Dalla reattività alla resilienza

Come Quantico ha migliorato la visibilità, ridotto le attività manuali e contenuto i tempi di risposta agli incidenti da diverse ore a pochi minuti

kaspersky cybersecurity true to business

QUANTICO

Servizi digitali e IT
Italia centrale

2019
anno di fondazione

oltre 1.000
host gestiti

oltre 2.000
risorse totali

Sostenere la trasformazione digitale in tutta l'Italia centrale

Fondata nel 2019 attraverso la fusione di tre aziende con vent'anni di esperienza, Quantico Srl è un'azienda di servizi digitali e IT con sede nell'Italia centrale. Con un team di oltre 50 dipendenti, Quantico opera in un ambiente IT ibrido che comprende endpoint Windows, Linux e macOS, un'infrastruttura VMware on-premise primaria, server cloud per le applicazioni proprietarie e gestione delle vulnerabilità.

L'azienda raccoglie dati di registro da endpoint, firewall, server, sistemi di connettività e applicazioni, con un volume medio di circa 1.500-2.000 eventi al secondo. Con oltre 2.000 risorse totali e più di 1.000 host gestiti, Quantico necessitava di un metodo più integrato per monitorare, amministrare e proteggere la propria infrastruttura, nonché delle competenze necessarie per gestire e rispondere a tutti i tipi di minacce.

Il costo delle operazioni di sicurezza frammentate

La decisione di investire è stata dettata dalla necessità di centralizzare le operazioni di sicurezza, ridurre la complessità gestionale e ottenere una visione più completa dell'infrastruttura. Anziché espandere la propria infrastruttura di sicurezza con molteplici soluzioni indipendenti, Quantico desiderava un'unica piattaforma in grado di semplificare le operazioni, migliorare la visibilità, estendere le capacità di risposta e, al tempo stesso, ridurre il carico di lavoro dei team interni.

Prima di adottare Kaspersky Next MXDR Optimum, Quantico si affidava a una configurazione di sicurezza più limitata che forniva una protezione essenziale degli endpoint e una protezione gestita, ma non disponeva della visibilità più ampia e delle capacità di analisi necessarie per gestire in modo efficiente un ambiente ibrido in crescita. Per tale motivo, il team interno si affidava a processi manuali di risposta agli incidenti, si trovava a gestire troppi avvisi senza una chiara priorità e impiegava molto tempo per le attività operative di routine.

Automazione del controllo in un ambiente ibrido

Quantico ha scelto Kaspersky Next MXDR Optimum per la sua capacità di combinare funzionalità di rilevamento estese con una protezione gestita da esperti in un'unica soluzione. Oltre alla perfetta integrazione con gli strumenti esistenti e alla facilità d'uso rispetto alla concorrenza, l'azienda ha apprezzato il supporto per un ambiente con sistemi operativi misti, la scalabilità e il solido supporto del vendor.

Questi requisiti erano particolarmente importanti in un ambiente eterogeneo che comprendeva Windows, Linux, macOS, VMware e infrastrutture cloud.

L'implementazione di Kaspersky Next MXDR Optimum comprendeva il monitoraggio degli endpoint, funzionalità avanzate di rilevamento e risposta, controlli di sicurezza e gestione delle patch, nonché strumenti per aiutare il team a identificare, assegnare priorità e mitigare i rischi in modo più efficace. Queste funzionalità sono state integrate da un monitoraggio continuo e dal supporto per la risposta fornito dagli esperti del SOC di Kaspersky.

Kaspersky Next MXDR Optimum

Kaspersky Next MXDR Optimum garantisce un monitoraggio 24 ore su 24, 7 giorni su 7 e l'assistenza degli esperti del team SOC di Kaspersky, di fama mondiale, mantenendo al contempo le funzionalità XDR essenziali all'interno dell'azienda.

Risposta più rapida, controllo più preciso e meno attività manuali

Grazie a Kaspersky Next MXDR Optimum, Quantico è passata da processi frammentati e manuali, con operazioni di sicurezza in gran parte senza automazione, a un modello di gestione della sicurezza più centralizzato e proattivo.

Attraverso la combinazione di una maggiore visibilità XDR con il monitoraggio continuo e il supporto per la risposta degli esperti del SOC di Kaspersky, l'azienda ha migliorato i flussi di lavoro quotidiani e ridotto le attività manuali.

- Implementazione scalabile in un ambiente con sistemi operativi misti
- Visibilità centralizzata su endpoint e infrastruttura
- Protezione dei sistemi, controlli e gestione delle patch
- Interfaccia semplice da gestire con requisiti di manutenzione ridotti
- Raccomandazioni di esperti a supporto delle operazioni di sicurezza

Le funzionalità di automazione, il controllo centralizzato e la gestione delle patch hanno ulteriormente semplificato le operazioni

La soluzione è intuitiva da utilizzare e da gestire, richiede attività minime dopo la configurazione iniziale ed è facilmente scalabile

Per Quantico, questo si è tradotto in un'importante ottimizzazione dei tempi, una maggiore efficienza operativa e un carico di lavoro inferiore per il team

L'impatto è visibile anche nella risposta agli incidenti. Una migliore visibilità su diversi endpoint, avvisi aggregati e prioritari e il supporto continuo degli esperti del SOC di Kaspersky hanno permesso ai team di Quantico di identificare, analizzare e rispondere agli incidenti in modo più efficiente.

Risultati aggiuntivi

1. Attività che prima richiedevano ore adesso possono essere completate in pochi minuti, consentendo al team di concentrarsi solo sugli incidenti a priorità più elevata.
2. È stata inoltre migliorata la copertura del rilevamento, con una maggiore copertura degli endpoint e un migliore allineamento con il framework MITRE ATT&CK.
3. Quantico ora è in grado di rilevare attività che in precedenza richiedevano un effort maggiore, tra cui movimenti laterali, utilizzo sospetto di PowerShell ed esecuzione di software non autorizzato.

Punti chiave

La visibilità è la base per una risposta più rapida

I risultati di Quantico dimostrano come una maggiore visibilità sugli endpoint e operazioni di sicurezza centralizzate possano aiutare i team a comprendere cosa sta accadendo nell'ambiente, ad assegnare priorità alle minacce e ad agire più rapidamente quando si verificano incidenti.

L'automazione riduce la pressione sui team snelli

Grazie alla combinazione di funzionalità Extended Detection and Response di facile utilizzo, automazione, gestione centralizzata e supporto di esperti, Quantico ha ridotto le attività manuali, migliorato i flussi di lavoro e ottimizzato il carico di lavoro quotidiano del team.

Una migliore gestione delle patch rafforza la sicurezza e l'efficienza

Una gestione ottimizzata delle patch ha permesso a Quantico di ridurre il rischio operativo, offrendo al tempo stesso al team un maggiore controllo sulle operazioni di sicurezza e IT di routine.

Nel complesso, Quantico ha ottenuto maggiore visibilità, capacità di risposta più rapide e precise, operazioni di sicurezza più semplici e una riduzione dei rischi grazie a una migliore gestione delle patch e degli endpoint.

Ugo Viti

Cofondatore e membro del consiglio di amministrazione - Quantico

«

La nostra esperienza con Kaspersky è stata estremamente positiva, soprattutto in termini di affidabilità e protezione completa dalle minacce. La piattaforma garantisce un'elevata visibilità sull'intero ambiente e migliora significativamente la nostra capacità di rilevare e rispondere rapidamente agli incidenti di sicurezza. Inoltre, la facilità di gestione e il controllo centralizzato hanno contribuito a semplificare le operazioni e a ridurre il carico di lavoro complessivo. Nel complesso, Kaspersky ha rafforzato il nostro livello di sicurezza, supportando al tempo stesso gli obiettivi di efficienza.

www.kaspersky.it

© 2026 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.

Per saperne di più

#kaspersky
#truetobusiness