CAME Group risparmia €1.8 milioni ed elimina oltre 100 dispositivi dalla rete, centralizzando i sistemi su piattaforme di sicurezza di nuova generazione Palo Alto Networks®

INFORMAZIONI

CAME Group opera in 118 Paesi con 480 filiali e rivenditori autorizzati. Grazie ai brand BPT e Urbaco, il gruppo ricopre un ruolo chiave nel mercato dell'automazione domestica, della pianificazione urbanistica e dell'alta sicurezza, in cui offre soluzioni integrate per la regolarizzazione e il monitoraggio di flussi di persone e access point. CAME Group opera per il 70% a livello internazionale. L'azienda è estremamente orgogliosa del suo patrimonio italiano e dà lavoro a oltre 1.200 persone. Le vendite hanno raggiunto i 215 milioni di euro nel 2013.

TROPPE RETI E DISPOSITIVI DIVERSI

Con 15 uffici in Italia e altri 50 in 40 Paesi, la rete CAME Group deve coprire lunghe distanze e proteggere moltissimi sistemi. CAME acquisisce dalle cinque alle sei compagnie ogni anno, il che fa lievitare il numero di utenti e della rete e di luoghi in cui opera. Per questo, si rendono spesso necessarie operazioni di integrazione e di protezione di una rete che impiega tecnologie disparate.

I 2.000 utenti di CAME si affidano ad applicazioni ERP e CRM, di posta elettronica e di business intelligence nonché a software aziendali basati su oggetti. Tutti i servizi vengono erogati dai tre grandi data center ubicati in Italia. Con il consolidarsi a livello internazionale delle compagnie che fanno capo a CAME Group, l'apertura di nuove sedi e l'acquisizione di nuove compagnie sono iniziati a sorgere i primi problemi. "La nostra rete era eterogenea e non eravamo in grado di implementare servizi in modo sicuro in tutte le filiali in modo centralizzato né di gestire l'IT in maniera efficiente," afferma Massimiliano Tesser, Group CIO, CAME Group. "I servizi Web, le transazioni commerciali e di e-commerce in tutto il mondo erano gestiti e protetti da 50 firewall Cisco ASA 5540 e da altri firewall, nonché e da circa 50 dispositivi e server proxy. Ogni dispositivo aveva funzionalità diverse, ad esempio alcuni erano dotati di integrazione con Active Directory e altri no."

FRUSTRAZIONE DEGLI UTENTI E COSTI

La mancanza di una tecnologia di rete standard creava problemi, legati ad esempio alla gestibilità, ai costi, all'accesso alle applicazioni e al controllo, alla latenza della rete e alla sicurezza. "Ogni dispositivo o server in ciascun ufficio era configurato da un partner IT o da un dipendente diverso, senza linee guida comuni," sostiene Tesser. "Senza una gestione centralizzata, era impossibile implementare le stesse impostazioni e policy di utilizzo in tutte le filiali."

La mancanza di policy uniformi per il controllo e l'utilizzo delle applicazioni rappresentava una fonte di frustrazione per gli utenti e sovraccaricava il personale IT. "Le regole non si adattavano agli utenti durante le trasferte," dice Cristiano Bedin, ICT Manager di CAME Group. "Se un utente viaggiava dall'Italia in Russia, doveva manualmente configurare o disabilitare le impostazioni del proxy, utilizzare un diverso nome utente e chiamare un diverso numero di interno. Tutti dovevano adattarsi alla località in cui viaggiavano."

CAMEGROUP

ORGANIZZAZIONE:
CAME Group

SETTORE:
produzione

LA SFIDA:
standardizzare l'IT per abilitare policy uniformi per l'utilizzo delle applicazioni, ridurre i dispositivi di rete e migliorare la sicurezza e le prestazioni della rete.

LA SOLUZIONE:
Due dispositivi Palo Alto Networks PA-3020 e 40 dispositivi PA-200, piattaforme di sicurezza di nuova generazione con sistema di prevenzione delle minacce, filtraggio degli URL, sistemi IPS, WildFire e Panorama eseguiti su un'applicazione di gestione M-100.

I RISULTATI:

- Riduzione dei costi IT pari a €1.8 milioni in tre anni
- Visibilità e controllo delle applicazioni e implementazione di policy uniformi per l'utilizzo delle applicazioni in quasi 50 uffici
- Rimozione di oltre 100 dispositivi dalla rete internazionale
- Standardizzazione e centralizzazione dell'IT
- Eliminazione dei costi di 50 consulenti e tecnici IT
- Aumento della sicurezza e riduzione della latenza della rete

paloalto NETWORKS®

"Palo Alto Networks ha risolto tutti i nostri problemi di sicurezza e prestazioni della rete, ben oltre le nostre aspettative. Abbiamo sostituito più di 100 dispositivi con soli 42 piattaforme di sicurezza Palo Alto Networks e in tre anni abbiamo risparmiato €1.8 milioni che prima spendevamo in consulenze tecniche, manutenzione, formazione e gestione della precedente rete decentralizzata."

Massimiliano Tesser
Group CIO
CAME Group

L'inefficienza della rete eterogenea di CAME assorbiva risorse. "Le consulenze IT per la gestione e la configurazione dei dispositivi ci costavano €36.724 a filiale ogni anno," confessa Tesser. "Dovevamo rivolgerci a tantissime persone, anche solo per modificare le configurazioni dei server proxy e per gestire le operazioni di rete."

Con così tanti dispositivi di rete diversi, tutti gestiti da vari consulenti e personale IT, garantire un livello di sicurezza elevato era un vero problema. "I firewall e gli altri dispositivi non erano in grado di identificare e di bloccare alcuni tipi di minacce o applicazioni rischiose o che non dovevano utilizzare la larghezza di banda," afferma Tesser. "Nel nostro settore, i progetti ingegneristici e altri tipi di allegati email sono molto comuni. I sistemi che utilizzavamo non riuscivano a rilevare alcune minacce presenti negli allegati. Inoltre, non eravamo in grado di identificare e controllare l'uso di Skype, che può veicolare virus e rappresenta un rischio di potenziali perdite di proprietà intellettuale, data la possibilità per gli utenti di scambiare file aziendali senza alcuna capacità di rilevamento."

L'incapacità di CAME di identificare, controllare e gestire le applicazioni e il traffico influiva sulla disponibilità di larghezza di banda, che a sua volta generava problemi di latenza della rete. "Le nostre filiali erano connesse tramite VPN o MPLS, ma durante i picchi di traffico si verificavano problemi di QoS della connettività," afferma Tesser. "La disponibilità delle applicazioni calava durante i picchi di traffico e i rumori di sottofondo oltre alle chiamate interrotte, soprattutto per i nostri call center, ponevano seri problemi,"

DEVE ESSERCI UN MODO MIGLIORE

La dirigenza di CAME ha riconosciuto a un certo punto che la rete decentralizzata influiva negativamente sulle prestazioni aziendali. "Ha quindi autorizzato il nostro team a centralizzare la gestione della rete, aumentare la protezione, raccogliere e segnalare meglio le informazioni sulla rete e standardizzare l'accesso alle applicazioni e le policy di protezione per tutte le sedi internazionali," afferma Tesser.

Fu quindi convocato lo storico partner tecnologico di CAME, NGS Srl, a cui va dato un merito importante per l'eccellente riuscita tecnica dell'intero progetto. Oltre a esaminare le soluzioni di Cisco e Fortinet, NGS Srl suggerì Palo Alto Networks. La piattaforma di sicurezza di nuova generazione Palo Alto Networks integra in modo nativo tutte le funzioni di sicurezza della rete, incluso un firewall di nuova generazione, sistemi di filtraggio degli URL, IDS/IPS e funzionalità di protezione avanzata dalle minacce. Tali funzioni sono sviluppate e integrate nella piattaforma e condividono in modo nativo le informazioni importanti in modo sinergico tra le rispettive finalità, per garantire una protezione superiore rispetto ai firewall legacy, agli UTM o ai prodotti di rilevamento di minacce specifiche. Con una velocità di elaborazione fino a 120 Gb/s, Palo Alto Networks è in grado di abilitare in modo sicuro l'uso di tutte le applicazioni, di garantire visibilità e controllo completi e di proteggere le imprese dagli attacchi informatici dai più comuni ai più sofisticati, conosciuti e sconosciuti.

TROVARE LA SOLUZIONE GIUSTA

Tesser e il suo team hanno esaminato le opzioni e scelto Palo Alto Networks. "Era evidente che la Palo Alto Networks fosse in grado di esaminare a fondo le applicazioni, di controllarle e autorizzarle consentendoci facilmente di applicare un nuovo standard di controllo e sicurezza in tutte le sedi," sostiene Tesser. "Ci consentiva inoltre di decidere quali utenti bloccare, quelli a cui concedere l'accesso a Skype e ad altre applicazioni per ottimizzare la larghezza di banda e aumentare la sicurezza."

"Da quando abbiamo consolidato i sistemi sulle piattaforme Palo Alto Networks, siamo in grado di implementare policy di sicurezza e di gestire tutte le piattaforme di sicurezza da un'interfaccia centralizzata. I nostri dirigenti non riescono a credere di poter accedere in tutta sicurezza alla rete da qualsiasi luogo, con tablet o telefoni cellulari proprio come farebbero dall'ufficio domestico."

Massimiliano Tesser
Group CIO
CAME Group

Il gruppo IT di CAME ha apprezzato i benefici della visibilità della rete offerta da Palo Alto Networks. "Abbiamo visto che potevamo impedire ai pacchetti non autorizzati di accedere alla rete e ottenere informazioni in tempo reale sui tentativi di intrusione, anche quelli che i dispositivi Cisco non riuscivano a identificare."

Un altro enorme vantaggio per CAME è stato Panorama, il software di Palo Alto Networks che fornisce la gestione centralizzata e le funzionalità di registrazione per gestire facilmente tutte le piattaforme di sicurezza e le policy Web da una singola posizione. "Abbiamo constatato che Panorama ci avrebbe permesso di creare, configurare e distribuire le medesime policy di sicurezza alle filiali in tutto il mondo con una singola soluzione."

IMPLEMENTAZIONE SEMPLICE IN UFFICI IN TUTTO IL MONDO

CAME ha acquistato e installato le piattaforme di sicurezza di nuova generazione Palo Alto Networks PA-3020 con alta disponibilità. Applicando i principi Zero Trust, una piattaforma di sicurezza Palo Alto Networks viene posizionata al cospetto di ciascuna zona e funge da firewall principale del data center.

Nelle filiali, CAME ha implementato 40 piattaforme di sicurezza PA-200 in Virtual Wire con connessioni VPN ridondanti e protette stabilite per gli utenti remoti. Ciascun ufficio CAME dispone ora della propria connessione a Internet attraverso un dispositivo di sicurezza Palo Alto Networks. Ogni piattaforma di sicurezza Palo Alto Networks implementata da CAME è dotata di sistemi di filtraggio degli URL e IPS per proteggere la rete dalle minacce conosciute. WildFire® offre la protezione integrata da malware e minacce avanzate attraverso l'identificazione proattiva e il blocco delle minacce sconosciute comunemente utilizzate nei moderni attacchi informatici. L'implementazione include il software Panorama eseguito su un'applicazione di gestione M-100 per la gestione centralizzata della configurazione dei dispositivi e l'implementazione delle policy per tutti i dispositivi Palo Alto Networks.

"Siamo soddisfatti di come Palo Alto Networks ci consenta di implementare in Virtual Wire," afferma Tesser. "Per noi ha significato la totale trasparenza sulla rete dell'introduzione delle piattaforme di sicurezza, fatto estremamente importante per noi."

SICUREZZA E ACCESSO PER TUTTI

Tesser e il suo team sono riusciti a soddisfare tutte le richieste della dirigenza CAME, inclusa la standardizzazione dell'IT, la gestione e il controllo centralizzati della rete, l'implementazione di policy di accesso utente uniformi, la sicurezza avanzata, una maggiore affidabilità delle applicazioni e servizi migliorati per gli utenti finali.

La gestione centralizzata garantisce uno dei principali vantaggi che Palo Alto Networks ha messo a disposizione di CAME. Tutto il traffico che affluisce attraverso ciascuna piattaforma di sicurezza viene registrato in Panorama, il che consente a CAME di eseguire analisi sul traffico, di indagare rapidamente e di rispondere agli incidenti di sicurezza e di raccogliere informazioni di controllo da una singola posizione centralizzata. "Gestiamo centralmente tutte le policy delle applicazioni e di sicurezza, inclusa la prevenzione delle minacce, e distribuiamo i servizi a tutti i siti, garantendone la qualità, dai nostri data center," afferma Tesser. "Questo ci ha resi molto più efficienti e ha facilitato l'integrazione di nuove filiali. Uno degli aspetti che più apprezzo della soluzione Palo Alto Networks è la capacità di adattarsi alle reti eterogenee delle compagnie che acquisiamo. Con Panorama, possiamo configurare, gestire e distribuire policy ai dispositivi Palo Alto Networks e raramente si verifica la necessità di comunicare con il nuovo ufficio."

Un ulteriore miglioramento sostanziale garantito da Panorama è la creazione di policy uniformi che assicurano coerenza per tutti gli utenti, a prescindere dalla posizione o dal tipo di dispositivo. "La capacità delle piattaforme di sicurezza Palo Alto Networks di riconoscere gli utenti e applicare le policy in qualsiasi luogo, anche su dispositivi mobili, è eccezionale," afferma Tesser. "Le regole sono valide e coerenti in qualsiasi filiale o località e gli utenti vengono automaticamente autenticati dalla rete senza necessità di modificare le credenziali." Non si spreca più tempo ad assistere il personale in trasferta con problemi di accesso. "Le chiamate relative ai problemi di accesso sono ormai totalmente azzerate," afferma Tesser. "I dirigenti ci dicono: 'Posso vedere tutto proprio come quando sono in ufficio'. Dopo anni di frustrazione, questa è una straordinaria conquista per loro."

RISULTATI DEGNI DI NOTA

La maggiore visibilità delle rete e il controllo di livello superiore hanno risolto i problemi relativi alla sicurezza e alla disponibilità della larghezza di banda. "Ora possiamo bloccare Skype e controllare tutte le altre attività di rete," dice Tesser. "Apprezziamo inoltre la flessibilità di poter definire diritti di accesso per lati specifici della rete: uno per l'accesso protetto dei consulenti e l'altro per utenti guest o accessi pubblici."

Le funzionalità di rilevamento delle minacce e di generazione di report della soluzione Palo Alto Networks sono ulteriori fattori che garantiscono ottimi risultati. "Possiamo facilmente generare e inviare report sugli elementi eliminati e controllati sulla rete," descrive Tesser. "Abbiamo inoltre posizionato un tabellone elettronico dietro la reception che mostra al consiglio e ai dirigenti tutti gli elementi rilevati e bloccati ogni giorno con Palo Alto Networks."

WildFire ricopre un ruolo chiave nel miglioramento della protezione della rete di CAME. "WildFire è molto importante," afferma Tesser. "Nel momento in cui rileva un elemento danneggiato o una potenziale minaccia, la identifica rapidamente e tutti i nostri sistemi vengono istantaneamente protetti. Il precedente sistema di protezione analizzava gli allegati di posta elettronica che attraversavano il nostro server di posta elettronica centralizzato. In molti casi, le minacce erano invisibili a tale sistema e penetravano attraverso la rete. WildFire risolve questo problema e ci garantisce lo stesso livello di scansione in tempo reale del traffico che affluisce dalla rete pubblica a quella privata. Una volta constatata l'efficacia di WildFire, lo abbiamo esteso a tutti i dispositivi e tutte le filiali."

La larghezza di banda e la latenza della rete non sono più un problema. "Diamo priorità ai pacchetti di traffico per assicurare la reattività delle applicazioni principali, abbiamo eliminato i rumori di sottofondo, le interruzioni delle chiamate e altri problemi di disponibilità delle applicazioni," sostiene Bedin.

Probabilmente la facilità di configurazione e implementazione della soluzione Palo Alto Networks è stato per CAME un fattore importante quanto i vantaggi stessi della soluzione. "La tecnologia è eccellente, ma è altrettanto importante collaborare con un partner in grado di fornire il provisioning, soprattutto per una grande compagnia con molti uffici in tutto il mondo," afferma Tesser. "La tecnologia Palo Alto Networks è configurata nel modo giusto e si integra facilmente con tutti i nostri servizi. In precedenza, non potevamo implementare tutti i servizi ERP e CRM in tutte le filiali; ora possiamo farlo in modo protetto, centralizzato ed efficiente."

RISPARMI NELL'ORDINE DEI MILIONI

Consolidando l'infrastruttura IT su piattaforme di sicurezza Palo Alto Networks, CAME è riuscita a ridurre i dispositivi sulla rete e ad eliminare le costose consulenze. "Abbiamo sostituito oltre 100 firewall e dispositivi proxy con soli 42 dispositivi di sicurezza Palo Alto Networks," afferma Tesser. "In tre anni, abbiamo risparmiato €36.724 in ciascuna filiale, ovvero circa €1.8 milioni in totale, che prima spendevamo per tecnici, consulenti, manutenzione, formazione del personale IT, configurazione e gestione di una rete eterogenea."

CAME sta reinvestendo i risparmi in altri progetti di business e servizi. "Il tempo e il denaro risparmiati sono significativi ed evidenti al nostro CdA," afferma Tesser. "Abbiamo riallocato le risorse IT su altri progetti aziendali, come la distribuzione efficace di un'applicazione CRM interna a tutte le filiali. Prima di adottare la soluzione Palo Alto, avevamo tre o quattro persone e almeno una persona in ciascuna filiale dedicate alla gestione del sistema CRM."

CAMBIARE PROSPETTIVA

CAME Group è entusiasta della decisione di installare le piattaforme di sicurezza di nuova generazione Palo Alto Networks. "Palo Alto Networks ha cambiato la prospettiva del nostro team IT riguardo ai problemi di sicurezza," sostiene Tesser. "Tutti i nostri problemi di sicurezza sono stati risolti ben oltre le nostre aspettative. I colleghi CIO in due compagnie in Australia e a Londra, operanti entrambe a livello globale, utilizzavano Cisco, ma ora stanno migrando alla soluzione Palo Alto Networks sulla base della mia esperienza."

paloalto NETWORKS®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com