

# Segmentazione della rete aziendale

Semplifica la segmentazione Zero Trust senza interruzioni delle attività

Con la promessa di efficienza, innovazione e produttività, la trasformazione digitale ha prodotto reti interconnesse e non segmentate, che sono suscettibili agli spostamenti laterali delle minacce e incapaci di proteggere il crescente numero di dispositivi dell'Enterprise of Things (EoT), connessi all'azienda estesa. Mentre i team IT sperimentano varie opzioni per implementare i controlli Zero Trust e aumentare la sicurezza, la paura di distribuzioni complicate e interruzioni costose delle attività mina la fiducia delle aziende e ne ferma i progressi. Le sfide comprendono:

- Timore di implementare progetti di segmentazione.
- Minacce e rischio di esposizione dovuti alla trasformazione digitale.
- Complessità operativa generata dalla presenza di fornitori diversi e dall'applicazione discontinua delle policy di segmentazione negli ambienti con più domini.
- Competenze, risorse e strumenti insufficienti per progettare, costruire e implementare progetti di segmentazione della rete efficaci per l'intero ambiente aziendale

## Perché Forescout: è la migliore soluzione per una segmentazione Zero Trust che non interrompe le attività.

Se queste sfide ti suonano familiari, ora è il momento ideale per valutare la soluzione Forescout, che semplifica la segmentazione Zero Trust e ottimizza la gestione dei rischi per la tua EoT connessa nell'ambiente esteso. La piattaforma Forescout accelera una segmentazione della rete dinamica e guidata dal contesto, senza complessità, costi eccessivi o impatti negativi sull'azienda.

Soddisfiamo le tue esigenze aiutandoti a:

- **Accelerare la segmentazione Zero Trust** in tutta l'azienda estesa.

**“Le tecnologie IoT e dei dispositivi di rete hanno introdotto una potenziale violazione di reti e aziende. [...] I team preposti alla sicurezza devono isolare, proteggere e controllare ogni dispositivo nella rete, continuamente”.<sup>1</sup>**

**FORRESTER RESEARCH**  
Giugno 2020

- Comprendere istantaneamente lo stato di segmentazione della rete, in tempo reale e su qualsiasi dispositivo, ovunque.
- **Ridurre la superficie di attacco e mantenere la conformità** tramite la segmentazione dinamica nei sistemi IT, IoT e IoMT (Internet of Medical Things, Internet delle Cose Mediche), facilmente applicabile a diversi ambienti verticali.
- **Semplificare l'analisi delle minacce** con meno strumenti, meno dashboard e più avvisi di pratico utilizzo.
- **Ridurre rischi e costi legati alla conformità gestendo in modo efficiente il rilevamento e risposta della sicurezza informatica**, con meno risorse qualificate.
- **Ottimizzare i flussi di lavoro fra i vari gruppi** e sfruttare gli investimenti esistenti con una policy di segmentazione uniforme in tutta l'azienda.

Forescout sa bene che non esiste una soluzione adatta a tutte le segmentazioni delle reti. Tutti gli strumenti di segmentazione hanno degli specifici punti di forza, casi di utilizzo e aree della rete dove possono essere meglio impiegati. La piattaforma Forescout, che include Forescout eyeSegment, collega tutte queste diverse tecnologie per accelerare progettazione, pianificazione e distribuzione della segmentazione della rete dinamica nell'azienda estesa, al fine di attuare policy Zero Trust efficaci, ridurre i rischi normativi e limitare la superficie di attacco.

Come mostrato nell'illustrazione qui sotto, una segmentazione su scala aziendale richiede un'architettura multi-livello, guidata dal contesto, per affrontare l'odierna e ampia diversità di tipi di dispositivo, a prescindere da dove si connettono alla rete. Forescout offre la piattaforma, gli strumenti e le competenze necessari per aiutarti a pianificare e implementare in modo efficiente tale soluzione.

**AUMENTA IL VALORE DEGLI INVESTIMENTI IN TECNOLOGIE INFORMATICHE E DI SICUREZZA**

- Consenti una segmentazione dinamica e non intrusiva
- Accelera in modo affidabile i progetti di segmentazione della rete Zero Trust
- Riduci il rischio di interruzione dell'attività
- Riduci i costi operativi
- Adeguati rapidamente ai requisiti normativi e di conformità
- Sfrutta gli investimenti esistenti nell'infrastruttura

**WORKSHOP DI SEGMENTAZIONE DELLA RETE**

Stai estendendo la tua distribuzione Forescout a scenari avanzati di controllo della segmentazione? I consulenti Forescout offrono ora un workshop per far sì che le tue policy di segmentazione della rete e l'implementazione siano in linea con la strategia aziendale. [Maggiori informazioni.](#)



### Componenti della soluzione

La piattaforma Forescout aiuta le aziende a elaborare le proprie strategie di segmentazione della rete su scala aziendale e ad accelerare le distribuzioni. Elenchiamo di seguito i principali prodotti della piattaforma.

#### Forescout eyeSight: contesto dettagliato per ogni indirizzo IP

Il prodotto eyeSight offre approfondimenti e contesto senza pari sull'intera rete connessa, dall'ambiente fisico al centro dati fino al cloud, trasformando il tuo inventario connesso in una tassonomia logica di dispositivi, applicazioni, utenti e servizi. Utilizza questa tassonomia per raggruppare tutti i dispositivi connessi in una gerarchia aziendale logica e segmentare la rete. Per maggiori dettagli visita <https://forescout.it/resources/eyeSight-datasheet/>.

#### Forescout eyeSegment: semplifica la segmentazione Zero Trust per qualsiasi dispositivo, ovunque

Forescout eyeSegment accelera progettazione, pianificazione e distribuzione della segmentazione Zero Trust dinamica in tutta l'azienda estesa.

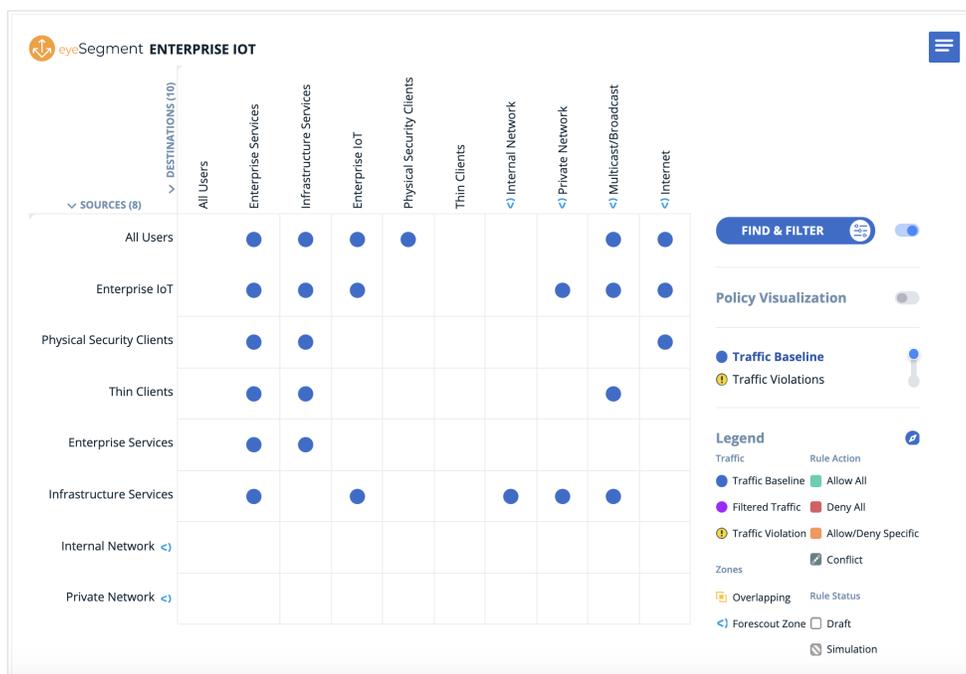
Consente alle aziende di abbracciare i principi Zero Trust per la sicurezza dell'EoT. eyeSegment abilita la rapida accelerazione dei progetti di segmentazione in tutta

l'azienda estesa, per ridurre la superficie di attacco, limitare il raggio di diffusione di un'aggressione e mitigare il rischio per l'impresa e le violazioni normative. Per maggiori dettagli visita <https://forescout.it/resources/eyeSegment-scheda-tecnica/>.

#### eyeControl/eyeExtend: coordina controlli uniformi in tutti i domini della rete e negli ambienti con più fornitori

La piattaforma Forescout ti permette di coordinare in modo dinamico le policy di segmentazione e di automatizzare i controlli fra tecnologie di imposizione eterogenee, avvalendosi dei prodotti Forescout eyeControl e eyeExtend.

- eyeControl abilita l'imposizione uniforme di policy e controlli di segmentazione, sensibili al contesto, alle esistenti tecnologie di base, eliminando la necessità di agent. Per maggiori informazioni visita <https://forescout.it/risorse/eyeControl-datasheet/>
- I prodotti eyeExtend coordinano i controlli tramite integrazioni pronte all'uso con i firewall di nuova generazione (NGFW) dei principali fornitori. Per maggiori informazioni sulle integrazioni NGFW di Forescout visita [www.forescout.com/platform/eyeExtend](http://www.forescout.com/platform/eyeExtend)



La soluzione di segmentazione Forescout ti permette di concentrarti sulle cose più importanti, così puoi analizzare e studiare un particolare andamento del traffico nel tuo ambiente, come mostrato nell'illustrazione qui sopra. Puoi comprendere istantaneamente lo stato corrente dei flussi di comunicazione e creare le policy di segmentazione Zero Trust desiderate. Questo metodo, che privilegia la visibilità, ti consente di creare facilmente delle zone di microsegmentazione e di proteggere la tua azienda assicurandone la continuità.

### Casi d'uso

La soluzione di segmentazione della rete Forescout trova un'ampia gamma di utilizzi in diversi segmenti verticali come sanità, OT (tecnologie operative), servizi finanziari, settore pubblico, retail e altri. Grazie alla sua flessibilità, in tutti i casi la piattaforma Forescout è in grado di ridurre il rischio di interruzione dell'attività e di ridurre al minimo i costi operativi legati ai progetti di implementazione e segmentazione Zero Trust. Per saperne di più, leggi la panoramica sui casi d'uso nella segmentazione della rete su scala aziendale.

### Riepilogo

Attualmente i progetti di segmentazione sono gestiti in modo isolato, a causa della complessità delle tecnologie intra-dominio. I fattori aggiuntivi quali la sicurezza Zero Trust, la trasformazione digitale e la conformità normativa, richiedono un approccio più globale e sistematico. La soluzione Forescout affronta i problemi delle aziende legati alla segmentazione intra-dominio per diversi casi d'uso nelle aziende estese. Tramite la comprensione istantanea e in tempo reale dello "stato corrente" della segmentazione, le policy sensibili al contesto, i gruppi strutturati a livello aziendale e le simulazioni proattive delle policy, la piattaforma Forescout abilita i controlli della segmentazione Zero Trust che abbracciano diverse tecnologie di imposizione e convalidano i risultati previsti. Il risultato è una rapida accelerazione dei progetti di segmentazione Zero Trust che includono controlli più granulari e un rischio ridotto in tutta l'azienda.

1. Mitigating Ransomware With Zero Trust, Forrester Research, Inc., 8 giugno 2020

Vedere non basta.  
Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

forescout.com/solutions/network-segmentation info-italia@forescout.com Tel. (internazionale) +1-408-213-3191