Akamai

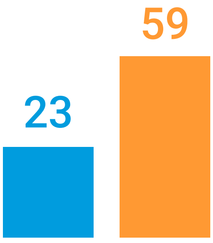
INFOGRAPHIC

The State of Segmentation for Healthcare & Life Sciences

Microsegmentation can reduce clinical and financial risk when expertly deployed

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

The number of ransomware attacks in the healthcare and life sciences industry has more than doubled in two years ...



... from 23 on average in 2021 to 59 in 2023.

94%

of IT security decision-makers agree that segmentation is critical to thwarting damaging attacks. But only 36% of healthcare organizations around the globe have segmented across more than two critical business areas in 2023 (compared to 25% in 2021).

The healthcare industry is most likely to have had an office-based employee/user be the source of an attacker gaining network access (47% compared to an average of 26% across other industries, including banking, ecommerce, and energy).

29% of respondents said that their healthcare organization started a segmentation project because they'd already fallen victim to a ransomware attack.

Extent of segmentation matters

After a breach, a healthcare and life sciences ransomware attack is stopped 11 hours faster when six areas are segmented.

Stop segmenting the hard way

Ensure your solution:

01 ✓
Is software-based so it covers all operating systems and devices, regardless of their physical location

02 ✓
Creates an interactive visual of all the connections being made in your entire IT environment

03 ✓
Provides time-saving, AI-powered policy recommendations and out-of-the-box policy templates

04 ✓
Offers top-tier technical support that partners with you throughout the deployment process

Download the full report

 | Support | Published 05/24