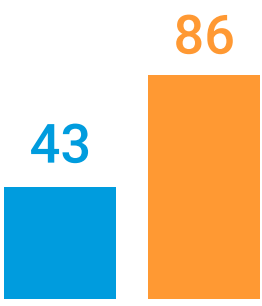
INFOGRAPHIC

The State of Segmentation 2023

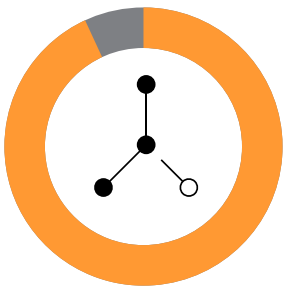
Overcoming deployment obstacles proves to be transformational

Facing double the number of ransomware attacks, only those with more advanced segmentation have transformed their defenses.

The number of ransomware attacks (successful and unsuccessful) has doubled in the past two years ...



from 43 on average in 2021 to 86 in 2023.



93%

of IT security decision-makers agree that segmentation is critical to thwarting damaging attacks.

89% say microsegmentation is at least a high priority for their organization, with 34% saying it is the top priority.

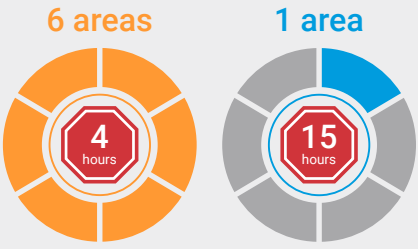
Despite this belief in the technology, segmentation deployments have been slow. Only 30% of organizations have segmented across more than two critical business areas in 2023 (compared to 25% in 2021), and 44% started a network segmentation project two or more years ago, suggesting efforts have stalled.

Adopting a Zero Trust framework is among the top reasons organizations began a segmentation project, but only two in five (40%) say their Zero Trust framework deployment is fully defined and complete.

Perseverance pays off. Those who have segmented six critical business areas have transformed their defense.

Extent of segmentation matters

After a breach, a ransomware attack is completely stopped 11 hours faster when six areas are segmented.



How can you speed your segmentation deployment?

Ensure your solution:

- Creates an interactive visual of all the connections being made in your entire IT environment
- Is software-based so it covers all operating systems and devices, regardless of their physical location
- Provides time-saving, AI-powered policy recommendations and out-of-the-box policy templates
- Offers top-tier technical support that partners with you throughout the deployment process

Download the full report

 | Support | Published 10/23