Le banche affidano i dati delle carte di credito a CCP Group e CPP si affida a Forcepoint per proteggerli

CPP Group è un'azienda globale di prodotti e servizi incentrata sui partner, specializzata nei mercati dei servizi finanziari e assicurativi. Si affida a Forcepoint per la prevenzione della perdita di dati, affrontando al contempo la duplice sfida di soddisfare i nuovi requisiti di conformità nei mercati globali e passare al cloud.

CPP Group ha una grande quantità di dati da proteggere, sia dati dei clienti diretti generati dalle linee di business di assistenza vita dell'azienda, sia dati ultrasensibili che banche e società di carte di credito le affidano affinché li salvaguardi nell'ambito dei suoi servizi di protezione delle carte e prevenzione delle frodi. L'azienda ha bisogno di un framework di protezione dei dati flessibile e in grado di proteggere i dati decentralizzati e distribuiti nei cloud in più paesi.

PROFILO CLIENTE
CPP sviluppa e fornisce prodotti assicurativi e di protezione del credito per i consumatori.

SETTORE
Servizi finanziari

SEDE CENTRALE
Regno Unito

PRODOTTO/I
› Forcepoint Web Security Cloud
› Forcepoint Data Loss Prevention

Fondata nel Regno Unito nel 1980, CPP Group oggi genera circa il 65% dei suoi ricavi in India, principalmente attraverso attività di protezione delle carte, garanzia estesa e assicurazione sulla telefonia mobile. Il cambiamento della geografia produttiva della sua attività ha creato nuove sfide per il team di sicurezza IT di CPP.

I servizi CPP per la protezione delle carte e l'assicurazione sulla telefonia sono particolarmente sensibili ai rischi per la sicurezza. Queste attività implicano la tutela dei dati finanziari sensibili dei titolari per gli emittenti di carte di pagamento di terzi, ad esempio banche e società di carte di credito. In qualità di società britannica, durante il trattamento di tali dati CPP deve rispettare il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea. Ma deve anche rispettare lo Standard PCI DSS (Payment Card Industry Data Security Standard), le linee guida ISO 27001 e gli standard nazionali di protezione dei dati nei singoli paesi in cui opera.

Ad esempio, l'India ha recentemente emanato leggi che impongono alle società di servizi finanziari che operano sul territorio di archiviare localmente i dati finanziari, come i dati sulle carte di pagamento ad uso di privati. Altri paesi in cui opera CPP, come la Turchia, stanno studiando normative simili per i dati finanziari.

Affrontare le sfide poste dalle nuove normative sulla residenza dei dati in India

Secondo Patrick Viner, IT Operations Manager di CPP, tutto questo ha messo sotto pressione CPP, spingendola a proteggere i dati a livello locale, consentendone comunque il trasferimento sicuro tra la sede centrale nel Regno Unito e altri uffici internazionali, se e quando necessario.

Fino a poco tempo fa, l'azienda conservava tutti i dati delle carte presso il suo data center nel Regno Unito e gestiva tutti i database sul suo sistema di policy nel Regno Unito. Ora, però, questi dati devono essere protetti in un ambiente cloud AWS (Amazon Web Services), nonché localmente nel Regno Unito, in India e in altre località globali, mentre la policy del database è ancora mantenuta e stabilita nel Regno Unito.

La sfida è quella di preservare la fluidità del flusso di lavoro e, allo stesso tempo, adottare una "policy di sicurezza dei dati più complessa, poiché un numero crescente di paesi esige che la residenza dei dati rimanga locale", ha dichiarato Viner. "Siamo nel bel mezzo di un imponente progetto di sviluppo di una nuova piattaforma per ospitare il modello in modo che tutti i dati siano conservati localmente nei paesi in cui l'azienda gestisce i servizi delle carte di pagamento".

Trasferimento degli standard di sicurezza locali al cloud

CPP è un cliente di lunga data di Forcepoint: utilizza le appliance Web Security locali per proteggere il traffico web mediante VPN e proxy web tramite il data center nel Regno Unito. Questo approccio di instradamento del traffico, però, ha cominciato a creare ritardi nella trasmissione delle informazioni, causando un calo della produttività poiché un numero crescente di attività quotidiane della CPP avveniva al di fuori del Regno Unito e, in particolare, in India.

L'azienda voleva recuperare quella perdita di produttività passando a operazioni IT più basate sul cloud, e continuando a salvaguardare i dati sia per proteggere i suoi clienti sia per motivi di conformità alle leggi e di continuità operativa. Per realizzare questo obiettivo, CPP ha scelto Forcepoint come suo partner.

"In primo luogo, siamo passati a un'architettura ibrida, adottando dei client endpoint di Web Security in alcuni dei paesi in cui operiamo", ha dichiarato Viner. "Poi, abbiamo deciso di smantellare il data center nel Regno Unito e passare a un ambiente VPC (Virtual Private Cloud). A quel punto, ho preso la decisione di eliminare tutte le appliance fisiche per passare completamente al cloud, dove attualmente svolgiamo tutte le nostre operazioni".

Sfide

La protezione del traffico mediante l'instradamento dei dati nel data center nel Regno Unito iniziava a causare ritardi e cali di produttività.

Per operare in più paesi era necessario ottemperare a diversi standard di protezione dei dati.

Soluzione

Passare a Forcepoint Web Security Cloud per migliorare il flusso di traffico senza compromettere la sicurezza.

Implementare Forcepoint Data Loss Prevention per aumentare la visibilità sul trasferimento dei dati e provvedere alla conformità a normative complesse.

Forcepoint DLP rileva i comportamenti che mettono a rischio i dati

Durante una prova di Data Loss Prevention (DLP) di Forcepoint, il team di sicurezza CPP ha scoperto che colleghi e partner commerciali in India erano potenzialmente in grado di adottare comportamenti a rischio come l'invio per e-mail di fogli di calcolo con i dati dei clienti senza supervisione, con il rischio che dati sensibili fossero inviati accidentalmente o intenzionalmente al destinatario sbagliato. Il team di sicurezza CPP ha notato anche l'assenza di qualsiasi misura volta a impedire ai colleghi di caricare i file dei potenziali clienti su siti web non protetti.

Forcepoint DLP ha aiutato CPP a far emergere questo comportamento potenzialmente rischioso e, allo stesso tempo, le ha evitato i cali della produttività che sarebbero stati causati dall'uso di checkpoint di sicurezza e dal lento instradamento del traffico dati con interruzione del flusso di lavoro.

Forse, come ha ribadito Viner, l'aspetto migliore è che il suo team è stato in grado di ottimizzare la policy DLP sulla base del feedback degli utenti stessi. La robusta libreria di policy pronta all'uso di Forcepoint DLP include policy predefinite che sono conformi alle normative regionali e di settore, come GDPR e PCI-DSS. Altre policy predefinite comunemente utilizzate sono realizzate per conformarsi alle normative sui dati sanitari protetti (PHI), come l'Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti e le normative finanziarie derivate dal Comitato di Basilea per la vigilanza bancaria nell'Unione europea.

> "Con l'aiuto di Forcepoint, abbiamo trovato il giusto equilibrio tra sicurezza e produttività".
>
> **PATRICK VINER,** IT OPERATIONS MANAGER, CPP GROUP

Viner sostiene che, grazie all'applicazione delle policy DLP appropriate, CPP è stata in grado di apportare modifiche minuziose per ridurre i falsi positivi e soddisfare tutti i requisiti di conformità, senza incidere sulla produttività dei dipendenti.

"È possibile applicare dei criteri molto restrittivi, ma in tal caso si penalizza la produttività degli utenti. D'altro canto un livello di severità troppo basso, senza monitoraggio e privo di allerte, mette a rischio la sicurezza", ha affermato. "Con l'aiuto di Forcepoint, abbiamo trovato il giusto equilibrio tra sicurezza e produttività".

Risultati

Identificare e bloccare il trasferimento rischioso dei dati e, al contempo, consentire il giusto equilibrio tra sicurezza e produttività.

Forcepoint