Azienda leader nel mercato dell'automazione degli edifici risparmia oltre 2,5 milioni di dollari grazie a una rete consolidata con prevenzione delle minacce e protezione degli endpoint

CAME
safety&comfort

“Palo Alto Networks fornisce a CAME la più completa soluzione di protezione per la rete e per tutti i dispositivi endpoint dell’azienda. Con un’infrastruttura protetta, anche le nostre attività sono al sicuro”.

Massimiliano Tesser | CIO | *CAME Group*

CAME Group

CAME Group opera in 118 Paesi con 480 filiali e rivenditori autorizzati. Con i brand Bpt, Urbaco, Parkare e GO, CAME Group ricopre un ruolo chiave nel mercato della domotica, della pianificazione urbanistica e dell’alta sicurezza, in cui offre soluzioni integrate per regolare e monitorare i flussi di persone e i punti di accesso. Circa il 70% delle attività di CAME Group si svolge a livello internazionale. L’azienda è molto fiera delle sue origini italiane e dà lavoro a oltre 1.500 persone; le vendite hanno raggiunto i 250 milioni di euro nel 2015.

Settore

Produzione

La sfida

Proteggere gli endpoint dagli attacchi informatici mirati, come CryptoLocker, per ridurre al minimo le interruzioni delle attività produttive ed eliminare i costi imprevisti delle riparazioni. Migliorare la sicurezza della rete in tutta l’azienda con policy coerenti per eliminare le vulnerabilità e il traffico non autorizzato che riducono le prestazioni delle applicazioni e la produttività dei dipendenti.

La soluzione

La piattaforma di protezione di nuova generazione Palo Alto Networks® implementata nel data center centrale e in 50 filiali offre maggiore visibilità e controllo del traffico di rete, tenendo automaticamente alla larga gli attacchi informatici dai dispositivi endpoint o dalla rete aziendale.

Servizi in abbonamento

Threat Prevention, URL Filtering (PAN-DB), WildFire™, Traps™, Panorama™

Applicazioni

PA-3020 (4), PA-200 (40), PA-500 (10), M-100 (1)

I risultati

- Risparmio di circa 2,5 milioni di dollari in tre anni grazie alla protezione consolidata
- Taglio dei costi di riparazione degli endpoint (250.000 dollari) in tre anni
- Blocco delle minacce informatiche sulla rete e sugli endpoint
- Miglioramento delle prestazioni della banda e delle applicazioni con un altissimo livello di visibilità e controllo del traffico di rete
- Implementazione di policy di sicurezza coerenti in tutta l’azienda

Riepilogo

CAME Group (CAME) offre sistemi di automazione residenziali e industriali per cancelli e porte, parcheggi e punti di controllo degli accessi. Con 50 filiali in 40 Paesi, tutte connesse alla sede italiana, CAME necessitava di un’architettura di rete in grado di proteggere gli endpoint e l’accesso alla rete. In passato, il gruppo ha subito spesso attacchi malware mirati, come CryptoLocker, che infiltrandosi su server e computer compromettevano la produttività aziendale e causavano costi di riparazione imprevedibili. I software antivirus tradizionali non erano una risposta efficace.

Con la piattaforma di protezione di nuova generazione Palo Alto Networks con Next-Generation Firewall, Threat Intelligence Cloud e Advanced Endpoint Protection, CAME è riuscita a impedire in modo efficace che le minacce informatiche infettassero i dispositivi endpoint e la rete aziendale. Grazie al consolidamento, CAME in tre anni ha risparmiato 2,5 milioni di dollari e 250.000 dollari in riparazioni dei dispositivi endpoint. Inoltre, il gruppo può ora contare su policy di sicurezza coerenti implementate in tutta l’azienda e su un altissimo livello di visibilità e controllo del traffico di rete che aiuta a razionalizzare il consumo di larghezza di banda e a migliorare le prestazioni delle applicazioni.

Stop agli attacchi sugli endpoint

Con attività in 118 Paesi, CAME Group si affida a una rete globale che collega dipendenti, clienti e partner 24 ore su 24, 365 giorni all’anno, nei 50 uffici dell’azienda, con connessioni remote o anche in movimento. Tuttavia, ogni volta che un utente accede a sistema CRM aziendale, condivide un file tramite email, usa Skype con un cliente o comunica e collabora online con i colleghi, si espone a potenziali minacce informatiche.

Pur implementando i migliori sistemi di protezione di rete disponibili sul mercato, gli endpoint di CAME erano esposti agli attacchi mirati sferrati da exploit sofisticati o al download e alla condivisione di file eseguibili dannosi. Come la maggior parte delle aziende, anche CAME disponeva di soluzioni antivirus tradizionali per proteggere gli endpoint aziendali. D’altro canto, i sistemi antivirus basati sulle firme nulla possono contro le odierne minacce in continua evoluzione e gli attacchi zero day avanzati ed estremamente rapidi.

Di fatto, CAME ha spesso dovuto fronteggiare attacchi simili, molti dei quali difficilmente rilevabili prima di aver già causato danni seri. La rimozione di CryptoLocker, in particolare, ha richiesto ingenti investimenti in termini di tempo e costi nonché spese aggiuntive per il ripristino dei dati perduti. A causa dell’aumento di attacchi dannosi, l’azienda si ritrovava con costi di riparazione del tutto imprevedibili che stravolgevano completamente il budget destinato all’IT.

"Abbiamo scelto Traps perché, a differenza di altri approcci, blocca in modo affidabile exploit e malware, anche sconosciuti, su tutti gli endpoint indipendentemente dalla posizione".

Massimiliano Tesser | CIO | *CAME Group*

Massimiliano Tesser, CIO di CAME Group, spiega la strategia dell'azienda per fronteggiare la situazione: "Prima di tutto abbiamo valutato l'impatto delle minacce avanzate sugli endpoint aziendali, quindi abbiamo cercato di individuare un modo per impedire gli attacchi".

CAME ha compreso che, fondamentalmente, tutti gli utenti erano vulnerabili se collegati a Internet. Un altro problema erano i rischi di esposizione involontaria alle minacce tramite l'uso di dispositivi rimovibili, ad esempio le unità USB. Con i tantissimi dipendenti che si spostano in ogni parte del mondo, il gruppo necessitava di una modalità coerente per proteggere i dispositivi degli utenti finali, a prescindere dalla modalità e dal luogo di connessione.

"È molto difficile proteggere gli endpoint in modo coerente sempre e dovunque", sottolinea Tesser. "Eravamo alla ricerca di una soluzione completa che ci permettesse di tenere sotto controllo tutti i computer con un livello di visibilità adeguato per rilevare la posizione degli attacchi e verificare che fossero stati correttamente bloccati".

CAME ha preso in considerazione soluzioni Trend Micro e McAfee di Intel Security, ma alla fine ha scelto Traps Advanced Endpoint Protection di Palo Alto Networks per affiancare le tecnologie e la piattaforma di sicurezza Palo Alto Networks già esistenti.

Tesser racconta: "Abbiamo scelto Traps perché, a differenza di altri approcci, blocca in modo affidabile exploit e malware, anche sconosciuti, su tutti gli endpoint indipendentemente dalla posizione".

Sicurezza informatica capillare

CAME ha implementato Traps all'interno di una strategia completa per la sicurezza informatica basata sulla piattaforma di protezione di nuova generazione Palo Alto Networks con Next-Generation Firewall, Threat Intelligence Cloud e Advanced Endpoint Protection. La piattaforma garantisce visibilità e controllo di applicazioni, utenti e contenuti, nonché protezione contro minacce informatiche conosciute e sconosciute.

In collaborazione con lo storico partner tecnologico, NGS Srl., Traps è stato distribuito su circa 1000 server, computer e laptop per proteggere a regime oltre 1600 dispositivi endpoint. Oltre a Traps Advanced Endpoint Protection, sono stati installati quattro firewall di nuova generazione PA-3020 Palo Alto Networks nella sede centrale, per mettere in sicurezza il data center. Altri firewall di nuova generazione, 40 PA-200 e 10 PA-500, sono stati installati nelle filiali con connessioni VPN ridondanti e sicure per gli utenti remoti. Tutti i firewall di nuova generazione Palo Alto Networks sono stati configurati con prevenzione delle minacce e filtraggio degli URL (PAN-DB). Panorama di Palo Alto Networks offre la gestione centralizzata delle configurazioni dei dispositivi, l'applicazione di policy coerenti e la generazione di report nell'intera rete protetta.

CAME ha inoltre implementato WildFire di Palo Alto Networks, che offre servizi cloud di intelligence per le minacce. WildFire identifica e blocca in modo proattivo le minacce informatiche più avanzate, conosciute e sconosciute, sfruttando funzionalità di intelligence centralizzate e adottando automaticamente misure di sicurezza preventive. L'integrazione di WildFire e Traps si è rivelata particolarmente importante per CAME.

"Traps si è dimostrata l'unica soluzione di protezione degli endpoint sul mercato integrata in modo nativo con WildFire", dichiara Tesser. "Questo aspetto è stato per noi particolarmente rilevante poiché ci ha permesso di proteggerci dagli attacchi zero day, un vero incubo per noi. WildFire fornisce analisi dinamica e aggiornamenti continui che bloccano anche le minacce sconosciute prima che riescano a compromettere un dispositivo endpoint o la rete. Gli altri prodotti intervenivano solo in una fase avanzata dell'attività malware, esponendo gli endpoint a seri rischi di interruzione".

Provare per credere

CAME ha potuto apprezzare i risultati di Traps subito dopo l'implementazione. Infatti, già dalle prime fasi della distribuzione, Traps ha identificato e bloccato un tentativo di CryptoLocker sui dispositivi endpoint in diverse filiali del gruppo.

"Abbiamo visto nella pratica quanto Advanced Endpoint Protection funzionasse", afferma Tesser. "Spesso si pensa che non ci siano problemi, ma solo perché non si è consapevoli di un attacco in corso. Grazie a Traps possiamo sapere cosa succede e assistere al blocco degli attacchi malware in tempo reale".

Traps non solo garantisce a CAME che i dispositivi endpoint siano al sicuro dalle minacce informatiche, ma ha anche eliminato i costi delle riparazioni, in passato frequenti e difficili da gestire.

"Traps si è dimostrata l'unica soluzione di protezione degli endpoint sul mercato integrata in modo nativo con WildFire". Questo aspetto è stato per noi particolarmente rilevante poiché ci ha permesso di proteggerci dagli attacchi zero day, un vero incubo per noi."

Massimiliano Tesser | Group CIO | *CAME Group*

"A seguito degli attacchi CryptoLocker, non solo abbiamo dovuto affrontare i costi di ripristino dei dati, ma anche quelli legati al tempo e alle risorse aziendali", racconta Tesser. "Grazie a Traps, ora quei costi sono solo un vago ricordo e prevediamo di risparmiare 250.000 dollari nei prossimi tre anni".

Questo risparmio va a sommarsi all'ancor più significativa riduzione dei costi ottenuta grazie all'implementazione della piattaforma completa di protezione di nuova generazione Palo Alto Networks. In precedenza, CAME impiegava oltre 100 firewall Cisco, ciascuno con diverse funzionalità. Ogni filiale configurava e gestiva il proprio dispositivo, spesso chiedendo l'intervento di consulenti, che costavano all'azienda 50.000 dollari per filiale ogni anno. Consolidando l'infrastruttura su una piattaforma di sicurezza Palo Alto Networks, CAME è riuscita a ridurre i dispositivi sulla rete e a eliminare le costose consulenze. In tal modo risparmierà circa 2,5 milioni di dollari in tre anni.

Controllo e prevenzione coerenti

Grazie alla piattaforma di protezione di nuova generazione Palo Alto Networks con Next-Generation Firewall, Threat Intelligence Cloud e Advanced Endpoint Protection, CAME può ora contare su una protezione capillare dalle minacce informatiche. Con una visibilità migliorata e le funzionalità di prevenzione integrate, il team addetto alla sicurezza può tenere sotto controllo tutto il traffico di rete, recuperare informazioni in tempo reale sui tentativi di intrusione e bloccare automaticamente i pacchetti non autorizzati che tentano di penetrare la rete o i dispositivi.

La capacità di identificare, controllare e gestire le applicazioni e il traffico influisce anche sulla disponibilità di larghezza di banda, eliminando i problemi di latenza della rete. In precedenza, il traffico non autorizzato causava problemi di connessione, soprattutto per il call center, nelle ore di punta. Anche la disponibilità delle applicazioni subiva una riduzione durante i momenti di picco. Ora questi problemi appartengono al passato.

"Abbiamo assegnato diverse priorità ai pacchetti di traffico per assicurare la disponibilità e la reattività delle applicazioni principali", sostiene Tesser. "Questo approccio libera anche la larghezza di banda, eliminando i disturbi e le interruzioni durante le chiamate, motivo di grande frustrazione per clienti e dipendenti".

Inoltre, tutto il traffico che affluisce attraverso ciascuna piattaforma Palo Alto Networks viene registrato in Panorama. Questo permette di analizzare il traffico, esaminare gli incidenti di sicurezza e adottare subito misure correttive, nonché raccogliere tutti i dati di controllo da una singola posizione centralizzata. Inoltre, per CAME aprire nuove filiali è ora più semplice ed efficiente.

"Uno degli aspetti che più apprezzo della piattaforma Palo Alto Networks è la capacità di adattarsi alle reti eterogenee delle compagnie che acquisiamo", sottolinea Tesser. "Grazie a Panorama, possiamo configurare, gestire e distribuire policy di sicurezza nell'intera piattaforma ed essere certi che siano applicate in modo coerente. In questo modo, tutti gli utenti, a prescindere dal luogo in cui si trovano e dal dispositivo endpoint che utilizzano, sono costantemente protetti".

Infrastruttura protetta, azienda al sicuro

In definitiva, la protezione capillare è fondamentale per la corretta esecuzione delle attività aziendali di CAME. Tesser sottolinea che le vulnerabilità espongono i PC agli attacchi malware e le reti agli hacker con conseguenze gravi come il furto di informazioni aziendali proprietarie. Tali minacce rallentano o interrompono del tutto la produttività e, nei peggiori casi, bloccano i flussi di ricavi e riducono la fiducia dei clienti.

"È fondamentale che tutti i dipendenti lavorino in un ambiente protetto e sicuro", afferma Tesser. "Questo si ottiene non solo mettendo in sicurezza la rete, ma anche proteggendo gli endpoint con tecnologie avanzate. I dispositivi endpoint, ad esempio computer o smartphone, sono infatti il primo contatto tra l'azienda e il mondo esterno, essi sono collegati ai server aziendali con i quali scambiano informazioni: qualsiasi vulnerabilità ci espone al rischio di potenziali attacchi o minacce. Ecco perché, se la rete è l'obiettivo di eventuali attacchi, Traps Advanced Endpoint Protection è la soluzione ottimale. Non c'è dubbio".

Tesser conclude: "Palo Alto Networks fornisce a CAME la più completa soluzione di protezione per la rete e tutti i dispositivi endpoint dell'azienda. Con un'infrastruttura protetta, anche le nostre attività sono al sicuro".