

STORIE DI CLIENTI AKAMAI

Un sistema sanitario di grandi dimensioni sceglie Akamai per migliorare il suo approccio alla conformità e per passare al cloud



Visibilità completa della rete



La segmentazione nelle infrastrutture IT



L'adozione sicura di nuove tecnologie

Riepilogo del cliente

Un sistema sanitario di grandi dimensioni cliente di Akamai è responsabile della protezione di oltre 6000 asset e dati dei pazienti da potenziali minacce.

Requisiti/sfide aziendali

Anche se l'organizzazione intendeva migrare alcuni carichi di lavoro importanti su Microsoft Azure, gli addetti al suo reparto IT hanno dovuto affrontare diversi ostacoli che si sono frapposti ad un'agevole adozione del cloud.

L'ambiente esistente presentava diversi rischi alla sicurezza, tra cui una rete relativamente semplice in cui i dispositivi dell'IoMT (Internet of Medical Things) potevano accedere in modo non sorvegliato al data center e disponevano di una policy BYOD (Bring Your Own Device) ormai consolidata. In questa situazione, una possibile violazione poteva causare facilmente una notevole diffusione laterale dell'attacco in grado di compromettere i dati dei pazienti e dei pagamenti presenti in altre applicazioni business-critical. Inoltre, considerando l'isolamento minimo, questo sistema aveva reso la valutazione della conformità per i revisori un'attività manuale che richiedeva un esame scrupoloso dei registri di sicurezza.

Ugualmente frustrante era la mancanza di visibilità sul traffico e sulle dipendenze delle applicazioni che stava compromettendo i tentativi di spostare i carichi di lavoro su Azure.

Perché Akamai?

L'utilizzo di VLAN o firewall per rimediare all'attuale mancanza di visibilità e alle sfide alla sicurezza dell'organizzazione avrebbe implicato un notevole livello di impegno e coordinamento tra diversi team già sotto pressione per l'esecuzione delle modifiche necessarie alla rete.

Pertanto, quando il team Akamai è riuscito a dimostrare che un approccio di segmentazione basato su software avrebbe potuto esaminare in modo granulare l'ambiente diversificato dell'organizzazione e applicare coerentemente apposite policy di segmentazione ai carichi di lavoro on-premise e nel cloud, le parti interessate hanno fissato il budget da spendere e i responsabili IT hanno deciso di passare alla fase di acquisto.

 Large Healthcare System

Settore
Assistenza sanitaria

Soluzione
[Akamai Guardicore Segmentation](#)

Vantaggi principali

- Prevenzione del movimento laterale non autorizzato
- Protezione delle applicazioni critiche
- Semplificazione e accelerazione della conformità
- Migrazione sicura verso il cloud



Vantaggi della soluzione Akamai Guardicore Segmentation

Semplificazione e accelerazione della microsegmentazione

Poiché Akamai Guardicore Segmentation utilizza un approccio basato su software indipendente dall'infrastruttura sottostante, il team addetto alla sicurezza del cliente è stato in grado di accelerare il progetto di segmentazione separatamente, limitando l'impatto su altri gruppi del reparto IT.

Con la nuova piattaforma, l'organizzazione è riuscita a isolare le applicazioni di importanza critica in modo rapido e a restringere strettamente l'accesso dei dispositivi al data center senza problemi di downtime e senza la necessità di apportare modifiche alle applicazioni o alla rete. Grazie alla nuova visibilità sui dati cronologici e in tempo reale, l'organizzazione ora può facilmente dimostrare ai revisori che tutte le risorse regolamentate sono isolate in modo efficace. Attualmente, l'azienda gestisce la sicurezza del suo data center con due soli dipendenti.

Finalmente, mappando le dipendenze delle applicazioni e creando le policy necessarie, il sistema sanitario è riuscito a conseguire i suoi obiettivi per l'adozione del cloud, garantendo, al contempo, la sicurezza delle future migrazioni di carichi di lavoro verso il cloud.

Per ulteriori informazioni, visitate il sito akamai.com/guardicore.



Sarebbe preferibile presentare a tutti i potenziali clienti del settore sanitario la soluzione [Akamai], cosicché possano vedere tutto il traffico del data center da un'unica panoramica e capire come sia semplice creare e applicare policy di sicurezza in ambienti cloud ibridi.

- Responsabile della sicurezza IT di un sistema sanitario di grandi dimensioni