

HAWORTH®

Haworth

Azienda internazionale usa Forescout per proteggere la rete IT e OT e ottiene un ROI straordinario

SETTORE

Manifatturiero

AMBIENTE

12.000 dispositivi cablati e wireless dislocati in 20 impianti di produzione e 55 uffici vendite nel mondo; 6.200 dipendenti.

SITUAZIONE

- Mancanza di visibilità su tutti i dispositivi della rete, dispositivi IoT e OT inclusi
- Visibilità insufficiente sullo stato di sicurezza delle aziende di nuova acquisizione
- Necessità di un'operatività ininterrotta nell'ambiente OT
- Piccola squadra incaricata della sicurezza con tempo e risorse limitate

SOLUZIONE

- Piattaforma Forescout
- Forescout Enterprise Manager
- Forescout Extended Module per Palo Alto Networks Next-Generation Firewall

CASI D'USO

- Visibilità sui dispositivi
- Conformità dei dispositivi
- Controllo degli accessi alla rete
- Segmentazione della rete
- Risposta agli incidenti

Introduzione

Con uno stile che privilegia l'innovazione e la produttività, Haworth Inc. progetta e produce spazi di lavoro flessibili, pavimenti sopraelevati, pareti divisorie scorrevoli, sistemi di arredo, sedute e sistemi di collaborazione in tempo reale Workware™ cablati e wireless. L'azienda, con sede a Holland nel Michigan, ha un organico 6.200 persone che lavorano in 20 impianti di produzione e 55 uffici vendita. In seguito alla recente acquisizione di alcune aziende di complementi d'arredo, Haworth ha avvertito la necessità di limitare l'accesso alla rete aziendale ai soli dispositivi autorizzati che soddisfano gli standard di sicurezza dell'azienda.

Per rispondere all'esigenza di implementare il controllo degli accessi e colmare le lacune di sicurezza, come il rilevamento e il contenimento dei dispositivi inaffidabili, Haworth ha scelto di implementare la piattaforma Forescout. Grazie alle sue funzionalità di visibilità e controllo granulari, la soluzione Forescout ha migliorato drasticamente lo stato di sicurezza degli ambienti informatici e di produzione e la sua integrazione con i firewall dell'azienda ha permesso di automatizzare le operazioni di sicurezza, alleggerendo notevolmente il carico di lavoro del reparto sicurezza IT di Haworth. Infine, la piattaforma Forescout ha dato prova del suo valore oltrepassando i confini della sicurezza e viene ora usata anche in altri ambiti operativi, come la gestione della rete.

La problematica aziendale

"Per i casi d'uso esposti avevamo l'esigenza di ottenere maggiore visibilità e controllo sui dispositivi, ma ci serviva anche la capacità di classificare i dispositivi, segmentare le reti in base ai dispositivi e reperire gli indicatori di compromissione in tempo reale."

– Joseph Cardamone, Senior Information Security Analyst e North America Privacy Officer, Haworth

Joe Cardamone, Senior Information Security Analyst e North America Privacy Officer, è il responsabile delle strategie di sicurezza informatica di Haworth. Fa parte di una squadra di sole tre persone che ha il compito di proteggere gli ambienti aziendali e di produzione di un'azienda globale come Haworth. La recente acquisizione di varie aziende a conduzione autonoma non ha fatto che complicare la situazione.

Ma i dispositivi di proprietà di queste nuove filiali non erano le uniche risorse su cui la squadra di Cardamone aveva insufficiente controllo e visibilità. Serviva, ad esempio, un modo più rapido ed efficace di individuare i dispositivi IoT ad alto rischio per impedire la trasmissione e la ricezione di comunicazioni non autorizzate, oltre che un modo facile per individuare e mettere in sicurezza i sistemi digitali di collaborazione Workware proprietari che vengono spostati continuamente tra le sedi e aggiornati frequentemente in termini di software e hardware.

RISULTATI

- Time to value rapido: Individuazione e classificazione immediata del 97% degli endpoint entro le prime sette ore dall'implementazione
- Visibilità in tempo reale sui dispositivi non appena si connettono alla rete
- Protezione più agevole dei dispositivi OT e di quelli che vengono continuamente spostati grazie alla segmentazione dinamica della rete
- Controllo degli accessi per le aziende appena acquisite che si inseriscono nella rete aziendale
- Risparmio di 20 ore a settimana grazie all'automazione delle operazioni di sicurezza
- Ulteriore risparmio tempo grazie all'automazione dei processi manuali di ricerca e messa in isolamento dei dispositivi ad alto rischio
- Miglioramento dell'efficienza della squadra di sicurezza composta da tre persone
- Visibilità granulare che aiuta la squadra di sicurezza, i gruppi IT e gli addetti alla rete
- Individuazione di una quantità di dispositivi del 60% maggiore rispetto alle previsioni

Perché Forescout**Un “generatore di informazioni” facile da implementare e da utilizzare**

Cardamone e la sua squadra hanno eseguito dei proof of concept sulla piattaforma Forescout e sulla soluzione di un concorrente i cui prodotti erano già presenti in azienda e che godeva dell'appoggio iniziale del team che si occupava delle reti in Haworth. La piattaforma Forescout è emersa come vincitrice indiscussa.

“La piattaforma Forescout è un generatore di informazioni facile da implementare e da utilizzare, diversamente dal prodotto della concorrenza,” dichiara Cardamone. “Nella sua interfaccia unificata posso vedere l'intera rete in grande dettaglio e gestire la protezione con un clic del pulsante destro del mouse. L'interfaccia grafica è estremamente intuitiva e i dati così chiari che persino i nuovi membri della squadra e chi lavora in altri reparti, come gli addetti alla rete, possono utilizzarli a proprio vantaggio.”

Impatto sul business**Implementazione rapida e time to value immediato**

Per implementare la piattaforma Forescout basta meno di un giorno. “Abbiamo iniziato l'implementazione all'ora di pranzo. Quando quella stessa sera ho acceso il computer, il 97% del nostro ambiente era già stato analizzato e classificato,” ricorda Cardamone. “Nel giro di sette ore avevamo ottenuto una visibilità dettagliata sul nostro ambiente globale. Straordinario.”

Valore lampante sin dall'inizio

La visibilità precisa che si ottiene grazie alla piattaforma Forescout ha dimostrato immediatamente la sua utilità. “Pensavamo che le nostre reti ospitassero circa 7.500 dispositivi, ma la piattaforma Forescout ha scoperto più di 12.000 indirizzi IP,” precisa Cardamone. “Sono emerse anche delle falle nella sicurezza di cui non ci eravamo resi conto, come le decine di access point wireless installati negli showroom. Il ritrovato controllo sul sistema ci ha permesso di bloccare quei dispositivi e di chiedere agli amministratori locali di eliminarli.”

“Ma questa è solo la punta dell'iceberg,” continua Cardamone. “La quantità di informazioni che raccoglie la piattaforma Forescout è incredibile. Gli altri strumenti si limitano a scoprire gli indirizzi IP degli endpoint, mentre Forescout li identifica e permette di controllare i sistemi. È davvero la migliore soluzione che abbia mai utilizzato. Per noi è diventata indispensabile.”

“Spesso possiamo applicare automaticamente l'azione su un endpoint, ma quando è necessario l'intervento umano, è sufficiente un semplice clic del tasto destro del mouse.” “Posso persino permettere al personale di Livello 1 o 2 di intraprendere azioni di Livello 3 in caso di crisi, senza per questo concedere accesso a funzioni privilegiate. Le potenti funzionalità della piattaforma Forescout sono pronte all'uso, ma possono essere facilmente personalizzate. Non c'è limite a quello che possiamo fare con Forescout.”

Visibilità sul livello di integrità dei dispositivi delle nuove aziende

La piattaforma Forescout ha fornito visibilità sulle reti delle nuove filiali e sul livello di integrità dei loro dispositivi. “Se i dispositivi non sono stati aggiornati da molto tempo, ora lo sappiamo e possiamo intervenire” dichiara Cardamone. “La piattaforma Forescout controlla anche lo stato delle patch di sicurezza, degli antivirus e dei sistemi operativi dei dispositivi delle filiali che tentano di connettersi alla rete aziendale. Quelli che non soddisfano i nostri criteri vengono bloccati.”



La quantità di informazioni che raccoglie la piattaforma Forescout è incredibile. Molti strumenti si limitano a scoprire gli indirizzi IP degli endpoint, mentre Forescout li identifica e permette di controllare i sistemi. È davvero la migliore soluzione che abbia mai utilizzato. Per noi è diventata indispensabile.”

– Joseph Cardamone, Senior Information Security Analyst e North America Privacy Officer, Haworth

Segmentazione di rete più semplice ma più personalizzabile

Grazie al Forescout Extended Module per Palo Alto Networks® Next-Generation Firewall, Cardamone è riuscito a integrare rapidamente la piattaforma Forescout con i firewall aziendali e a realizzare la segmentazione della rete al volo basandosi sulle informazioni contestuali precise e puntuali fornite dalla soluzione Forescout. “L’integrazione Forescout-Palo Alto Networks ci permette di andare oltre la segmentazione basata su semplici identificatori come indirizzo IP o VLAN,” spiega Cardamone. “Abbiamo molte più opzioni rispetto a quelle che offre solo 802.1X perché possiamo impostare la segmentazione su profili endpoint molto più ricchi e precisi.”

Nell’ambiente di produzione di Haworth, ad esempio, Cardamone utilizza la piattaforma Forescout per identificare e classificare tutti i dispositivi IoT ad alto rischio, partendo da quelli che non sono più supportati dal produttore, come i sistemi operativi Windows® XP e Windows 2000. La segmentazione dinamica della rete quindi impedisce automaticamente a questi dispositivi di ricevere o trasmettere informazioni, se non in particolari situazioni autorizzate.

Enorme e quantificabile risparmio di tempo con l’integrazione e l’automazione

L’integrazione Forescout-Palo Alto Networks ha permesso anche a Haworth di rendere automatici alcuni laboriosi processi manuali. Consideriamo i sistemi che usano la tecnologia Workware di Haworth, per esempio. Sono presenti nelle sedi e negli showroom di Haworth di tutto il mondo e vengono eseguiti su VLAN. Fino a poco tempo fa a ciascuno veniva assegnato un indirizzo IP statico che era autorizzato a comunicare con la rete ospite superando il firewall. Dato che ci sono 130 sistemi di questo tipo solo nelle sedi centrali, aggiornamenti costanti di software e hardware e spostamenti che modificano gli indirizzi IP, un processo manuale non era in grado di offrire un controllo degli accessi adeguato.

Oggi, invece, la piattaforma Forescout trova i sistemi, li classifica e li colloca in gruppi di accesso dinamici collegati a una policy firewall che consente agli indirizzi IP del gruppo di comunicare con la rete ospite sulle porte e le applicazioni che lo richiedono. “Anche se il sistema viene portato in Cina o in Germania, Forescout lo trova e il firewall sa cosa fare,” dichiara Cardamone. “Quello che era un processo manuale continuo e quasi irrealizzabile è diventato un processo totalmente automatico.”

“Se sommiamo tutto il tempo che risparmiamo nelle varie situazioni da quando abbiamo installato la piattaforma Forescout e l’abbiamo integrata con il firewall, direi che parliamo di un risparmio di circa 20 ore a settimana, metà delle ore di lavoro di un dipendente a tempo pieno,” dichiara Cardamone. “La nostra piccola squadra può proteggere meglio l’ambiente aziendale lavorando meno.”

I vantaggi della visibilità Forescout vanno oltre la sicurezza

Anche il personale operativo di Haworth ha ricavato dei benefici dall’implementazione della piattaforma Forescout. I tecnici dell’assistenza la usano per geolocalizzare i dispositivi. Gli addetti alla gestione del software la usano per individuare le applicazioni non conformi. Gli addetti alla rete la usano ogni settimana per reperire informazioni su porte e switch. E nuovi impieghi sono già in previsione. Ad esempio, Forescout avrà un ruolo di rilievo quando l’azienda adotterà in futuro una policy BYOD.

Maggiori informazioni su
www.forescout.it



FORESCOUT

forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 Stati Uniti

E-mail info-italia@forescout.com
Tel. (internazionale) +1-408-213-3191
Assistenza +1-708-237-6591

© 2019 Forescout Technologies, Inc. Tutti i diritti riservati Forescout Technologies, Inc. è una società del Delaware. Un elenco dei nostri marchi e brevetti è reperibile alla pagina <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Altri marchi, prodotti o nomi di servizi possono essere marchi o marchi di servizio dei rispettivi titolari. **Versione 11_19**