Forescout eyeControl

Imposizione e automazione dei controlli basati su policy per ridurre proattivamente la superficie d'attacco e rispondere rapidamente agli eventi

I team della sicurezza IT sono sommersi da un numero crescente di problemi di sicurezza e conformità segnalati da una vasta serie di strumenti di sicurezza che generano costantemente allarmi senza alcuna possibilità di agire. Sfortunatamente, tali strumenti non dispongono di informazioni relative al contesto del dispositivo sufficienti per la prioritizzazione dei dispositivi o di capacità di automazione per l'applicazione di controlli per la riduzione dei rischi. Di conseguenza, team di sicurezza altamente qualificati perdono tempo a risolvere manualmente problemi a basso impatto, senza potersi concentrare sulla riduzione proattiva del rischio o su una rapida risposta alle minacce.

Applicazione dei controlli basati su policy

Forescout eyeControl, alimentato da ricche informazioni sul contesto dei dispositivi di Forescout eyeSight, consente ai team di sicurezza di assegnare le priorità, applicare e automatizzare i controlli basati su policy con sicurezza. Le aziende possono migliorare la protezione della sicurezza, ridurre la loro superficie d'attacco e accelerare la risposta e l'attività di remediation per mitigare rapidamente minacce, incidenti di sicurezza e lacune nella conformità.

In base alle iniziative dedicate alla sicurezza, è possibile implementare azioni di rete ed endpoint utilizzando eyeControl. Per orchestrare le azioni della rete, eyeControl si integra direttamente con infrastrutture di rete fisiche e virtuali eterogenee: switch, reti wireless, VPN, software-defined e cloud. Le azioni degli endpoint possono essere implementate senza agent su endpoint windows, Mac e Linux oppure utilizzando SecureConnector™..

eyeControl

In evidenza

- Proteggi i dati sensibili dalle minacce esterne
- Evita che dispositivi infetti, vulnerabili o non conformi diffondano malware
- Evita che attacchi mirati sottraggano dati o forzino tempi di inattività della rete
- Aiuta a garantire accesso e disponibilità della rete a dipendenti, terze parti e clienti
- Applica la conformità con policy interne e normative esterne
- Automatizza le azioni di controllo per fornire la giusta azione per ogni situazione

Figura 1. Applicazione delle policy sulla rete e sugli endpoint, aumentando l'automazione nel tempo.

Automatizza i controlli con sicurezza

eyeControl sfrutta un motore delle policy intuitivo e flessibile che permette alle aziende di applicare controlli granulari mirati. È possibile implementare flussi di lavoro complessi e azioni combinate con controlli dinamici di facile utilizzo, logica Booleana e policy a cascata. La funzione Policy Graph facilita la creazione precisa di policy, l'analisi dei flussi delle policy e l'ottimizzazione delle stesse prima di attivare azioni di imposizione.

Azioni di controllo possono essere avviate manualmente dai team della sicurezza oppure, per migliorare l'efficienza delle operazioni di sicurezza, l'automazione può essere introdotta gradualmente. Partendo dalle attività di base ripetitive per passare nel tempo a controlli più complessi, l'automazione può liberare risorse IT qualificate che possono concentrarsi su problemi di maggiore impatto. Questo approccio aiuta a ridurre al minimo l'interruzione dell'attività migliorando in modo significativo l'accesso alla rete, la conformità dei dispositivi, la segmentazione della rete e le iniziative di risposta agli incidenti.

> "Spesso possiamo automatizzare l'azione su un endpoint, ma quando è necessario l'intervento umano, è sufficiente un un semplice clic del tasto destro del mouse." – *Joseph Cardamone, Senior Information Security Analyst e North America Privacy Officer, Haworth*

Sfide

- Dispositivi non conformi o non automatizzati sulla rete rappresentano un grande rischio
- Reti flat sotto-segmentate lasciano le aziende vulnerabili alle minacce laterali
- Incapacità di rispondere in modo rapido ed efficace a minacce e incidenti di sicurezza
- Capacità limitata di applicare un comportamento costante del dispositivo tramite gli strumenti di sicurezza
- Il rischio di interruzione dell'attività limita l'automazione dei controlli di sicurezza

Applica l'accesso alla rete

Controlla l'accesso alle risorse aziendali in base a profilo utente (ospite, dipendente, terza parte), classificazione del dispositivo e comportamento di sicurezza.

- Abilita l'accesso differenziato per dispositivi ospiti e BYOD.
- Applica policy di accesso alla rete con o senza autenticazione 802.1X
- Agisce su dispositivi sospetti, inaffidabili o shadow IT sulla rete
- Limita o blocca l'accesso alla rete per dispositivi violati o dannosi
- Mette in quarantena o isola i dispositivi non conformi fino a quando i problemi di conformità non vengono risolti

"Uno dei motivi per cui abbiamo scelto la piattaforma Forescout è che questa tecnologia non fa affidamento sul protocollo 802.1X, semplificando notevolmente la distribuzione. L'idea di non installare agent assicura anche elevate prestazioni e semplicità."
—Juan Ignacio Gordon, Head of IT Security, ACCIONA

Migliora la conformità del dispositivo

Automatizza la valutazione della conformità e applica i controlli di remediation per una conformità costante con le policy di sicurezza interne, gli standard esterni e normative del settore.

- Aiuta a garantire la corretta configurazione degli endpoint e avvia il processo di remediation per le violazioni critiche alla configurazione, incluse password automatiche o non sicure
- Aiuta a garantire che le applicazioni e gli agent di sicurezza necessari siano installati, eseguiti e aggiornati
- Disabilita o blocca applicazioni non autorizzate che potrebbero introdurre rischi o gravare inutilmente sulla larghezza di banda della rete o sulla produttività delle risorse
- Identifica vulnerabilità ad alto rischio e patch critiche mancanti e avvia le azioni di remediation
- Definisce proattivamente azioni di remediation come l'installazione di software di sicurezza richiesto, l'aggiornamento degli agent o l'applicazione di patch di sicurezza
- Implementa policy e automatizza i controlli per la conformità della configurazione nelle distribuzioni cloud, tra cui AWS, Azure e VMware®

"Con la soluzione Forescout, prevediamo di risparmiare milioni grazie a revisioni esponenzialmente più rapide che producono un minor numero di risultati e richiedono una ridotta attività di remediation."
— Phil Bates, Chief Information Security Officer, Stato dell'Utah

Implementa la segmentazione dinamica della rete

Applica policy di segmentazione dinamica della rete tra diverse tecnologie di imposizione nell'azienda estesa tramite una struttura di policy comune.

- Assegna dinamicamente i dispositivi ai gruppi di segmentazione sulla base delle proprietà, classificazione e comportamento di sicurezza del dispositivo.
- Applica i controlli di segmentazione tramite controlli VLAN, ACL, WLAN e assegna tag nelle reti di campus e OT.
- Applica controlli di segmentazione tramite gruppi/tag di sicurezza in ambienti cloud pubblici e privati come AWS e VMware NSX.
- Segmenta dispositivi non conformi e vulnerabili in zone separate - in particolare quelli cui è possibile applicare patch o azioni di remediation entro finestre di manutenzione pianificate - per abilitare la business contiuity riducendo la superificie d'attacco.
- Imponi policy di segmentazione a dispositivi di zona e flussi di dati critici dal resto della rete, come richiesto dalle normative quali HIPAA, PCI e SWIFT CSP.

"Forescout non solo è in grado di isolare i dispositivi ed effettuare la segmentazione della rete, può anche individuare le reti non scoperte in precedenza." *–Deputy CISO, importante azienda sanitaria*

Accelera la risposta agli eventi

Contieni in modo rapido ed efficace le minacce e rispondi agli eventi di sicurezza per ridurre al minimo le interruzioni delle operazioni e i danni all'azienda.

- Identifica i dispositivi ad alto rischio che non sono stati arginati o corretti.
- Identifica gli indicatori IOC (Indicator Of Compromise) sui dispositivi al momento della connessione per ridurre il tempo medio di risposta (MTTR).
- Isola e limita rapidamente i dispositivi violati o dannosi per evitare la propagazione laterale del malware.
- Automatizza la risposta agli incidenti e avvia flussi di lavoro di remediation sui dispositivi violati.
- Riduci il tempo medio di risposta fornendo preziose informazioni di contesto relative al dispositivo (connessione, ubicazione, classificazione e comportamento di sicurezza) ai team di risposta agli eventi interfunzionali e alle tecnologie isolate.

"Con Forescout è come avere un cacciatore automatico di minacce nel team che cerca minacce 24 ore su 24 su tutta la nostra rete globale. Ora possiamo gestire problemi che prima non riuscivamo ad affrontare. Compiti che prima richiedevano ore adesso vengono svolti in pochi minuti".
— Nick Duda, Principal Security Engineer, HubSpot

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 Stati Uniti

Numero verde (USA) 1-866-377-8771
Tel. (Internazionale) +1-408-213-3191
Assistenza 1-708-237-6591

Maggiori informazioni su Forescout.com