

Il Gruppo SeSa rafforza le proprie difese adottando soluzioni di sicurezza avanzate.

Il noto fornitore di soluzioni IT ha bloccato gli attacchi ransomware, ottenuto una visione approfondita delle attività forensi e automatizzato le attività di sicurezza che richiedono tempo



LA SFIDA

Il Gruppo SeSa, uno dei maggiori fornitori di servizi e soluzioni IT in Italia, è stato soggetto di alcuni attacchi ransomware, con frequenza maggiore nel corso del 2018, che hanno richiesto un impegno consistente da parte del reparto di Cyber Security per le attività di controllo, rimozione ed eventuale disinfestazione dei sistemi .

Il team di Cyber Security ha deciso quindi di realizzare una Software Selection con l'obiettivo di individuare una soluzione che incrementasse sensibilmente il perimetro di Cyber Security e non influenzasse negativamente le performance delle workstation dei propri collaboratori . Al termine dell'indagine, Il team valutò positivamente Bitdefender GravityZone Ultra Security.

Alberto Santini, Chief Information Security Officer di SeSa, ha spiegato, "Dopo averlo provato, Bitdefender ha dimostrato la migliore efficacia nel rilevare e risolvere le minacce, oltre a essere molto facile da usare. GravityZone Ultra offre funzionalità di rilevamento e risposta per gli endpoint e protegge la nostra intera gamma di ambienti virtuali, cloud, e fisici nel data center, e le workstation.

LA SOLUZIONE

Bitdefender GravityZone Ultra ha offerto a SeSa capacità di protezione, rilevamento e risposta per endpoint (EDR) in grado di coprire le sue 2.000 workstation Apple e Windows, oltre ai server Windows, operative nelle 20 diverse sedi della società e in Microsoft Azure cloud.

Le applicazioni protette da Bitdefender includono il sistema di gestione delle relazioni con i clienti personalizzato per SeSa, Zucchetti enterprise resource planning, oltre a Microsoft Active Directory e File Server.



SeSa S.p.A., con sede a Empoli, in Italia, fornisce alle organizzazioni soluzioni IT avanzate, tra cui software aziendale per server, sistemi di archiviazione e rete, oltre a servizi di infrastruttura, outsourcing, intelligence e gestione aziendale. L'azienda ha ottenuto ricavi per circa 1,775 milioni di euro e un EBITDA di 74,3 milioni.

Settore

Servizi e soluzioni IT

Sedi principali

Empoli, Italia

Dipendenti

2.500 (staff IT: 28)

Risultati

- Blocco completo degli attacchi ransomware
- Una visibilità sulla completa catena di eventi e comportamenti forensi che migliora la postura di sicurezza
- Il risparmio di tempo consentito dall'automazione della sicurezza ha permesso una riallocazione più intelligente delle risorse del personale IT
- Azzeramento dei problemi di sicurezza, rispetto a una media mensile precedente di circa 10

SeSa utilizza anche GravityZone Patch Management per automatizzare l'installazione delle patch dei sistemi operativi e delle applicazioni, e GravityZone Full-Disk Encryption per automatizzare la gestione della cifratura, entrambi gestiti dalla stessa console di GravityZone Ultra.

I RISULTATI

Le capacità EDR e di protezione degli endpoint combinate di GravityZone Ultra proteggono SeSa dalle minacce avanzate, consentendo al tempo stesso ai suoi analisti della sicurezza di condurre uno proattivo Threat Hunting e un'analisi delle cause alla radice. SeSa sfrutta le funzionalità di Endpoint Risk Management and Analytics per valutare, prioritizzare e affrontare i rischi derivanti da errate configurazioni e vulnerabilità degli endpoint, rafforzando ulteriormente la sua posizione di sicurezza.

"GravityZone Ultra ci offre delle ottime funzioni di automazione, Machine Learning e reportistica", ha dichiarato Santini. "Da quando abbiamo impiegato GravityZone, non abbiamo subito nemmeno un solo attacco di successo. Anche in caso di attacchi zero-day, che non hanno firme, GravityZone analizza il comportamento e blocca i malware quasi subito.

"Prima eravamo ciechi rispetto ad alcune minacce. Grazie all'accesso alle funzionalità di analisi forense di alto valore di GravityZone, possiamo visualizzare l'intera catena di eventi e il comportamento degli utenti, così da poter rispondere in modo più pronto, acquisendo al tempo stesso preziose informazioni per il futuro."

GravityZone ha anche protetto l'infrastruttura del data center virtuale di SeSa, come ha illustrato Santini: "GravityZone ha svolto un lavoro straordinario impedendo ai malware di sfruttare le vulnerabilità e diffondersi attraverso la nostra rete di server virtuali".

Santini ha apprezzato l'automazione di GravityZone delle attività molto onerose in termini di tempo, dando così al team la possibilità di concentrarsi su priorità fondamentali: "Con pochi clic nella console di GravityZone, siamo in grado di impiegare l'agente, impostare le policy, ecc. GravityZone si occupa di buona parte del lavoro che prima dovevamo fare manualmente."

Infatti, ora Santini ha assegnato degli ingegneri di sistema junior per creare le policy, impiegare gli endpoint, valutare gli incidenti ed estrarre i rapporti di valutazione. Così gli ingegneri di sistema senior hanno più tempo per focalizzarsi sulle attività di livello superiore, più in linea con la loro esperienza.

Inoltre, GravityZone ha migliorato l'esperienza e la produttività di migliaia di utenti di SeSa.

Santini ha dichiarato, "I nostri utenti si sentono più protetti e non sperimentano più prestazioni diminuite quando si eseguono gli aggiornamenti. Il numero di richieste relative a problemi di sicurezza si è praticamente azzerato, rispetto a una media mensile di una decina. In caso di problemi, Bitdefender li rileva e risolve prima ancora che l'utente ne venga a conoscenza."

Inoltre, SeSa attribuisce un grande valore alla stretta collaborazione con Bitdefender.

"La capacità di Bitdefender di ascoltare le nostre esigenze e il loro supporto clienti hanno superato notevolmente l'esperienza avuta con altri fornitori", ha aggiunto Santini. "La loro profonda conoscenza ed esperienza dei nostri requisiti di sicurezza ha reso Bitdefender il partner ideale per aiutarci nel nostro viaggio nella sicurezza informatica."

"Da quando abbiamo impiegato GravityZone, non abbiamo subito nessun attacco di successo... Grazie all'accesso a funzionalità di analisi forense di alto valore di GravityZone, possiamo visualizzare l'intera catena di eventi e il comportamento degli utenti, così da poter rispondere in modo più pronto, acquisendo al tempo stesso preziose informazioni per il futuro." Alberto Santini, Chief Information Security Office di SeSa

Impronta di Bitdefender

- GravityZone Ultra Security
- Integrazione di GravityZone Patch Management
- GravityZone Full-Disk Encryption

Ambiente IT

- Microsoft Active Directory
- Microsoft Azure
- Microsoft Exchange
- Microsoft SharePoint

Sistemi operativi

- Apple (Mac)
- Microsoft Windows
- Red Hat Enterprise Linux