FIVE STEPS TO SECURING THIRD-PARTY VENDOR REMOTE ACCESS

1. CONSOLIDATE REMOTE ACCESS TOOLS
   - Require all of your vendors (and internal employees) to use a single, centralized remote access solution to connect to systems and applications on your network.

2. SHUT OFF ALL OTHER REMOTE ACCESS
   - Block access from any unapproved remote access tools to eliminate open ports that are often compromised by hackers.

3. ENFORCE UNIQUE CREDENTIALS & MULTI-FACTOR AUTHENTICATION
   - Require every third-party technician who accesses your network to use unique credentials and two-factor authentication to reduce the risk of stolen vendor credentials and improve compliance.

4. EMPLOY GRANULAR PERMISSIONS
   - Choose a remote access tool that includes permission settings by vendor or team so you can restrict which systems third parties can directly access, and when.

5. CAPTURE A SECURE AUDIT TRAIL & SET UP ALERTS
   - Capture a secure audit trail of every action third-parties execute on your systems, and set up alerts for abnormal activities.

Find out how Bomgar can help you improve vendor access security: www.bomgar.com/access-management