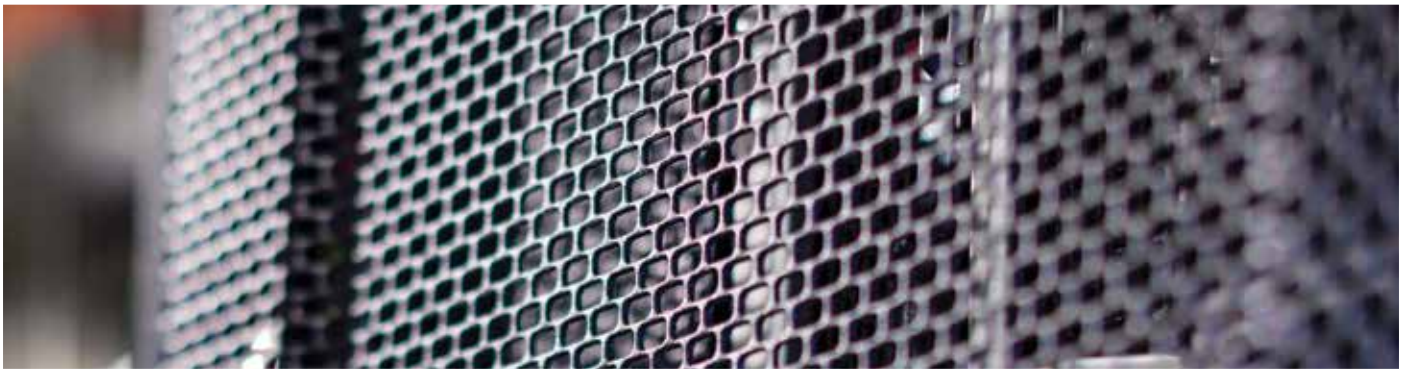
HPE
POINTNEXT

Brochure

Build secure and compliant enterprise in Hybrid IT

HPE Cloud Protection Services and Solution



Security for the digital IT era should be information centric, built in, adaptive, and proactive. HPE Pointnext, services experts of Hewlett Packard Enterprise and services experts from HPE Pointnext can help you proactively deal with the new security dynamics and compliance requirements to protect both your physical and virtual assets, as well as data in the cloud addressing your Hybrid IT needs.

Top threats to cloud computing
Hewlett Packard Enterprise contributes and aligns to the "Top threats to cloud computing" produced by the CSA Cloud Threat Initiative. The document is updated regularly and reflects expert consensus on the probable threats which organizations should be concerned about. CSA identifies the following seven key threats:

- Abuse and nefarious use of cloud computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities
- Data loss and leakage
- Account, service, and traffic hijacking
- Unknown risk profile

HPE Cloud Protection Services

A holistic approach to hybrid cloud security

For most IT executives considering or moving into the cloud, security and compliancy are the two biggest stumbling blocks. Many of these threats are also present in the traditional data center environment—threats like data breaches, system vulnerabilities, or malicious insiders will continue to exist regardless of where the data is stored and processed.

Supporting the HPE cloud architecture that is open, heterogeneous, and extensible as well as complementing the HPE Cloud Solutions, the HPE Cloud Protection Services can help organizations mitigate common threats. These threats have been defined by the Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA).

The Cloud Protection Services cover the people, product, process, procedure, and policy aspects of hybrid cloud security from business, functional, technical, and implementation levels guided by the HPE Cloud Protection reference architecture.

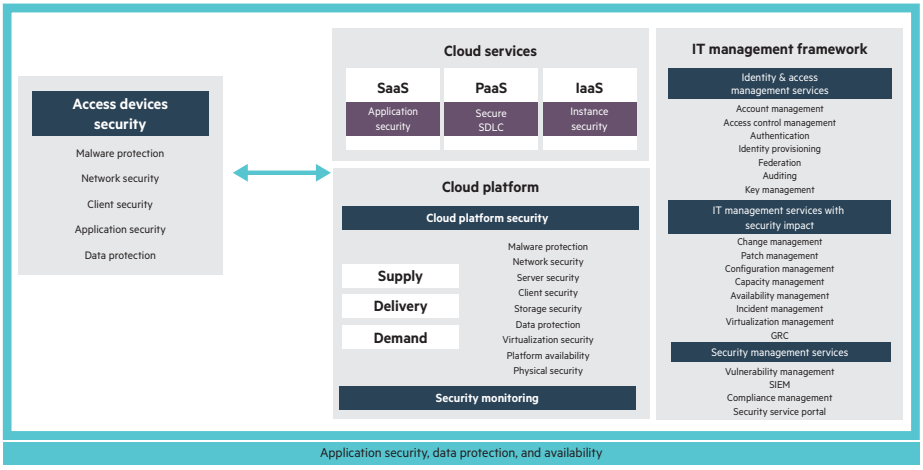


Figure 1. HPE Cloud Protection reference architecture—functional framework

An important building block of the HPE Cloud Protection reference architecture is the P5 security controls model, which is part of the HPE Information Security Service Management (ISSM) methodology used to define complete security programs for customers. The P5 model highlights that building a secure hybrid cloud, requires more than just technology and products. If you want to have a complete, end-to-end secure hybrid cloud solution, you also must take into account people, policy and procedures, processes, products, and the proof

P1: People

- Determines if the right staff is performing the correct roles to oversee hybrid cloud security.

P2: Policy and procedures

- Determines if the right set of policies and procedures are in place to govern the security and continuity of a hybrid cloud.

P3: Processes

- Determines if the proper security and continuity process models are in place to safeguard the transference of data in a hybrid cloud.

P4: Products

- Determines if the appropriate defense in-depth technologies and solutions are in place to manage and mitigate risk in a hybrid cloud.

P5: Proof

- Determines if the correct validation methods, metrics, and key performance indicators (KPIs) are used to track security control effectiveness in a hybrid cloud.

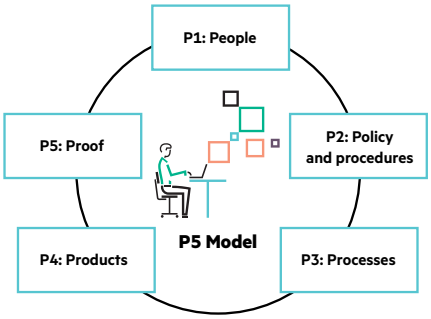


Figure 2. HPE P5 model for cloud security

Service framework

Securing the hybrid cloud requires a proven solution architecture methodology
The HPE Cloud Protection Services utilize the HPE IT strategy and architecture (ITSA) methodology. It also uses the HPE Cloud Protection reference architecture as the building blocks to create a comprehensive cloud security design that is customized to your organization's hybrid cloud maturity, business objectives, and requirements.

HPE ITSA provides an architectural methodology for defining and describing complex IT solution architectures that align top down from an organization's risks, goals, and business requirements so that final implementation is a success. The result is a holistic and unified hybrid cloud solution architecture, which incorporates the viewpoints and interests of all stakeholders involved. The HPE ITSA approaches solution architecture using four viewpoints:

- The business view answers the question, "why are we building a hybrid cloud and why do we want to secure it?"
- The functional view answers the question, "what should the hybrid cloud solution do and what security functions do we need?"
- The technical view answers the question, "how should the hybrid cloud solution and its underlying security controls work?"
- The implementation view answers the question, "with what will the hybrid cloud solution and its security controls be built?"

A structured service approach

Hewlett Packard Enterprise can provide the following cloud protection services to help you build well-protected and compliant hybrid clouds:

HPE Hybrid Cloud Protection Transformation Workshop helps with in-depth discussion, consensus building, and high-level recommendations for your cloud security strategy. The workshop provides an opportunity to:

- Share cloud security best practices and understand the cloud security threat landscape
- Gain organizational stakeholder alignment and confidence for implementing cloud security
- Identify and prioritize strategic initiatives related to cloud security

HPE Cloud Protection and Compliance Analysis Service defines cloud security control recommendations for a new or existing cloud environment as well as related recommendations for your overall information security program to mitigate risks and meet compliance requirements for a hybrid cloud environment.

The service allows organizations to:

- Evaluate changes needed with existing security policies, procedures, and products
- Define business and functional requirements that can drive future cloud adoption
- Guide your private and hybrid cloud design activities in the future

Key questions
The Cloud Protection services help organizations answer the following key questions:

- Do you understand your cloud security and compliance needs and gaps?
- Do you know what security products and technologies can best secure the cloud services you consume and deliver?
- Is your cloud infrastructure properly hardened and secured?
- Do you know how to provide enterprise level security and hardening for your cloud environment?
- Do you have a unified security delivery and services across cloud and traditional IT environments?
- Have you identified roles, responsibilities, policies, and procedures for cloud security?
- Do you want an adaptive cloud security strategy that addresses the security concerns and requirements of your business stakeholders?
- Do you want to make sure that your hybrid cloud computing environment is compliant with regulatory requirements?

HPE Cloud Protection Architecture and Design Service defines a highly secure, high-level, and detailed design that is tailored to the organization's hybrid cloud platform. The service builds on the HPE Cloud Protection reference architecture and HPE ITSA solution architecture methodology. The service leverages the outcomes of the HPE Cloud Protection Workshop and the HPE Cloud Protection and Compliance Analysis Service, and helps you architect the building blocks of your organization's hybrid cloud.

HPE Platform Protection and Compliance Service helps with locking down operating system and application platforms. It also performs assessments and remediation of the security posture of cloud platforms. The service provides security lock down for operating system and application platforms based on your organization's specific policies and compliance requirements.

HPE Pointnext advantage
To cope with the security challenges in Hybrid IT, you must have a clear understanding and alignment to your business and IT risks and goals, as well as an aligned governance, risk, and compliance program that is tailored to the cloud. You must then lay out an adaptive security architecture for your current and future cloud-based services.

Services from HPE Pointnext are designed to accelerate your secure digital transformation, building upon our heritage and strengths in security, continuity, infrastructure, our OpenStack® experience, and our capability to deliver an outstanding customer experience.

Learn more at
HPE Pointnext
hpe.com/services/securityconsulting

Hewlett Packard Enterprise

4AA6-3098ENN, July 2017, Rev. 1