

RANSOMWARE SO FAR & BEYOND



This has been around for a while. **Why is it a concern now?**

62% increase of incidents just in the United States.

82% increase in ransomware globally with payouts averaging **\$500,000**.

4X increase in vulnerabilities tied to ransomware.

5 Ransomware attacks every minute globally

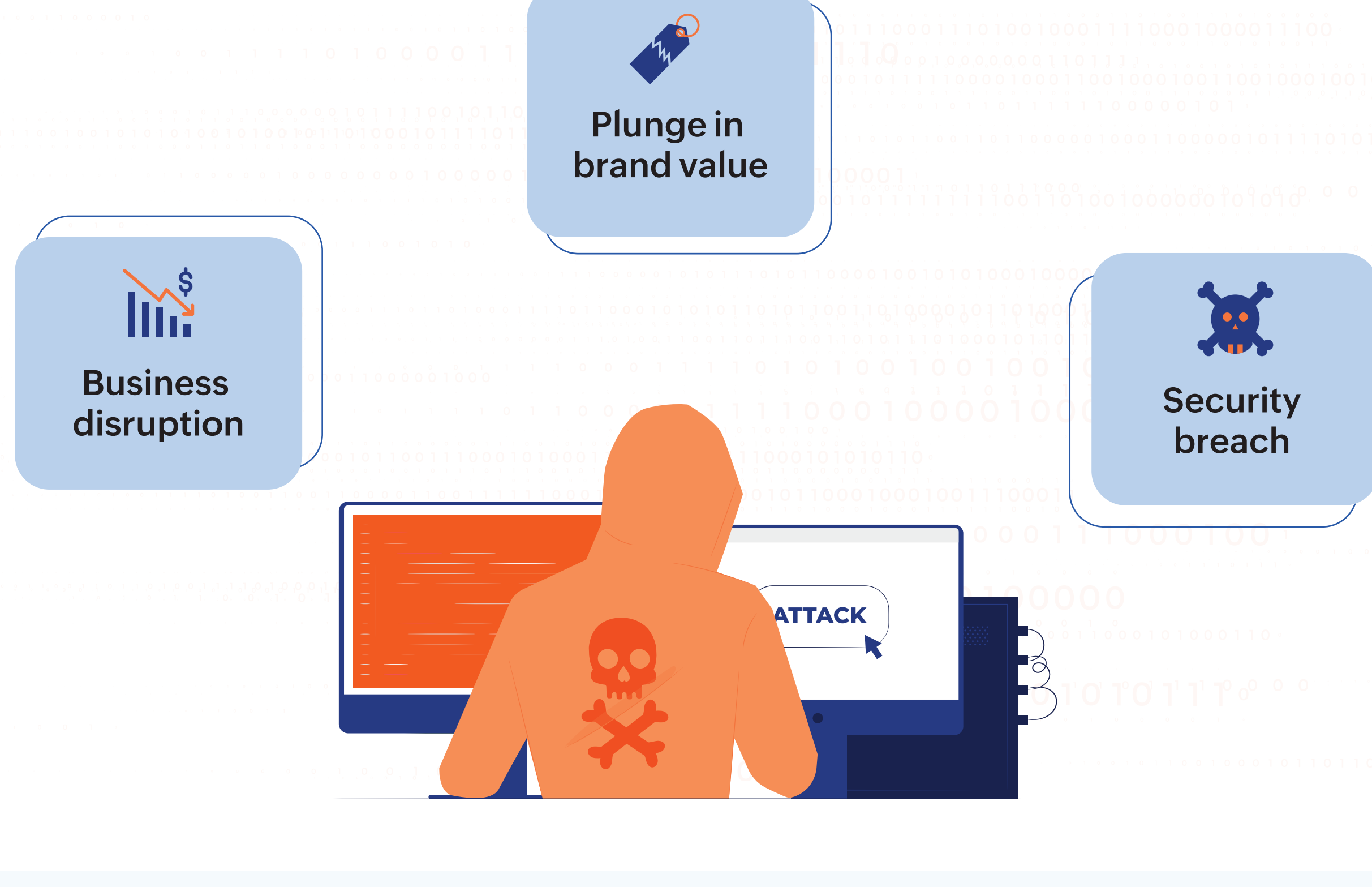
80% of the enterprises that paid a ransom were still hit by ransomware a second time.

236.1 million ransomware attempts were made in the first half of 2022 alone!



95% of cybersecurity problems are due to **human error**, according to the World Economic Forum's 2022 Global Risks Report.

Ransomware goes beyond the ransom

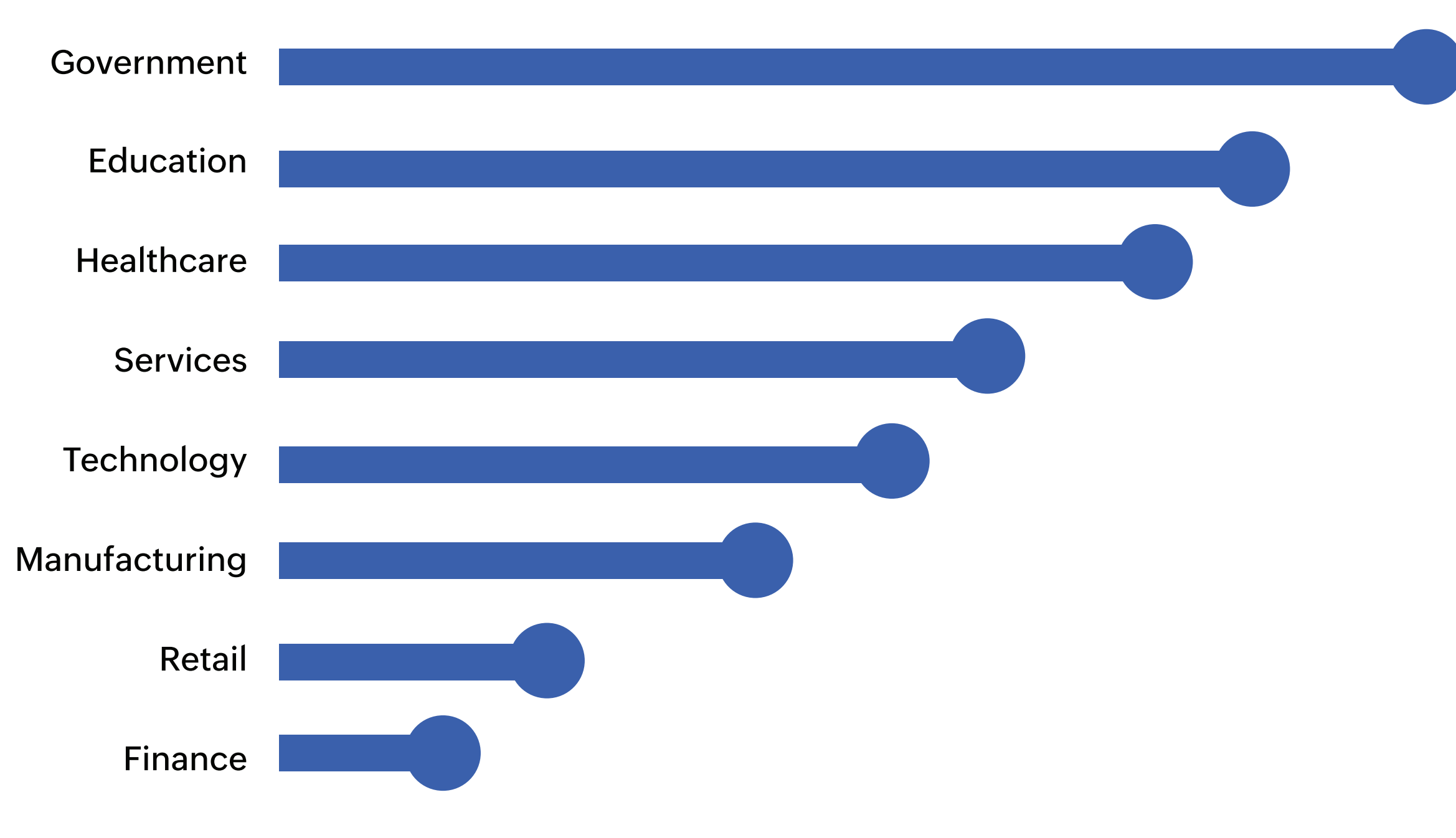


Consequences for businesses



Why should you be concerned

The Industries Most Affected by Ransomware
Number of reported ransomware attacks worldwide by sector



Where is it heading

Ransomware has become an industry. Its more than just the final extortion.

The initial access broker



Threat actors that sell cybercriminals access to corporate networks.

Lateral movement



Broaden and cement that foothold of initial access whilst gaining further access to valuable data or systems.

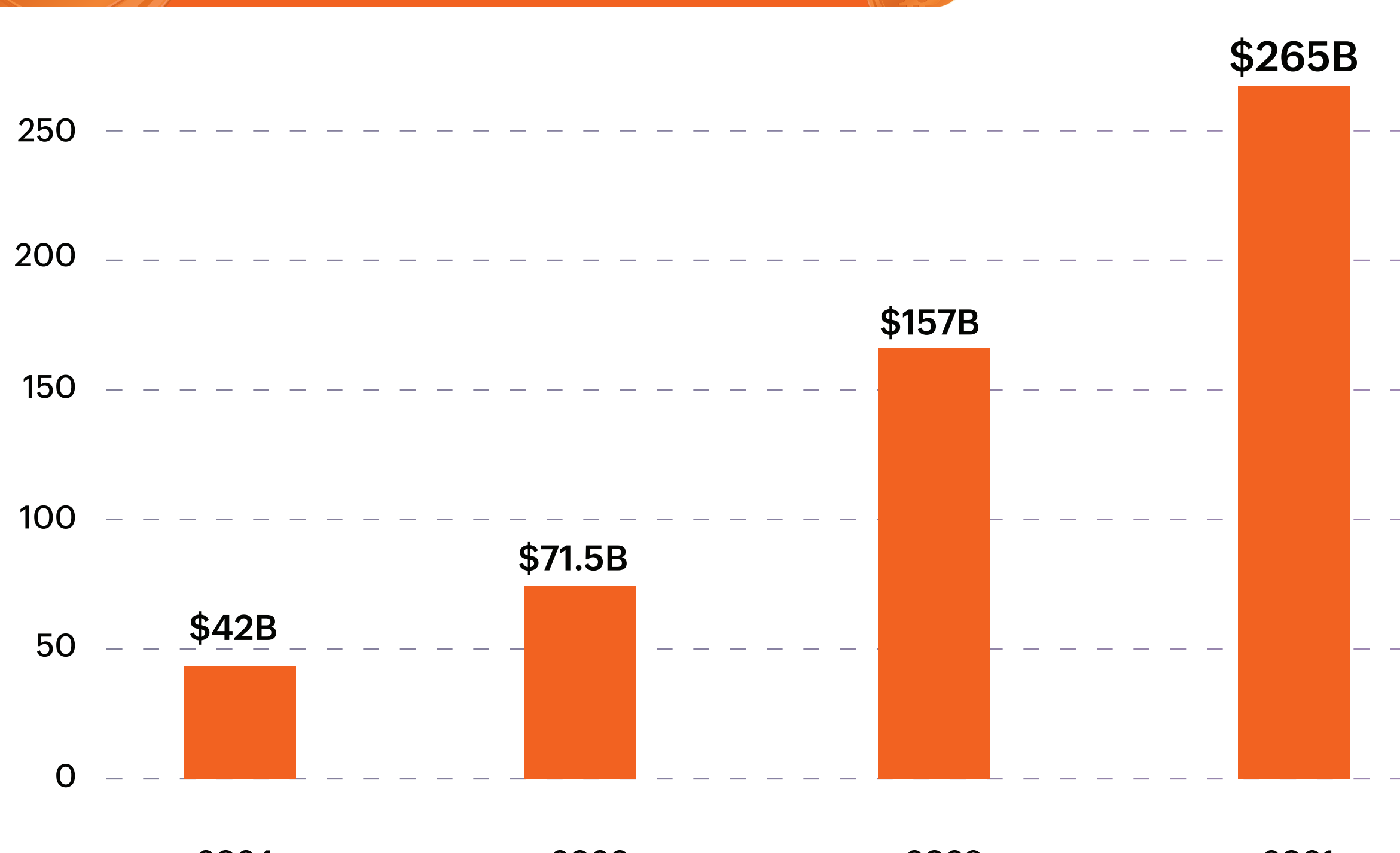
Over **90%** of ransomware attacks are preventable, a Gartner analysis indicates.

At least **75%** of organizations will be targeted more than once by 2025.

700% increase in the number of ransomware attacks by 2025 is forecast.

Gartner

The Cost of Ransomware by 2031



Ransomware attacks will inevitably continue to evolve, and so will ManageEngine's defense mechanism.

You'll never WannaCry with Endpoint Central



ENDPOINT CENTRAL FREE TRIAL