Ransomware attacks are on the rise. In 2020, the number of attacks worldwide increased by 485% year over year.1 Because recovering from a ransomware attack can be a costly, time-consuming process that hinders an organization’s ability to conduct normal business, you need to take steps now to properly protect yourself and ensure you can recover effectively should an attack occur.

To reduce your ransomware exposure, you first need to understand where gaps may exist within your defenses and then develop a proactive cybersecurity strategy to close those gaps. Through Coalfire’s ransomware readiness assessment, you will gain an understanding of your risks and evaluate what options you have for recovery.

COALFIRE RANSOMWARE READINESS ASSESSMENT

During the assessment, our experts will help you answer the following questions, so you can improve the effectiveness of your cybersecurity strategy:

- **How are you managing vulnerabilities?** What is your patching program coverage and execution for systems in your environment?
- **Do you have an incident response plan?** Are you prepared for ransomware outages and have your policies been updated for ransomware scenarios?
- **What is your communications plan?** Do you have plans to communicate the impact of ransomware outages internally and externally?
- **Where does your important data live?** Is it accessible from servers, workstations, or storage area networks?
- **What are your backup policies and procedures?** Are your backups air-gapped? Do you know how long it would take to restore?
- **Are you following best practices for data protection?** What are you keeping? Should you archive data? Can you make restoration simpler?

1 Bitdefender. “2020 Consumer Threat Landscape Report.”