Cybersecurity for Remote Workers

A recent WFH Research study found that ~40% of surveyed full-time U.S. resident employees are either fully remote or working in a hybrid arrangement. This finding underscores the need for policies that ensure secure and effective remote work for a diverse U.S. workforce. Employers currently support remote or hybrid workers by providing them with company-owned-personally enabled (COPE) devices and other infrastructure. Despite security measures organizations implement including mobile device management (MDM) and other endpoint protection solutions, cyber threat actors continuously exploit vulnerabilities in virtual private networks (VPNs), mobile operating systems, and unprotected networks in the U.S. and globally. Fully remote or hybrid work arrangements add value to organizations by enhancing flexibility, increasing employee satisfaction, saving costs, and expanding talent pools. However, these benefits come with the need for heightened security measures.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.