



# **HPE Security Assessment Services**

## **HPE Lifecycle Event Services**

Your corporate information and intellectual property are important assets that you want to protect from unauthorized users. Developing and maintaining a sound security strategy may help you to manage your company's risks associated with network intrusion, data theft, system misuses, privilege abuse, tampering, fraud, or service interruption.

HPE Security Assessment Services will assist you in identifying the combination of technical, resource, and process controls that your company can use to manage security risks. Conducted by a Hewlett Packard Enterprise security consultant, these in-depth assessments identify the strengths and weaknesses of your current security posture as well as vulnerabilities to security threats.

Our security consultant works with you to determine the appropriate mix of security assessments to address your business needs. Because security threats and mitigation technologies change continually, HPE recommends performing these services annually, and even more frequently for systems that are connected to the Internet. Regular security assessments will help you to become more aware of your potential security vulnerabilities, enabling you to address security risks proactively.

### **Service benefits**

- Assists you in identifying your company's exposure to security threats
- Identifies sound security policies and practices
- Provides an in-depth analysis of your current security posture
- Helps you to understand how your security measures compare to industry standards
- Enables more informed decisions, allowing you to better manage your company's exposure to threats associated with doing business over the Internet
- Provides recommendations for reducing exposure to currently identified security risks

### **Service feature highlights**

HPE Security Assessment Services encompass the following offerings:

- The HPE Security Quick Assessment Service provides an HPE-facilitated self assessment of your security posture against industry best practices. Hewlett Packard Enterprise security consultants will direct you through a criteria-based assessment and analyze your responses, identifying potential weaknesses in your information security management system. This service is intended to provide you with an awareness of potential vulnerabilities and to suggest priorities for service improvement.
- The HPE Intranet Security Healthcheck Service provides a network-based vulnerability assessment for business-critical systems connected to your company's network. Network scanning targets devices connected to the network to identify security weaknesses through comprehensive, automated network security vulnerability detection and analysis. The service helps you understand the risks within the technology supporting your business-critical services and identifies the steps required to improve your security infrastructure.
- The HPE System Security Healthcheck Service focuses on the operating-system level of your critical servers, using a host-based approach to detect platform security weaknesses that are not visible to network scanning. Your system-specific security risks are identified, analyzed, and prioritized. You receive recommendations for implementing the appropriate corrective actions.

- The HPE Custom Security Assessment Service provides a comprehensive review of security risks within your IT environment. The assessment takes a holistic approach to information security management across multiple IT components, including the status of your policy and procedures for information security management according to the BS7799 (ISO 17799) standard; the security posture of servers, storage, operating systems, applications, and databases; and the configuration and management of the physical environment. Fully customizable and defined in a Statement of Work, the service identifies key areas of risk and proposes practical and effective responses to those vulnerabilities.

**Table 1. Service features**

Feature	Delivery specifications
<b>HPE Security Quick Assessment Service - HB069AE or HB069A1</b>	<p>The Security Quick Assessment Service is an HPE-facilitated one-day workshop that allows Customers to compare their security practices, policies, processes, and IT infrastructure with industry best practices for information security management. It provides:</p> <ul style="list-style-type: none"> <li>• A criteria-based questionnaire developed on the basis of industry standards and Hewlett Packard Enterprise experience</li> <li>• Awareness of security concepts and information security management best practices, identifying security strengths and potential weaknesses in the delivery of reliable IT services</li> <li>• Analysis and presentation of workshop findings with best practice recommendations</li> </ul> <p>This service is recommended for Customers who are seeking awareness of potential security vulnerabilities in the people, processes, and technologies supporting their business.</p>
<b>HPE Intranet Security Healthcheck Service - HA190AE or HA190A1</b>	<p>This service covers a selected set of IP addresses and provides:</p> <ul style="list-style-type: none"> <li>• Scan of the identified devices attached to a network, including key servers, network switches, and routers, to identify security weaknesses</li> <li>• Analysis of the results of the scan</li> <li>• Presentation of a written report that details key findings and proposes a follow-up action plan</li> </ul>
<b>HPE System Security Healthcheck Service - HA185AE or HA185A1</b>	<p>This service covers a selected server and includes:</p> <ul style="list-style-type: none"> <li>• Server-based security scan of the identified system(s), analyzing security weaknesses that are not visible to network scanning</li> <li>• Analysis of the results of the scan</li> <li>• Presentation of a written report that details key findings and offers specific recommendations for improvements</li> </ul>
<b>HPE Custom Security Assessment Service - HA330AE or HA330A1</b>	<p>This service may be customized to the Customer's desired level of assessment for security risks. It provides assessment of the security risks associated with the Customer's IT infrastructure and business information environment, plus a structured Statement of Work process to identify key areas to be assessed. As specified in the Statement of Work, this service can encompass the examination of multiple security domains, such as security management, infrastructure, IT service management, user management, and system and service development. Typical service activities may include:</p> <ul style="list-style-type: none"> <li>• Analysis of overall security posture and procedures, including policy (BS7799) analysis, process and procedure review, and staff training and awareness</li> <li>• Review of physical security controls, including access controls, system location, security monitoring, and site security and layout</li> <li>• Review of system-level security strengths and weaknesses, including physical console access, password management, existence of known system vulnerabilities, configuration issues, and redundant (unnecessary) Windows® services system-level processes or daemons</li> <li>• Review of internal and network boundary security, including dial-up access control, intrusion detection, existence of known vulnerabilities, network configuration issues, and traffic-related issues</li> <li>• Review of firewall and defenses, including rule configuration, monitoring for alarms, virus protection, and real-time intrusion detection</li> <li>• Review of application and database security, including hardening, password and user authentication, data integrity, backup procedures, and software development</li> <li>• Review of client security, including desktop security, PDA and mobile management, access to the Internet, remote working practices, permissions, and virus protection</li> <li>• Identification of security deficiencies based on a combination of interviews with key IT and security staff and audits, which may include assessment of compliance with the organization's security policies and procedures, configuration audit, and onsite review of physical security. Automated tools may be used to assess network, system, and database vulnerabilities and to assess online security and policy compliance.</li> <li>• A written report that details the results of the security risk assessment, with recommendations for improvement</li> </ul>

## Service limitations

For all HPE Security Assessment Services:

- The engagement is limited to identification of security issues. Hewlett Packard Enterprise will not make changes to the Customer's configurations, hardware, or applications as a result of this review. Any corrective measures to mitigate the risks identified by this service are the responsibility of the Customer.
- The assessment is valid only for the time period in which it is performed. Because security threats and countermeasures are constantly changing, continued security vigilance is the responsibility of the Customer.
- The assessment will only address the Customer's applications, networks, and systems specifically designated for the service. These will be agreed upon between the Customer and Hewlett Packard Enterprise.
- Hewlett Packard Enterprise does not guarantee that services will identify all security vulnerabilities. HPE shall not be liable for any security breaches or for the security performance of the Customer's applications, networks, or systems.

For the HPE Intranet Security Healthcheck Service:

- This service provides an analysis of up to 30 nodes.

For the HPE System Security Healthcheck:

- This service is delivered on a per-system basis; one system consists of a single server configuration. The following operating systems are supported:
  - HP-UX
  - All versions of Windows
  - Red Hat Linux®
  - SUSE Linux®

## Customer responsibilities

The Customer must assume the following responsibilities in order for Hewlett Packard Enterprise to deliver any of the onsite HPE Security Assessment Services:

- Ensure that appropriate IT staff members participate in meetings and interviews
- Assist in gathering the information required for the security analysis
- Provide appropriate access to the designated systems for the appropriate data collection, scanning, and analysis tasks
- Allow removal from the company premises of all collected system data and associated media for review by Hewlett Packard Enterprise security consultants at Hewlett Packard Enterprise facilities
- Assign a project manager at each reviewed site who has responsibility for coordinating all aspects of this engagement

## For more information

For more information on Hewlett Packard Enterprise support services, contact any of our worldwide sales offices or visit the following website:

[www.hpe.com/services/support](http://www.hpe.com/services/support)

[www.hpe.com/services/lifecycleevent](http://www.hpe.com/services/lifecycleevent)

