WHITE PAPER

Come superare gli ostacoli per la cybersicurezza con la segmentazione basata su software

Akamai Guardicore Segmentation aiuta a migliorare la sicurezza degli accessi e a ridurre i costi dei rischi informatici nel settore finanziario europeo

Panoramica

Il settore finanziario è una parte cruciale dell'economia dell'Unione Europea e i sistemi finanziari sono considerati infrastrutture critiche da alcuni governi e autorità di regolamentazione europei. I prodotti e i servizi forniti dalle organizzazioni di servizi finanziari dipendono fortemente da sistemi IT altamente disponibili e dall'accesso tempestivo alle informazioni fornite tramite molteplici canali e parti.

Tuttavia, gli attacchi ransomware e di cryptomining hanno dimostrato con quanta rapidità gli autori delle minacce possono disabilitare questa infrastruttura critica per giorni o addirittura settimane, riuscendo a diffondersi a terze parti e peer collegati.

È fondamentale che le istituzioni finanziarie europee adottino funzionalità digitali all'avanguardia per il perseguimento della competitività, dell'acquisizione e della fidelizzazione dei clienti. Tuttavia, i crescenti requisiti normativi in materia di controlli e creazione di rapporti di sicurezza stanno rallentando in modo significativo il tasso di adozione del cloud. Il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea, ad esempio, può imporre sanzioni fino al 4% del fatturato globale alle aziende che non sono in grado di proteggere i propri clienti.[1]

Inoltre, recenti normative come il CSP SWIFT (Programma di sicurezza del cliente della Società per la Telecomunicazione Finanziaria Interbancaria Mondiale e le aspettative di controllo sulla resilienza informatica della Banca centrale europea (CROE BCE) richiedono specificamente una segmentazione della rete più granulare.

Gli approcci di segmentazione tradizionali e le relative procedure manuali non sono un approccio praticabile per tenere il passo con l'innovazione tecnologica, l'aumento dei rischi per la sicurezza e le normative sempre più severe.

Le organizzazioni devono non solo adottare nuovi strumenti, ma anche modificare radicalmente i propri processi di sicurezza e segmentazione per garantire semplicità, trasparenza e automazione.

Questo white paper illustra:

- Le principali sfide in materia di cybersicurezza che il settore finanziario europeo si trova ad affrontare oggi
- Come le banche e gli istituti finanziari possono affrontare questi rischi con un approccio semplice e conveniente alla segmentazione
- In che modo l'approccio di Akamai Guardicore Segmentation aiuta le aziende a semplificare i processi di sicurezza, riducendo significativamente i costi e accelerando la conformità

L'odierna cybersicurezza è complessa e costosa da gestire

Nonostante l'impegno delle banche e degli istituti finanziari europei a garantire la sicurezza delle organizzazioni e la protezione dei dati dei clienti, il percorso verso un maggiore livello di sicurezza non è un percorso facile nel mondo di rischi, esigenze di accesso di terze parti e requisiti di conformità in continua evoluzione di oggi.

Un maggiore rischio informatico aumenta le perdite monetarie

I rischi associati ai crimini informatici sono particolarmente gravi per gli istituti finanziari. Il settore finanziario sta già spendendo più di qualsiasi altro settore per contrastare gli attacchi, con un costo medio di 5,72 milioni di dollari per violazione dei dati.[2]

Tuttavia, anche ottenere un solido livello di sicurezza è costoso. L'applicazione dei controlli di sicurezza per proteggere non solo più piattaforme ma anche l'accesso di terze parti, che è fondamentale per la fornitura di servizi aziendali, è un'attività complessa. Ciò comporta un aumento significativo delle infrastrutture e dei costi di manodopera.

Aumento dei costi della conformità

Le organizzazioni di servizi finanziari in Europa hanno assistito a un notevole aumento dei costi, dei tempi e delle risorse complessive necessarie per prepararsi e convalidare la conformità. Sebbene le normative contribuiscano a garantire la stabilità del settore finanziario, la continua introduzione di nuovi obblighi di cybersicurezza sta incidendo sulla redditività e sulla crescita, rallentando la trasformazione digitale e richiedendo investimenti sostanziali.

L'aumento della pressione per inasprire le policy è iniziato con il GDPR ed è stato seguito dalla Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS), dal documento CROE della BCE e, più recentemente, dal regolamento UE sulla cybersicurezza. Complessivamente, con l'aggiunta dei requisiti dei fornitori come il CSP SWIFT, ottenere la conformità oggi significa soddisfare un vasto numero di requisiti tecnici e di creazione di rapporti.

Pertanto, oltre ad aggiornare la propria tecnologia, le banche e gli istituti finanziari devono anche trovare modi per semplificare la gestione e ridurre i costi operativi relativi alla cybersicurezza e alla conformità.

Vulnerabilità della sicurezza delle interazioni con terze parti e con i mercati finanziari

La direttiva sui servizi di pagamento rivista (PSD2) dell'UE, volta a migliorare la comodità e la trasparenza degli utenti, ha amplificato i rischi di accesso di terzi e di compromissione dei dati personali. C'è anche una crescente pressione, da parte dei colleghi dei servizi finanziari e delle autorità di regolamentazione, per l'efficienza e la trasparenza dei processi aziendali e tecnologici.

Ulteriori richieste da parte dei clienti in materia di sicurezza, mobilità e nuovi servizi hanno portato a una maggiore dipendenza da infrastrutture tecnologiche di informazioni e comunicazioni di terze parti, fornitori di outsourcing e relative supply chain.

Con gli ambienti che diventano sempre più connessi, la protezione di tutti i tipi di comunicazioni, comprese le transazioni interbancarie e intrabancarie automatizzate, richiede molte risorse.

Oggi, una singola violazione del data center di una parte potrebbe avere un effetto domino, in quanto agli autori di attacchi basterebbe sfruttare solo una singola risorsa per spostarsi lateralmente tra le parti interconnesse, compresi gli istituti finanziari e i mercati finanziari, mettendo a rischio la sicurezza e la continuità operativa dell'intero ecosistema dei servizi finanziari europeo.

Il cloud ibrido richiede un nuovo approccio alla sicurezza

I requisiti di conformità, insieme alle linee guida dell'Autorità bancaria europea[3], stanno plasmando le tendenze di adozione del cloud nel settore finanziario. Anche se l'adozione del cloud è in aumento in Europa, le normative hanno aumentato la complessità della migrazione dei sistemi locali al cloud.

Per questo motivo, è più probabile che le aziende europee mantengano le funzioni principali on-premise e adottino ambienti cloud ibridi piuttosto che ambienti basati completamente sul cloud. Molte banche sono anche passate all'utilizzo di diversi provider di servizi cloud, diventando un'infrastruttura multicloud.

Tuttavia, le organizzazioni in genere cercano qualcosa di più che un semplice maggiore livello di sicurezza. Stanno anche cercando di risparmiare sui costi e migliorare l'efficienza operativa mediante la modifica dei processi. L'automazione e la modernizzazione dei processi sono diventati fondamentali per il successo.

Affrontare le principali sfide della cybersicurezza con la visibilità e la segmentazione della rete

Queste sfide sono accomunate dalla necessità di isolare in modo sicuro le applicazioni e i carichi di lavoro critici, per dirla in altre parole, la segmentazione. La segmentazione consente agli istituti finanziari di raggiungere la sicurezza su larga scala in base alle esigenze aziendali e dimostrare un approccio basato sul rischio in linea con i requisiti normativi.

I firewall tradizionali non sono la risposta

I motivi per cui la segmentazione non è stata più ampiamente adottata e implementata dalle banche e dalle istituzioni finanziarie europee sono diversi.

Elevata richiesta di manutenzione e risorse: molti professionisti della sicurezza e IT esitano a implementarla, adducendo come motivazione il fatto che richiede tempi lunghi, l'impiego di più team e un numero di risorse estremamente elevato. Questa esitazione è comprensibile, dal momento che i metodi tradizionali tendono ad essere sia complicati che dispendiosi in termini di tempo. La configurazione di VLAN, ACL e firewall in più sedi e ambienti è molto spesso un processo laborioso, lento e soggetto a errori. Inoltre, i metodi tradizionali si basano largamente su dati di identità inaffidabili, come gli IP, che sono poco significativi e possono cambiare frequentemente.

Mancanza di visibilità: le organizzazioni sono inoltre scoraggiate da una mancanza di visibilità nel traffico est-ovest, che complica l'identificazione delle dipendenze tra segmenti e la creazione di policy di segmentazione che non interrompano i componenti critici. Anche l'uso di TAP di rete o tecnologie simili non ovvia al problema, perché la visione che ne consegue non dispone delle sofisticate traduzioni di contesto tra IP e porte. Negli ambienti dinamici, come le piattaforme PaaS (Platform-as-a-Service), questa soluzione si rivela impossibile.

Dipendenza dall'infrastruttura: Se i carichi di lavoro si estendono al cloud, cosa sempre più comune, il processo diventa ancora più complicato. L'installazione di un firewall hardware in ogni punto di uscita dei dati ha un costo proibitivo. Le complesse configurazioni di rete generano ulteriori problemi di gestione. Queste configurazioni sono necessarie per soddisfare le esigenze di diversi ambienti con risorse virtualizzate o legacy oltre a cloud e container.

> "In alcune aree, il regime normativo ha faticato a tenere il passo con l'innovazione tecnologica, ma lo stesso hanno fatto anche i sistemi di gestione e controllo del rischio delle imprese".
>
> - Financial Markets Regulatory Outlook 2023, Centre for Regulatory Strategy EMEA Deloitte

Introdurre un cambiamento dei processi fondamentali

Anche le organizzazioni di servizi finanziari di medie dimensioni con poche centinaia di server possono generare migliaia di voci di policy di segmentazione. Gestirli manualmente è inefficace, soprattutto in ambienti con delivery automatizzata delle applicazioni, utilizzando strumenti come Jenkins e cicli CI/CD in cui il contesto è fondamentale.

Ecco perché Akamai Guardicore Segmentation fa un ulteriore passo avanti, aiutando le organizzazioni a spostare i cicli di creazione e aggiornamento delle policy da un processo fondamentalmente manuale a uno automatizzato.

Con Akamai Guardicore Segmentation, una volta automatizzata la profilazione di un'applicazione e mappate tutte le dipendenze, la creazione e gli aggiornamenti delle regole possono essere trasformati in un processo ripetibile in cui le parti interessate e i proprietari dell'applicazione devono solo approvare le policy generate automaticamente. Ciò elimina quasi completamente la necessità di un intervento manuale, che può rallentare notevolmente i progetti, e riduce il rischio di configurazioni errate ed errori umani.

La creazione automatizzata delle regole mantiene la coerenza strutturale delle regole e la scalabilità della policy stessa, contribuendo a un utilizzo dei firewall più ottimizzato.

Accelerare la trasformazione dell'IT per creare un vero ambiente Zero Trust

I processi manuali e le risorse limitate non dovrebbero impedire agli istituti finanziari di raggiungere la segmentazione su larga scala. Un vero modello Zero Trust richiede non solo la tecnologia appropriata, ma anche la modernizzazione dei processi di creazione, modifica e manutenzione delle policy di sicurezza.

I firewall basati su host o software rappresentano un approccio diretto ed economico alla sicurezza a livello di applicazione. Questo approccio accelera notevolmente l'implementazione, semplifica la manutenzione continua e, in definitiva, è più efficace nel mitigare le minacce. Akamai Guardicore Segmentation è stato appositamente progettato per contribuire a rendere la segmentazione semplice, conveniente e veloce per le organizzazioni di tutte le dimensioni.

Offre una mappa visiva di tutte le applicazioni nel data center e delle relative dipendenze. Gli operatori della sicurezza possono creare e applicare policy di sicurezza a livello di rete e di singoli processi per isolare e segmentare le applicazioni e le risorse critiche. Questo approccio di sovrapposizione definito dal software garantisce l'indipendenza dall'infrastruttura soggiacente, nonché la protezione dei carichi di lavoro distribuiti on-premise, su sistemi esistenti, VM, container e cloud. È possibile creare policy relative ad applicazioni singole o raggruppate logicamente, indipendentemente da dove risiedono. Queste policy determinano quali componenti possono e non possono comunicare tra loro, creando le basi per un approccio Zero Trust alla sicurezza.

Ridurre in modo efficiente i rischi e i costi informatici

Gli istituti finanziari che utilizzano Akamai Guardicore Segmentation sono riusciti ad affrontare alcuni dei loro problemi di sicurezza più urgenti riducendo i costi in un breve periodo tramite:

Riduzione dei costi dei rischi informatici applicando l'igiene della sicurezza della rete e le best practice in ambienti sempre più complessi e interconnessi.

Semplificazione della gestione della conformità tramite una visibilità contestuale granulare e policy di segmentazione per mappare e isolare rapidamente le risorse correlate alla conformità e le applicazioni business-critical. Utilizzando un approccio unificato, un istituto finanziario può ragionevolmente dimostrare che sta adottando misure per proteggere le risorse critiche, mitigare il rischio di frode e proteggere la privacy dei clienti.

Protezione degli accessi di terze parti imponendo percorsi per il traffico di terze parti con segmentazione basata sull'identità, isolando e impedendo agli utenti di spostarsi tramite una rete Ciò rafforza la sicurezza delle interazioni con terze parti e con i mercati finanziari, impedendo gli attacchi dall'attecchire ed espandersi tramite un sistema compromesso di terzi.

Isolamento dei sistemi di pagamento e di trasferimento di denaro dall'IT generale per soddisfare i requisiti dei sistemi di trasferimento e pagamento elettronico di fondi, in particolare SWIFT, per una rigorosa separazione dei servizi SWIFT dall'ambiente IT generale di un'istituzione. La segmentazione granulare consente ai team IT delle banche di impostare confini basati sul contesto (utente, dominio) delimitando la "zona" di un fornitore di servizi per limitare ulteriormente l'accesso non autorizzato.

Migrazione rapida e sicura al cloud mappando i carichi di lavoro ed effettuando l'inventario di tutte le applicazioni critiche e delle relative dipendenze prima della migrazione. Le policy di isolamento possono utilizzare queste mappe come base per una sicurezza coerente che segua i carichi di lavoro durante tutto il processo di migrazione. Questo approccio consente una migrazione al cloud più rapida e sicura, applicando gli stessi controlli di sicurezza indipendentemente dalle modifiche dell'applicazione o dell'infrastruttura.

Garanzia della continuità operativa con un'efficiente mitigazione delle violazioni tramite una visibilità granulare del traffico est-ovest e indicatori di violazione per avvisare in caso di movimenti anomali per fermare gli autori delle minacce prima che estraggano dati finanziari e sensibili dei clienti.

Riduzione dei rischi tramite la limitazione del movimento laterale. Oggi, la maggior parte del traffico del data center si sposta lateralmente tra le applicazioni (est-ovest), anziché entrare nel data center dall'esterno (nord-sud). L'impostazione di confini interni delimitando applicazioni e sistemi business-critical riduce efficacemente la superficie di attacco, proteggendo dalla diffusione laterale degli attacchi e limitando i danni in caso di violazione.

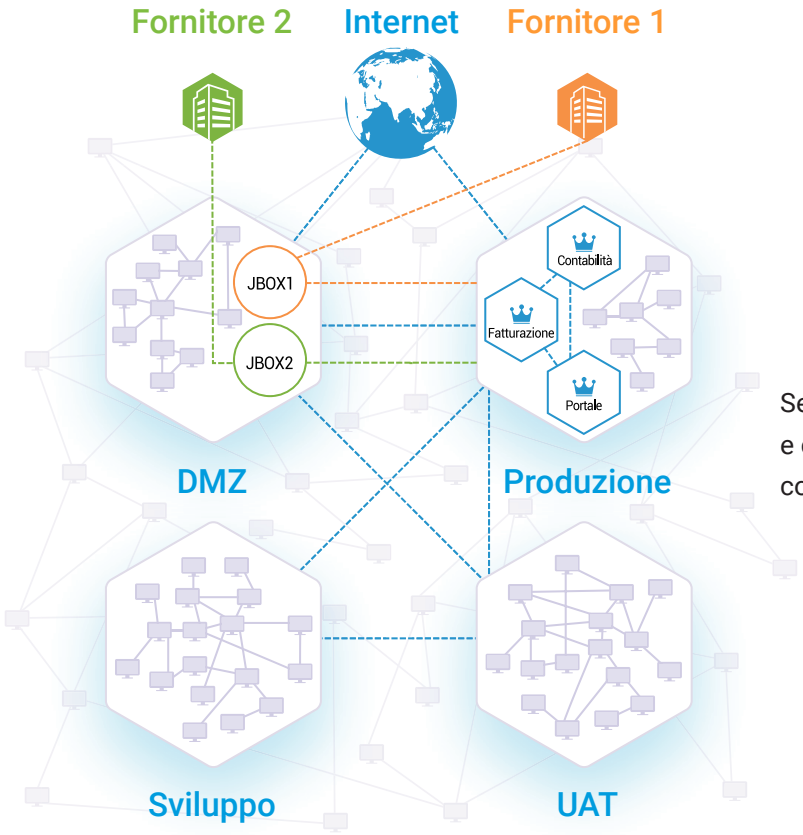
Case study: Riduzione dei costi di conformità di una grande banca multinazionale europea

Una grande banca europea era alla ricerca di un approccio nuovo ed efficiente alla segmentazione della rete, necessario per soddisfare i requisiti tecnici di più agenzie di regolamentazione, tra cui la Federal Reserve Bank di New York (FRBNY), la Monetary Authority of Singapore (MAS), la BCE, ecc.

L'utilizzo da parte della banca di approcci tradizionali di segmentazione, regole firewall e VLAN si è rivelato inefficace, con conseguenti elevati costi annuali di non conformità. Stava inoltre incidendo sulle operazioni IT con notevoli downtime della produzione e risorse necessarie per creare e aggiornare le policy.

Per raggiungere gli obiettivi di segmentazione della banca era necessario un approccio più conveniente e di facile implementazione. Il requisito fondamentale per una nuova soluzione era un impatto minimo sull'infrastruttura e sulle risorse della banca, garantendo al tempo stesso la piena conformità alle normative pertinenti.

Dopo un processo di valutazione approfondito che ha coinvolto più fornitori, i responsabili delle decisioni nell'infrastruttura della banca e nei team di sicurezza IT sono giunti a una conclusione unanime: Akamai Guardicore Segmentation offriva il percorso più semplice e diretto verso la microsegmentazione.



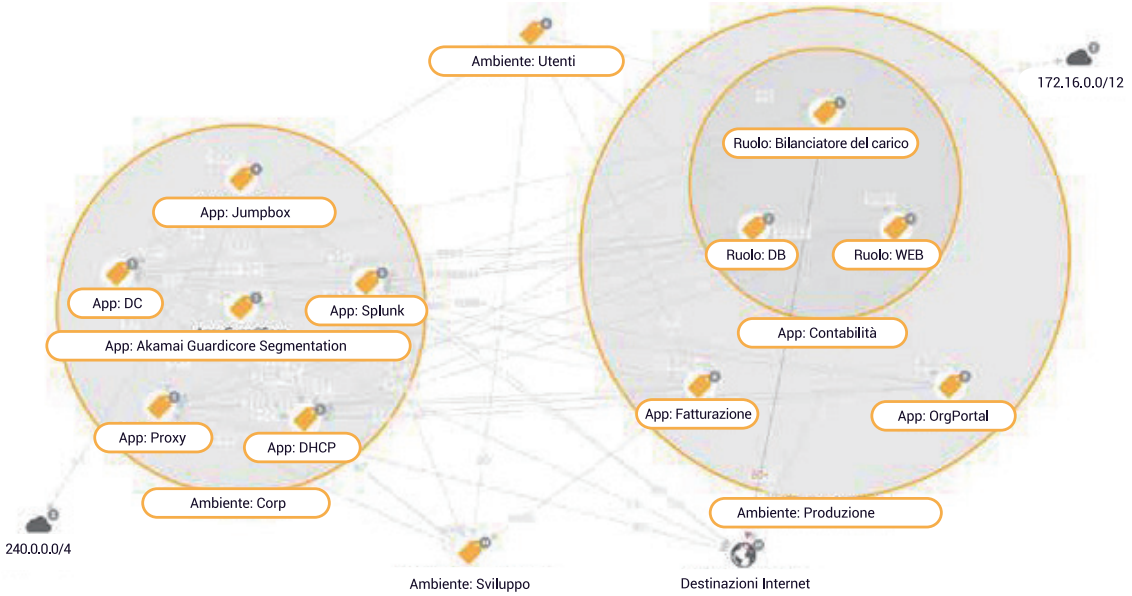
Segmentazione degli ambienti e controllo degli accessi di terze parti con Akamai Guardicore Segmentation.

Semplificazione e accelerazione della segmentazione

La banca ha implementato Akamai Guardicore Segmentation in più aree geografiche e in diversi tipi di infrastrutture IT, inclusi i container, senza richiedere modifiche alle applicazioni e non causando, pertanto, problemi di downtime nell'ambiente di produzione. Ha inoltre consentito alla banca di ottenere rapidamente una visibilità centralizzata sui carichi di lavoro dei data center e di isolare gli ambienti di produzione, test e sviluppo. Utilizzando Akamai Guardicore Segmentation, il cliente è stato anche in grado di limitare l'accesso ai server da stampanti, altri dispositivi IoT e utenti non autorizzati.

In meno di tre mesi, il progetto è stato completato. Il completamento è stato 10 volte più veloce di quanto inizialmente stimato con i metodi di segmentazione tradizionali. Grazie alla rapida mappatura dell'ambiente e alla creazione di policy basate sulle informazioni raccolte, la banca ha migliorato la propria posizione di sicurezza e ha affrontato i requisiti di conformità per oltre 10.000 risorse non conformi. La rapida implementazione ha comportato una riduzione del rischio nonché un notevole risparmio di costi e risorse.

Il team Professional Services di Akamai ha aiutato la banca a trasformare completamente i processi di segmentazione. Oggi, le policy di etichettatura e segmentazione delle risorse sono completamente automatizzate e integrate nei processi di sviluppo e distribuzione delle applicazioni. La creazione di etichette, la gestione delle modifiche, gli incidenti di sicurezza e le richieste di assistenza sono completamente integrati nei workflow di ServiceNow. Il cliente è rimasto estremamente soddisfatto dei risultati della piattaforma e del valore che ha fornito insieme ai team dell'assistenza tecnica competenti e dedicati di Akamai.



Ulteriori informazioni su Akamai Guardicore Segmentation sono disponibili sul sito akamai.com/guardicore

1 "Che cosa sono le sanzioni del GDPR?" GDPR.eu, 13 febbraio 2019.

2 "Il costo di una violazione di dati nel 2022", IBM.

3 "Guida completa all'adozione del cloud nel settore bancario in Europa", Techerati, 31 ottobre 2019.

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 ed evolvere la vostra strategia di sicurezza per favorire il modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS, offrendovi la sicurezza necessaria per concentrarvi costantemente sull'innovazione, sull'espansione e sulla trasformazione di tutto il possibile. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 06/23.