Case Study

INAIL mette al sicuro dati e servizi con l'approccio integrato di Intel Security

Istituto Nazionale Assicurazione contro gli Infortuni sul Lavoro - INAIL

Azienda

L'Ente pubblico che gestisce l'assicurazione obbligatoria e tutela i lavoratori contro gli infortuni sul lavoro e le malattie professionali.

Settore

Pubblica Amministrazione.

Ambiente IT

Alla base di tutti i servizi e composto da due Data Center, circa 2000 host Server, 15mila client/endpoint. Piattaforme fisiche, virtuali e cloud che erogano servizi via web.

La sfida

Fornire al pubblico servizi di alto livello e con la massima disponibilità, in linea con la mission aziendale.

Soluzioni Intel Security

- McAfee® ePolicy Orchestrator® (McAfee ePO)
- McAfee VirusScan® Enterprise
- McAfee Host Intrusion Prevention
- McAfee Complete Data Protection Advanced
- McAfee Total Protection for Data Loss Prevention
- McAfee Network Security Platform
- McAfee Global Threat Intelligence
- McAfee Advanced Threat Defense
- McAfee Threat Intelligence Exchange
- McAfee Endpoint Threat Protection
- McAfee Web Gateway
- McAfee Event Reporter

Servizi professionali McAfee

- Servizi di distribuzione McAfee

Il patrimonio di dati e informazioni sensibili a disposizione di INAIL e i servizi che l'Ente fornisce a cittadini, aziende e Pubblica Amministrazione impongono strategie e scelte in ambito sicurezza IT senza compromessi in fatto di efficacia. Un approccio evoluto e multilivello è imprescindibile per un'organizzazione pubblica moderna e matura e comprende, oltre a una visione globale e lungimirante, anche il consolidamento di una cultura aziendale per diffondere la consapevolezza che un uso responsabile degli strumenti informatici individuali sia di beneficio per tutti.

Servono però anche soluzioni all'altezza delle esigenze di un ente come INAIL, in grado di abilitare un modello di security integrato su tutti i livelli di rete fino agli endpoint per abbattere i rischi e ridurre i casi di attacchi. L'obiettivo? Ottenere una generale riduzione dei costi e aumentare l'operatività del personale per mantenere alta la qualità dei servizi erogati. Da più di dieci anni INAIL lavora insieme con Intel Security per mettere al riparo le risorse IT in modo completo e flessibile e per adottare un approccio integrato di gestione della sicurezza.

Anche la PA è in trasformazione

Fondato nel 1933, INAIL lavora a contatto con cittadini, imprese e PA per gestire l'assicurazione contro gli infortuni sul lavoro e le malattie professionali che tutti i datori di lavoro che occupano lavoratori dipendenti e lavoratori parasubordinati nelle attività che la legge individua come rischiose devono sottoscrivere. L'evoluzione dei processi lavorativi e la costante introduzione di tecnologie più avanzate ha imposto l'estensione dell'obbligo assicurativo INAIL a quasi tutte le attività della produzione e dei servizi. L'INAIL svolge un ruolo fondamentale anche nella pianificazione delle politiche di prevenzione e sicurezza sul lavoro e nella sensibilizzazione e divulgazione della conoscenza in materia.

L'IT è il cuore dell'operatività in INAIL ed è costituito da due Data Center progettati con sistemi di Business Continuity e Disaster Recovery e attualmente oggetto di un processo di ammodernamento in ottica TIER 3, secondo gli standard ANSI/TIA-942 per i CED. L'ambiente comprende circa 2mila host Server e oltre 15mila postazioni client/endpoint su cui funzionano 300 applicativi, lungo un'architettura composta da piattaforme fisiche, virtuali e cloud attraverso cui sono erogati servizi via web a dipendenti e a utenti esterni. Si tratta di numeri e complessità che necessitano necessariamente di un sistema di sicurezza totalmente integrato e in grado di sfruttare ogni tipo di informazione e intelligenza per garantire protezione a ogni livello.

La sicurezza nel cuore dell'IT

Stefano Tomasini è il Direttore centrale dell'Organizzazione Digitale dell'Ente. "La sicurezza per INAIL è di vitale importanza", precisa Tomasini. "Ricondurre a un unico dipartimento l'intera responsabilità dell'IT Security ci permette una visione completa anche degli aspetti organizzativi e dei comportamenti dei nostri collaboratori, sempre più complementari per adottare strategie di sicurezza efficaci".

Non a caso INAIL ha costituito una Unità Locale di Sicurezza cui afferiscono i Team del CERT, del SOC e della Sicurezza Applicativa, chiamata ad applicare le Best Practice in ambito sicurezza IT definite dall'Ente. Ma sono tutti gli uffici dell'INAIL a essere coinvolti nei processi di Event Management e Incident Response. La mission dell'ente è trattare la sicurezza come un processo che come tale può essere continuamente migliorato in funzione dell'esperienza sul campo e della maturità degli attori coinvolti.

I risultati

- Gestione intelligente della sicurezza
- Riduzione dei casi di endpoint infetti
- Blocco degli attacchi da Internet
- Identificazione proattiva delle vulnerabilità nell'ambiente IT
- Maggiore visibilità a ogni livello
- Radicamento di una cultura aziendale di IT Security

I servizi di INAIL non devono mai essere a rischio di indisponibilità a causa di attacchi informatici, in linea con la mission aziendale. L'inasprimento delle minacce, sempre più mirate e efficaci, comporta anche per INAIL l'adozione di strategie di sicurezza di nuova generazione. "La diffusione di malware avanzato, gli attacchi DDOS, il Cybercrime e il rischio informatico legato a ciò che facciamo è cresciuto sino a raggiungere livelli preoccupanti", dichiara Tomasini. Senza contare i nuovi trend tecnologici e le opportunità consentite dall'uso di dispositivi mobili, dalla virtualizzazione, dal cloud e dagli strumenti social e di collaborazione. "Era fondamentale pianificare un adeguamento delle politiche e delle soluzioni di sicurezza poste a garantire l'operatività nel nostro ambiente IT".

Non solo. Oltre alla protezione dei dati sensibili, le realtà come l'INAIL devono rispettare la conformità alle normative vigenti e l'aderenza agli standard di sicurezza della PA che prevedono impegno costante sia nel miglioramento dei processi di gestione che nella difesa dai Ransomware e dagli attacchi DDOS.

Intel Security, l'approccio integrato

Da più di dieci anni Intel Security svolge un ruolo importante nell'IT Security di INAIL. La struttura unificata e adattiva di Intel Security consente infatti una totale integrazione tra tutti i prodotti e servizi, anche quelli di terze parti, favorendo la condivisione della conoscenza sulle minacce e sul contesto in tempo reale. Il modello integrato di Intel Security, lungo tutti i livelli di sicurezza (endpoint, server, rete), è in grado, pertanto, di dare supporto nella riduzione dei rischi, del volume degli eventi e del tempo di risposta, abbassando inoltre i costi generali e l'impegno del personale operativo.

Le soluzioni Intel Security utilizzate dall'Istituto proteggono gli host, controllano il movimento dei dati, schermano il perimetro di rete dagli attacchi, normalizzano i contenuti Web della navigazione Internet e riportano agli amministratori le potenziali vulnerabilità degli asset informatici gestiti.

Al fianco delle tradizionali tecnologie anti-virus e anti-intrusione, INAIL può fare leva sulle capacità di Sandboxing e di Analisi Dinamica Avanzata del codice malevolo e in aggiunta beneficia della condivisione in tempo reale delle informazioni su potenziali attacchi o file dannosi non ancora classificati, grazie all'integrazione con il Cloud di Intel Security.

La protezione mette al riparo il business

Il primo e più evidente beneficio della sicurezza endpoint e perimetrale di Intel Security è stato lo stop delle nuove minacce.

Da un punto di vista strategico, INAIL riesce a correlare con più facilità i dati relativi a ciò che accade nell'ambiente IT, questo crea un patrimonio informativo che contribuisce ulteriormente a ridurre il rischio di infezioni e gli attacchi perpetrati via Internet. Si possono rilevare le vulnerabilità, quindi classificarle per gravità e portare a termine azioni mirate per un generale aumento della visibilità su tutto ciò quello che accade in rete. Questo consente a INAIL di verificare e valutare il ROSI, (Ritorno degli Investimenti di Sicurezza Informatica) su cui l'Istituto ha costruito un modello di riferimento in modo da valutare, sia ante che post, il valore quantitativo di una contromisura di sicurezza.

Nella pratica quotidiana, l'Unità Locale di Sicurezza può usufruire dei vantaggi della gestione automatizzata e correlazione degli eventi, sia in termini operativi che per attività di reportistica. I dati raccolti non restano sterili resoconti, ma permettono di evitare situazioni pericolose, attivando velocemente le giuste contromisure alla minaccia individuata.

Le soluzioni Intel Security hanno permesso inoltre a INAIL di ottimizzare la gestione della sicurezza IT e di rispondere ai principali requisiti di conformità imposti dalle normative vigenti e dagli Standard di Sicurezza internazionali. Senza contare il miglioramento dell'immagine dell'Ente grazie a processi, tempi e costi dell'esecuzione dell'attività in linea con le richieste di un'azienda moderna. "Il nostro operato viene valutato in base alla prontezza e alla qualità di esecuzione di un progetto, fino alla soddisfazione dei fruitori dei nostri servizi".

"Il modello integrato di Intel Security ci supporta nella riduzione dei rischi e dei tempi di risposta, diminuendo inoltre i costi generali e l'impegno del personale operativo."

— Stefano Tomasini, CIO

Tecnologia scalabile a gestione intelligente

L'approccio integrato consentito dalle soluzioni Intel Security permette di avere a disposizione più tecnologie con un sistema di gestione unico, con ritorni in efficienza, possibilità di sfruttare al massimo le sinergie tra le soluzioni e la correlazione degli eventi in ambito sicurezza, per un abbattimento generale dei costi di gestione.

"La filosofia Security Connected di Intel ci permette di utilizzare un sistema omogeneo, flessibile e centralizzato di prodotti che parlano la stessa lingua e che si gestiscono in maniera intuitiva e integrata", aggiunge Tomasini.

Grazie a queste caratteristiche, in futuro INAIL potrà aggiungere nuovi moduli alla piattaforma con il minimo sforzo e con effetti immediati. È il caso degli add-on per le nuove tecnologie messi a disposizione da Intel Security. "Strumenti come McAfee Data Center Security Suite e i connettori per i Cloud Provider, entrambi integrati totalmente con ePO, rispondono positivamente alle nuove esigenze di sicurezza derivate delle importanti trasformazioni tecnologiche dei nostri asset informatici e dalle normative internazionali: come noto, ad Aprile 2016 il Parlamento UE ha ratificato il 'Regolamento europeo sulla protezione dei dati' che entrerà in vigore in tutta l'Unione Europea nel 2018. Il Regolamento dovrebbe aiutare l'Europa ad affrontare i cambiamenti dell'era digitale e rafforzare i diritti dei cittadini europei, offrendo un concreto strumento per il controllo dei propri dati personali e definendo un quadro unificato e semplificato di regole e adempimenti previsti per chi come noi gestisce dati personali."

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com