FORESCOUT
Active Defense for the Enterprise of Things™

eyeControl

Applicazione di controlli basati su policy

NON INTRUSIVO

Opzioni di controllo degli accessi e distribuzione flessibili, con o senza il protocollo 802.1X.

SENZA AGENT

Valuta lo stato dei dispositivi e li sottopone a correzione automatica imponendone la conformità senza ricorrere ad agent.

EFFICACE

Implementazione del modello di sicurezza degli accessi Zero Trust tramite un motore di gestione delle policy centralizzato.

NON RICHIEDE AGGIORNAMENTI

Opera con l'infrastruttura esistente e non richiede aggiornamenti software o hardware.

MINORE COSTO DI PROPRIETÀ

Flessibile, non intrusivo, non richiede agent e supporta soluzioni di vendor diversi: queste qualità concorrono ad abbassare i costi operativi, di distribuzione e manutenzione e ad accelerare la redditività dell'investimento.

Applicazione e automazione dei controlli per l'Enterprise of Things su reti eterogenee

Forescout eyeControl garantisce il controllo degli accessi più flessibile e lineare possibile per le reti aziendali eterogenee. Impone l'applicazione automatica di policy basate sul principio del privilegio minimo di Zero Trust per l'accesso a tutti i dispositivi gestiti dell'Enterprise of Things. I controlli basati su policy vengono applicati per imporre la conformità dei dispositivi, ridurre proattivamente la superficie d'attacco e rispondere rapidamente agli incidenti.

ACCESSO ALLA RETE SICURO

L'accesso alla rete è controllato in base all'utente, all'ID del dispositivo e al suo stato di sicurezza

Distribuzione su reti eterogenee con o senza 802.1X

IMPOSIZIONE DELLA CONFORMITÀ DEI DISPOSITIVI

Assicura la conformità a policy, standard e normative di sicurezza

Avvia azioni di remediation e mitigazione dei rischi

AUTOMAZIONE DELLA RISPOSTA AGLI INCIDENTI

Reagisce automaticamente agli incidenti di sicurezza

Contiene le minacce, ne riduce la diffusione e limita le interruzioni dell'attività

AUTOMATIZZA I CONTROLLI IN MODO AFFIDABILE

L'applicazione automatica delle policy Zero Trust può avvenire solo se si dispone di dati contestuali completi sui dispositivi, vale a dire di una conoscenza in tempo reale dell'identità di ogni utente e dell'identità, dello stato di sicurezza e del profilo di rischio di tutti i dispositivi che si connettono. L'implementazione di controlli in mancanza di una visibilità completa può essere alquanto rischiosa e provocare interruzioni dell'attività. eyeControl utilizza le dettagliate informazioni sul contesto dei dispositivi che offre eyeSight per applicare e automatizzare con sicurezza i controlli basati su policy Zero Trust.

Il nucleo fondamentale di eyeControl è costituito da un motore di gestione delle policy intuitivo e flessibile che permette di applicare controlli granulari mirati. Questo motore di gestione delle policy Zero Trust offre:

- Raggruppamento e controllo dinamico dei dispositivi in base alla logica aziendale e ai dati contestuali sulle risorse
- Implementazione di flussi di lavoro sofisticati grazie alla combinazione di condizioni ed azioni che usano 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
- Possibilità di avviare manualmente azioni di controllo e di introdurre gradualmente l'automazione per migliorare l'efficienza delle operazioni di sicurezza

Le policy sono attivate e valutate automaticamente in tempo reale da eventi e cambiamenti che si verificano su uno specifico dispositivo o nella rete. La Figura 1 illustra la serie di azioni di controllo disponibili in eyeControl quando una policy viene attivata.

CONTROLLO MODERATO

Rete

- Spostamento nella rete ospite
- Modifica del ruolo dell'utente wireless
- Assegnazione alla VLAN di auto-remediation
- Limitazione dei dispositivi o delle infrastrutture inaffidabili

Host

- Avvio di applicazioni/processi obbligatori
- Aggiornamento di antivirus/agent di sicurezza
- Applicazione di aggiornamenti/patch del sistema operativo
- Conformità dei drive esterni

AUTOMAZIONE DEL CONTROLLO BASATO SU POLICY

STRIKT

Rete

- Quarantena del dispositivo (VLAN, firewall virtuale)
- Disattivazione della porta dello switch
- Blocco dell'accesso wireless o VPN
- Utilizzo degli ACL per limitare l'accesso

Host

- Chiusura delle applicazioni non autorizzate
- Disabilitazione di schede di rete/host dual-homed
- Disattivazione della periferica
- Attivazione di sistemi/azioni di remediation

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

CONTROLLO

Accesso alla rete sicuro

eyeControl rappresenta la soluzione di controllo degli accessi più flessibile, eterogenea e non intrusiva disponibile per le aziende. Con eyeControl è possibile imporre modalità di accesso sicuro in reti cablate e wireless per tutti i sistemi EoT gestiti e non, soddisfare i requisiti di auditing, ridurre la superficie di attacco e mitigare rapidamente le minacce. Le funzionalità disponibili sono:

- Applicazione dell'accesso di rete Zero Trust per dispositivi personali, di dipendenti, ospiti e collaboratori
- Individuazione e blocco dei dispositivi inaffidabili, non autorizzati, shadow IT e di spoofing
- Messa in quarantena o isolamento dei dispositivi ad alto rischio o non conformi finché non vengono risanati
- Disponibilità di un'ampia gamma di metodi di controllo degli accessi, con o senza autenticazione 802.1X
- Integrazione della valutazione dello stato di sicurezza senza ricorrere ad agent e implementazione di azioni nella rete e negli endpoint tramite un motore di gestione delle policy Zero Trust centralizzato
- Interazione con l'infrastruttura esistente senza aggiornamenti software o hardware
- Integrazione diretta con centinaia di modelli di prodotti appartenenti a più di 30 vendor di infrastrutture di rete

CONFORMITÀ

Imposizione della conformità dei dispositivi

Automatizza la valutazione dello stato di sicurezza e l'applicazione dei controlli di remediation per una conformità costante con policy di sicurezza interne, standard esterni e normative del settore.

- Verificare la corretta configurazione degli endpoint e avviare il processo di remediation per le violazioni critiche alla configurazione
- Individuare e correggere i dispositivi gestiti che presentano agent guasti o mancanti
- Individuare e disattivare applicazioni non autorizzate che introducono rischi, limitano la larghezza di banda o intralciano la produttività

eyeControl è la SOLUZIONE per:

Dispositivi non autorizzati, inaffidabili o di spoofing della rete che comportano rischi e presentano problemi di conformità.

Lacune della sicurezza causate da strumenti basati su agent che non sono stati aggiornati o non funzionano correttamente.

Reti non segmentate in modo sufficiente o adeguato che rendono le aziende vulnerabili alle minacce e incrementano il raggio di diffusione di un'intrusione.

Rischi di interruzione dell'attività causati da dispositivi vulnerabili, patch critiche mancanti e applicazioni non autorizzate.

Propagazione laterale degli attacchi dovuta all'incapacità di isolare e bloccare rapidamente i dispositivi violati o dannosi.

Mancata conformità causata dall'incapacità di monitorare e imporre la conformità dei dispositivi connessi con continuità.

Difficoltà di implementazione del controllo degli accessi alla rete in ambienti eterogenei in cui sono presenti sistemi di più vendor e in reti cablate.

forescout.com/platform/eyeControl info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

- Individuare i dispositivi con vulnerabilità ad alto rischio e patch critiche mancanti e avviare le azioni di remediation
- Applicare azioni di remediation e di mitigazione dei rischi su Windows, Mac, Linux e dispositivi IoT/OT senza utilizzare agent
- Implementare policy e automatizzare i controlli per la conformità della configurazione nelle distribuzioni cloud, tra cui AWS, Azure e VMware

AUTOMAZIONE

Accelerazione della risposta agli incidenti

- Contenere in modo rapido ed efficace le minacce e rispondere agli incidenti di sicurezza per ridurre al minimo le interruzioni delle operazioni e l'impatto per l'azienda Automatizzare le attività di risposta agli incidenti semplici e ripetitive per liberare risorse IT qualificate che possono concentrarsi su questioni prioritarie e problemi di maggiore impatto
- Identificare gli indicatori di compromissione sui dispositivi e i rischi al momento della connessione per ridurre il tempo medio di risposta
- Isolare e bloccare rapidamente i dispositivi violati o dannosi per evitare la propagazione laterale del malware
- Automatizzare la risposta agli incidenti e avviare flussi di lavoro di remediation sui dispositivi
- Ridurre il tempo medio di risposta fornendo preziose informazioni di contesto relative al dispositivo (connessione, ubicazione, classificazione e stato di sicurezza) ai team di risposta agli incidenti di diverse aree funzionali e alle tecnologie isolate

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/platform/eyeControl info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

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

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

Maggiori informazioni su Forescout.it