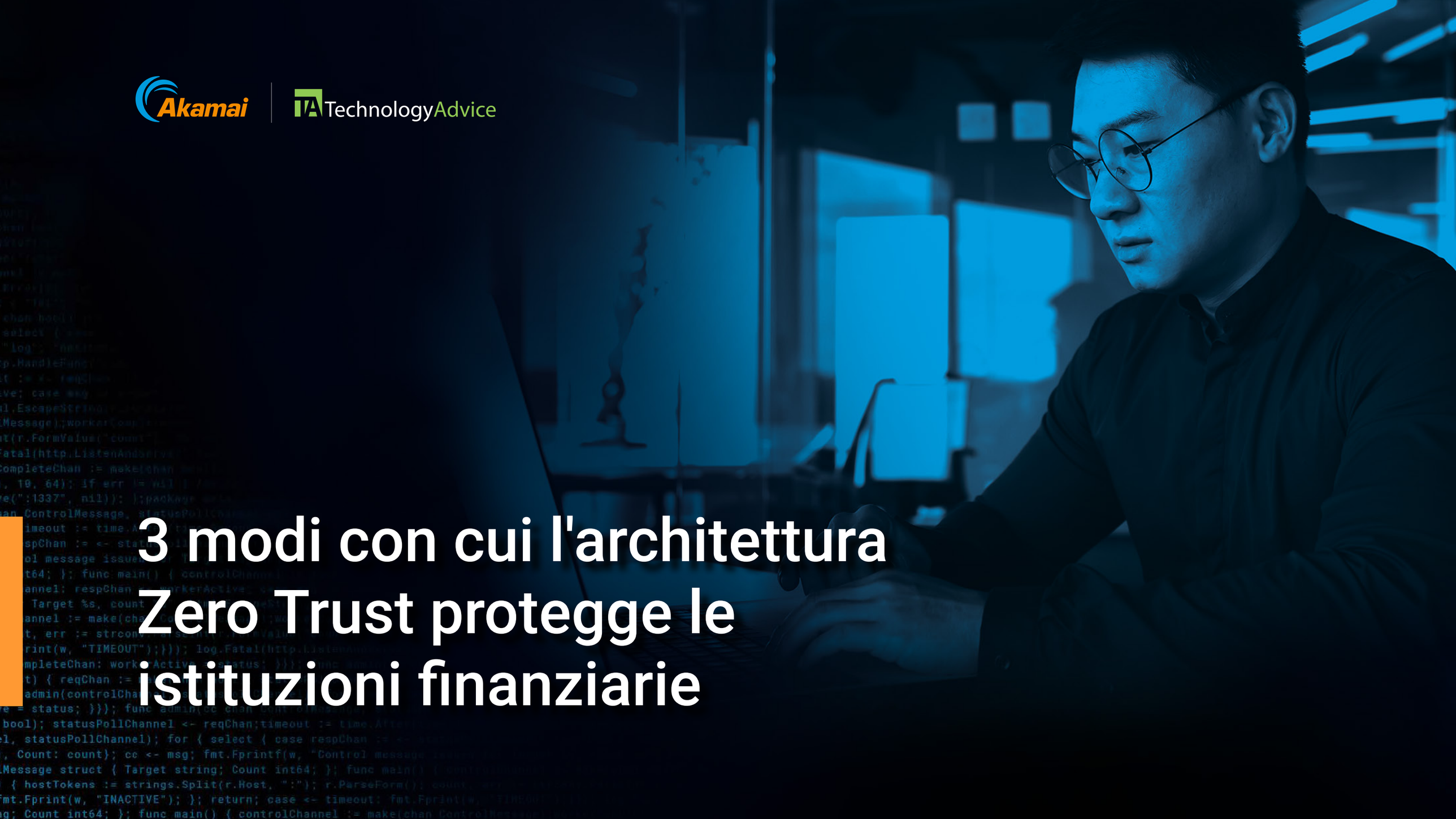
Akamai | TechnologyAdvice



3 modi con cui l'architettura Zero Trust protegge le istituzioni finanziarie

Le istituzioni finanziarie, che hanno registrato un aumento del 65% negli attacchi alle applicazioni web e alle API tra il 2° trimestre del 2022 e lo stesso periodo del 2023, rimangono uno degli obiettivi principali per i criminali. Questo inarrestabile assalto delle minacce informatiche in continua evoluzione non solo prosciuga le risorse disponibili, ma distoglie anche l'attenzione dalle principali funzioni aziendali.

Le tradizionali soluzioni di firewall ed endpoint considerano implicitamente attendibili endpoint, dispositivi e utenti che superano il controllo iniziale, a volte rafforzato dall'autenticazione multifattore (MFA), immettendo la corretta combinazione di nome utente e password. Le applicazioni, le API e i servizi di sistemi presenti all'interno della rete spesso funzionano senza un controllo di sicurezza oltre il monitoraggio standard che rileva eventuali programmi malware sugli endpoint. Ora, le istituzioni finanziarie stanno adottando il modello Zero Trust per affrontare le crescenti minacce ransomware, le rigide normative in materia di conformità e le sfide correlate con la migrazione nel cloud.

Il modello Zero Trust elimina il concetto di fiducia implicita verificando continuamente i permessi di accesso per tutti gli utenti, i dispositivi e le applicazioni, in base al contesto delle richieste e delle autorizzazioni. Anche se un criminale può violare un dispositivo o abusare delle credenziali necessarie per accedere ad una rete, è possibile limitare strettamente l'accesso e ridurre notevolmente i danni causati.

Ma esattamente in che modo un sistema Zero Trust protegge un'istituzione finanziaria?

Conformità alle normative in continua evoluzione

Le istituzioni finanziarie devono dedicare un numero consistente di risorse per dimostrare la loro conformità a varie normative, come il noto standard PCI DSS (Payment Card Industry Data Security Standard) o l'incombente DORA (Digital Operational Resilience Act), la cui piena applicazione è prevista per gennaio 2025. Gli audit aumentano regolarmente in termini di complessità, costi e tempi necessari a causa di requisiti confusi, discordanti e in continua evoluzione. Tuttavia, le istituzioni finanziarie devono investire in questo settore perché il mancato superamento di un audit può condurre anche a perdite di ricavi, sanzioni normative, multe o pene, nonché danni alla reputazione e potenziali responsabilità legali.

I rapporti sulla conformità richiedono un resoconto chiaro e accurato dei sistemi che trattano dati regolamentati, oltre a dimostrare che tali sistemi sono adeguatamente protetti. Tuttavia, nelle grandi istituzioni finanziarie, gli ambienti IT sono eccessivamente grandi, dettagliati e complessi per tenere facilmente traccia di risorse e accessi.

Le soluzioni di protezione dei firewall e degli endpoint di tipo legacy monitorano e proteggono principalmente utenti e risorse tradizionali. Affidarsi a questo approccio convenzionale alla segmentazione della rete pone diverse sfide in termini di scalabilità delle operazioni, ostacola la creazione e l'applicazione delle policy e limita la flessibilità aziendale.

Per superare le sfide legate agli ambienti legacy con la tecnologia allineata alla strategia futura, le istituzioni finanziarie devono disporre di una visibilità granulare sul traffico est-ovest e della possibilità di applicare policy di segmentazione nei loro ambienti multicloud e container. Con la crescente esigenza di gestire più aree geografiche e diversi tipi di infrastrutture IT, inclusa la tecnologia dei container, le istituzioni finanziarie devono seguire il percorso più semplice e diretto per la microsegmentazione con l'automazione, l'integrazione del team DevOps e la flessibilità delle policy.

Se non vengono eseguite regolari operazioni di identificazione, monitoraggio e protezione di tutte le risorse, un'istituzione finanziaria non può garantire che l'accesso ai dati regolamentati sia completamente controllato e protetto. Sottovalutare o monitorare in modo inadeguato dati, utenti, applicazioni o dispositivi aumenta notevolmente i rischi di subire un attacco informatico e il potenziale insuccesso di un audit di conformità.

L'architettura Zero Trust nega automaticamente l'accesso e tutte le connessioni devono essere esplicitamente concesse solo all'utente autorizzato su un dispositivo autorizzato con l'accesso autorizzato ai dati richiesti. Il modello di accesso Zero Trust si basa per impostazione predefinita sul privilegio minimo, che blocca le connessioni legacy sconosciute o dimenticate. La soluzione di Akamai identifica rapidamente i dispositivi dannosi, gli utenti legacy (persone, API o applicazioni) e le fonti di dati dimenticate che infestano le precedenti filiali o gli ambienti tecnologici legacy delle aziende acquisite.

L'architettura Zero Trust di Akamai si applica indipendentemente dalla posizione dell'utente, anche se il relativo contesto può essere incluso nel processo decisionale relativo all'accesso. I team addetti alla sicurezza possono eseguire le operazioni di controllo e creazione di rapporti necessarie per analizzare rapidamente e gestire completamente l'accesso alle risorse presenti nelle reti locali, nei data center o nel cloud.

In seguito all'aumento delle pressioni normative che impongono di salvaguardare le applicazioni più importanti e proteggere il traffico est-ovest, le istituzioni finanziarie si stanno focalizzando nell'intento di migliorare la visibilità e la comprensione dei loro ambienti. Tramite i principi Zero Trust, ora le istituzioni finanziarie possono identificare e segmentare facilmente le risorse non conformi, consentendo ai team dedicati alle applicazioni di gestire autonomamente le policy di segmentazione. Questo approccio garantisce un workflow efficiente e semplifica il processo di creazione dei rapporti.

La visibilità completa e dettagliata sul traffico est-ovest facilita la mappatura e l'isolamento delle app business-critical, senza richiedere modifiche all'infrastruttura o alle applicazioni. Questa funzionalità consente alle istituzioni finanziarie di restringere gli accessi di terze parti e di migliorare la sicurezza complessiva.

L'acquisizione della visibilità agevola la protezione della migrazione nel cloud, mentre l'integrazione della segmentazione nel ciclo DevOps garantisce immediati aggiornamenti delle policy senza dover apportare sostanziali modifiche all'infrastruttura, diversamente dalle precedenti pratiche VLAN. Inoltre, Akamai consente di creare, applicare e generare rapporti in modo semplice e uniforme sulle policy di conformità per diverse infrastrutture tramite una maggiore visibilità, la mappatura delle dipendenze delle applicazioni, le policy di segmentazione automatizzate, l'automazione delle policy DevOps e un'agevole integrazione della gestione dei cambiamenti.

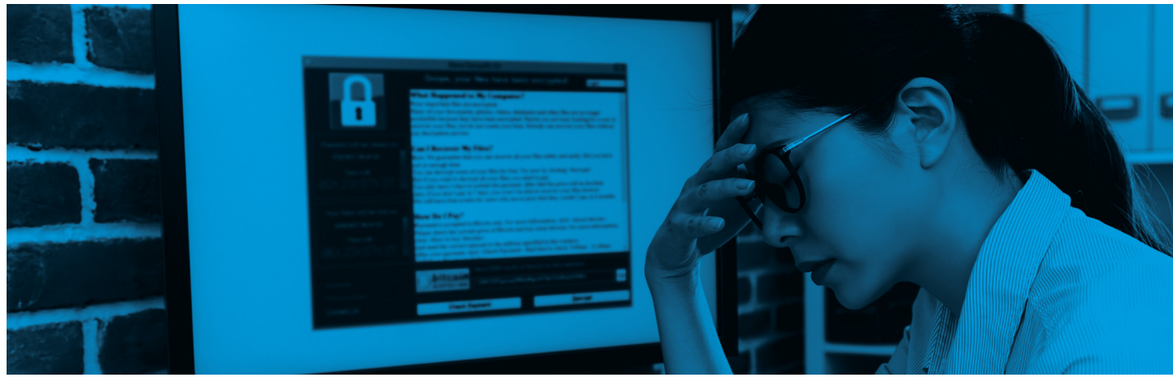
Prevenire la diffusione del ransomware

Dalle filiali alle istituzioni finanziarie a livello globale, gli attacchi ransomware richiamano l'attenzione e creano problemi in tutto il mondo. "Entro il 2031, i ransomware attaccheranno un'azienda, un consumatore o un dispositivo ogni due secondi", secondo il rapporto sul mercato dei ransomware 2022 di Cybersecurity Ventures.

Poiché le società di servizi finanziari spesso si espandono tramite fusioni e acquisizioni, in molti casi non hanno la visibilità necessaria sul proprio ecosistema tecnologico, il che crea vulnerabilità sfruttate dagli hacker. Gli autori di attacchi ransomware sfruttano le vulnerabilità disponibili oppure usano il phishing per rubare le credenziali o rilasciare malware sconosciuti sugli endpoint eludendo il loro sistema di difesa.

Un'autenticazione incentrata sulle password e policy per l'accesso degli utenti eccessivamente permissive consentono ai criminali di bypassare i firewall, eludere il rilevamento degli endpoint e ottenere un accesso illimitato alle reti che considerano implicitamente attendibili traffico, utenti e dispositivi connessi. Gli autori di attacchi ransomware, che spesso operano in gruppi organizzati, come il CL0P, sfruttano le risorse violate e si spostano lateralmente nella rete per rilevare e sfruttare altre risorse vulnerabili. Le vulnerabilità zero-day, come la vulnerabilità MOVEit SQL injection, consente ai criminali di ottenere l'accesso e diffondere l'attacco rapidamente tramite script automatizzati per crittografare i sistemi, rubare i dati e avviare richieste di riscatto.

Le soluzioni Zero Trust di Akamai consentono alle istituzioni finanziarie di identificare e isolare i sistemi di importanza critica e di restringere l'accesso alla rete in entrata e in uscita da questi sistemi. Questo approccio riduce al minimo la probabilità, l'impatto e il tempo necessari per rimediare ad un attacco ransomware. Inizialmente, Akamai tiene traccia e monitora i domini e gli indirizzi IP dannosi, implementando appropriati blocchi di quarantena per prevenire il lancio di molti attacchi.



Successivamente, con una visibilità quasi in tempo reale sul traffico di rete, Akamai osserva e controlla il traffico fino ai livelli dei processi e dei servizi. Queste informazioni dettagliate offrono ai team dei centri operativi di sicurezza e di rete la possibilità di identificare e sferrare specifiche minacce in modo preciso.

Quindi, anche un attacco riuscito verrà strettamente limitato nella portata dalla microsegmentazione integrata in Akamai Guardicore Segmentation. Le credenziali e le autorizzazioni verranno continuamente verificate ad ogni richiesta di accesso e le connessioni alle applicazioni protette da Akamai Enterprise Application Access verranno negate.

Inoltre, applicazioni, server e altre risorse non richiesti da un utente vengono automaticamente nascosti dal rilevamento per prevenire eventuali spostamenti laterali o estensioni degli accessi per i criminali. Infine, il rilevamento delle anomalie di Akamai Hunt segnala comportamenti insoliti per avvisare i team addetti alla sicurezza in modo da aiutare ad identificare gli attacchi prima che i dati vengano esfiltrati o crittografati.

Semplificazione della trasformazione digitale

Per migliorare il loro livello di flessibilità, scalabilità e modernizzazione, molte istituzioni finanziarie spostano le app nel cloud. Tuttavia, questa migrazione introduce nuove sfide.

Innanzitutto, le istituzioni finanziarie non possono migrare risorse e connessioni non rilevate e sconosciute. Inoltre, le migrazioni nel cloud non solo espandono la superficie di attacco, ma le integrazioni multicloud e nel cloud ibrido locale spesso danneggiano le applicazioni e introducono falle nei livelli di sicurezza tradizionali. Infine, l'infrastruttura implementata da software (container, macchine virtuali, ecc.) viene distribuita automaticamente in modo rapido per proteggere o monitorare efficacemente con l'utilizzo di soluzioni legacy,

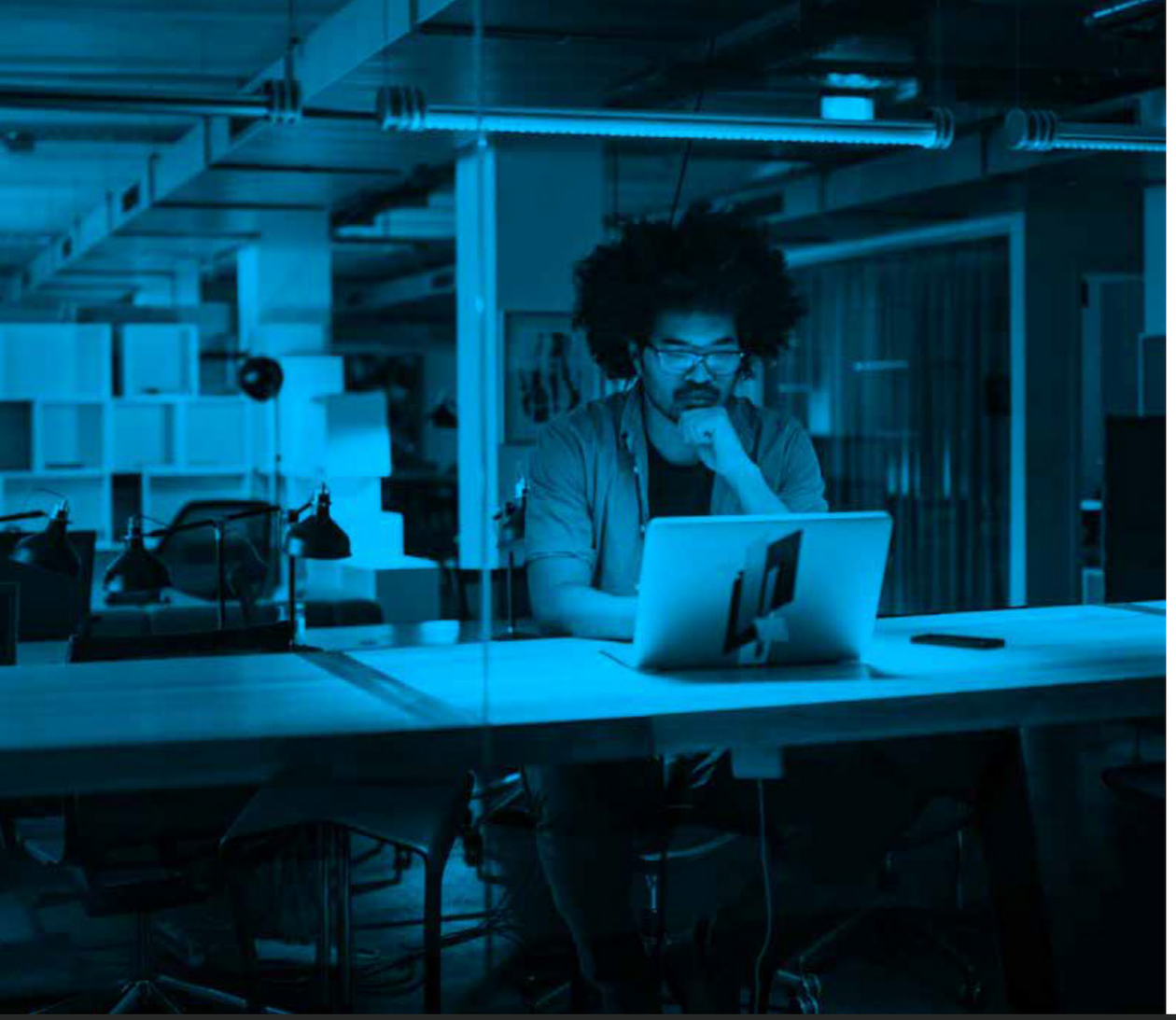
Le soluzioni Zero Trust consentono alle istituzioni finanziarie di implementare le loro applicazioni basate sul cloud più facilmente con protezioni più robuste e ridotti costi di gestione. Le soluzioni Zero Trust di Akamai tengono traccia di tutti i flussi di dati per identificare rapidamente la potenziale superficie di attacco e applicare le policy senza interrompere le attività aziendali.

Una volta identificata la superficie di attacco, i team addetti alla sicurezza e alle operazioni possono usare il controllo centralizzato di Akamai per segmentare e proteggere le applicazioni e per monitorare i flussi di dati. Akamai offre un controllo granulare, riducendo contemporaneamente la complessità e i costi operativi. Per i team addetti alla sicurezza e alle operazioni nelle istituzioni finanziarie, l'applicazione di policy universali garantisce una modernizzazione delle infrastrutture agile e tempestiva grazie al solido sistema di sicurezza offerto dalla segmentazione Zero Trust basata sul privilegio minimo, che fornisce una potente protezione dalle minacce in continua evoluzione.

Le istituzioni finanziarie non possono permettersi di ignorare il modello Zero Trust

Gli attacchi sferrati contro la tecnologia di tipo tradizionale possono condurre ad importanti violazioni di dati, costare milioni di danni e distruggere la fiducia di clienti e partner. Gli attacchi stanno diventando più sofisticati e rapidi; inoltre, senza una piena visibilità sull'ecosistema tecnico, le istituzioni finanziarie possono creare nuove vulnerabilità.

Akamai fornisce una maggiore visibilità sulla rete, limita in modo intelligente l'accesso degli utenti, cerca continuamente nuove minacce e segnala eventuali anomalie per consentire gli appropriati controlli di sicurezza. Scoprite di più su come soddisfare le esigenze delle istituzioni finanziarie con la gamma di soluzioni Zero Trust di Akamai.



Ulteriori informazioni sulla protezione delle finanze digitali con Akamai

Ulteriori informazioni

TechnologyAdvice | Akamai

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn.