WHITE PAPER

Come trasformare la conformità in un vantaggio competitivo con le soluzioni per la sicurezza di Akamai

Un approccio basato su quattro pilastri fondamentali per ottimizzare la sicurezza e prepararsi per gli audit

I quattro pilastri della sicurezza fondamentali per spianare la strada verso la conformità

Attualmente, le organizzazioni in tutto il mondo si trovano a dover affrontare un dedalo di regolamenti sempre più impegnativo, dal GDPR all'HIPAA fino al PCI DSS e ad una crescente serie di obblighi a livello locale. Tuttavia, dimostrare di essere preparati in vista della conformità non significa solo soddisfare i requisiti previsti dagli enti di controllo, ma diventa una pratica essenziale per mantenere la fiducia dei clienti e delle parti coinvolte all'interno delle aziende, come i dirigenti e i membri del consiglio di amministrazione.

In realtà, le implicazioni legate alla mancata conformità si estendono oltre le dirette sanzioni normative perché includono, tra gli altri, i costi derivanti dall'interruzione delle attività aziendali durante le fasi di indagine e mitigazione dei problemi, i danni alla reputazione e la maggiore esposizione a livello legale. Se un'organizzazione non rispetta i requisiti di conformità, si può verificare una perdita di entrate in seguito all'abbandono dei clienti e agli elevati costi operativi poiché le risorse interne devono occuparsi della mitigazione dei problemi piuttosto che dell'innovazione. Nel 2024, le 35 maggiori violazioni a livello globale hanno raggiunto i 3 miliardi di dollari in sanzioni e 23 di queste violazioni, secondo Forrester, sono state causate da una mancata conformità al regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea.

In passato, i team addetti alla sicurezza si occupavano della conformità quando richiesto dalle normative. Attualmente invece, con la tecnologia che avanza rapidamente e gli attacchi che diventano sempre più numerosi e sofisticati, la conformità deve essere un aspetto da considerare al momento di valutare strumenti e modelli da adottare. I team devono chiedersi: "In che modo le opzioni di sicurezza che abbiamo scelto ci aiuteranno a soddisfare i requisiti di conformità attualmente e in futuro?".

Akamai aiuta i suoi clienti a rispondere a questa domanda focalizzando la conversazione sui quattro pilastri fondamentali per le best practice della sicurezza, che fanno naturalmente progredire le aree principali di preparazione in vista della conformità. Questi quattro pilastri fondamentali sono:

- Raggiungere la visibilità sul patrimonio IT
- Prevenire il movimento laterale (all'interno di reti, app e API)
- Prevenire gli accessi non autorizzati
- Proteggere i dati sensibili e le informazioni sugli account dei clienti

Mettendo in pratica questi pilastri fondamentali, ne risulta un chiaro vantaggio competitivo. Le organizzazioni non sono solo più sicure, ma anche meglio preparate a superare gli ostacoli normativi. Inoltre, grazie ai maggiori livelli di sicurezza e conformità che raggiungono, possono anche riuscire meglio a guadagnare la fiducia dei clienti e dei dirigenti interni.

Pilastro 1.

Raggiungere la visibilità sul patrimonio IT

La preparazione in vista della conformità inizia con una visibilità completa su tutte le risorse digitali. Le organizzazioni non possono proteggere ciò che non vedono e gli enti di controllo richiedono sempre più di dimostrare di disporre di un inventario completo delle risorse, di strumenti di monitoraggio continuo e di una consapevolezza delle minacce da affrontare,

il che non è così semplice. Un recente studio condotto da Forrester nel 2024 ha rilevato che più della metà (52%) delle società finanziarie è (decisamente) d'accordo sul fatto di non disporre di una piena visibilità sul proprio patrimonio IT. Sfortunatamente, in caso di mancata conformità, la posta in gioco è alta per ogni settore. Il numero di organizzazioni che ha pagato più di 100.000 dollari in sanzioni normative è salito quasi al 20% tra il 2023 e il 2024.

Per molte organizzazioni, la sfida per raggiungere una visibilità completa risiede nel fatto di riuscire a monitorare il traffico della rete e delle API. Di seguito, vengono riportati alcuni regolamenti e standard che richiedono una chiara visibilità sui rischi correlati:

- Il PCI DSS (Payment Card Industry Data Security Standard) contiene indicazioni utili per verificare se un software aziendale utilizza in modo sicuro le funzioni di componenti esterni, come le API che trasmettono i dati dei pagamenti da un'app mobile ad un sistema bancario.
- Alcuni standard, come l'ISO (International Organization for Standardization) IEC 27001, richiedono di separare i dati e le relative strutture di elaborazione in caso di violazione della rete da parte di un criminale.
- La legge sulla sicurezza dei dati in Cina richiede rigorosi controlli di sicurezza per proteggere l'accesso alle informazioni personali dei clienti tramite tecnologie in grado di scambiare i dati sensibili all'interno di diversi sistemi IT.

Molte aziende dispongono di strumenti o processi che possono soddisfare alcuni di questi requisiti. Tuttavia, in seguito alla loro espansione verso ambienti di computing ibridi e in più aree geografiche, il monitoraggio diventa di gran lunga più difficile, soprattutto per le API. Secondo una ricerca di Akamai, solo il 27% degli addetti alla sicurezza che dispongono di inventari completi delle API sa effettivamente quali delle loro API restituiscono dati sensibili, una percentuale in calo rispetto ad un già preoccupante 40% registrato nel 2023.

Infine, le organizzazioni devono sapere dove si trovano i loro dati sensibili e chi vi accede per individuare le aree in cui devono focalizzare il loro impegno in termini di sicurezza, pertanto, devono disporre della visibilità sui seguenti componenti:

- Le risorse che comunicano con la rete (con viste cronologiche e in tempo reale), tra cui processi di livello 7 e traffico sull'edge, all'interno di ambienti cloud ibridi e on-premise
- L'inventario delle API, incluse quelle nascoste e zombie, che mostra le aree in cui si integrano con le fonti di traffico e con il codice
- Il codice JavaScript lato client, che risulta particolarmente importante per soddisfare i più recenti requisiti previsti dal PCI DSS

La gamma delle soluzioni di Akamai può aiutare i team addetti alla sicurezza ad ottenere la visibilità di cui hanno bisogno.

Akamai Guardicore Segmentation è in grado di identificare e visualizzare le risorse che comunicano con la rete nel patrimonio IT, inclusi processi a livello 7, hash e dettagli sulla riga di comando. Inoltre, la soluzione offre la visibilità cronologica necessaria per dimostrare, durante gli audit di conformità, che le risorse in questione non sono state compromesse Le visualizzazioni del traffico nord-sud/est-ovest mostrano anche i punti in cui si verificano gli accessi.

API Security fornisce un inventario delle API in tempo reale di cui le organizzazioni hanno bisogno per i loro processi di conformità, che può aiutarle ad identificare le aree e il momento in cui i dati non crittografati potrebbero essere trasmessi tramite le API.

App & API Protector fornisce una visibilità a livello delle applicazioni, che include l'inventario delle API, il rilevamento dell'esposizione dei dati sensibili e l'analisi del traffico in tempo reale.

Client-Side Protection & Compliance fornisce la visibilità sugli script lato client richiesta dal PCI DSS v4.

Un'azienda sanitaria ha implementato Akamai Guardicore Segmentation per soddisfare i requisiti di conformità imposti dall'HIPAA e dal SOC 2. La soluzione ha fornito un'eccellente visibilità sui flussi di traffico tra le varie app, quindi il team addetto alla sicurezza è riuscito ad ispezionare i dettagli granulari superando i limiti dei registri del livello 4: ID utente, input della riga di comando e, persino, correlazioni dei servizi.

Pilastro 2.
Prevenire il movimento laterale

Analogamente ai team addetti alla sicurezza, molti enti di controllo ritengono che, anche con un solido sistema di sicurezza, le violazioni si possono verificare, pertanto vogliono essere rassicurati sul fatto che le aziende siano in grado di limitare gli eventuali danni ad esse correlati, come richiesto dalle normative vigenti, ad esempio:

- L'articolo 32 del GDPR richiede alle aziende "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".
- Analogamente, il PCI DSS v4 richiede alle organizzazioni di "implementare i firewall per proteggere i dati dei titolari di carte di credito e assicurarsi che i firewall siano configurati in modo da restringere le connessioni tra reti affidabili e non affidabili".
- **L'ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27001** richiede di separare le informazioni e le strutture di elaborazione dei dati per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.

Anche se la maggior parte delle organizzazioni dispone di un firewall, la limitazione del movimento laterale, una volta penetrato un criminale all'interno della rete, richiede un maggior livello di controllo, il che rende la microsegmentazione, preferibilmente quella definita da software, uno strumento fondamentale per soddisfare i requisiti di conformità. Akamai offre tutti gli strumenti adatti per soddisfare i requisiti dei revisori per quanto riguarda il movimento laterale.

Akamai Guardicore Segmentation limita il movimento laterale per garantire alle organizzazioni di rimanere conformi alle normative vigenti. Modelli di policy pronti all'uso facilitano una rapida applicazione delle iniziative di conformità con controlli granulari al livello 7. Inoltre, poiché la soluzione è definita da software, fornisce lo stesso livello di protezione granulare indipendentemente dalle posizioni in cui si trovano le risorse. La soluzione consente anche di identificare le app che comunicano all'interno della rete e i tentativi di comunicazione tra le zone segmentate, fornendo ai revisori un'ulteriore conferma della capacità delle aziende di mitigare le eventuali minacce.

I criminali trovano nuove opportunità per eseguire il movimento laterale nella rete grazie alla proliferazione delle API, in particolar modo gli endpoint delle API che sono vulnerabili agli attacchi BOLA (Broken Object Level Authorization), riuscendo a manipolare gli ID degli oggetti nelle richieste delle API. Una volta penetrati nella rete, i criminali riescono a bypassare i controlli di autorizzazione, a scalare i privilegi necessari e ad ottenere l'accesso ai dati dei clienti.

Akamai API Security è in grado di segnalare le API che espongono i dati sensibili senza un'adeguata autenticazione e identificare le API con controlli di accesso deboli o configurati in modo errato, che potrebbero condurre ad accessi ai dati non autorizzati e al movimento laterale. L'integrazione con la soluzione WAF (Web Application Firewall) di Akamai consente ad API Security di bloccare le minacce in tempo reale.

Un cliente di Akamai, una società di servizi finanziari a livello globale, ha implementato API Security per risolvere i problemi riscontrati con le API sconosciute nel suo ambiente. L'implementazione ha ridotto notevolmente la proliferazione delle sue API e ha migliorato il processo di conformità in quanto Akamai API Security classifica i dati sensibili per aiutare a soddisfare i requisiti dei regolamenti vigenti, come il GDPR, l'HIPAA e molti altri. Durante gli audit normativi, queste implementazioni sono servite per dimostrare che l'azienda aveva intrapreso le misure tecniche appropriate.

Le minacce basate sull'AI di oggi sono gli ostacoli normativi di domani

Attualmente, un'analisi dei sistemi di difesa della cybersecurity di un'organizzazione deve riguardare lo spettro dell'AI. La rapida proliferazione di applicazioni basate sull'AI, grandi modelli linguistici (LLM) e API correlate all'AI generativa hanno introdotto nuove vulnerabilità di cui molte organizzazioni non sono ancora consapevoli. Tra gli esempi di questi tipi di applicazioni, figurano le chatbot basate sull'AI, i motori delle recensioni nel settore del retail, gli strumenti di diagnostica medica e i motori di ragionamento sui rischi.

Nel contempo, i criminali stanno sfruttando l'AI per sferrare attacchi più sofisticati, pertanto, ovunque emergono minacce alle operazioni aziendali e al pubblico, le appropriate normative non tardano a seguire.

Le organizzazioni che cercano di proteggere i loro investimenti effettuati nell'AI, i loro dati e i loro clienti si rivolgono ad Akamai per assistenza. In qualità di provider di servizi per la sicurezza con una solida reputazione per la sua capacità di soddisfare gli attuali requisiti in termini di visibilità, movimento laterale e controllo degli accessi, Akamai ha investito in modo proattivo nell'intento di aiutare a conseguire i requisiti dell'AI in futuro. Akamai ha sviluppato avanzate funzionalità basate sull'AI per rafforzare i suoi prodotti per la sicurezza e ha introdotto una soluzione in grado di aiutare le organizzazioni a proteggere i loro investimenti effettuati nell'AI.

Akamai Firewall for AI fornisce una sicurezza completa per le applicazioni basate sull'AI identificando e mitigando le minacce e gli attacchi basati sull'AI che i tradizionali strumenti di sicurezza non sono progettati per affrontare. Tra i sistemi di difesa appositamente progettati all'interno della soluzione Firewall for AI, figurano i seguenti:

- **Difesa dagli attacchi di tipo injection dei prompt:** la soluzione protegge dalla manipolazione dei modelli di AI effettuata dai criminali con input dannosi
- **Prevenzione della perdita di dati (DLP):** rileva e blocca le fughe di dati sensibili nelle risposte generate dall'AI e protegge dalla ricezione di dati sensibili nelle richieste
- **Filtraggio di contenuti inappropriati e dannosi**: la soluzione segnala la presenza di contenuti di incitamento all'odio, informazioni errate e contenuti offensivi prima di trasmetterli
- **Protezione dell'AI dai criminali**: la soluzione protegge dall'esecuzione di codice remoto, dalle backdoor dei modelli e dagli attacchi di data poisoning
- **Mitigazione degli attacchi DoS (Denial-of-Service)**: mitiga gli attacchi DoS basati sull'AI controllando l'eccessivo utilizzo delle query e il sovraccarico dei modelli

Inoltre, Firewall for AI può aiutare le organizzazioni a conformarsi alle linee guida esistenti su privacy, integrità e sicurezza. Applicando le policy di sicurezza specifiche dell'AI, le aziende possono mitigare i rischi relativi alle normative in materia di protezione dei dati, ad un utilizzo etico dell'AI e agli obblighi di governance aziendale.

Pilastro 3.
Prevenire gli accessi non autorizzati

Il controllo degli accessi a sistemi e dati sensibili rappresenta un caposaldo della conformità praticamente all'interno di tutti i quadri normativi. Le organizzazioni devono conoscere il livello di sicurezza delle app e delle API di cui dispongono per prevenire abusi e accessi non autorizzati. A tal scopo, è necessario autenticare gli utenti in modo appropriato, autorizzando gli accessi in base alle effettive necessità e mantenendo record dettagliati di tutte le attività di accesso.

Per un controllo degli accessi completo che rispetta i requisiti normativi, le organizzazioni devono risolvere principalmente tre problemi. La gamma delle soluzioni per la sicurezza di Akamai può aiutare a fornire sistemi di difesa approfondita in grado di risolverli tutti:

1. **Conoscere il livello di sicurezza di tutte le app e le API di cui si dispone**

App & API Protector di Akamai consente alle organizzazioni di applicare le policy relative al traffico in tutti gli ambienti in cui vengono eseguite, mentre Akamai API Security è in grado di segnalare ad un'organizzazione il verificarsi di eventuali attività insolite e di accessi ai dati non autorizzati o configurati in modo errato, che sono tutte considerazioni importanti per i revisori. Nel contempo, Akamai Guardicore Segmentation consente di monitorare tutte le app che comunicano all'interno della rete e di stabilire uno standard di riferimento per le attività.

2. **Monitorare i comportamenti degli utenti e limitare gli accessi alle informazioni sensibili**

Akamai Guardicore Segmentation limita gli accessi alla rete in base alle identità degli utenti, mentre **App & API Protector** consente di applicare le policy relative al traffico con strumenti di rilevamento delle minacce basati sull'AI per prevenire eventuali violazioni. Infine, **Client-Side Protection & Compliance** consente di monitorare il comportamento dell'esecuzione di JavaScript per mitigare gli attacchi lato client.

3. **Rilevare e limitare le attività fraudolente**

API Security può aiutare a rilevare eventuali comportamenti anomali delle API e controlli di autenticazione configurati in modo errato per bloccare gli attacchi ad alto rischio. Akamai Guardicore Segmentation protegge la rete segnalando e bloccando collegamenti sospetti che potrebbero indicare un'attività fraudolenta. App & API Protector rileva e mitiga le minacce identificate dall'OWASP per ridurre ulteriormente il rischio di frodi.

La protezione degli accessi con la NIS2

La direttiva NIS2 (Network and Information Security 2) aggiornata è stata concepita per creare un livello comune di cybersecurity negli stati membri dell'UE. Tra le recenti aggiunte alla NIS2, figura un requisito che impone alle aziende di creare un sistema di gestione della sicurezza delle informazioni allo scopo di valutare le persone, le policy e gli strumenti tecnologici necessari per proteggere i dati sensibili e per garantire la resilienza operativa. Inoltre, la NIS2 sottolinea maggiormente l'importanza di proteggere le supply chain IT e le relazioni con i fornitori di terze parti.

Pilastro 4.

Proteggere i dati sensibili e le informazioni sugli account dei clienti

L'ultimo pilastro fondamentale alla base di un approccio completo per la preparazione in vista delle normative richiede alle organizzazioni di mettere in atto iniziative di protezione dei dati sensibili. La protezione dei dati di clienti, pazienti e partner, tra gli altri, è il fulcro delle normative maggiormente incentrate sulla sicurezza.

Ad esempio, l'Act on the Protection of Personal Information (APPI) del Giappone impone di valutare l'impatto della protezione dei dati per identificare e mitigare i rischi per le tecnologie che elaborano grandi volumi di dati personali o che implicano attività di trattamento dei dati ad alto rischio.

Per le istituzioni finanziarie negli Stati Uniti, il Consiglio d'esame delle istituzioni finanziarie federali (FFIEC) richiede controlli tali da garantire che le API concedano solo l'accesso a dati specifici per utenti autorizzati tramite un sistema di sicurezza multilivello, che include, ad esempio, le operazioni di monitoraggio, registrazione e generazione di rapporti.

Per realizzare questo pilastro, bisogna iniziare con il rilevamento delle minacce. **App & API Protector**, la soluzione di protezione delle applicazioni web e delle API di Akamai, offre il primo livello di difesa, mentre **Akamai Guardicore Segmentation** consente di monitorare e segmentare il traffico nord-sud/est-ovest. La **gamma delle soluzioni per la protezione dagli abusi e dai bot** offerta da Akamai aggiunge un ulteriore livello di sicurezza dalle minacce automatizzate e dagli attacchi sferrati dai criminali.

Tuttavia, per identificare correttamente le minacce, le organizzazioni devono anche conoscere il comportamento standard all'interno della loro rete. Ecco come le funzionalità delle soluzioni per la sicurezza di Akamai possono fornire queste importanti informazioni:

- Akamai API Security e Akamai Guardicore Segmentation, rispettivamente, consentono di sapere quali API e app comunicano all'interno della rete per segnalare eventuali comportamenti anomali.
- Adaptive Security Engine, una tecnologia fondamentale di App & API Protector, apprende i modelli degli attacchi utilizzando dati locali e globali per apportare ai sistemi di protezione modifiche specifiche in base ai clienti, adattandoli, al contempo, alle minacce future.
- Akamai Hunt, un servizio gestito di ricerca delle minacce che sfrutta gli esperti del team addetto alle ricerche di Akamai, consente alle aziende di adottare un approccio più proattivo ai sistemi di difesa.

DORA e sicurezza dei dati

Il DORA (Digital Operational Resiliency Act) è una normativa concepita per aiutare le società di servizi finanziari negli stati membri dell'UE a resistere e a riprendersi dagli attacchi informatici. Con il DORA, il settore presenta un quadro normativo completo e vincolante per la gestione dei rischi nei servizi ICT (Information and Communication Technology). L'articolo 3 del DORA impone alle organizzazioni di utilizzare processi e soluzioni ICT in grado di:

- Minimizzare i rischi correlati ai dati, gli accessi non autorizzati e i difetti tecnici
- Impedire la mancata disponibilità e la perdita dei dati, oltre alle violazioni di integrità e riservatezza
- Garantire la sicurezza nel trasferimento dei dati

Da una conformità isolata al vantaggio competitivo

I programmi di conformità efficaci devono dimostrare l'impatto aziendale oltre che soddisfare semplicemente i requisiti normativi. Le organizzazioni che hanno implementato le soluzioni per la sicurezza di Akamai incentrate sulla conformità hanno registrato significativi miglioramenti in tre aree principali:

Riduzione dei costi di conformità

Le organizzazioni che dispongono di comprovati programmi di conformità, di solito, spendono di meno nelle attività ad essa correlate rispetto alle aziende che adottano un approccio ad-hoc. Automatizzare la raccolta delle prove tramite piattaforme di sicurezza integrate può ridurre notevolmente il tempo necessario per la preparazione in vista degli audit di conformità, nonché consolidare specifiche soluzioni su una piattaforma completa.

Miglioramento del livello di rischio

Oltre alla riduzione dei costi, una migliore conformità diminuisce i rischi in modo tangibile. Le organizzazioni che hanno implementato le soluzioni per la segmentazione di Akamai possono restringere i percorsi vulnerabili per il movimento laterale, affrontando direttamente i principali requisiti di conformità e riducendo, al contempo, i rischi per le aziende.

Le funzionalità complete di monitoraggio migliorano la visibilità, il che si traduce direttamente in una riduzione dei rischi mediante l'eliminazione dei punti ciechi in cui le violazioni di conformità potrebbero passare inosservate.

Efficienza operativa

La terza area in cui si avverte l'impatto della conformità riguarda i miglioramenti in termini di efficienza operativa. I controlli preapprovati e i modelli di sicurezza coerenti possono tradursi in approvazioni della sicurezza molto più rapide per le nuove applicazioni, il che migliora la soddisfazione degli sviluppatori diminuendo i problemi legati ai processi di revisione della sicurezza e accelerando il time-to-market per le nuove applicazioni.

Ottimizzazione della conformità

In un periodo in cui i requisiti normativi continuano ad evolversi e le organizzazioni ad espandersi, è necessario adottare un approccio flessibile alla conformità. Le soluzioni integrate per la sicurezza di Akamai forniscono la base per una strategia per la conformità in grado di anticipare le tendenze nelle normative e di scalare in base all'espansione aziendale.

- I sistemi delle policy configurabili possono adattarsi ai nuovi requisiti senza la necessità di apportare notevoli cambiamenti all'architettura, mentre le funzionalità complete per la generazione dei rapporti possono soddisfare i crescenti requisiti di attestazione man mano che le normative si evolvono.
- L'implementazione automatizzata delle policy per le nuove risorse garantisce l'ampliamento automatico della copertura della conformità parallelamente all'espansione aziendale.
- Le funzionalità di gestione centralizzata consentono di mantenere una visibilità completa ovunque, mentre il supporto completo delle API aiuta ad automatizzare i processi di conformità per gestire la crescente complessità.

Inoltre, le organizzazioni devono adottare un approccio proattivo stabilendo di esaminare regolarmente le normative vigenti per aggiornare di conseguenza i loro controlli di conformità. Akamai fornisce aggiornamenti regolari alle sue soluzioni per la sicurezza, specificamente progettate per affrontare i requisiti di conformità in continua evoluzione, garantendo ai clienti di rimanere costantemente conformi, indipendentemente dai cambiamenti apportati alle normative.

Conclusione: la conformità come elemento di differenziazione concorrenziale

Un'efficace conformità non significa più semplicemente soddisfare i requisiti normativi, ma rappresenta un imperativo aziendale strategico che influisce direttamente sulle performance delle organizzazioni, sulla fiducia dei clienti e sul posizionamento dell'azienda rispetto alla concorrenza. Indipendentemente dal settore o dall'area geografica in cui un'azienda opera, un approccio proattivo verso la conformità garantisce un livello di sicurezza solido e agile.

Implementando un approccio alla sicurezza integrato attraverso i quattro pilastri fondamentali che consentono di prepararsi in vista della conformità (visibilità sul patrimonio IT, prevenzione del movimento laterale, prevenzione degli accessi non autorizzati e, infine, protezione dei dati sensibili e delle informazioni sugli account dei clienti), le organizzazioni possono stabilire una base sostenibile per risultare conformi che fornisce un effettivo valore aziendale oltre che ottemperare semplicemente alle normative vigenti.

Le organizzazioni che hanno maggiormente successo sono quelle che sono riuscite a trasformare i processi di conformità da un costo necessario per svolgere le loro attività in un vantaggio strategico che favorisce la trasformazione digitale, proteggendo, al contempo, le loro risorse più importanti: la fiducia dei clienti, l'integrità dei dati e la reputazione aziendale.

Contattateci per scoprire come Akamai può aiutare la vostra organizzazione.

Contattateci