Forescout eyeSegment

Progettazione, costruzione e implementazione affidabile di progetti di segmentazione di portata variabile

Forescout eyeSegment velocizza la progettazione, la pianificazione e l'implementazione dei progetti di segmentazione dinamica della rete nell'intero ambiente aziendale semplificando il processo di creazione di criteri di segmentazione sensibili al contesto e consentendo di visualizzarne e simularne l'applicazione prima dell'effettiva attivazione affinché sia possibile valutare l'efficacia del progetto e apportare correzioni.

eyeSegment estende le funzionalità della piattaforma Forescout fino alla gestione di progetti di segmentazione che abbracciano più domini e casi di utilizzo, oltre a consentire alle aziende di adottare i principi Zero Trust per tutti i sistemi connessi tramite IP, compresi i dispositivi IoT (Internet of Things) e OT (Operational Technologies). Il risultato è un'applicazione dei progetti di segmentazione nell'intero ambiente aziendale decisamente più rapida che riduce la superficie esposta agli attacchi, contiene la propagazione laterale e il raggio di diffusione dell'aggressione, mitiga il rischio per l'impresa e le violazioni normative e di conformità.

Problematiche

- Timore di applicare progetti di segmentazione
- Rischio di esposizione dovuto al potenziale spostamento laterale delle aggressioni all'interno delle reti piatte
- Dati di contesto incompleti su dispositivi, applicazioni e utenti
- Proliferazione dei criteri e impossibilità di applicarli in modo uniforme su tecnologie eterogenee
- Complessità operativa generata dalla presenza di fornitori diversi e dall'applicazione discontinua dei controlli di segmentazione nei vari domini della rete
- Competenze, risorse e strumenti insufficienti per progettare, costruire e implementare progetti di segmentazione della rete efficaci per l'intero ambiente aziendale

eyeSegment

Vantaggi

- Segmentare la rete in modo rapido e affidabile
- Determinare preventivamente l'impatto dei criteri per ridurre al minimo le interruzioni dell'attività
- Ridurre il rischio di interruzione dell'attività
- Esercitare attività di controllo omogenee su tecnologie e domini di rete eterogenei adottando un unico insieme di criteri
- Adeguarsi ai requisiti normativi e di conformità
- Ridurre la complessità operativa dei progetti di segmentazione
- Abilitare un modello Zero Trust per implementare controlli di sicurezza granulare

In breve

- Creare dei criteri di segmentazione sensibili al contesto adottando una tassonomia di business logica di utenti, app, servizi e dispositivi
- Verificare velocemente l'impatto dei criteri di segmentazione prima di applicarli
- Monitorare e convalidare su base continuativa l'integrità della segmentazione
- Reagire rapidamente alle violazioni dei criteri di segmentazione che avvengono nell'intero ambiente aziendale

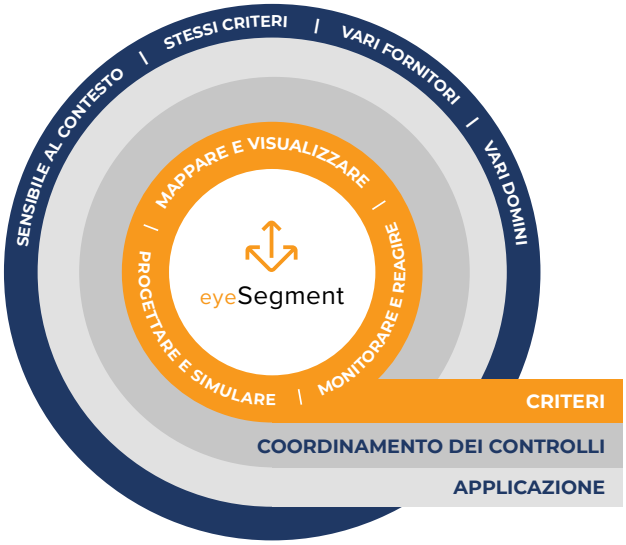

Figura 1: Forescout consiglia di strutturare l'architettura su tre livelli, partendo dal "livello dei criteri" gestito da eyeSegment.

Trasformazione della segmentazione della rete aziendale

Forescout eyeSegment sfrutta la funzionalità di visibilità avanzata sui dispositivi e i dati contestuali approfonditi e aggiornati in tempo reale forniti da Forescout eyeSight per mostrare i flussi di traffico e le dipendenze che intercorrono tra utenti, applicazioni, servizi e dispositivi. Sulla base di questi dati, gli utenti possono progettare, testare e monitorare i criteri per valutare l'impatto che avranno sull'ambiente aziendale. Tramite Forescout eyeControl e eyeExtend, i criteri vengono coordinati attraverso vari punti di controllo della segmentazione nell'intero ambiente fisico, nei data center e nelle reti cloud. eyeSegment aiuta le aziende a progettare, costruire e implementare in modo affidabile progetti di segmentazione della rete di portata variabile da applicare all'intero ambiente aziendale.

Mappare e visualizzare i flussi di traffico

Senza ricorrere all'uso di agent, Forescout eyeSegment associa automaticamente i dati sul traffico a una tassonomia logica di utenti, applicazioni, servizi e dispositivi appartenenti alla rete aziendale. Ciò permette di monitorare il traffico della rete in tempo reale e di creare criteri di segmentazione granulari sensibili al contesto. Un tipico caso d'uso potrebbe prevedere la definizione di controlli che consentano soltanto ai dipendenti del reparto contabilità di accedere alle applicazioni per il pagamento in esecuzione nei diversi domini. Un altro caso d'uso potrebbe prevedere l'individuazione, e quindi la segregazione, dei servizi generici di cui hanno bisogno i dispositivi medici che eseguono sistemi operativi legacy.

La griglia della connettività di eyeSegment (Figura 2) è una visualizzazione grafica dei flussi di traffico. Definisce una baseline del traffico, registra i dati del traffico nel tempo e mostra i flussi in tempo reale tra le zone di partenza e le zone di arrivo definite dai criteri di segmentazione.

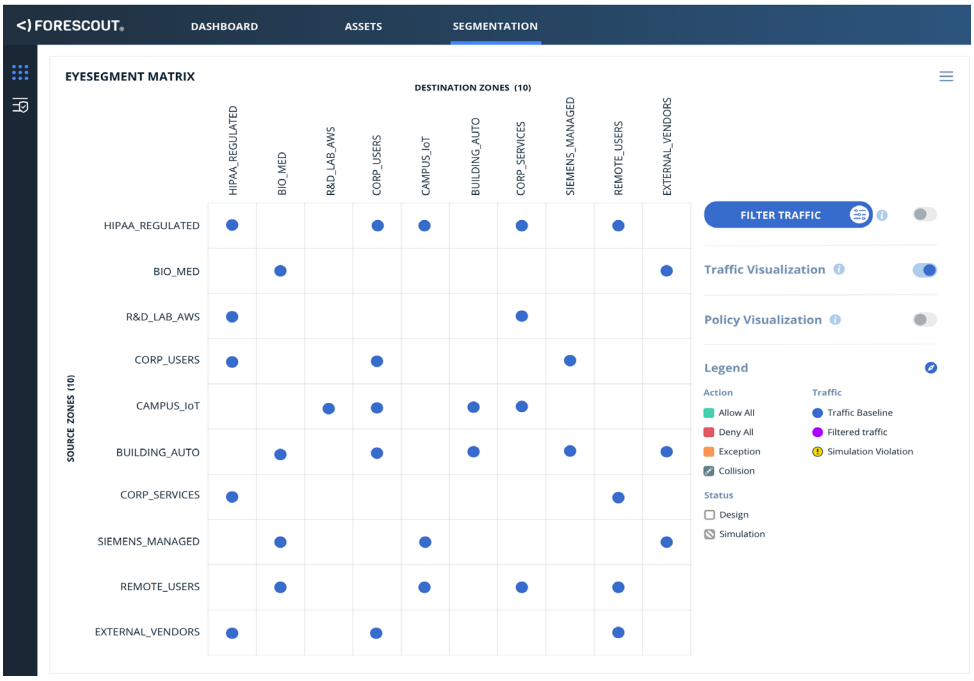

Figura 2: Griglia della connettività di eyeSegment con i flussi logici del traffico aziendale.

Progettare e simulare i criteri di segmentazione

Forescout eyeSegment aiuta a progettare, creare e perfezionare criteri di segmentazione efficaci basati su una tassonomia aziendale logica che può essere applicata a tutte le tecnologie di base esistenti. È possibile simulare l'implementazione dei criteri prima di attivarli effettivamente per valutarne l'impatto e limitare l'eventualità che provochino interruzioni dell'attività.

Creare criteri di segmentazione coerenti e granulari

Un criterio di segmentazione è un insieme di regole che disciplina se autorizzare in toto, bloccare in toto o autorizzare parzialmente il traffico dei dati tra specifiche zone di partenza e arrivo. Le zone vengono definite in base a gruppi di criteri standard e possono essere popolate manualmente o automaticamente tramite l'applicazione di criteri. Possono essere considerate zone anche singoli indirizzi IP e oggetti Forescout creati dalla segmentazione che fanno parte di gruppi. Ogni zona di segmentazione può essere impostata come zona di partenza, zona di arrivo o di entrambi i tipi.

Con un'unica console è possibile creare criteri di segmentazione con cui negare o autorizzare esplicitamente traffico specifico in transito attraverso domini di rete e tecnologie diversi. Ogni criterio può essere applicato al traffico proveniente da una specifica zona di partenza e diretto a una specifica zona di arrivo. Per impostazione predefinita, è autorizzato il traffico proveniente da qualsiasi zona di partenza e diretto a qualsiasi zona di arrivo ma, definendo criteri ed eccezioni, è possibile stabilire il traffico autorizzato e quello rifiutato così da permettere agli utenti di specificare azioni diverse per singoli sottogruppi e servizi.

Visualizzare i criteri e le dipendenze del traffico

Abilitare la visualizzazione dei criteri e del traffico per vedere i criteri di segmentazione creati e il relativo stato nella griglia della connettività (vedi di seguito). Le funzioni di filtro consentono di configurare singoli criteri per filtrare il traffico in base al servizio oppure all'intersezione tra zone della griglia precisando le zone di partenza e arrivo.

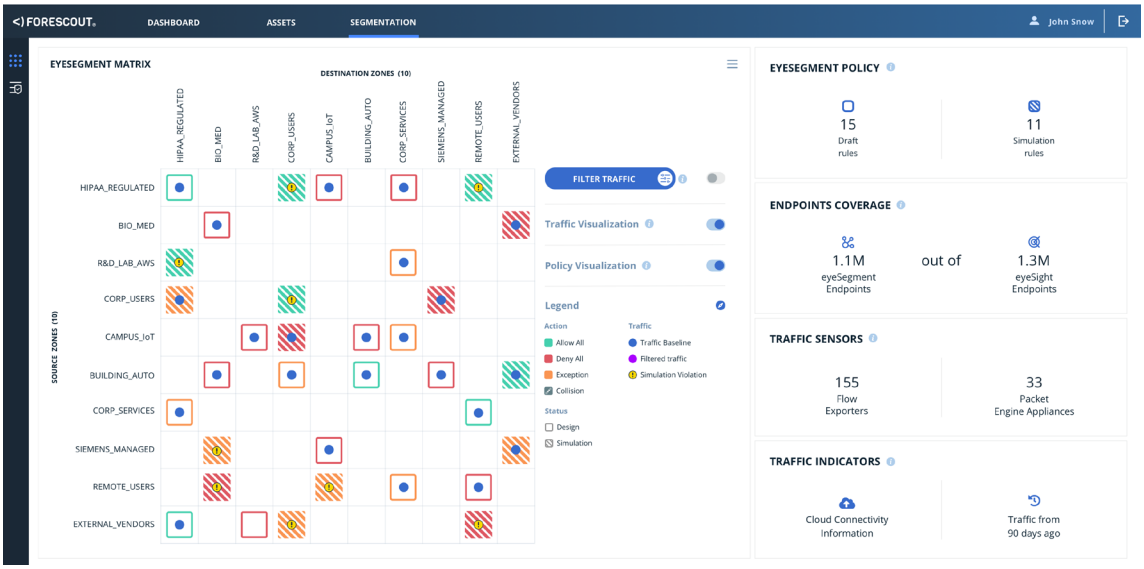

Figura 3: Visualizzazione e simulazione dei criteri.

Monitorare e reagire

La funzione di gestione complessiva dei criteri e il dashboard di eyeSegment consentono di monitorare in modo centralizzato i flussi di traffico tra le varie zone di partenza e arrivo. La capacità di monitorare costantemente e di reagire ai criteri di segmentazione separandoli dai controlli sottostanti rappresenta un prezioso aiuto, particolarmente quando l'infrastruttura non esercita alcun controllo. eyeSegment esercita anche un monitoraggio continuo sui controlli dell'infrastruttura aziendale per assicurarsi che le regole di segmentazione vengano implementate e funzionino correttamente nell'intero ambiente a cui sono applicate.

Casi d'uso

La piattaforma Forescout prevede la gestione di un'ampia gamma di scenari di segmentazione della rete. Grazie alla sua flessibilità, in qualsiasi scenario la piattaforma Forescout è in grado di ridurre il rischio di interruzione dell'attività e ridurre al minimo i costi operativi legati ai progetti di segmentazione.

Ecco alcuni casi d'uso comuni:

Protezione delle applicazioni critiche per l'azienda	• Per proteggere ininterrottamente le applicazioni critiche per l'azienda, è necessario assicurarsi che vengano applicati correttamente e sistematicamente controlli intra-aziendali e interaziendali su diversi servizi, applicazioni e domini • Controllare l'accesso da parte degli utenti ai servizi critici per l'azienda nei vari domini. Per proteggere le applicazioni critiche per l'azienda dall'abuso da parte degli utenti, è necessario assicurarsi che i controlli vengano applicati correttamente e sistematicamente
Configurazione di privilegi per accedere all'infrastruttura IT critica	• Limitare ai soli amministratori IT l'accesso ai dispositivi di rete sensibili (switch, NGFW, ecc.), ai data center e ai carichi di lavoro cloud (Active Directory/LDAP, DNS, Oracle Cluster, ecc.) definendo amministratori (accesso basato sul ruolo), riservando gli endpoint agli amministratori IT (tramite crittografia, aggiunta dei PC a un dominio, ecc.) e proteggendo le comunicazioni (utilizzo di porte o servizi specifici)
Protezione dei dispositivi IoT/OT aziendali (stampanti, fotocamere, VoIP, lettori di schede, impianti di condizionamento, ecc.)	• Proteggere la rete IT dai dispositivi IoT/OT • Proteggere i dispositivi IoT/OT dagli attacchi esterni
Segmentazione sicura dell'intero ambiente aziendale	• Verificare che tutti i punti di controllo presenti nei diversi domini (ambiente fisico, data center e IoT) e gestiti da altri team siano configurati come previsto e rispettino i requisiti dei criteri di segmentazione
Contenimento dei dispositivi vulnerabili	• Limitare l'accesso da e verso i dispositivi vulnerabili (WannaCry, non aggiornati, a fine vita, ecc.) presenti nella rete
Protezione dei dispositivi che utilizzano applicazioni e sistemi operativi obsoleti	• Ridurre la superficie di attacco segregando i dispositivi su cui sono installati sistemi operativi e applicazioni legacy • Mitigare il rischio di attacchi ai dispositivi che eseguono sistemi operativi a fine vita che non possono più essere aggiornati

FORESCOUT

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