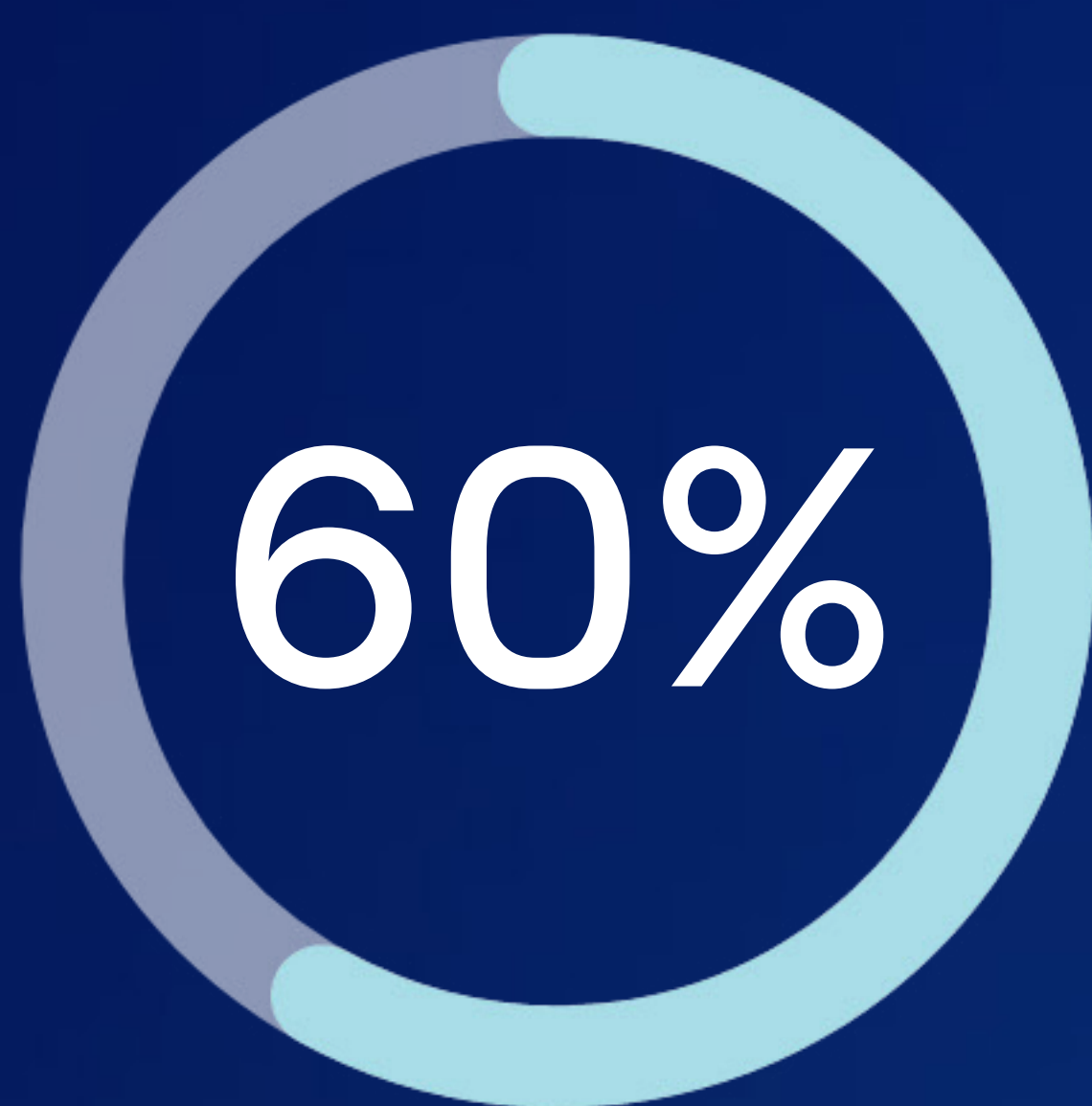


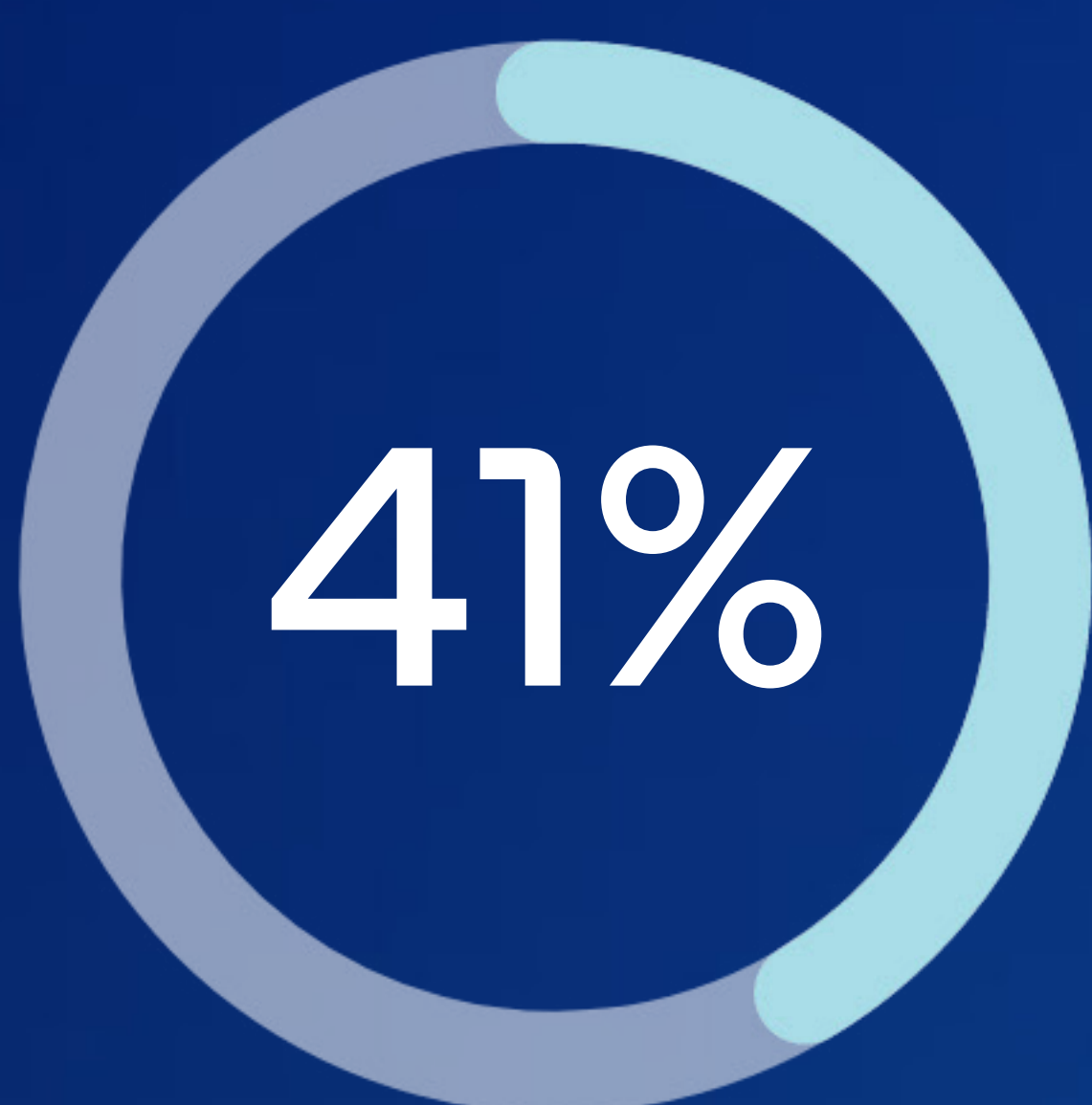
Prepare Your Endpoints For Zero Trust Compliance

Its core concept of “never trust, always verify” helps you discover vulnerable endpoints to mitigate threats.

3 Reasons Zero Trust is Gaining Steam:



of 815 enterprise executives say they will use Zero Trust network architecture for all endpoints by 2026¹

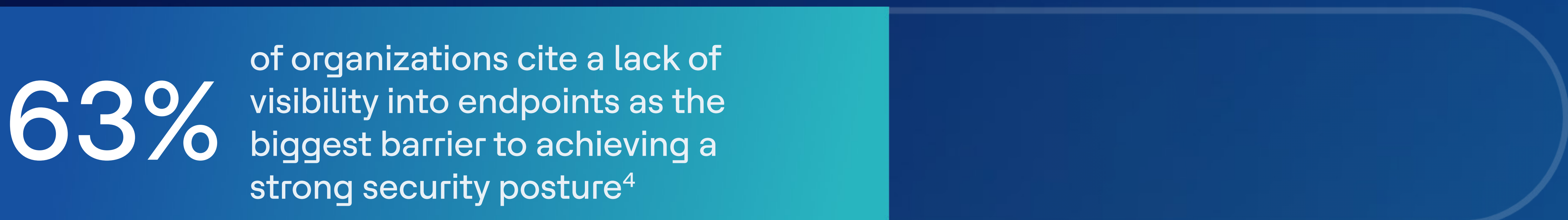


of organizations surveyed in 2022 reported they have already deployed a Zero Trust approach, compared to 35% in 2021²



of 300 IT decision-makers cited ransomware threats, and 53% cited remote worker risks as top Zero Trust drivers³

2 More Reasons Everyone is Moving to Zero Trust



of organizations cite a lack of visibility into endpoints as the biggest barrier to achieving a strong security posture⁴



The average breach cost saved by organizations that have deployed Zero Trust, compared to those that haven't⁵

1 Step You Can Take Today: Enable Immediate Patching



Organizations rank **unpatched vulnerabilities** as the riskiest entry point for ransomware⁶

Learn How NIST 800-207 and Zero Trust can Help You Deploy Modern Endpoint Management for:

- Discovery
- Visibility
- Remediation
- Continuous Compliance



Optimize Endpoint Management Today

To successfully implement Zero Trust organizations must: identify and manage all devices; grant secure access on a need-to-know basis; continuously monitor endpoints; and identify vulnerabilities to manage configurations.



EXPLORE HOW HCL BIGFIX CAN HELP YOU ADVANCE ZERO TRUST SECURITY IN YOUR ORGANIZATION.

- Download eBook
- Talk to an Expert