

# HPE SECURITY ASSESSMENT FOR REMOTE WORKFORCE

## SERVICE OVERVIEW

The COVID-19 pandemic has driven business leaders to transform operating models and adapt business operations to continue to deliver value and meet Customer expectations. The rapid adoption of new enterprise and consumer-grade technologies, combined with the continued and exponential growth in use of cloud services and explosion of connectivity, enables enterprises to continue operations even with a stay-at-home workforce. This rapid change, however, puts significant pressure on the security posture of the enterprise and significantly increases its risk exposure.

Business and security operations face increased challenges resulting from remote workforce, including:

- Remote access challenges leading to relaxation of security controls to meet demand
- Limited to no supply of approved devices forcing the adoption of BYOD
- Insufficient mobile device management capabilities to enforce policy compliance
- Adoption of unapproved and insecure collaboration tools by employees
- Storage of sensitive organizational data on untrusted devices
- Co-mingling of corporate and personal computing resources on remote devices
- Increased exposure to COVID-19 phishing attempts

Some of these security risks are not new but have been exacerbated by the pressure to adopt cost-effective and minimally tested solutions to sustain business operations. Security programs and risk management practices need to be updated to support the shift to work from home and the rapid adoption of new tools and technologies. Some of the key questions that need to be addressed include:

- Does the business have visibility into and understand the risks resulting from the shift to work from home?
- What policies, procedures, and technology changes are needed to support business objectives?
- How does the business prioritize and manage the identified risks effectively?
- Does the business understand the risks they are accepting?

The HPE Security Assessment for Remote Workforce service helps organizations take an objective look at their organization's security and continuity of operations resources and practices. The service combines the P5 model—people, policies, processes, products, and proof—and the Center for Internet Security (CIS) Top 20 Critical Controls to evaluate certain control properties to help assess security-related controls of the organization operating with a remote workforce.

## SERVICE BENEFITS

The HPE Security Assessment for Remote Workforce service equips organizations with insights, which is designed to help you:

- Understand the gaps in assessed security controls and processes and the associated security and risk exposure along with HPE recommendations. This is based upon HPE’s findings intended to help address the identified security concerns
- Identify potential ways to reduce ongoing technology operation and adoption risk by leveraging HPE expertise and proven security reference architectures
- Prepare your organization for security incidents resulting from remote work, and help identify potential ways to lower their likelihood and impact
- Continue to be supportive of organizational policies and requirements
- Identify what security controls may need to be implemented to help protect the organization, while extending the virtual IT ecosystem to include unknown networks, devices, and software

**TABLE 1.** Service features

	HPE works toward performing the tasks identified in this table for up to five business days (not to exceed 40 hours):
<b>Assessment of security essentials to drive alignment to security best practices</b>	Working with the Customer, HPE assesses certain Customer IT remote workforce security practices against the CIS Top 20 Critical Controls—Implementation Group 1. These CIS Top 20 Critical Controls are scored on the P5 model
<b>Assessment of remote access environment</b>	Up to 25 supplemental interview questions may be used to help assess the existing remote access environment. Additional information may be sourced by HPE as appropriate
<b>Reporting and presentation</b>	Reporting on output of HPE’s findings in PowerPoint format of up to 10 slides, along with one Customer debrief session to be delivered via teleconference

## SERVICE LIMITATIONS

- HPE and Customer shall agree upon the project schedule, which shall be based upon the allotted hours as set forth in Table 1, inclusive of 12 hours required by HPE for report generation and presentation
- HPE may conduct up to six interviews per the agreed project schedule
- HPE delivers the service remotely, with interviews conducted electronically using a mutually agreed facility (phone, audio/video conference)
- HPE may review up to three Customer documents as part of the assessment
- No scanning tools are used in the performance of this service
- HPE does not require remote access to Customer network



## CUSTOMER RESPONSIBILITIES

### The Customer will:

- Provide all relevant documentation required by HPE to perform these services at least two business days prior to the start of interviews
- Ensure all attendees with appropriate skills and knowledge are available for interviews as scheduled

### General provisions and exclusions

- Services are provided remotely during HPE standard local business workdays and hours, excluding HPE holidays
- HPE stops work upon completion of 40 hours of effort
- Any deliverables are accepted upon delivery
- HPE's ability to deliver the services is dependent upon the Customer's full and timely cooperation with HPE, as well as the accuracy and completeness of information and data the Customer provides to HPE
- The Customer acknowledges and agrees that HPE may use resources outside the country of purchase for delivery of these services
- HPE reserves the right to reprice for services not scheduled and delivered within 180 days
- To the extent HPE processes personal data on your behalf in the course of providing the services, the HPE Data Privacy and Security Agreement Schedule—HPE Support and Professional Services (Services) found at [hpe.com/us/en/legal/customer-privacy.html](https://hpe.com/us/en/legal/customer-privacy.html) shall apply

## LEARN MORE AT

[hpe.com/services/security](https://hpe.com/services/security)

Make the right purchase decision.  
Contact our presales specialists.



Chat



Email



Call



**HPE support**



**Get updates**