DESCRIZIONE DELLA SOLUZIONE AKAMAI

Gestione degli accessi e delle identità degli utenti con la segmentazione

Un ulteriore livello di controllo critico per i moderni data center ibridi

Ridurre la superficie di attacco per gli ambienti IT odierni non significa semplicemente creare controlli rigorosi per applicazioni specifiche, isolandole per proteggerle. Questo è un ottimo primo passo e può sicuramente essere utile per alcuni casi di utilizzo come il contenimento delle violazioni o la conformità. Tuttavia, senza una soluzione di segmentazione che supporti la gestione degli accessi e delle identità degli utenti, la vostra organizzazione avrà un punto cieco di sicurezza che include ogni singola persona che utilizza o accede alla vostra rete.

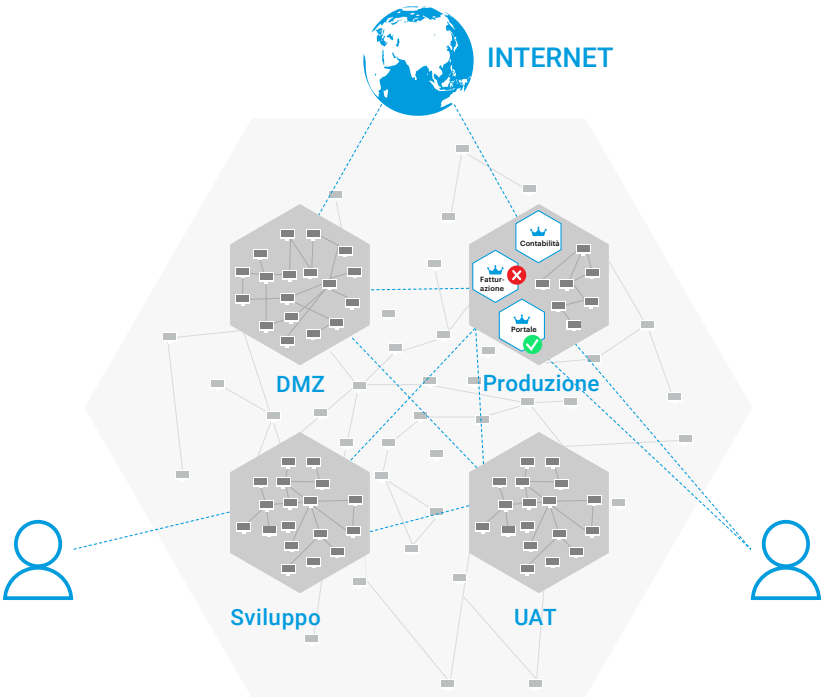
Una volta implementata la segmentazione delle applicazioni, il prossimo passo essenziale è quello di sfruttare la vostra soluzione di segmentazione per creare policy su chi può accedere a queste applicazioni, assicurando che siano altrettanto sicure su ogni altra architettura della vostra rete.

Radley e Pets at Home - Segmentazione per gli accessi e le identità degli utenti

Gestione degli accessi degli utenti

Utilizzando un gruppo di utenti di Active Directory, Akamai Guardicore Segmentation può controllare l'accesso degli utenti a qualsiasi applicazione o carico di lavoro, da qualsiasi ambiente. Gruppi di utenti specifici hanno accesso a server specifici, su porte o processi specifici, mentre altri no. I gruppi di utenti dispongono delle proprie autorizzazioni, mentre tutti gli altri accessi possono essere bloccati. Senza la necessità di un firewall centralizzato, potete utilizzare il controllo granulare degli accessi tra i carichi di lavoro su segmenti specifici della rete.

Controllo degli accessi degli utenti



Perché la segmentazione per il controllo degli accessi degli utenti?

Controllo degli accessi degli utenti in qualsiasi luogo
Le policy funzionano su laptop, desktop, VDI, server virtuali o bare metal e infrastruttura cloud

Segmentazione definita dal software
Nessuna modifica alla rete o all'architettura, nessun cavo, nessun downtime del server e nessun riavvio dei sistemi

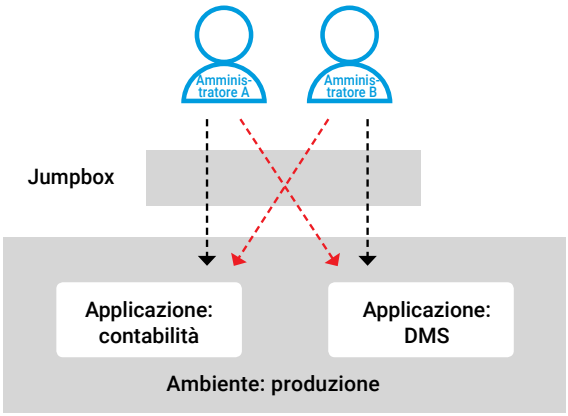
Rapidità e potenza
Le policy sono semplici e intuitive da creare e hanno effetto immediato sia sulle nuove sessioni che su quelle attive

Convenienza
Rispetto a casi di utilizzo simili riscontrati con l'infrastruttura jumpbox tradizionale, è stata dimostrata una riduzione dei costi fino al 60%.

Akamai

Gestione dell'accesso simultaneo degli utenti

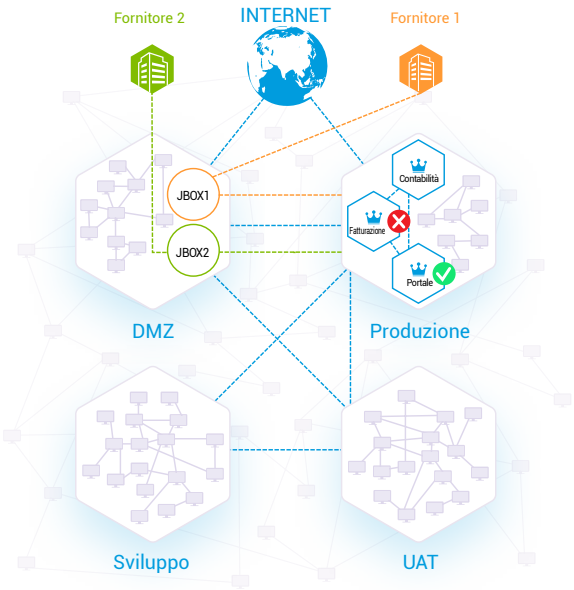
Gli amministratori possono accedere a diverse applicazioni tramite lo stesso jumpbox o terminal server, anche quando sono connessi contemporaneamente. Nel frattempo, le diverse policy funzioneranno in modo ottimale, consentendo a un utente l'accesso in base ai propri diritti, mentre l'altro utente rimarrà bloccato, senza interrompere il relativo servizio o l'accesso per entrambi gli utenti.



Controllo degli accessi di terze parti

In base all'identità dell'utente, Akamai Guardicore Segmentation può controllare la gestione degli accessi di terze parti, ad esempio di fornitori esterni o provider SaaS. Grazie ai gruppi di utenti, è possibile definire policy di accesso per ogni connessione di terze parti sia per il data center che per applicazioni specifiche, concedendo solo le autorizzazioni necessarie all'utente per il proprio ruolo.

Controllo degli accessi di terze parti



Insieme, la segmentazione delle applicazioni e la gestione degli accessi e delle identità degli utenti offrono il massimo vantaggio per proteggere il moderno data center aziendale.

Volete sapere come funzionano in sinergia? Contattateci per parlare con uno dei nostri esperti.