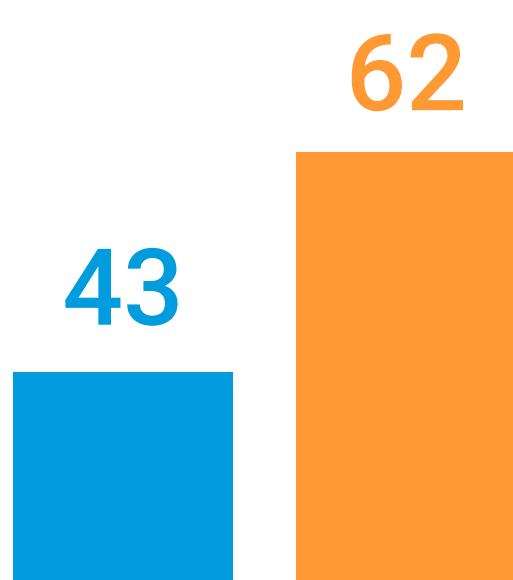


Segmentazione: la chiave per il percorso dei servizi finanziari verso il modello Zero Trust

Superare i problemi di implementazione per proteggere i sistemi bancari più importanti

Di fronte al notevole aumento degli attacchi ransomware, solo le istituzioni finanziarie che hanno adottato una soluzione di segmentazione avanzata hanno potuto trasformare la propria strategia difensiva e ridurre il carico operativo e finanziario.

Il numero di attacchi ransomware (riusciti o meno) è raddoppiato negli ultimi due anni...



...passando da una media di 43 attacchi nel 2021 ad una media di 62 attacchi nel 2023.



Percentuale di responsabili della sicurezza IT che concorda nel ritenere la segmentazione una componente cruciale nella lotta agli attacchi più dannosi.

88%

Percentuale di istituzioni finanziarie secondo cui la microsegmentazione è tra le priorità aziendali; per il 39% di queste si tratta della massima priorità.



Nonostante la fiducia in questa tecnologia, i ritmi di impiego della segmentazione sono lenti. Solo il 39% delle società di servizi finanziari ha segmentato più di due delle aree aziendali più importanti nel 2023 (rispetto al 26% nel 2021), mentre il 45% ha avviato un progetto di segmentazione della rete almeno due anni fa, il che suggerisce uno stallo.

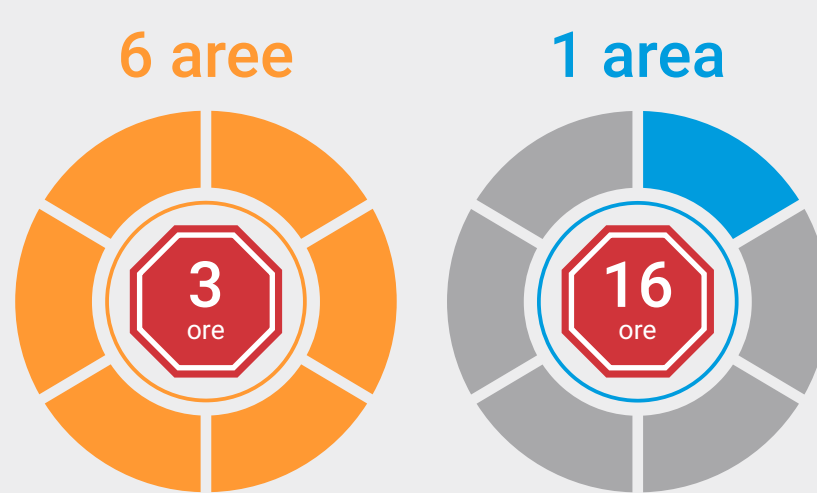
L'adozione di un sistema Zero Trust è uno dei motivi principali per cui le istituzioni finanziarie hanno avviato un progetto di segmentazione, ma meno della metà di esse (47%) afferma che l'implementazione del sistema Zero Trust sia pienamente definita e completata.



La perseveranza dà i suoi frutti. Le organizzazioni che hanno segmentato sei delle aree aziendali più importanti sono riuscite a trasformare i propri sistemi di difesa.

La portata della segmentazione fa la differenza

Dopo una violazione, un attacco ransomware viene bloccato con una velocità più di 5 volte maggiore laddove sono state segmentate sei aree aziendali.



In che modo le istituzioni finanziarie possono trarre vantaggio dalla segmentazione?

01



Semplificate e accelerate la conformità normativa con una visibilità granulare

02



Proteggete i sistemi essenziali, come trasferimenti di denaro, pagamenti e applicazioni dei clienti

03



Prevenite il movimento laterale non autorizzato isolando adeguatamente l'accesso di terze parti e gestendo le vie di accesso

04



Adottate il cloud, il PaaS e altre tecnologie emergenti in modo conveniente e sicuro

Scaricate il rapporto completo per iniziare il percorso Zero Trust