



HPE Private Cloud Enterprise air-gapped

Security brief

Deploy your most sensitive workloads in a fully disconnected on-prem private cloud leveraging the best of HPE security controls

HPE Private Cloud Enterprise air-gapped security framework

Security is integrated into every layer of the HPE Private Cloud Enterprise air-gapped architecture, beginning in the integrated platform control plane through the service stacks from bare metal as a service (BMaaS) to virtual machines as a service (VMaaS) and containers as a service (CaaS). Every layer is secured with strong authentication and authorization, protection of data at rest, confidentiality, and integrity of data in transit using the latest cipher suites and algorithms, mature key management practices, and a secure CI/CD pipeline.

Encryption: HPE Private Cloud Enterprise air-gapped has implemented Federal Information Processing Standards (FIPS) standards as the baseline for encryption.

All data is encrypted as rest.

Communication between services in HPE Private Cloud Enterprise air-gapped uses Transport Layer Security (TLS) 1.2 by default.

HPE Private Cloud Enterprise air-gapped manages keys for storage encryption through an internal Key Management Service (KMS). Integration with a customer KMS is supported to give customers greater control of the encryption keys in use.

Certificates are issued by a known certificate authority that supports certificate revocation list (CRL).

Identity and access: HPE Private Cloud Enterprise air-gapped can integrate with any customer-provided Security Assertion Markup Language (SAML) compliant identity provider.

Administrative tools allow customer management of user identities, access privileges, and definition of roles and policies. The granular privilege definition allows tight governance of which users or groups of users can access specific resources and platform functions.

Access permissions are assigned based on job roles and responsibilities. Role-based access control ensures that users only have access to the resources necessary for their tasks.

It supports granular, administratively defined policies allowing governance over cloud or tenant admins and consumers' actions.

Vulnerability management: HPE Private Cloud Enterprise air-gapped hosts an onboard vulnerability scanner that probes its internal components. Paired with secure development processes (detailed as follows), HPE monitors and updates HPE Private Cloud Enterprise air-gapped in accordance with policy guidance based on the severity of discovered/reported vulnerabilities. Details of these vulnerability scanning activities are available to the customer.

Continuous improvement and innovation

HPE maintains a dynamic security road map for HPE Private Cloud Enterprise air-gapped incorporating protection from emerging threats, evolving technology, and customer feedback. Security measures are continually improved to stay ahead of emerging risks.

Innovative technologies such as AIOps from OpsRamp, a Hewlett Packard Enterprise company are delivered with HPE Private Cloud Enterprise air-gapped. Other emerging capabilities in artificial intelligence (AI) and machine learning (ML) will be researched and integrated, as appropriate, into the security framework to enhance threat detection, automate responses, and improve overall security posture.

HPE Private Cloud Enterprise air-gapped security design and development

The development of HPE Private Cloud Enterprise air-gapped follows the secure development lifecycle with the insertion of security spanning design through operations. HPE Private Cloud Enterprise air-gapped developers adhere to a mature set of security processes to help ensure the design, code, and development environment are secure. These enhanced security processes include:

Secure DevOps: All development activities in PCE are required to go through numerous automated security checks, including static code analysis, secrets scanning, malware scanning, container security scanning, dependency vulnerability scanning, and cloud security posture management scanning.

Architectural threat analysis: All new and updated service architectures are required to undergo rigorous security architecture reviews that verify the implementation of security best practices and policy compliance and identify potential security defects.

Security code review: All new and updated services are required to undergo a detailed manual security analysis of developer code for misconfigurations and poor security implementations.

Penetration testing: A team of dedicated security experts continuously performs penetration testing (pen tests) for all HPE Private Cloud Enterprise air-gapped services.

Security hardening: HPE Private Cloud Enterprise air-gapped components are hardened to STIG and CIS benchmark standards, through a defined process. Hardening details are available on request.

Security training: HPE mandates that developers receive security training to keep knowledge of secure coding current.

Customer security to support HPE Private Cloud Enterprise air-gapped

The security of HPE Private Cloud Enterprise air-gapped on a customer premise is ultimately a shared responsibility. HPE is responsible for the security of the cloud, the HPE Private Cloud Enterprise air-gapped internal platform and control plane. The customer is responsible for security in the cloud, securing the data and workloads that run on HPE Private Cloud Enterprise air-gapped.

HPE Private Cloud Enterprise air-gapped relies on the infrastructure security of the customer that surrounds it on the customer presence. The customer decides what if any external network connectivity is needed for their workloads. HPE Private Cloud Enterprise air-gapped has no requirement for internet connectivity (secure patching processes will be defined with the customer).

To provide the customer visibility into HPE Private Cloud Enterprise air-gapped, integration with a customer SIEM such as Splunk, for logging and monitoring is available.

To provide customer control of encryption keys, integration with customer Key Management Service is available for storage encryption.

Visit [HPE.com](https://www.hpe.com)

Learn more at

[HPE Private Cloud Enterprise](#)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00144829ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

