HPE POINTNEXT SERVICES

HPE CONTINUOUS SECURITY IMPROVEMENT SERVICE

Advisory and Professional Services from HPE Pointnext Services

SERVICE OVERVIEW

HPE Continuous Security Improvement Service is designed to provide ongoing improvement of your organization's security posture to keep pace with digital transformations, prepare for the dynamic threat landscape, and enable compliance with regulations. Anchored by an annual security posture assessment based on ISO/IEC 27002:2013, an assigned security advisor (ASA) will work with you throughout the year and will act as the conduit to other HPE deep-domain security specialists and resources to help you stay on track in meeting your unique security goals.

Based on a yearly subscription term, HPE Continuous Security Improvement Service is available with the following options:

- **HPE Continuous Security Improvement Service Essential** includes one annual posture and compliance assessment with documented findings and remediation recommendations presented over a briefing session; an ASA who will oversee and coordinate service-related activities; and two remote security expert advisory sessions (up to two hours each) on security subjects of your choice.
- **HPE Continuous Security Improvement Service Advanced** includes HPE Continuous Security Improvement Service Essential, plus a midyear review that focuses on incremental changes since the annual assessment, and two additional remote security expert advisory sessions (up to two hours each) on security subjects of your choice.
- **HPE Continuous Security Improvement Service Premium** includes HPE Continuous Security Improvement Service Advanced, plus one network vulnerability/penetration test and two additional remote security expert advisory sessions (up to two hours each) on security subjects of your choice.

The Service features table provides additional information on the features and options available under this service.

SERVICE BENEFITS

- Accelerate your security program to keep pace with the security requirements of current and anticipated digital transformations
- Ongoing improvement and maturing in security posture to mitigate risks and meet compliance requirements
- Ability to show year-over-year comparison and improvements
- Access to an HPE security advisor who understand your environment and security advisory sessions with HPE security experts on subjects of your choice

SERVICE FEATURE HIGHLIGHTS

- HPE Continuous Security Improvement Service Essential
- HPE Continuous Security Improvement Service Advanced
- HPE Continuous Security Improvement Service Premium

COVERAGE

- Services will be provided during local HPE standard business days and hours excluding HPE holidays

SPECIFICATIONS

TABLE 1. SERVICE FEATURES

Feature	Delivery specifications
HPE Continuous Security Improvement Service Essential	This service includes the following: • One annual security assessment A detailed security assessment based on the widely adopted international standard, ISO 27002:2013; provides an in-depth review of 114 security practices and controls using HPE innovative P5 model: People, Policies, Processes, Products, and Proof. Under this service feature, Hewlett Packard Enterprise provides the following: – Interview with key security stakeholders (up to 10), security awareness surveys (up to 250 employees), customer security artifact reviews (up to 12), and collection and review of other related information – Input data into the HPE assessment tool to document the current state of security and continuity controls as described by ISO 27002:2013 – Derive up to two Equivalency Scores (ISO 27002 cross-mapped to other standards) ▫ Cloud Security Alliance (CSA) ▫ Cloud Controls Matrix (CCM) ▫ CSA Big Data working group ▫ HIPAA/HITECH ▫ PCI DSS ▫ NIST 800–53 ▫ CSA CIAQ (mobility) – Create a Microsoft®-based Word document report presenting the analysis and recommendations. The report will contain the following components: ▫ Security solution inventory report ▫ Findings and recommendations report ▫ Findings and recommendations presentation – Present the result of the assessment via a remote briefing session using Microsoft PowerPoint – Conduct assessment activities both on-site and remotely • An ASA An HPE security advisor, your single point of contact and coordinator for this service, will provide coaching and information of interest that apply to your unique environment. Under this service feature, Hewlett Packard Enterprise provides the following: – Monthly check-in calls (up to 2 hours) – Monthly status report (up to 5 pages) that documents activities undertaken by HPE as part of this service during the prior month • Two remote security expert advisory sessions (up to two hours each): Sessions with HPE deep-domain security experts to address security subjects of particular interest or gaps found in your organization to address relative and pressing security issues Under this service feature, Hewlett Packard Enterprise provides the following: – Prepare and conduct two remote security expert advisory sessions

SPECIFICATIONS (CONTINUED)

TABLE 1. SERVICE FEATURES (CONTINUED)

Feature	Delivery specifications
HPE Continuous Security Improvement Service Advanced	HPE Continuous Security Improvement Service Advanced includes the HPE Continuous Security Improvement Service Essential plus one additional Equivalency Score during the annual security assessment, midyear review and two additional remote security expert advisory sessions (up to two hours each). • Midyear review: A midyear review using a lite version of the annual assessment methodology to capture your progress, so you can make the necessary adjustments to reach your year-end security and protection goals. Under this service feature, Hewlett Packard Enterprise provides the following: – Interview with key security stakeholders (up to five), security awareness surveys (up to 125 employees), customer security artifact reviews (up to 6), and collection of other related information – Input data into the HPE assessment tool to document the current state of security and continuity controls as described by ISO 27002:2013 – Derive up to one Equivalency Score (ISO 27002 cross-mapped to other standards) ▫ CSA CCM ▫ CSA Big Data working group ▫ HIPAA/HITECH ▫ PCI DSS ▫ NIST 800–53 ▫ CSA CIAQ (mobility) – Create a Microsoft-based Word document report presenting the analysis and recommendations. The report contains the following components: ▫ Security solution inventory report ▫ Findings and recommendations report ▫ Findings and recommendations presentation – Present the result of the assessment via a remote briefing session using Microsoft PowerPoint – Conduct assessment activities both on-site and remotely • Additional two remote deep-domain security expert advisory sessions (up to two hours each) (for a total of four sessions per year): Sessions with HPE security experts to address security subjects of particular interest or gaps found in your organization to address relative and pressing issues Under this service feature, Hewlett Packard Enterprise provides the following: – Prepare and conduct two additional remote security expert advisory sessions
HPE Continuous Security Improvement Service Premium	HPE Continuous Security Improvement Service Premium includes HPE Continuous Security Improvement Service Advanced plus one additional Equivalency Score during the annual security assessment and midyear review, one network vulnerability/penetration test and two remote security expert advisory sessions (up to two hours each). • Network vulnerability/penetration test: Scanning of your internal and/or external network to find vulnerabilities that could lead to data leakage and outages; includes penetration testing by HPE ethical hackers to find unauthorized points of entry into your network Under this service feature, Hewlett Packard Enterprise provides the following: – Scanning of one internet-facing domain name and associated IP addresses for vulnerabilities or scanning of up to 128 internal network IP addresses for vulnerabilities (using a VPN and "jump box") – Penetration testing of up to six IP addresses (systems) using ethical hacking techniques to determine if system is exploitable – Documentation of ethical hacking activity and results (including screenshots) – Recommendations for addressing any successful exploits – Vulnerability and penetration testing conducted remotely • Additional two remote security expert advisory sessions (up to two hours each) (for a total of six session per year): Sessions with HPE deep-domain security experts to address security subjects of particular interest or gaps found in your organization to address relative and pressing issues Under this service feature, Hewlett Packard Enterprise provides the following: – Prepare and conduct two additional remote security expert advisory sessions

CUSTOMER RESPONSIBILITIES

- Provide complete and accurate responses to all queries from Hewlett Packard Enterprise
- Communicate openly about IT infrastructure governance practices and needs to support their business objectives
- Communicate openly on the relevant elements of the financial budgeting and service costing structure of the subject information and asset protection controls and security organization
- Assign a contact person to organize project logistics

- Assign a project sponsor and be available for two (2) to four (4) hours per week to discuss logistics, preparation, outcomes, and data gathering during the annual and midyear assessment period
- Provide access to right management level (functional management or higher)
- Ensure interviewees are available as per the mutually agreed upon interview schedule
- Provide all requested documents and artifacts as per the agreed upon project schedule and HPE document requests
- Complete the HPE provided inventory form for capturing security and continuity technology and solutions
- Provide subject matter experts (SMEs) as required to clear up any areas of confusion or uncertainty
- Perform other reasonable activities to help HPE identify or resolve problems as requested by HPE
- Provide a suitable work area for delivery of the service, including access to an outside telephone line, power, and any network connections required
- Allow Hewlett Packard Enterprise all necessary access to all locations and networks where the service is to be performed
- Review and approve assessment report(s)
- Supply a scanning platform that meets HPE requirements for the service
- Provide VPN access (including tokens, accounts, procedures, and so on) access to the internal scanning platform to conduct scanning and testing activities for internal network vulnerability scanning/penetration testing
- Ensure that all routes, protocols, and ports are open on switches, routers, and firewalls to allow the scanning platform to scan and test the desired endpoints for network vulnerability scanning/penetration testing
- Provide written permission for HPE to perform a vulnerability scan and penetration test of the customer network
- Monitor and notify HPE about any service degradation or disruption during the vulnerability scan/penetration testing
- Notify HPE ASA for security expert advisory session topics (at least two weeks in advance)

SERVICE LIMITATIONS

- Limitation of each service feature is outlined in the Service features table; additional charges will incur for any additional service required.
- This service cannot be used as a formal external audit (attestation) or certification qualification purpose.
- Assessment findings depend on the quality of the information available at the time the assessment is conducted. Hewlett Packard Enterprise does not warrant that all security gaps within the environment will be discovered.
- Vulnerability/penetration test findings depend on the information/access available at the time the test is conducted. HPE does not warrant that all vulnerabilities within the customer environment will be discovered at the time the scan occurs.
- HPE will not be liable for any loss or damage resulting from the vulnerability scan/penetration testing.
- Monthly 2-hour session/communication with ASA will expire at the last business day of each month and cannot be carried over or “banked.”
- All available security expert advisory session hours will expire at the end of each subscription term and cannot be carried over or “banked.”
- The engagement is delivered under the legal responsibility of the customer.
- The on-site/off-site schedule of the HPE team will be mutually agreed prior to the commencement of services. HPE and customer will plan a schedule that leverages remote work when possible.
- All deliverable documentation created for this engagement will be available in electronic format.
- Services are deemed accepted upon performance.
- HPE respects customer confidentiality and will make every effort to avoid contact with customer data. Any contact or access to customer data will be coincidental in nature and immediately reported to the customer point of contact.

GENERAL PROVISIONS AND OTHER EXCLUSIONS

Our ability to deliver this service is dependent upon the customer's full and timely cooperation with Hewlett Packard Enterprise, as well as the accuracy and completeness of any information, data, and access the customer provides to HPE.

To the extent HPE process personal data on the customer's behalf in the course of providing services, the HPE Data Privacy and Security Agreement Schedule—HPE Support and Professional Services found at hpe.com/info/customer-privacy.html shall apply.

SUPPLEMENTAL TERMS

The following supplemental terms apply to these services and take precedence in the event of any conflict:

- Upon receipt of an acceptable order, HPE will contact the Customer within seven (7) business days to organize a service delivery date. Service delivery dates are subject to resource availability and may be scheduled up to 30 days from the order acceptance date.
- The Customer must schedule and receive delivery of these services within 180 days from order acceptance. HPE reserves the right to reprice for services not scheduled and delivered within 180 days. Backorders or shipment delays may affect the delivery timeline. Orders for services will expire after 365 days (one year) from the order acceptance date for services not scheduled and delivered, and the Customer will not be entitled to a refund for the unused services.

ORDERING INFORMATION

Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations. To obtain further information or to order HPE Continuous Security Improvement Service, contact a local HPE sales representative and reference the following product numbers:

- HT6X8A1 and HT6X5A1 for HPE Continuous Security Improvement Service Essential
- HT6X9A1 and HT6X6A1 for HPE Continuous Security Improvement Service Advanced
- HT6Y0A1 and HT6X7A1 for HPE Continuous Security Improvement Service Premium

LEARN MORE AT

hpe.com/us/en/services/consulting

Hewlett Packard Enterprise

a00025579ENW, October 2019, Rev. 2