DESCRIZIONE DEL PRODOTTO AKAMAI

Akamai Guardicore Segmentation

Ferma il movimento laterale con una visibilità granulare e i controlli di microsegmentazione

L'infrastruttura IT aziendale continua ad evolversi dai tradizionali data center on-premise alle architetture cloud e cloud ibride con un mix di piattaforme e modelli di distribuzione delle applicazioni. Questa trasformazione digitale sta aiutando molte organizzazioni a raggiungere una maggiore flessibilità aziendale, ridurre i costi delle infrastrutture e favorire il lavoro remoto, ma sta creando anche una superficie di attacco più ampia e complessa che non presenta un perimetro ben definito. Ogni singolo server, ogni macchina virtuale, ogni istanza cloud e ogni endpoint ora sono diventati vulnerabili. Inoltre, con la crescita di minacce come i ransomware e le vulnerabilità zero-day, i criminali stanno diventando più abili nel movimento laterale verso obiettivi di alto valore, quando non riescono addirittura a penetrare all'interno dei loro sistemi.

Akamai Guardicore Segmentation fornisce il modo più semplice, rapido e intuitivo per applicare i principi del modello Zero Trust alla vostra rete. Questa soluzione è progettata per fermare il movimento laterale con la visibilità delle attività negli ambienti IT, l'implementazione di precise policy di microsegmentazione e il rapido rilevamento di possibili violazioni.

VANTAGGI PER LE AZIENDE

- Prevenire i ransomware
- Adottare il modello Zero Trust
- Accelerare la conformità
- Isolare le applicazioni di importanza critica
- Garantire la sicurezza delle migrazioni sul cloud
- Salvaguardare i dipendenti remoti
- Proteggere gli endpoint
- Spostarsi oltre i firewall interni

Principali funzionalità della soluzione

Segmentazione granulare e basata sull'intelligenza artificiale

Implementate le policy con pochi clic utilizzando i consigli dell'intelligenza artificiale, modelli per la correzione del ransomware e altri comuni casi di utilizzo, nonché precisi attributi del carico di lavoro come processi, utenti e nomi di dominio

Visibilità cronologica e in tempo reale

Associate flussi e dipendenze delle applicazioni fino ai livelli di utenti e processi su base cronologica o in tempo reale

Ampio supporto di piattaforme

Garantite la copertura di sistemi operativi moderni e tradizionali in server bare-metal, macchine virtuali, container, IoT e istanze cloud

Etichettatura delle risorse flessibile

Aggiungete maggiori informazioni sul contesto con una gerarchia personalizzabile per garantire visibilità, applicazione e integrazione con gli strumenti di coordinamento e i database di gestione della configurazione e per sfruttare le potenzialità di un'etichettatura automatizzata

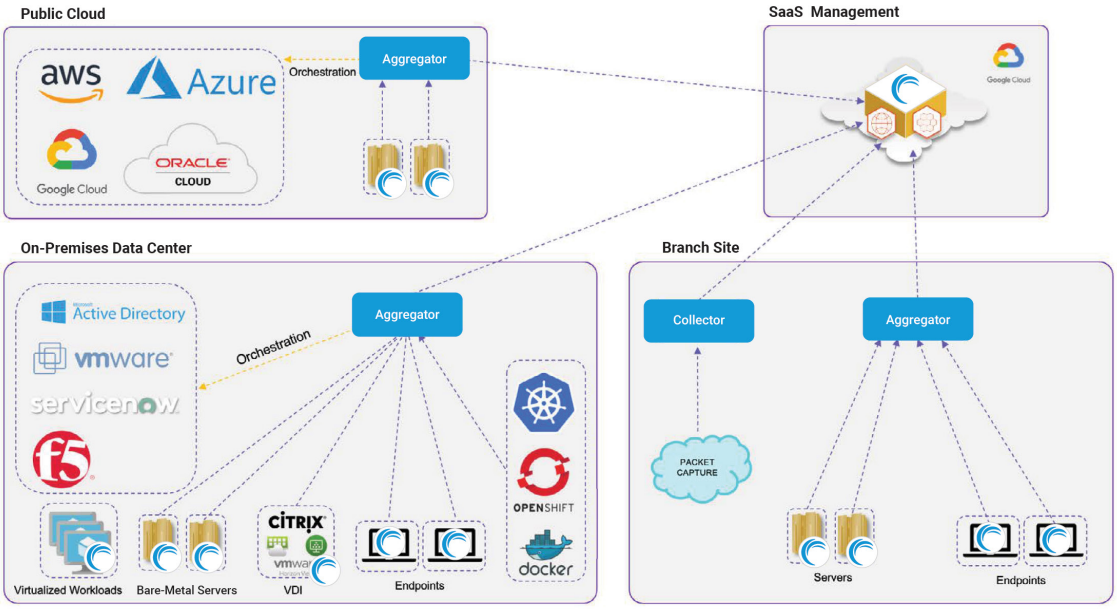
Più metodi di rilevamento

Integrazione con l'intelligence sulle minacce, con i sistemi di difesa e con le funzionalità di rilevamento delle violazioni per ridurre il tempo di risposta agli incidenti

Come funziona

Akamai Guardicore Segmentation raccoglie informazioni dettagliate sull'infrastruttura IT di un'organizzazione tramite un mix di sensori basati su agenti, strumenti di raccolta dei dati basati sulla rete, registri di flussi cloud privati e virtuali forniti da provider di servizi cloud e integrazioni compatibili con le funzionalità senza agenti. Il contesto rilevante viene aggiunto a queste informazioni tramite un processo di etichettatura flessibile e altamente automatizzato che include l'integrazione con origini dati pre-esistenti, come i sistemi di coordinamento e i database di gestione della configurazione.

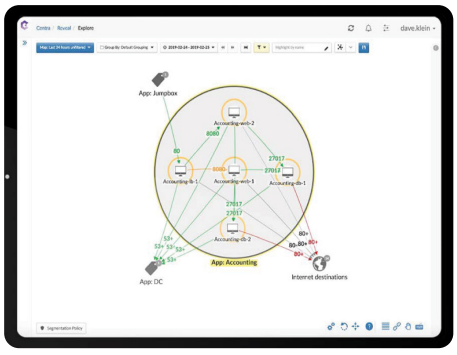
Topologia dell'infrastruttura



La maggior parte dei clienti utilizza la gestione SaaS, ma sono disponibili anche opzioni di gestione on-premise.

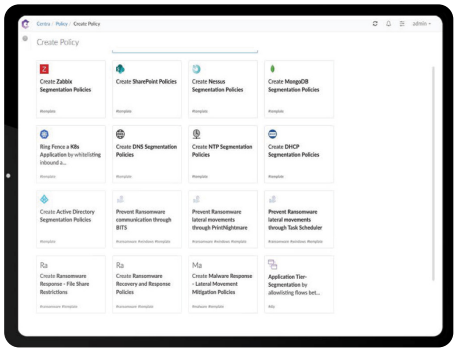
Mappa della rete

La soluzione crea una mappa visiva dinamica dell'intera infrastruttura IT che consente ai team addetti alla sicurezza di visualizzare le attività con una granularità a livello di utenti e processi in tempo reale o su base cronologica. Queste informazioni dettagliate, insieme ai workflow delle policy basate sull'intelligenza artificiale, rendono la creazione delle policy di segmentazione rapida, intuitiva e basata sui carichi di lavoro reali.



Modelli

La creazione delle policy è semplificata grazie all'utilizzo di modelli predefiniti per i casi di utilizzo più comuni. L'applicazione delle policy viene completamente svincolata dall'infrastruttura sottostante, in modo da facilitare la creazione o la modifica delle policy di sicurezza senza complessi cambiamenti della rete o problemi di downtime. Inoltre, le policy seguono il carico di lavoro ovunque si trovi, sia nei data center on-premise che nel cloud pubblico. Le nostre funzionalità di segmentazione sono integrate con alcune sofisticate funzioni di difesa dalle minacce e di rilevamento delle violazioni, nonché con Akamai Hunt, il nostro servizio gestito di ricerca delle minacce.



Protezione completa su vasta scala

Tutti gli ambienti

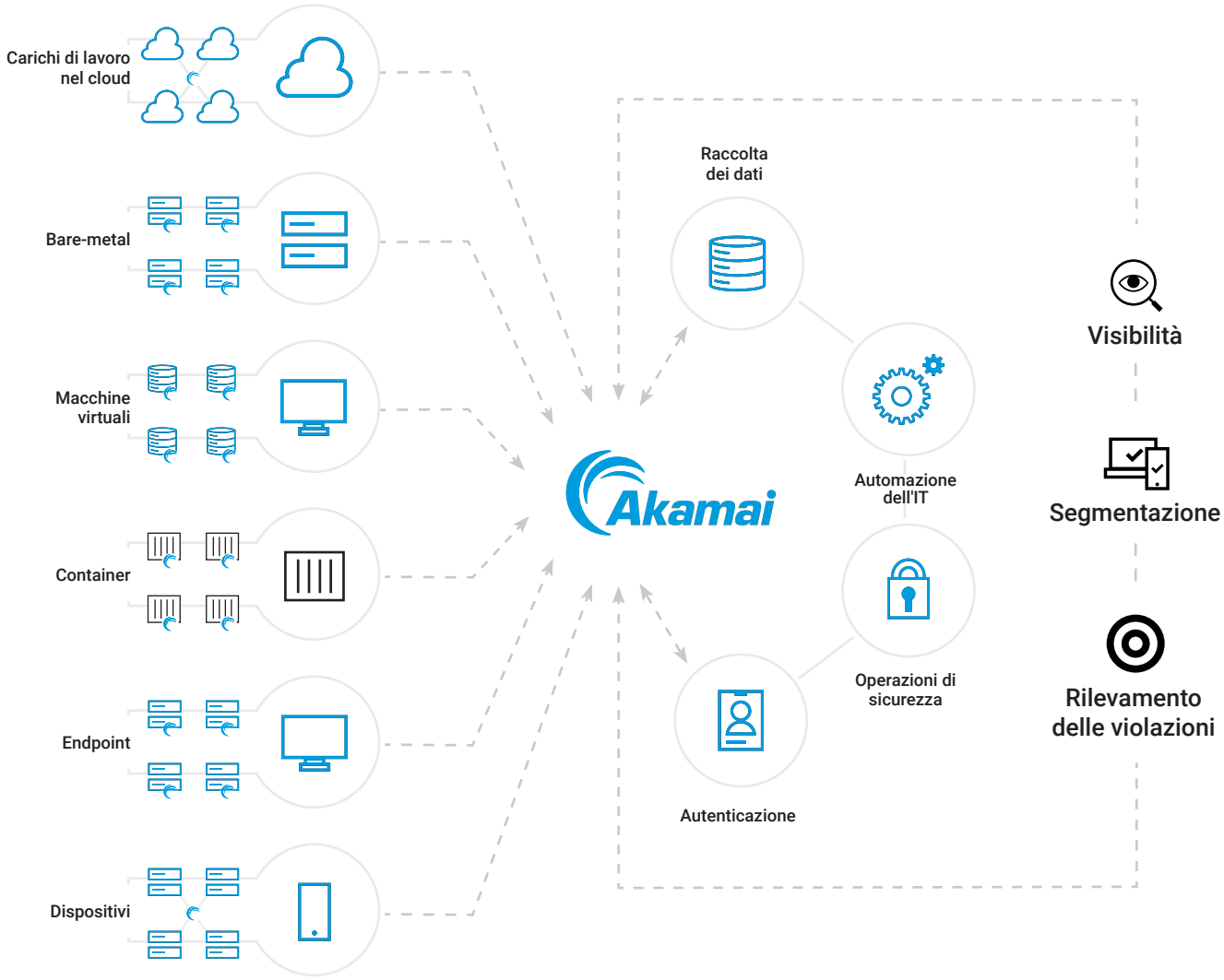
Proteggete i carichi di lavoro nei complessi ambienti IT con una combinazione di carichi di lavoro on-premise, macchine virtuali, sistemi tradizionali, container e strumenti di coordinamento, istanze di cloud pubblico/privato e dispositivi IoT/OT

Sicurezza semplificata

Semplificate la gestione della sicurezza con un'unica piattaforma in grado di fornire visibilità della rete, segmentazione, difesa dalle minacce, funzionalità di rilevamento delle violazioni e applicazione guidata delle policy per le iniziative Zero Trust

Scalabilità e performance aziendali

Iniziate con una protezione mirata delle vostre risorse digitali più importanti fino a proteggere l'intera azienda senza complessità, modifiche all'infrastruttura o colli di bottiglia nelle performance



Tecnologie e piattaforme supportate

- La soluzione Akamai Guardicore Segmentation è progettata per integrarsi con la vostra infrastruttura esistente.
- Il nostro supporto del sistema operativo si espande continuamente in base alle esigenze dei nostri clienti.
- Visitate la nostra pagina relativa ai partner tecnologici per un elenco completo delle nostre integrazioni.

Sistemi operativi

Linux

Apple

Microsoft

Unix

Provider di cloud pubblico

Hypervisor

Coordinamento hypervisor

Gateway di sicurezza

Coordinamento e motori dei container

Browser per console web

Requisiti minimi di sistema e memoria

Management Server
32 GB RAM, 8 vCPUs, 530 GB

Aggregator
4 GB RAM, 4 vCPUs, 30 GB

Deception Server
32 GB RAM, 8 vCPUs, 100 GB

ESC Collector
2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Per ulteriori informazioni su Akamai Guardicore Segmentation o per richiedere una demo del prodotto personalizzata, visitate il sito akamai.com/guardicore.