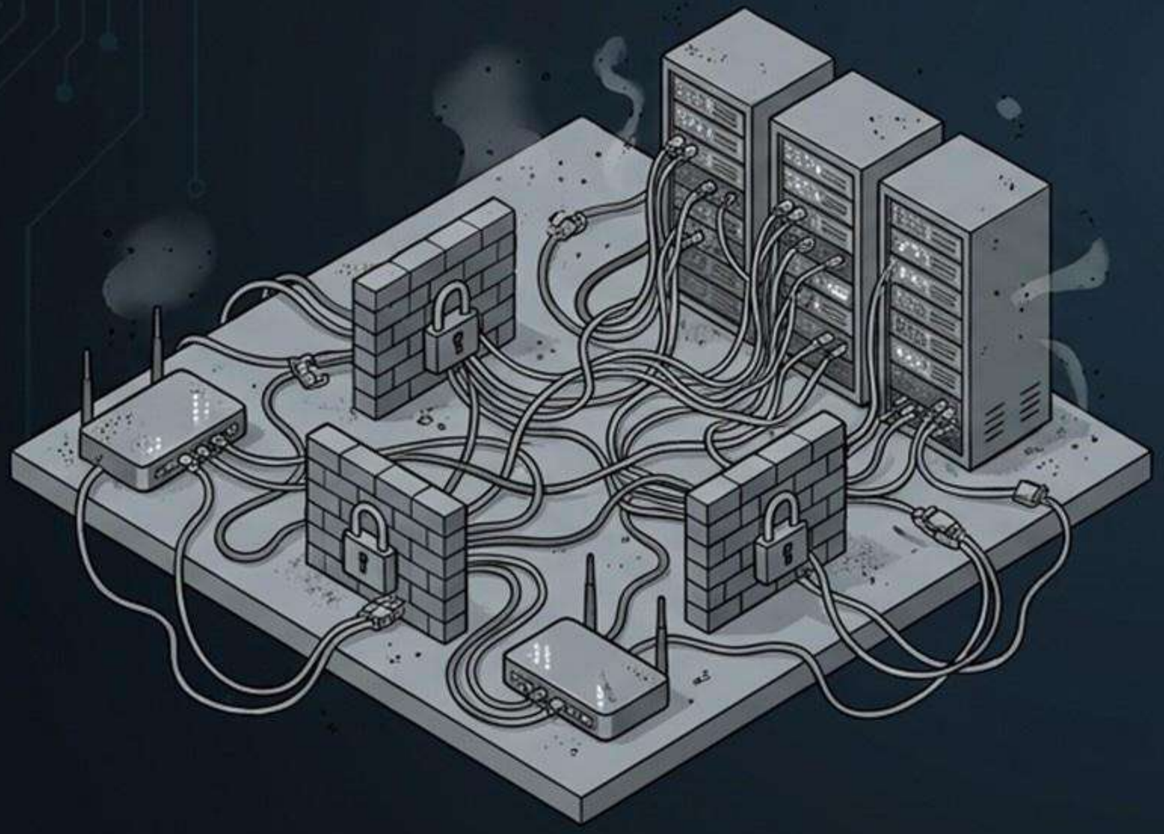
Identità, Non IP

Policy basate su metadati e identità logiche, non su indirizzi di rete fisici

Evoluzione Architetturale: Rete vs. Identità

Passato: Segmentazione di Rete

- Basata su costrutti fisici (IP, VLAN, Subnet)
- Richiede ampie modifiche all'architettura di rete
- Struttura rigida, molto complessa da scalare nel cloud

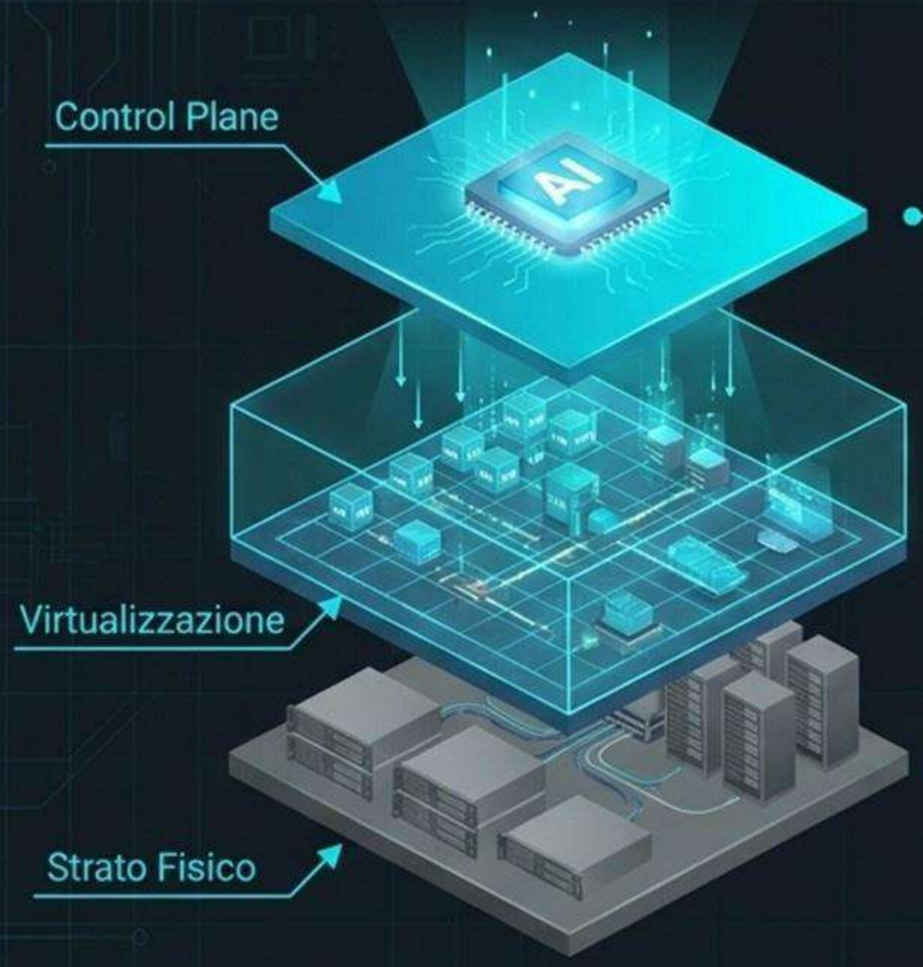


Presente: Microsegmentazione Moderna

- Basata sull'identità del workload logico (Tag, Ruoli)
- Totalmente agnostica rispetto all'infrastruttura sottostante
- Dinamica: le policy seguono il workload ovunque si sposti

L’Astrazione del Controllo

Separare la Sicurezza dall’Infrastruttura



Indipendenza Topologica

La microsegmentazione via software crea isolamenti logici completamente indipendenti dalla rete sottostante, dalle VLAN o dalle subnet fisiche.

La Policy Segue il Dato

Se una VM viene spostata da un data center on-premise al public cloud, la sua bolla di sicurezza crittografica e le relative policy viaggiano con essa in tempo reale.

Performance vs Latenza

Supera i limiti operativi delle tradizionali regole iptables, offrendo un motore ottimizzato specificamente per processare enormi volumi di traffico Est-Ovest senza colli di bottiglia.

Tassonomia: I Tre Approcci alla Microsegmentazione

Basata sulla Rete (SDN)

Controllo a livello di hypervisor (Kernel). Indipendente dal sistema operativo guest.

Esempio: VMware NSX

Basata sull'Host (Agent)

Software installato sul SO. Eccellente per visibilità Layer 7 e sistemi legacy.

Esempi: Akamai Guardicore, Illumio

Cloud-Native

Progettata per container effimeri e cluster Kubernetes. Sfrutta controlli nativi.

Esempio: Tigera Calico

La Trappola del Movimento Laterale

Il perimetro è compromesso, l'interno è vulnerabile

La Cecità

I firewall tradizionali non riescono a ispezionare il traffico est-ovest su larga scala. Le reti interne piatte offrono libertà di movimento agli attaccanti.

L'Espansione

Il ransomware sfrutta questa mancanza di attrito per muoversi lateralmente, trasformando la compromissione di un singolo endpoint in una violazione su vasta scala.

Il Rischio Operativo

La segmentazione tramite VLAN o reti tradizionali richiede tempi lunghissimi, modifiche infrastrutturali pesanti e rischia di interrompere le applicazioni critiche.

L’Anatomia dell’Attacco: Il Ciclo Vitale del Ransomware

1. Infiltrazione:

L’attaccante supera le difese perimetrali colpendo un bersaglio morbido.

2. Ricognizione:

Scansione silente della rete interna per mappare server e database.

3. Movimento Laterale

L’attaccante si sposta orizzontalmente (Est-Ovest) da workload a workload, effettuando Privilege Escalation.

4. Esfiltrazione e Cifratura:

Furto dei dati ad alto valore ed esecuzione del payload ransomware.

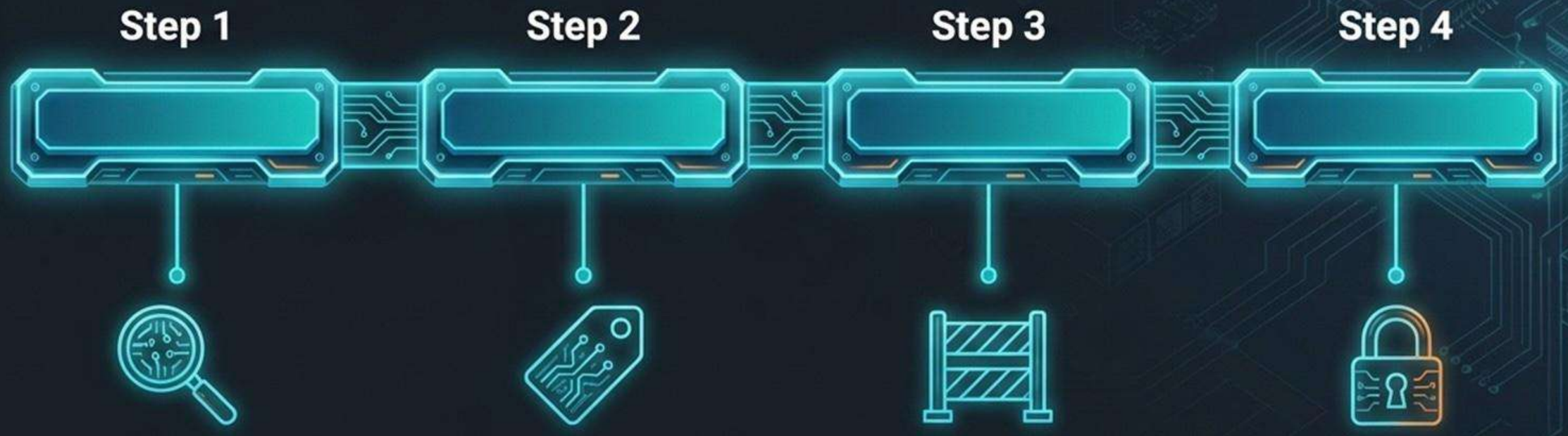
Il movimento laterale è il fulcro operativo del ransomware. Senza la capacità di spostarsi liberamente all’interno del datacenter, l’attacco rimane isolato e inefficace.

L’Evoluzione dell’Enforcement: Layer 4 vs. Layer 7

	Approccio Tradizionale (Layer 4)	Approccio Moderno (Layer 7 Process-to-Packet)
Focus	 Indirizzi IP, Porte, Protocolli (es. 10.100.0.10 tcp/80).	 Identità del processo, utente, servizio, metadati (es. env=prod, app=database).
Limiti	 Cieco al contesto. Gli indirizzi IP sono effimeri. Non rileva attacchi su porte legittime (es. Ransomware su RDP/SMB).	 Visibilità granulare fino all’eseguibile del sistema operativo (es. blocca una shell non autorizzata sulla porta 80).
Risultato	 Falsi positivi elevati, policy impossibili da scalare, vulnerabilità al piggybacking.	 Policy precise, adattamento dinamico ai container, protezione totale dalle anomalie applicative.

Metodologia di Implementazione: Roadmap Esecutiva

Una transizione sicura e calibrata per non interrompere la continuità operativa del business.



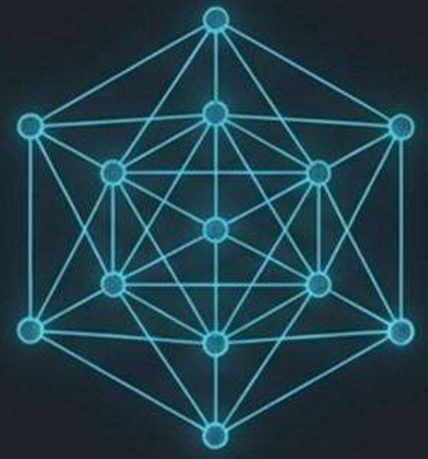
Step 1: Visibilità Globale - Mappare silenziosamente tutte le comunicazioni e le dipendenze applicative in tempo reale.

Step 2: Etichettatura (Labeling) - Raggruppare logicamente i workload in base all'ambiente e al ruolo (es. env=produzione).

Step 3: Ring-Fencing - Creare policy iniziali per isolare le applicazioni più critiche (es. database) dal resto della rete.

Step 4: Policy Zero Trust - Passaggio finale automatizzato a regole 'Deny All', permettendo solo il traffico esplicitamente autorizzato.

Sintesi e Prospettive Future: La Sicurezza Autonoma

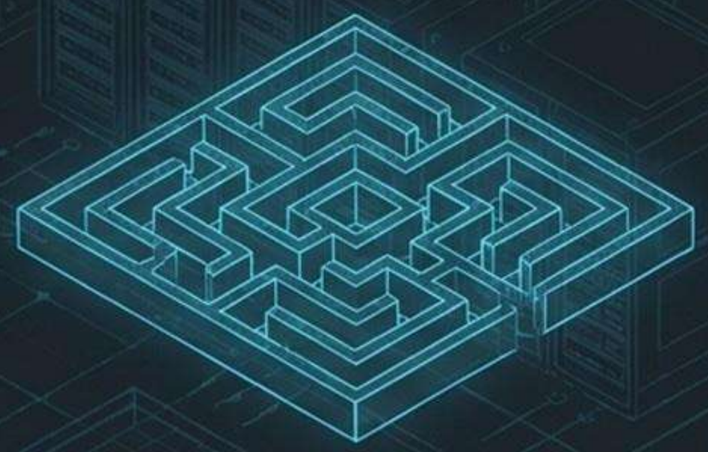


Da IP a Identità

La sicurezza non si basa più sulla topologia fisica, ma sull'identità crittografica e sui processi (Layer 7).

Isolamento Dinamico

Il contenimento delle violazioni e la prevenzione del movimento laterale sostituiscono l'illusione di un perimetro impenetrabile.



Governance Guidata dall'AI

Il Machine Learning è l'unico strumento capace di mappare dipendenze complesse e generare policy Zero Trust senza interrompere le operazioni.

La microsegmentazione trasforma i datacenter da reti reattive e vulnerabili a topologie trasparenti, resilienti dal punto di vista operativo e matematicamente ostili al movimento laterale delle minacce.

neacademy

DATAFEST

Fabrizio Bruzzese

Head of Network Project Team
Engineering

THANK YOU!

fabrizio.bruzzese@eng.it
+39 348 1511410