HPE GreenLake

Technical Documentation
CONFIDENTIAL | AUTHORIZED HPE PARTNER USE ONLY

WHITE PAPER: SECURITY IN HPE GREENLAKE PRIVATE CLOUD

Version 1.0

Contents

Document Revision History

Change request# (Optional)	Document version	Date	Prepared / Modified by	Section and text revised
	1.0	17-April-2024		Initial Release

Executive Summary

The advent of cloud computing and aaS (as a Service) offerings has freed businesses from purchasing and maintaining Infrastructure and allowed focus to be placed on business applications. This approach shifts the costs from Capital Expense (Capex) to an Operating Expense (OpEx), resulting in cost savings as the need for overprovisioning to handle short-term consumption spikes is eliminated and addressed by the elastic nature of the cloud computing model.

While the public cloud provides the advantages of cloud and aaS, it also introduces new risk concerns for the business. Confidential and customer data stored safely in the confines of the corporate Intranet are now traversing the Internet, and the data at rest is stored outside of the physical confines of the business by a third party. These and other factors such as data gravity, performance, and latency have resulted in the formation of a Private Cloud Computing model. The Private Cloud provides the elasticity of the cloud and allows the customer to retain data on their physical premise and ensure data sovereignty while also providing performance advantages from minimized network latency.

Public or Private Clouds alone cannot meet a customer's varying needs. HPE recognizes that a Hybrid Cloud approach is needed, using the best solution to address specific business needs and providing interoperability between Clouds and service offerings as needed. Cloud solutions are often comprised of best-of-breed components to create a seamless experience. HPE Private Cloud is designed with this model in mind, providing transparent integration into the customer environment and delivering a secure environment with on-premise data protection.

Effective and efficient security requires that security be one of the fundamental design principles built into the architectural foundation. This paper describes the Private Cloud Enterprise (PCE) security methodology, processes, and functionality.

Security in a PCE deployment is jointly owned between HPE and the customer. It is important that customers clearly understand the shared responsibility model, what security aspects they are responsible for, what security aspects HPE is responsible for (and how those are delivered), and what aspects require joint responsibility.

This white paper outlines the comprehensive security framework for HPE's Private Cloud Enterprise, which combines the robust HPE-provided Infrastructure with part of the management plane hosted on the public cloud. The architecture is designed to ensure the highest level of security for customer data and applications. The paper also delineates where the security responsibility is owned by HPE, is shared between HPE and the customer, or is customer-owned. (See Also PCE Shared Security Model)

1. Architecture Overview

HPE GreenLake Private Cloud Enterprise (PCE), offered by Hewlett Packard Enterprise, is a hybrid cloud platform and operating model rooted in Infrastructure as a Service (IaaS). A base PCE environment consists of racked equipment, built and delivered by HPE, with an enhanced set of services provided in the PCE Control Plane or bare metal, virtual machines, and containers. Each solution is standardized but configured to meet the customer's specifications and provides an experience similar to public cloud offerings but securely hosted in the customer environment.

1.1 Hybrid Cloud Components

The architecture consists of a management plane hosted on the public cloud, while the infrastructure is deployed in the customer's data center or colocation facility, utilizing HPE's standardized HPE GreenLake cloud modules. The HPE Control Plane is built onto the IaaS, providing essential services and integrating additional capabilities on bare metal.

1.2 Management and Control Plane Functionality

The Control Plane orchestrates and manages resources, ensuring seamless integration between the HPE cloud-hosted management plane and on-premises Infrastructure via secure communications.

The Management plane is hardened using public cloud foundational best practices, Cloud Security Posture Management (CSPM) toolsets and access is enforced via policies based on the principle of least privilege.

1.3 Integration of VMs and Containers

The private cloud platform offers virtual machine and container services, providing flexibility and scalability for diverse workloads.

Posture Management (CSPM) toolsets and access is enforced via policies based on the principle of least privilege.

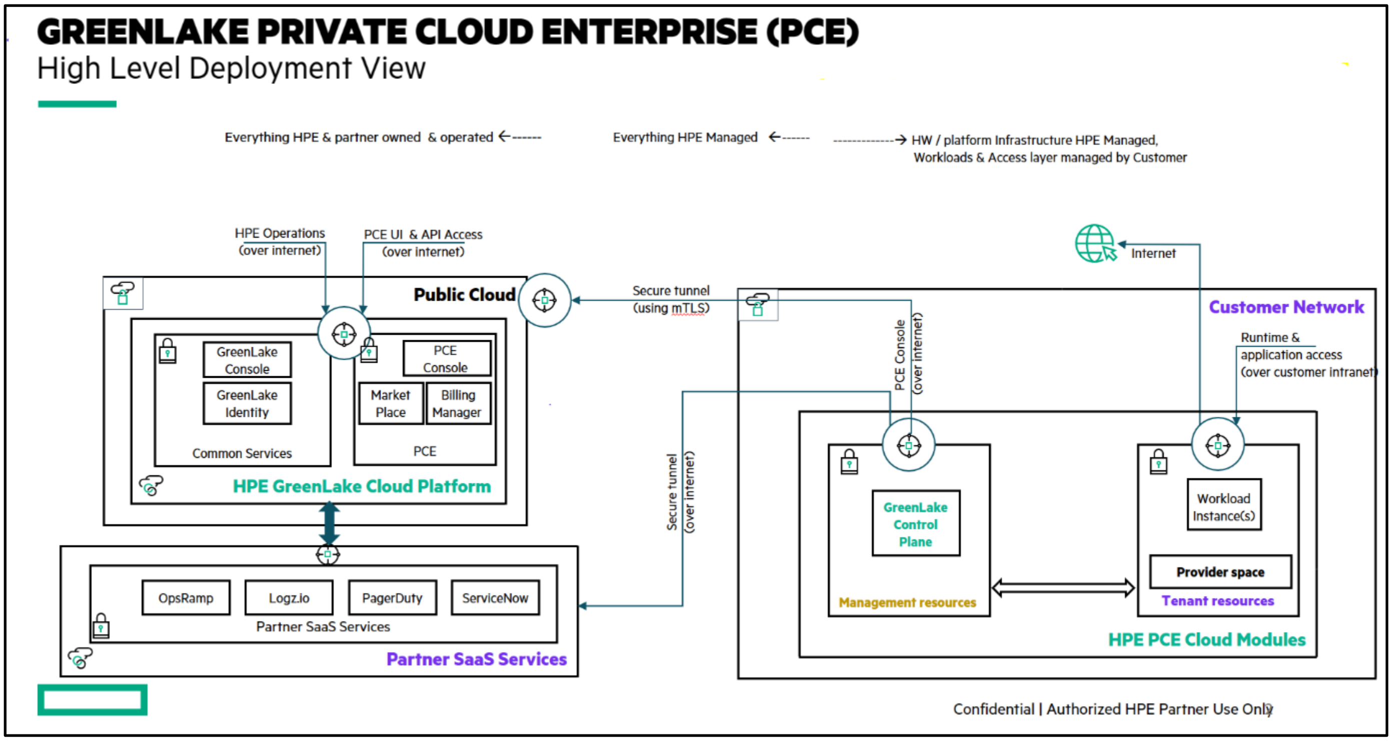
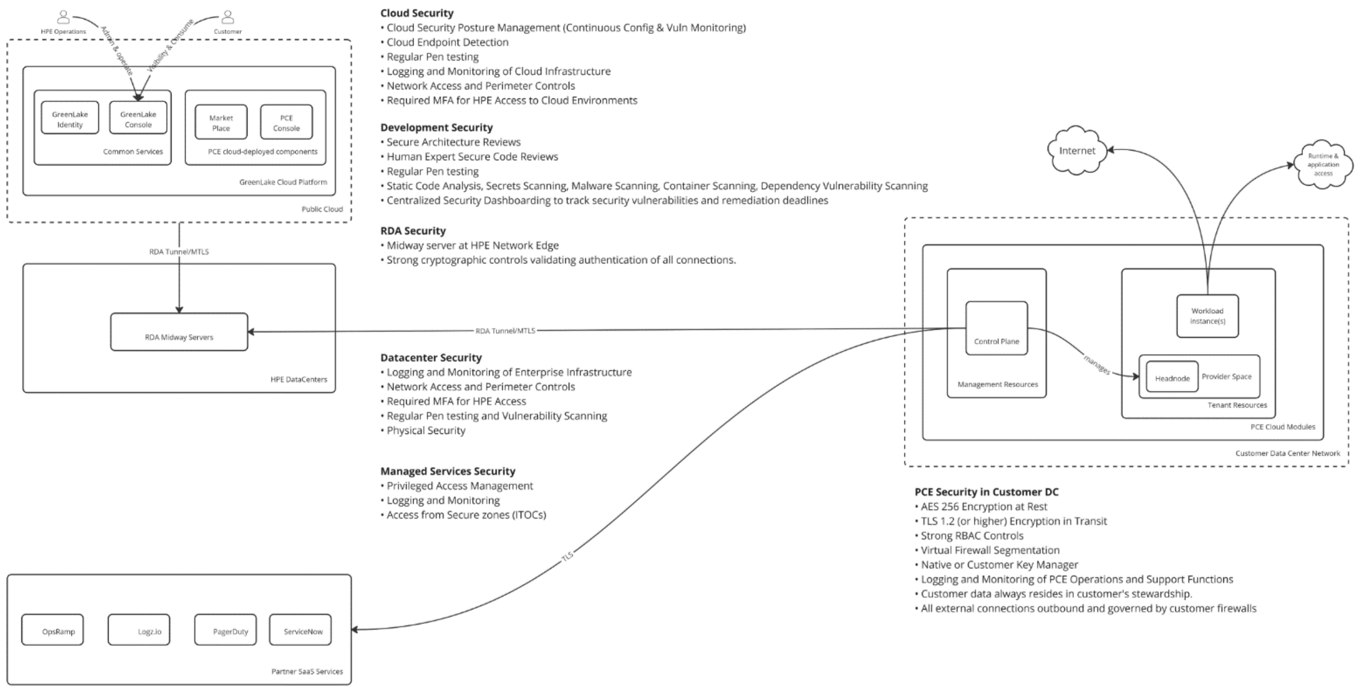

GREENLAKE PRIVATE CLOUD ENTERPRISE (PCE)
High Level Deployment View
Everything HPE & partner owned & operated ←------
Everything HPE Managed ←------
-------------→ HW / platform Infrastructure HPE Managed, Workloads & Access layer managed by Customer
HPE Operations (over internet)
PCE UI & API Access (over internet)
Internet
Public Cloud
Secure tunnel (using mTLS)
Customer Network
Runtime & application access (over customer intranet)
GreenLake Console
GreenLake Identity
Common Services
PCE Console
Market Place
Billing Manager
PCE
HPE GreenLake Cloud Platform
PCE Console (over internet)
Secure tunnel (over internet)
GreenLake Control Plane
Management resources
Workload Instance(s)
Provider space
Tenant resources
HPE PCE Cloud Modules
OpsRamp
Logz.io
PagerDuty
ServiceNow
Partner SaaS Services
Partner SaaS Services
Confidential | Authorized HPE Partner Use Only

Figure 1. PCE High-Level Deployment View

1.4 Data Flow

The following diagram depicts the primary data flow patterns in a PCE deployment and associated security. From the on-premise environment, any data used by HPE is transmitted in outbound only connections to HPE GreenLake Cloud Platform and partner SaaS (Software as a service) services.



Cloud Security
- Cloud Security Posture Management (Continuous Config & Vuln Monitoring)
- Cloud Endpoint Detection
- Regular Pen testing
- Logging and Monitoring of Cloud Infrastructure
- Network Access and Perimeter Controls
- Required MFA for HPE Access to Cloud Environments

Development Security
- Secure Architecture Reviews
- Human Expert Secure Code Reviews
- Regular Pen testing
- Static Code Analysis, Secrets Scanning, Malware Scanning, Container Scanning, Dependency Vulnerability Scanning
- Centralized Security Dashboarding to track security vulnerabilities and remediation deadlines

RDA Security
- Midway server at HPE Network Edge
- Strong cryptographic controls validating authentication of all connections.

Datacenter Security
- Logging and Monitoring of Enterprise Infrastructure
- Network Access and Perimeter Controls
- Required MFA for HPE Access
- Regular Pen testing and Vulnerability Scanning
- Physical Security

Managed Services Security
- Privileged Access Management
- Logging and Monitoring
- Access from Secure zones (ITOCs)

PCE Security in Customer DC
- AES 256 Encryption at Rest
- TLS 1.2 (or higher) Encryption in Transit
- Strong RBAC Controls
- Virtual Firewall Segmentation
- Native or Customer Key Manager
- Logging and Monitoring of PCE Operations and Support Functions
- Customer data always resides in customer's stewardship.
- All external connections outbound and governed by customer firewalls

1.5 High Availability Design

PCE is designed to deliver high availability within a data center or a colocation facility. The solution includes:

Network

- Redundant network modules
- A resilient control plane cluster
- Resilient storage modules with redundant controllers and advanced RAID technology
- Dual-homed, workload computer modules

Multisite high availability for virtual machines

- VMware vSphere replication-based approach for virtual machines
- vSphere Metro Storage Cluster (vMSC)

Synchronous Replication provides a zero-recovery point objective, ensuring no data loss in the event of an array or onsite failure or requirement for host reconfiguration

2. PCE Security Framework

Security is integrated into every layer of the PCE architecture, beginning in the Public Cloud management plane and the on-premises 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.

2.1 Secure Design and Development

Development of PCE follows the Secure Development Lifecycle with the insertion of security spanning design through operations.   PCE Developers adhere to a mature set of security processes to 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. Architectural Threat Analysis engagements are led by experienced security architects and seek to vet security end to end, including AuthN, AuthZ, data security, logging & monitoring, cryptography, session management & input validation, etc.
- 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. Human security experts conduct these reviews and are a complimentary function to automated static analysis processes, providing defense in depth, and addressing any potential gaps in automated tooling.
- Penetration Testing: A team of dedicated security experts continuously pen-tests all PCE services. Testing is mandated to occur at least quarterly and includes automated authenticated and unauthenticated scans and manual testing of APIs and other service interfaces and surrounding Infrastructure for security vulnerabilities.
- Security Training: PCE management mandates that developers receive security training to keep knowledge of secure coding current. Additionally, all HPE staff are trained in security practices, policies, and procedures based on the individual’s role and level.
- The development team’s conformance to security practices is periodically audited for each service.
- A security dashboard is used to track Security Key Risk Indicators (KRI), including security vulnerabilities and alerts and associated policy compliance information.

2.2 Secure Deployment and Installation

2.2.1 Secure CI/CD Pipeline

The CI/CD pipeline is an automated process through which developers build, submit for review, and release their code. This process includes automated security checks, including static code analysis, secrets scanning, malware scanning, container security scanning, dependency vulnerability scanning, and cloud security posture management scanning.

2.2.2 Day 0/Day 1 Build Security

In the installation and start-up phase, an HPE specialist coordinates the factory build process in accordance with defined customer requirements provided before the build. Any specific customer build configuration is provided to a Factory Engineer via the HPE Smart Customer Intent Document (SCID) system. Most of the customer-specific configuration details, including passwords, IP addresses, etc., are provided via SCID.

Once the racked and cabled equipment is available (still in the HPE factory) and ready for configuration, an HPE engineer logs into a PCE Provisioning system with their HPE credentials. The engineer downloads a Day 0 bundle from the JFrog Artifactory using their JFrog credentials. This Day 0 bundle contains all the information that drives the processes and automation to build the PCE hardware and software solution stacks in the HPE factory. The engineer executes scripts via the HPE GreenLake cloud module Orchestrator Toolkit (CMO) to build out the HPE GreenLake Control Plane and configure the HPE GreenLake cloud modules for use by the BMaaS, VMaaS and CaaS services. Once completed, the

PCE solution is shipped to the customer, where an onsite engineer executes the necessary steps to integrate the PCE system into the customer's network.

In the process of building the Control Plane, packages from following public-facing repositories must be downloaded to complete the HPE PCE solution. Downloads from these repositories are integrity checked against provided checksums or cryptographic hashes.

jfrog.io

docker.io

elastic.co

gcr.io

k8s.io

pkg.dev

quay.io

python.org

percona.com

pythonhosted.org

pypi.org

terraform.io

2.3 Secure Operations

2.3.1 General Operations Security

- PCE Cloud Production environments are continuously monitored by an industry-leading Cloud Security Posture Management (CSPM) tool that identifies and remediates risk by automating visibility, threat detection, and remediation workflows to search for misconfigurations in a cloud environment.
- Cloud-native security tools are leveraged to continually log and monitor cloud environments, providing dashboarding to security and engineering teams to identify and track vulnerabilities to remediation.
- Cloud production environments are penetration-tested through automated scans and manual testing on regular schedules.
- Under the Shared Responsibility Model, HPE is responsible for the hardware and software that runs HPE GreenLake services. This includes patching the infrastructure software and configuring infrastructure devices. HPE manages security patches, updates firmware, and maintains the PCE equipment. HPE also monitors the PCE environment's performance, health, and metrics and determines whether maintenance is required. All access to the control plane system is made through the operations console and is audited through a collection of console recordings and logs.

2.3.2 Security Auditing

The Public Cloud management components and the on-premise PCE components within the control plane (BMaaS, VMaaS, and CaaS) generate security-relevant logs and aggregate them to LogZ.io. HPE is developing a PCE Security Information and Event Management system (SIEM) integration to provide simplified, self-service process to send logs and monitoring data to a customer's logging and/or SIEM solution if the customer requirements dictate the need. HPE can provide raw/unprocessed logs at customer request until full SIEM integration is available.

- Logs are transmitted via encrypted communication
- Logs are collected, aggregated, and are immutable.
- Logs are reviewed regularly by HPE support personnel
- High-priority events trigger alerts to Pager Duty for immediate attention
- Logs are currently retained for 90 days.

Security Operations Center (SOC) ingest of PCE logs is being developed. This will offer the same monitoring capabilities that HPE uses internally and will be used to monitor the on-premise private cloud infrastructure components managed by HPE.

2.3.3 Security Monitoring

The security of HPE-managed environments in PCE, both on the public and private side, are actively monitored for security threats.

- CrowdStrike endpoint detection and response runtime protection is deployed on all HPE Public management plane endpoints.

2.3.4 Threat Detection and Response

A well-defined Incident Response Plan (IRP) outlines the steps to be taken in a security incident. The plan includes containment, eradication, recovery, and post-incident analysis procedures.

2.3.5 Regulatory Compliance

The platform adheres to industry-specific and regional regulatory requirements, such as GDPR and others, to ensure customer data is handled in accordance with legal standards.

Frequent security audits and penetration tests are conducted to evaluate the effectiveness of security controls. Vulnerabilities are identified and addressed promptly.

3. Public Cloud Security

3.1 Authentication and Authorization

Identity and Access Management (IAM) is an HPE service leveraging OKTA that helps administrators securely control access to HPE resources. IAM administrators from HPE control who can be authenticated (signed in) and authorized (have permissions) to use PCE resources. This enables customers to create users and groups under the customer GreenLake IAM (GL-IAM) account. Customers control the permissions that users must have to perform tasks using GLC resources.

Currently, user and access management tasks, including password management, are performed by HPE.

3.1.1 Multi-Factor Authentication (HPE Personnel)

HPE staff are required to enroll in and authenticate with a certificate-based multi-factor authentication token. On initial authentication to the HPE network and subsequent authentication to privileged resources, the user must present the certificate and an eight-digit PIN code to prove identity actively. These MFA checks are present in the flow of any access to PCE resources, either in the cloud or on customer premises.

All HPE personnel with roles in PCE management are authenticated using a standard Authentication framework and Multi-Factor Authentication (MFA)/SSO.

MFA is enforced for all HPE user accounts, requiring multiple forms of authentication for access. This adds an extra layer of security beyond traditional passwords.

3.1.2 Role-Based Access Control (RBAC)

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

3.1.3 Least Privilege Policies

Users are granted the least amount of access needed to perform their duties. Access levels are regularly reviewed and adjusted to reflect changing responsibilities.

The principles above are extended to customer accounts accessing their environment through the HPE GreenLake user interface.

3.1.4 HPE GreenLake Platform Identity

All HPE GreenLake Platform customers start with a user login ID that is local to their tenant. If requested by the customer, HPE can add more local users. Local authentication verifies the username and password of users within a local HPE GLC environment. To access resources and services in GLC, roles with the appropriate permissions must be assigned to the user group to which the user is a member or as an individual user.

OKTA-based OAuth2.0 compliant Access Tokens similarly verify all API service call authentications and authorizations.

3.2 Data Security – HPE Collected and Managed

HPE GreenLake PCE conforms to the HPE shared responsibility model, which includes regulations and guidelines for data protection. HPE is responsible for protecting the cloud infrastructure that runs all HPE services, and it maintains control over the data it collects and hosts on this Infrastructure, including the security configuration controls for handling customer content and personal data.

3.2.1 HPE Managed Data

Data required to be collected and stored for managing and maintaining PCE implementations is encrypted, regardless of where it is stored. Encryption is applied to data both in transit and at rest, ensuring that even if accessed, it remains unreadable without proper decryption keys.

Clear policies govern the retention and disposal of data stored by HPE processes and systems. Redundant or obsolete data is securely deleted to reduce the potential attack surface.

3.3 Transport Encryption

HPE encrypts all control traffic between the customer's PCE solution and HPE GLC in transit. Data hosted on the customer's PCE solution will not be transferred without an explicit request (or when included in the SOW (Statement of Work)).

Connections between GLC and the customer's PCE solution are implemented using secure communications via HPE Remote Device Access (RDA), establishing a tunnel between the customer's PCE solution and the HPE GLC management plane. The customer controls the configurations for access, and all connections are initiated on the customer side

- All communications between services in PCE and the on-premise and GLC management plane use Transport Layer Security (TLS) 1.2 by default, with some components supporting TLS 1.3.
- Certificates are issued by a known Certificate Authority that supports Certificate Revocation List (CRL)

3.4 Data at Rest Encryption

Data collected and stored by HPE in both GLC and in HPE-managed components of PCE, such as the control plane, are encrypted at rest.

3.5 Defense in Depth

The security architecture of the public cloud employs multiple layers of defense to protect against varying attack vectors. This includes physical security measures (implemented by the cloud provider in their facilities), network segmentation at multiple points in the public cloud platform, two-factor authentication, strong access controls at both the infrastructure and application levels, malware scanning in the CI/CD pipeline, encryption in transit, and data encryption at rest.

3.6 Zero Trust Architecture

All interactions, whether internal or external, are treated as untrusted. Access is granted based on strict authentication and authorization policies, regardless of the source or destination.

Users and systems are granted the minimum level of access required to perform their specific tasks, thus limiting potential damage in case of a compromise, and reducing the attack surface.

4. Security of Private Cloud

HPE encrypts all control traffic between the customer's PCE solution and HPE GLC in transit. Customer workload data on the PCE solution will not be transferred without an explicit request (or when included in the SOW (Statement of Work).

4.1 North South – Inbound/Outbound Connections

- The customer controls all inbound connections to PCE. Inbound connections are configured using HPE Remote Device Access (RDA) and initiated by the Client Access Server (CAS) client, whose configuration defines which endpoints HPE can connect to for troubleshooting or maintenance.
- Connectivity to GLC is enabled via the Control Plane using secure persistent connections over HPE RDA and restricted to defined IP ranges.
- All PCE outbound connections are limited to a predefined set of external sites and are proxied
- through a VPN established on the control plane.
- All transport is by default TLS 1.2 or higher, with no mechanism for down select.

4.2 East West – Internal Network Connections

- Network communications internal to PCE are segmented, with increasing isolation moving internally from the data center perimeter down to the smallest deployable computing unit, the pods. Segmentation is implemented via VLANs and ACLs (Access Control List) to isolate distinct parts of the infrastructure to prevent lateral movement in case of a breach.
- A separate Virtual Routing Framework (VRF) and VLAN isolation are used to integrate PCE with customer on-premises networks. This allows the customer to deploy their workloads onto PCE, and the customer controls East-West communications in those networks.

4.3 Network Segmentation Strategies

The PCE network is isolated via trust zones, implemented from the least trusted (publicly exposed APIs, if applicable) to the most trusted, moving inward from the external data center perimeter into the local area network, to the Kubernetes cluster, and to the pods.

- Routing for customer deployed VMaaS workloads and the associated customer networks they are attached to are defined in route tables provided through VMWare NSX Edge Gateways and NSX Edge Logical Routers.
  - Customers can specify IP addresses, internet gateways, local gateways, virtual private gateways, and peering connections as destinations.
  - Every VMaaS-based workload inherits the main route table from its NSX policy.
  - Custom routing tables and direct L2 connectivity to a customer network can be created and explicitly associated with a customer network.
- By default, customer deployed VMaaS workloads use the virtual networking feature of NSX for DNS (Domain Name System) resolution. If preferred, customers can use their DNS servers.
- Local gateways provide a local interconnect virtual router(s) that enable communication between the customer-deployed workloads and other customer resources.
- Kubernetes Isolation
  - Logical separation - unique workspace isolated from other workspaces
    - RBAC controls access to namespaces with defined roles and actions using role-binding
    - Quota limits are set for each namespace
  - Network Isolation – communications to and from applications controlled by network rules
  - Physical Isolation – applications are deployed onto dedicated nodes
  - Access to Kubernetes Nodes is limited via:
    - Controlling access to the Kubernetes API
    - Transport Layer Security
    - API Authentication and Authorization
    - Restricted access to etcd
- Security Groups
- HPE-managed networks and customer-deployed workloads/resources are separated via physical network infrastructure and separate Virtual Routing Frameworks (VRF). Further separation in those VRFs is provided by VLANs as well as ACLs and a virtual firewall for the HPE-managed networks and NSX and HPE Customer inter-network security policies for the customers' networks.

4.4 Other Network Access Controls

HPE Support Personnel are authenticated in the GLC, and identity is validated via certificate-based multi-factor authentication. Access for HPE Support Personnel is restricted in the control plane via ACL (Access Control List) and RBAC. A subset of support personnel will have access to the ESX level as a support necessity, but that access is restricted to a predefined resource pool. Any creation of VMs outside that resource pool would be considered anomalous and would be logged and alerted on. Logging and alerting are performed by Logz.io, managed by a separate group of administrators and permissions from the support team previously discussed.

4.5 Authentication and Authorization

Identity and Access Management is an HPE service leveraging OKTA that helps administrators securely control access to HPE resources. IAM administrators from HPE control who can be authenticated (signed in) and authorized (have permissions) to use PCE resources. This enables customers to create users and groups under the customer GLC account. Customers control the permissions that users must have to perform tasks using GLC resources.

Currently, user and access management tasks - including password management, are performed by HPE.

By default, IAM users do not have PCE resources and operations permissions. An IAM Role must be attached to IAM users or groups that explicitly grant the required permissions to allow IAM users to manage PCE resources.

4.5.1 HPE GreenLake Platform Identity

All HPE GreenLake Platform customers start with a user login ID that is local to their tenant. If requested by the customer, HPE can add more local users. Local authentication verifies the username and password of users within a local GLC environment. To access resources and services in GLC, roles with the appropriate permissions must be assigned to the user group to which the user is a member or to the user as an individual.

GLC’s identity for customer users is optimally provided by an industry-standard, secure, OKTA-based SAML federation. The federation of the customer's identity store to GLC is easily configured and will allow customer organizations to manage the onboarding and offboarding of their GL PCE users.

OKTA-based OAuth2.0 compliant Access Tokens similarly verify all API service call authentications and authorizations.

4.5.2 PCE Identity

By default, the customer’s HPE GreenLake Tenant for PCE is configured with two roles, “Private Cloud Tenant Owner” and “Private Cloud Tenant Contributor,” which appear in HPE GreenLake Platform. These roles can be attached to GLC users in the customer organization.

- Users with the “HPE - Private Cloud Tenant Owner” role can control policies, VM images, create PCE subnets, routers, infrastructure groups for resource isolation, etc. Also, they can create custom roles with custom permissions for resources within a HPE GreenLake Tenant.
- Users with the “HPE - Private Cloud Tenant Contributor” role can consume the cloud and perform operations like creating VMs, apps, blueprints, etc.
- Supports multi-factor authentication (MFA) to tightly control access to private cloud resources and services.

4.5.3 Role-Based Access Control (RBAC) and Least Privilege Policies

Administrative tools allow managing user identities, accessing privileges, and defining roles and policies.

- The granular privilege definition allows tight governance of which users or groups of users can access specific resources and platform functions.

  - Custom roles from predefined categories
- 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.
- Supports granular, administratively defined policies allowing governance over cloud or tenant admins and consumers' actions.
  - These are either enforced globally or via roles, groups, or clouds.

4.5.4 HPE Operational Support to Control Plane and PCE Services

HPE operational support personnel with responsibility for troubleshooting the Control Plane and PCE Services are granted access using credentials and privileges established during Day 0/Day 1 operations. As part of this build, an LDAP server is configured, and components that support LDAP are integrated. Role-Based Access Control is established for both LDAP and non-LDAP components during this build out.

On-going maintenance of access is managed by CSP (cloud service providers) Team Lead through periodic review and updates.

In this case, SUSE Linux Enterprise Server (SLES) OS, ArgoCD, and K3S are integrated with LDAP Servers, whereas HPE iLO, OneView, and Aruba Fabric Composer (AFC), are not.

The components which are not integrated with LDAP require local standard user account creation and management. These accounts are also established on the build out of services in Day 0/Day 1 operations. Passwords for these accounts are retrieved via HPE’s Control Plane vault (HashiCorp) as required.

The Control Plane vault is also integrated with LDAP and HPE personnel who are part of the CSP team for a given customer have access to the Control Plane vault to retrieve credentials for those components which do not have LDAP integration.

Troubleshooting and resolution of issues in Control Plane components is performed either directly via the OpsRamp console or the Troubleshooting VM (TSVM). For example, interfaces for which a web browser is required, cannot be accessed via the OpsRamp console, and require use of the TSVM. It should be noted, however, that the TSVM is only accessible via OpsRamp.

HPE personnel use HPE managed credentials with SSO to access the OpsRamp Console and from there they either perform troubleshooting via the console or they connect to the TSVM using a shared account, with credentials retrieved from the Control Plane vault. From the TSVM, access to the target system is performed via either LDAP or locally established credentials as outlined above

Administrative access to VCenter follows the same pattern whereby HPE personnel using HPE managed credentials with SSO to access the OpsRamp Console and from there they connect to the TSVM. Once connected to the TSVM there are two ways to access VCenter:

- HPE personnel authorized to retrieve admin/root credentials for the target VCenter can connect directly over SSH (Secure Shell) and log in with credentials retrieved from the Control Plane vault. Access to VCenter via this method is used only in urgent situations.
- HPE personnel open a browser on the TSVM and enter the URL for the VCenter Console they need to access and via LDAP elevation of privilege, log in to the VCenter Console

Troubleshooting and resolution of issues in Bare Metal, VMaaS, and CaaS, is performed following the same general pattern as management of the components control plane. Access is provided via OpsRamp and troubleshooting takes place therein, or via TSVM based on the following patterns:

If the target component does not provide access via graphical user interface (GUI) all management is through the OpsRamp Console.

- HPE Personnel connect to the OpsRamp console via HPE GreenLake Central using HPE credentials with SSO
- Connect to target system using supported protocols such as SSH
- Login using LDAP credentials with privilege defined by group membership
- In the event a system is not integrated with LDAP, login with root after extracting target system credentials from the Control Plane vault.

If the target component provides access via GUI, management is via the Troubleshooting Virtual Machine (TSVM)

- HPE Personnel connect to the OpsRamp console via HPE GreenLake Central using HPE credentials with SSO
- From OpsRamp Console, connect to the TSVM using LDAP credentials.
- From a browser on the TSVM, connect to the target URL (e.g., ArgoCD, Pulp, Harbor, etc.) using LDAP credentials
- In the event a target system is not integrated with LDAP, login with root/admin after extracting target system credentials from the Control Plane vault.

Additional controls for TSVM connectivity to target systems are implemented using access control lists configured at the network layer. In standard PCE implementations this is configured in the Aruba switches. Customer specific implementations may vary, and, in some cases, these ACLs may be configured in the pfSense.

For LDAP integrated components, end to end troubleshooting process security auditing is performed through logging on those components. Auditing gaps may exist for components not integrated with LDAP, especially where access is gained through shared admin credentials from the Control Plane vault. Work is ongoing to integrate all components in the control plane with LDAP. HPE investigating methods for implementing MFA throughout the control plane.

HPE has a defined password policy which is followed during the build, deployment, and maintenance of PCE. The policy followed includes:

- Password complexity incorporating upper- and lower-case letters, numbers, and special characters.
- Minimum length of seventeen (17) characters
- 90-day rotation
- Lockout after X attempts

Deviations from policy may be required for devices which do not support complexity and length requirements.

4.6 Encryption in Transit

Connections between GLC and the customer's PCE solution are implemented using secure communications via HPE RDA, which establishes a tunnel between the customer’s PCE solution and the GLC management plane. The customer controls the configurations for access, and all connections are initiated on the customer side.

All internal communications in PCE are minimally implemented with Transport Layer Security (TLS) 1.2 by default, while most support TLS 1.3. In certain configurations, mTLS governs communications between the microservices in any given layer of the stack.

4.7 Data Security

HPE customers are responsible for any company-owned or personal data they put in the workload they deploy on PCE.

4.7.1 HPE Customer Hosted Data

The block storage arrays used in PCE comply with the standards set forth by the National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) 140-2 and use data-at-rest encryption (DARE) using self-encrypting drives (SED). The full-disk encryption (FDE) based on AES-256 is handled at the drive level. Authentication keys are set by HPE and can be changed by the customer at their request by accessing the local key manager (LKM) using a simple management interface. This key is required to unlock the drive when power is restored.

- In addition, if the customer has an enterprise secure key manager (ESKM), it can be used instead of the local key manager (LKM). Customers can choose to encrypt all PCE data on the HPE storage array, leveraging their own encryption keys and key management system, thereby making HPE access to data cryptographically impossible without key access.
- Customers can also choose to leverage their keys and key management to encrypt at the VM level. However, that does impact certain compression and deduplication advantages in PCE VMs.

When a VM instance is stopped and deleted, the memory allocated to it is scrubbed (set to zero) by the hypervisor before it is allocated to a new instance, and every storage block is reset.

4.7.2 Control Plane Vault

The Control Plane provides a Vault (Hashicorp) for storing and managing secrets used on systems in the control plane and the as a Service (aaS) offerings deployed as part of PCE.

- Passwords are generated and stored in the Control Plane vault.
- 90-day rotation minimum (Customer can specify shorter rotation periods)
- Upon updating a credential, there is automated detection of an update to impacted systems.

4.8 Security Auditing

HPE-managed on-premise PCE components within the control plane, BMaaS, VMaaS, and CaaS, generate security-relevant logs that are aggregated to LogZ.io. These logs can be provided to the customer upon request. HPE is developing a means to provide the logs continuously to customers who want to integrate them into a logging and monitoring SIEM-based solution. HPE can also provide raw/unprocessed logs at customer request until full SIEM integration is available.

- Logs are collected, aggregated, and are immutable.
- Logs are regularly reviewed by HPE support personnel
- High-priority events trigger alerts to Pager Duty for immediate attention
- Logs are currently retained for 90 days.

Work is underway to stream and ingest PCE logs into the HPE SOC. This will offer the same monitoring capabilities that HPE uses internally and be used to monitor the PCE components.

5. Incident Response and Disaster Recovery

5.1 Incident Identification and Reporting

Clear procedures are in place for customers to report any suspicious activity or security incidents. Immediate action is taken to investigate and address reported incidents.

5.2 Remediation and Recovery

In the event of a security incident, a coordinated response is executed to contain the breach, eradicate the threat, and restore affected systems to a known good state. Customers are provided with guidance and support throughout the remediation process.

5.3 Business Continuity and Disaster Recovery (BCDR)

Comprehensive Business Continuity and Disaster Recovery plans are in place to ensure minimal downtime and data loss in case of catastrophic events. These plans are regularly tested and updated to meet evolving needs.

6. Continuous Improvement and Innovation

6.1 Security Roadmap

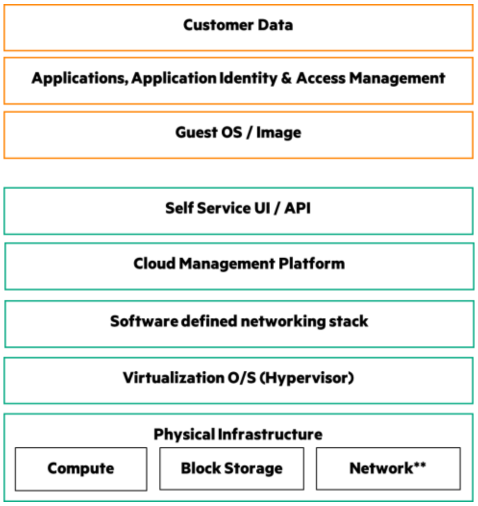
The cloud provider maintains a dynamic security roadmap incorporating emerging threats, evolving technology, and customer feedback. Security measures are continually improved to stay ahead of emerging risks.

6.2 Integration of Emerging Technologies

Cutting-edge technologies such as 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.

7. Shared Responsibility Model

Security & compliance of services from HPE GreenLake for Private Cloud Enterprise is a shared responsibility between you and HPE. This shared model can help relieve your operational burden as HPE operates, manages, and controls the components from the host operating system and virtualization layer down to the PCE equipment. You assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as the configuration of the HPE-provided network security policy firewall. You should carefully consider the services you choose, as your responsibilities vary depending on the services used, the integration of those services into your IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security 'of' the Cloud versus Security 'in' the cloud.


Customer Data
Applications, Application Identity & Access Management
Guest OS / Image
Self Service UI / API
Cloud Management Platform
Software defined networking stack
Virtualization O/S (Hypervisor)
Physical Infrastructure
Compute
Block Storage
Network**

HPE responsibility “Security of the Cloud” – HPE is responsible for protecting the infrastructure that runs all the services offered by PCE. This Infrastructure comprises hardware, software & networking that run HPE GreenLake services. Since PCE is deployed at your facility, you will be responsible for physical & perimeter security, and PCE will inherit the security posture of the facility and network segment.

Your responsibility “Security in the Cloud” – Your responsibility will be determined by the HPE GreenLake services that you select, which will determine the amount of configuration work you must perform as part of your security responsibilities. For example, a service such as PCE is categorized as Infrastructure as a Service (IaaS), requiring you to perform all the necessary security configuration and management tasks. With this service, you will be responsible for managing the guest operating system (including updates and security patches), any application software or utilities installed on the instances, and the configuration of the HPE-provided firewall (using network security policies) for each instance. For abstracted services, such as HPE GreenLake for containers, HPE operates the infrastructure layer, the operating system, and platforms, and you access the endpoints to deploy your container pods. You will be responsible for managing your data (including encryption options), classifying your assets, and using IAM tools to apply the appropriate permissions.

This customer/HPE shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between HPE and its customers, so is the shared management, operations, and verification of IT controls. HPE can help relieve your burden of operating controls by managing those controls.

Below are examples of IT controls that are managed by HPE, HPE Customers, and/or both:

Shared Controls – Controls that apply to the infrastructure and customer layers but in separate contexts or perspectives. In shared control, HPE provides the requirements for the infrastructure, and the customer must provide their control implementation within their use of HPE services. HPE responsibilities include:

- Design, deployment, configuration, operations, monitoring, maintenance, and management of the physical compute, storage, networking, and control plane infrastructure
- Full lifecycle management for all underlying software (VMware ESXi, VMware NSX-T, Kubernetes, and others) and firmware (updates, patches, minor releases, and major releases)
- Implementation and software maintenance of all human and programmatic interfaces (GUIs, CLIs (Command Line Interface), and APIs)
- Implementation and software maintenance of supplemental administrative tools and services (consumption analytics and capacity monitoring)
- Patch Management – HPE is responsible for patching and fixing flaws in the infrastructure, but customers are responsible for patching their guest operating systems and applications.
- Configuration Management – HPE maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their operating systems, databases, and applications.
- Awareness & Training – HPE trains HPE employees, and customers must train their employees.

Customer Specific – Controls which are the sole responsibility of the customer based on the application they are deploying

- Physical space, power, cooling, and physical security at a data center or colocation facility
- Internet uplinks and perimeter (network border) security
- Bare-metal host operating systems and technology stacks, VM guest operating systems, containers, workloads, and user and application data

- Application lifecycle management and configuration management
- Identity and access management (IAM) for cloud or tenant admins, cloud consumers, and applications
- Configuring and populating the self-service catalog with customer’s templates and images for the resources they wish to make available to their users for provisioning.
- Monitoring and management of customer’s workloads, storage, and network components.
- Approval process to implement HPE-identified actions to address incidents.
- Assessment and authorization process of the change request.

As an additional service, HPE can extend the scope of our activities to encompass the workloads and resources you provide and manage these in-cloud resources on your behalf. Any activities would need to be defined and scoped according to your specific requirements.

Best Practices for Customers

Security Recommendations

HPE GreenLake places a high degree of emphasis on building a secure PCE service for our customers, including the control plane collocated in the customer’s data center. However, HPE also has an organizational philosophy of “Defense in Depth” whenever and wherever possible and recommends customers evaluate the following controls to augment PCE’s already robust security profile.

- Segmentation: Place services into controlled network zones with similar systems to simplify network monitoring, minimize attack surfaces, and enforce access controls.
- Safelisting: Restrict East/West traffic to only approved endpoints, either through IP controls or micro-segmentation.
- Logging & Monitoring: Review relevant security logs, either directly or via a centralized logging and monitoring solution. GLCS can provide access logs currently and is working towards making all relevant security logs available in the future.

Customers are encouraged to follow best practices for securing their applications and data within the cloud environment. This includes regular password changes, secure coding practices, and regular vulnerability assessments.

Collaboration

A collaborative approach is essential to ensure the continued security of the hybrid cloud environment. HPE and its customers should engage in ongoing communication, sharing insights, and working together to align security efforts. Clear communication channels, incident reporting procedures, and regular security reviews foster a strong partnership in maintaining a secure cloud ecosystem.

By adhering to the shared responsibility model, both HPE and its customers contribute to a comprehensive security posture that safeguards data and applications in the hybrid cloud. This model promotes transparency and accountability, creating a secure foundation for the cloud ecosystem.

8. Conclusion

The hybrid cloud ecosystem, combining HPE’s Private Cloud Enterprise service stack with public cloud management components, presents a robust and secure platform for hosting applications and data. The comprehensive security measures outlined in this white paper demonstrate the commitment to safeguarding customer assets, adhering to industry standards, and continuously improving security practices.

By adhering to these security principles and measures, customers can have confidence in the security of their workloads in this private cloud environment. Ongoing collaboration and communication between the cloud provider and customers will ensure that security remains a top priority, adapting to evolving threats and technological advancements.

This document contains confidential and/or legally privileged information. It is intended for Hewlett Packard Enterprise and Channel Partner Internal Use only. If you are not an intended recipient as identified on the front cover of this document, you are strictly prohibited from reviewing, redistributing, disseminating, or in any other way using or relying on the contents of this document.

Released: April 2024

Hewlett Packard
Enterprise