DESCRIZIONE DELLA SOLUZIONE AKAMAI

Confidential computing: proteggere i dati in uso

Di fronte alla portata, alla scala e alla sofisticazione sempre maggiori delle minacce, i team addetti alla sicurezza riescono in genere a vincere la sfida, soprattutto quando si tratta di crittografare i dati mentre vengono trasferiti e limitare l'accesso quando vengono archiviati. Risulta sempre più evidente, tuttavia, che i team devono proteggere i dati anche mentre vengono attivamente modificati, letti o elaborati; in altri termini, devono proteggere i *dati in uso*.

Questa lacuna nella protezione dei dati in uso sta diventando sempre più importante alla luce dell'evoluzione del computing e dello sviluppo dell'intelligenza artificiale. La diffusione del computing ibrido e multicloud ha ampliato le modalità di raccolta e archiviazione dei dati da parte delle organizzazioni. Allo stesso tempo, per avvalersi dell'intelligenza artificiale, le organizzazioni utilizzano enormi set di dati, che spesso includono quelli più preziosi e sensibili, in ambienti in cui non vengono crittografati né protetti.

Questi rischi stanno alimentando l'interesse per il confidential computing, un approccio alla sicurezza che garantisce la crittografia e la protezione corrette dei dati sensibili utilizzati da applicazioni, processi o servizi.

Le API aumentano la complessità

Le API proliferano perché svolgono funzioni critiche in due aree in cui le aziende continuano a investire: ambienti e servizi cloud e modelli di intelligenza artificiale. Nel cloud, le API sono essenziali per consentire alle tecnologie di comunicare e condividere i dati. Per quanto riguarda l'intelligenza artificiale, i Large Language Model (LLM) utilizzano le API per accedere ai dati e combinarli per svolgere attività complesse come la comprensione del linguaggio naturale e la generazione di testo.

Purtroppo, i team addetti alla sicurezza non dedicano alle API la stessa attenzione che riservano alle applicazioni e all'infrastruttura. I criminali approfittano di questa lacuna nella sicurezza: l'84% delle organizzazioni ha subito incidenti di sicurezza delle API negli ultimi 12 mesi[1]. Per proteggere i dati sensibili a cui accedono tutte le API correlate al cloud e all'intelligenza artificiale, le aziende devono disporre di funzionalità di sicurezza delle API complete nei loro ambienti di confidential computing.

Chiudere tutte e tre le porte

Anche quando i dati archiviati e in transito sono sotto chiave, un'altra porta, quella dei dati in uso, può ancora rimanere aperta, esponendo le aziende a rischi.

Nel confidential computing, i dati vengono elaborati in un ambiente ritenuto affidabile a livello hardware. Con le API, le organizzazioni possono implementare le proprie istanze private di apprendimento automatico create appositamente per proteggere il traffico API invece di utilizzare il servizio API di un cloud pubblico, riducendo drasticamente la superficie di attacco. Eseguire una soluzione per la sicurezza delle API in un ambiente di confidential computing crea un ulteriore livello di sicurezza. Anche se una parte del sistema viene compromessa, i dati all'interno dell'ambiente protetto rimangono al sicuro. L'esecuzione dell'analisi delle API su questi dati in un ambiente affidabile è più sicura ed elimina i rischi presenti negli ambienti tradizionali.

Questa combinazione di intelligenza artificiale, sicurezza delle API e confidential computing aiuta a impedire che entità non autorizzate, come l'hypervisor, il proprietario dell'infrastruttura del sistema host o chiunque abbia accesso fisico, possano visualizzare o modificare il

Vantaggi per il business

Sicurezza dei dati potenziata
Limitate l'accesso ai dati in uso con controlli rigorosi, riducendo la superficie di attacco e proteggendo i processi sensibili basati su API dagli accessi non autorizzati

Protezione per le API
Eseguite analisi approfondite del traffico API senza rinunciare alla crittografia dei dati sensibili in uso, riducendo il rischio di esposizione durante il monitoraggio

Maggiore conformità
Rispettate le rigorose normative globali sulla protezione dei dati in costante evoluzione, garantendo la conformità agli standard governativi e del settore

1. Akamai, Studio sull'impatto della sicurezza delle API, 2024

codice o i dati durante l'esecuzione. Questo protegge sia dalle minacce interne (come amministratori di sistema malintenzionati o carichi di lavoro eseguiti su un'infrastruttura non affidabile) sia da quelle esterne (come i criminali informatici che approfittano delle vulnerabilità).

I vantaggi

Con la proliferazione delle minacce alle API e il bersaglio allettante costituito dai dati in uso, gli attacchi non si faranno attendere a lungo. Le organizzazioni lungimiranti stanno iniziando ad adottare il confidential computing per una serie di motivi:

- Limitare in partenza l'accesso ai dati in uso, attraverso controlli rigorosi
- Analizzare il numero crescente di API in modo sicuro
- Soddisfare nuovi e più rigorosi requisiti di conformità in materia di protezione dei dati in tutto il mondo, grazie ai controlli messi a disposizione dalla tecnologia di confidential computing

Il confidential computing è particolarmente prezioso per chi opera in settori altamente regolamentati, come un'azienda di servizi finanziari che vuole tutelare le transazioni online o un'azienda sanitaria che protegge i dati dei pazienti. Questo approccio può aiutare anche un fornitore di software indipendente a salvaguardare un modello di intelligenza artificiale distribuito ai clienti in più sedi, dall'edge al cloud. In realtà, ogni organizzazione IT aziendale che esegue analisi in tempo reale sui propri dati essenziali deve prendere in considerazione il confidential computing.

Come possiamo aiutarvi insieme ai nostri partner

Per essere efficace, il confidential computing richiede una serie integrata di soluzioni che operano in stretta collaborazione per fornire controllo e protezione completi. Akamai, insieme ai suoi partner Intel e IBM, garantisce la sicurezza dei dati in uso a partire dal livello hardware fino al cloud e alle API.

Per prima cosa, Intel® TDX (Trust Domain Extension) fornisce ambienti di esecuzione affidabili che:

- Proteggono dalle intrusioni esterne, che si tratti di criminali o di entità non malintenzionate che tuttavia non dovrebbero avere accesso
- Migliorano la sicurezza del software che controlla la tecnologia utilizzata per creare risorse virtuali nel cloud, come reti, server e storage
- Aggiungono un importante livello di sicurezza intorno alle persone che gestiscono questi sistemi distribuiti, riducendo il rischio di errori in buona fede e la possibilità di attività illecite all'interno del sistema

Inoltre, la verifica e i token di Intel Tiber™ Trust Authority consentono alle organizzazioni di limitare e controllare l'accesso ai dati in uso non crittografati.

La soluzione Akamai API Security fornisce un inventario delle API utilizzate nell'azienda, quindi monitora e rileva il modo in cui vengono utilizzate. Rileva e blocca automaticamente le richieste API dannose analizzando comportamenti e modelli del traffico, neutralizzando efficacemente le minacce sull'edge della rete senza alcun intervento manuale. Ciò consente una protezione in tempo reale dagli attacchi alle API, come violazioni dei dati, accessi non autorizzati e abusi della logica.

Insieme, i motori di apprendimento automatico remoti di Akamai e i processori Intel Xeon® su IBM Cloud Virtual Server, a loro volta protetti da Intel TDX e certificati da Intel Tiber Trust Authority, offrono un ambiente privato iperscalabile progettato per impedire a qualsiasi minaccia esterna di accedere ai dati non crittografati nella fase finale del loro utilizzo, che si tratti di attacchi con bot basati su intelligenza artificiale o di hacker umani.

È venuto il momento di proteggere i dati in uso

Le organizzazioni hanno bisogno di un ambiente altamente affidabile per proteggere i dati aziendali più importanti, non solo durante l'archiviazione o l'accesso, ma anche quando sono effettivamente in uso. Per ottenere una sicurezza completa, si rivolgono ad Akamai e ai nostri partner. Insieme, questi marchi di fiducia nel campo informatico garantiscono la sicurezza dei dati in ogni fase del loro ciclo di vita.

Scoprite come la nostra partnership per il confidential computing può aiutarvi a proteggere i vostri dati sensibili.
Ulteriori informazioni su Akamai API Security.