Hewlett Packard Enterprise

Technical white paper

Check if the document is available in the language of your choice.

HPE GREENLAKE CENTRAL SECURITY

CONTENTS

EXECUTIVE SUMMARY

Enterprises across all market segments readily acknowledge that hybrid cloud offers a wide range of services to accelerate the efficient development and delivery of applications and services to meet the ever-increasing demands from lines of business. One of the major concerns with cloud solutions, however, is ensuring the security of the environments and the consistency of security controls across cloud providers, which may have different implementations. While the core concepts may be similar, the terminology and supplied mechanisms often differ. This can be confusing and, more importantly, lead to security risks. HPE GreenLake Central (GLC) provides a platform in which the customer has a single point of administration for all workloads managed by HPE GreenLake running on public and private clouds.

HPE GreenLake Central and associated services are developed with security as a cornerstone. Providing a robust, secure solution requires the foundation of a mature, secure software development lifecycle (SDLC) methodology. This is a critical aspect of the platform's security, which is usually not noticed directly by users. Strict adherence to the secure SDLC is required to manage risk and achieve a demonstrably secure system.

HPE GreenLake Central is used in all HPE GreenLake service offerings and is not intended to be used stand-alone. This paper will focus on the security aspects of HPE GreenLake Central. Details of specific HPE GreenLake service offerings can be found in other documents—see the "Additional resources" section.

This paper will help customers understand the security functions and services that are embodied in HPE GreenLake Central. In addition to this information, which is visible to the customer when using the services, this paper will provide insight into the security processes and practices employed in the development, deployment, and operation of HPE GreenLake Central.

Target audience

The target audience for this document includes customer security and administrative personnel, as well as risk management teams, who will be working with HPE GreenLake Central.

HPE GREENLAKE CENTRAL OVERVIEW

HPE GreenLake Central is a cloud platform that provides secure and role-based access to trial, subscription, and consumption of HPE GreenLake service offerings. HPE GreenLake Central provides service orchestration, a unified cloud experience to applications and data across the customer's HPE GreenLake estate, including private and public clouds, edge to core.

Within HPE GreenLake Central, the HPE GreenLake services are accessible through a **widget**—such as **HPE GreenLake for private cloud**. Each HPE GreenLake subscription is represented by a specific widget, which often contains summary details about the service. When the customer selects the service and clicks on the corresponding widget, they will be taken to the page dedicated to that service.

HPE GreenLake Central provides the single point of entry for cloud management and services within HPE GreenLake. Given the strategic importance, it is built with significant security protections and a high level of availability.

With HPE GreenLake Central, the customer can also:

- Move faster with a self-service, point-and-click cloud experience
- Deliver a tailored cloud experience with role-based access for IT, CIOs, DevOps, and finance users
- Gain quick insights across all functions with high-level KPIs, such as monthly costs, capacity, and compliance conditions

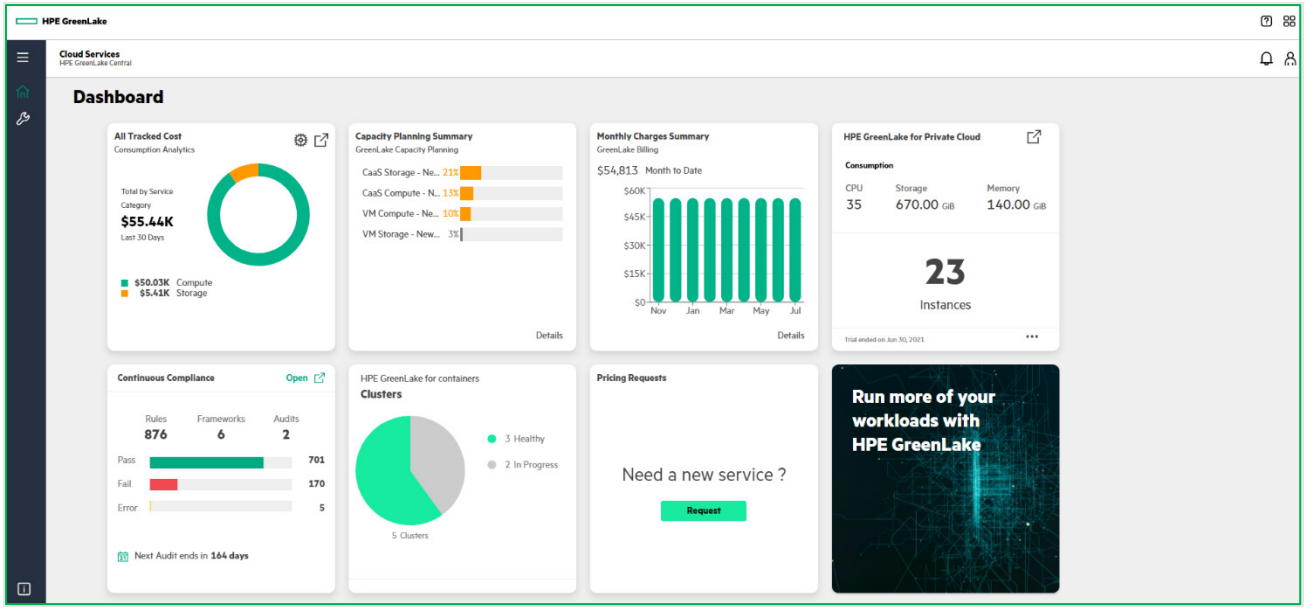

FIGURE 1. HPE GreenLake Central dashboard

HPE GreenLake Central architecture

HPE GreenLake Central is the user interface for operations and access to all HPE GreenLake services. It consists of the portal, a services catalog, identity and access management (IAM), and notification services, as shown in the following figure:

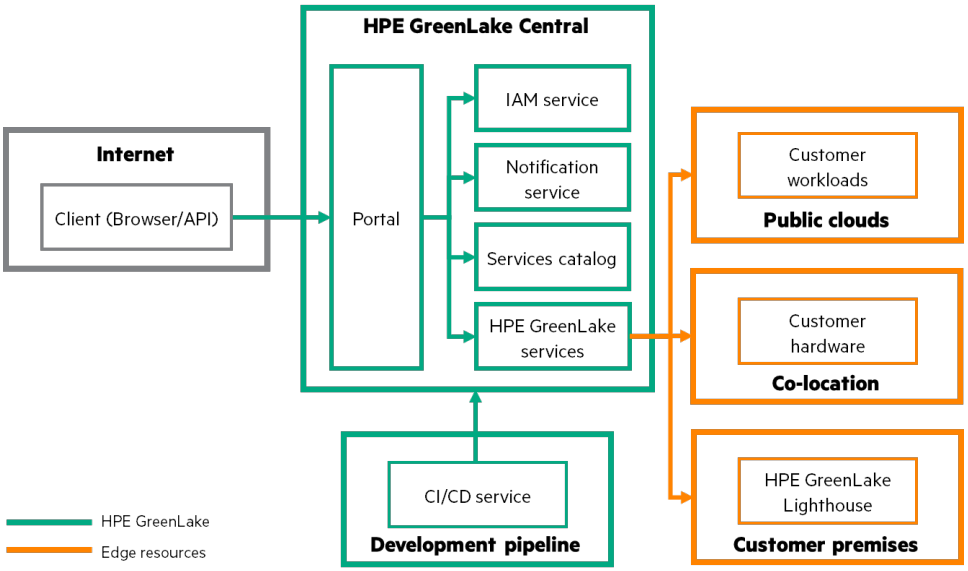

FIGURE 2. HPE GreenLake Central architecture

The portal is the interface through which users can access HPE GreenLake Central securely via the internet, using the transport layer security (TLS) 1.2 protocol through a browser or API call. The IAM service manages authorization controls for users while providing an abstracted interface to an identity service broker through a cloud service providing authentication and authorization. HPE GreenLake Central provides a REST-based API, enabling access to all its features. The API facilitates automation of system communication, allowing customers to integrate their software seamlessly to HPE GreenLake Central. The services catalog provides a list of all resources available for deployment in HPE GreenLake Central.

Upon user login, the IAM service validates the credentials to authenticate the user and to determine the appropriate authorizations. Upon successful authentication, HPE GreenLake Central queries the services catalog, displaying the services the user has access to as part of their overall company subscriptions. Additionally, the user may also request new services or trials through the portal. The HPE GreenLake environment contains extensive monitoring capabilities, which can be configured to provide notification of various events.

HPE GreenLake Central and some HPE GreenLake services can control the customer's workloads running on a hybrid cloud environment, including select public cloud providers and private cloud environments on the customer's data center or on a third-party co-location provider. Optionally, when the customer subscribes to one or more HPE GreenLake cloud services on-premises, the HPE GreenLake service components will communicate directly with the HPE GreenLake Lighthouse infrastructure hosted on the customer's premises. HPE GreenLake Lighthouse is a secure, cloud-native, and intelligent infrastructure, built with HPE Ezmeral software to autonomously optimize different cloud services and workloads by composing resources to deliver the best performance and lowest cost.

Figure 2 also depicts how the HPE GreenLake services and updates are delivered to the customer. The HPE GreenLake team is constantly developing and updating functionality to improve the user experience and meet new and emerging customer needs. The continuous integration and development (CI/CD) pipeline allows the rapid deployment of these changes. This approach ensures that the appropriate development and security practices are applied and adhered to and is further explained in the "Secure SDLC" section of this paper.

IDENTITY AND ACCESS MANAGEMENT

Identity and access management (IAM) in HPE GreenLake Central is how a customer controls **who** can perform **what actions to what objects**, under **what conditions**, in an HPE GreenLake environment. In this context, IAM is a service that allows an administrator to securely control who can sign in (authenticate), have what permissions (authorize) to consume which HPE GreenLake services, and store logs of all accesses (accounting).

There are two types of users in HPE GreenLake Central:

- **Customer administrator**: Also known as **IAM owner or tenant administrator**, it refers to the user assigned to the customer's environment that has the authority to create, delete, or change objects in the HPE GreenLake environment, including determining which other users can be assigned roles that enable them to make changes to specific subsets of services or resources.
- **Customer user**: Also known as **end user** or **tenant user**, it refers to the person in the customer's organization that can consume the HPE GreenLake services.

NOTE
All HPE GreenLake Central users have some degree of administrative privilege, as they are required to manage cloud environments and services. To ensure the best level of security, it is recommended that all users follow internal customer security policies and procedures to be authorized to perform administrative tasks.

A tenant is an isolated environment with users and workloads, and it hosts the resources dedicated to a single customer in HPE GreenLake Central. Each tenant owned by a single identity—such as a person, a company, or an organization—and is associated with at least one default customer email domain. Every tenant has a dedicated identity directory for all HPE GreenLake service instances the customer subscribed to for that tenant. Also, all resources are tenant aware to ensure that customer data is restricted to a single tenant.

In IAM, every physical or virtual asset that can be managed by a user is called a **resource**. To validate the level of access a user has on a specific resource, IAM uses roles and associated permissions. A **role** is a collection of permissions. The concept of **role-based access control** (RBAC) is applied when the customer needs to set fine-grained permissions, allowing the tenant administrator to assign predefined or custom roles for each user or user group. Using RBAC enables the configuration of layered policies that are compatible with industry-standard **identity governance and administration** (IGA) tools. IAM also employs the principle of **least privilege** to provide access management delegation and separation of duties, where a user is only granted the minimum permissions to perform their intended activities.

HPE GreenLake Central uses industry-standard open protocols to provide authentication, such as OIDC and SAML v2. IAM supports strong authentication through multi-factor authentication (MFA). Access to a tenant is governed by tokens generated by IAM, which are valid for a single user and contain the tenant ID. Access tokens are short lived and can be refreshed by using limited-duration refresh tokens or by reauthenticating. After users are logged in to HPE GreenLake Central, they are automatically logged in to other HPE GreenLake services to which they have been granted access.

Using HPE GreenLake Central, a customer can create a collection of resources, which is known as a **space**, similar to an access control group, to manage several resources at the same time and simplify operations. By default, a resource is associated only with the space in which it is created, but it can later be associated with other spaces within the same tenant.

For more information on HPE GreenLake Central IAM, check the HPE GreenLake Central User Guide.

SECURITY FOUNDATION

All HPE GreenLake customers benefit from an infrastructure architecture that is built to meet the requirements of the most security-sensitive organizations.

HPE GreenLake Central acts as the management plane and only handles customer contact information and credentials—user ID, password, access tokens and roles. This data is always encrypted, whether in transmission or at rest, and is also securely backed up and protected by isolation within Kubernetes (K8s) containers. All data transmission within HPE GreenLake Central and between external networks to and from HPE GreenLake Central is protected by encryption using TLS 1.2. Customer data is not transmitted through nor stored in HPE GreenLake Central.

Shared responsibility model

Both HPE GreenLake and the customer have a responsibility in controlling security, either in the cloud or on-premises, where applicable. HPE GreenLake follows industry-standard best practices for developing and deploying the software, hosting, and managing the physical infrastructure and software to provide the cloud services, preventing unauthorized access to user profile data.

HPE GreenLake Central allows customers to manage access to HPE GreenLake services and resources securely and with ease. Fine-grained access control to their users is available by managing IAM roles, access, and permissions. This simplifies the customer's operations, allowing them to increase focus on their enterprises.

Customers are responsible for managing their workloads, guest operating systems and images, data, and applications—and for implementing recommended security best practices, such as requiring strong passwords, allocating appropriate privileges, and managing the lifecycle of users in their respective tenants.

Secure SDLC

To provide a robust and secure solution, HPE GreenLake adheres to strict security methodologies throughout the development lifecycle. This is used by all HPE GreenLake service offerings, and this document will focus on HPE GreenLake Central. Optimal security, as provided in HPE GreenLake Central and associated services, begins with a secure software development lifecycle (SDLC) methodology, as detailed in the following figure:

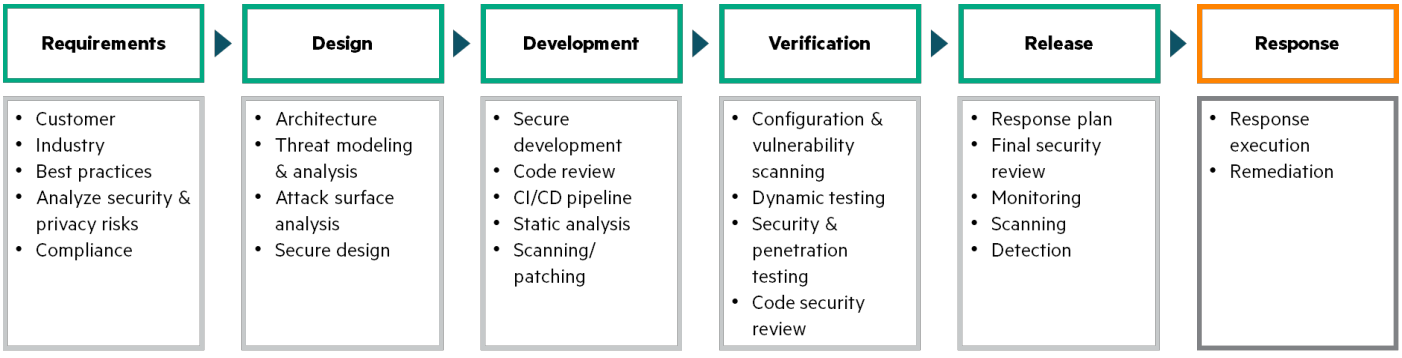

FIGURE 3. Software development lifecycle

Additionally, the methodologies employed by the HPE GreenLake Central team include:

- Required security training for developers
- Static and dynamic code analysis
- Security-specific code reviews
- Tracking, investigating, and mitigating security defects
- Periodic security scanning and penetration testing

The secure development of HPE GreenLake Central is supported by multiple security scans, integrated into the secure SDLC environment. Source code scanning detects security-based coding flaws by searching for specific rules or patterns in the code. Malware scanning detects malicious content that might appear in the build environment or the product itself. Dependency scanning detects known vulnerabilities in open-source and third-party libraries. Network vulnerability scanning can detect network-based vulnerabilities or network port usage that deviates from the HPE GreenLake architectural specifications. Any code flaw detected via scanning generates an immediate notification to the responsible engineer.

To maintain the security and integrity of HPE GreenLake Central, it is essential that the CI/CD pipeline include appropriate tools, gates, and checkpoints. For example, code changes must be performed within the change control management guidelines; and access controls and peer review of code must be performed before code can move through the pipeline. The pipeline includes various gates and measures that must be passed before moving on to the next stage.

Architectural threat analysis

The architectural threat analysis is a process through which every HPE GreenLake software product is reviewed. Security experts examine the design of the architecture, its interfaces, components, and data to identify potential weaknesses, which could be exploited. This includes checking the architecture diagram to identify potential security threats, breakdown of each component and interaction between components, determining the risk associated with identified threats, assigning impacts and priorities for actions, and planning mitigations. The architect responsible for the project will create all the documentation, defining functional and design specifications and submit it for analysis.

Development security

DevSecOps is the concept of applying security in DevOps. This implements security in all phases of the product lifecycle and facilitates early detection of issues, providing effective layered security and producing a secure product. From the requirement phase through deployment, the HPE GreenLake team uses tools and processes to build the software securely and to detect and remediate flaws early in the lifecycle.

In this phase, all systems and software are locked down, disabling unneeded protocols, ports, and services. Security must be implemented by design, considering security up front and throughout and applying industry-standard best practices, such as the Open Web Application Security Project (OWASP).

The following are a few of the principles used to provide embedded security guardrails and enforce security best practices in the HPE GreenLake Central software development process:

- **Minimize attack surface:** Enforce all service API exposure to be explicit and closed by default
- **Establish secure default:** Secure defaults are provided throughout the workflow to ensure developers start secure
- **Provide least privilege:** Services are isolated, resource sharing is structurally prohibited, and all privilege escalation must be explicit and approved
- **Offer continuous verification:** Validate security parameters upon deployment, continuously validating that all security parameters are appropriate and performing continuous threat detection for bad actors in the system
- **Don't trust services:** All services are only accessed via public APIs and access is explicitly authenticated and authorized, rather than by network proximity or segmentation
- **Ensure separation of duties:** Independent service delivery and isolation ensure a strict separation of duties for all services
- **Avoid security by obscurity:** Use tools to ensure secrets management, secrets rotation, and handling of confidential information are all at the highest security standards
- **Keep security simple:** Intrusion detection, security benchmark verifications, and dependency vulnerability scanning are built into platform, requiring no conscious effort to implement
- **Fix issues correctly:** Actively scan software artifacts for known vulnerabilities and automatically stop the integration process, enabling teams to remediate identified issues

Secure code review and testing

Industry best practices dictate that code submissions should be peer reviewed, that is, a review by a competent developer besides the author of the code. In addition to the peer review process, security sensitive HPE GreenLake components also undergo security focused code review by a security analyst. Secure code review is the process of analyzing the source code to pinpoint security flaws. HPE GreenLake Central uses both manual code review and automatic static application security testing (SAST) tools to inspect the code during development phases. These code reviews are based on industry standards, such as OWASP and other best practices.

Deployment security

In the deployment phase of new versions or updates to the HPE GreenLake Central software, it is imperative that the security and integrity of the new or updated software is maintained. HPE GreenLake uses a high degree of automated deployment practices to minimize errors that could be introduced by manual processes, which includes numerous checks to ensure the quality of the code before deployment. The deployment also manages the protection of sensitive data that is required by applications running in the production environment—for instance, to securely move from repositories to protected storage in production environments.

The HPE GreenLake platform adheres to proven software security principles, which are embedded into the workflow process, ensuring consistent application and enforcement of those principles across the teams. The deployment process provides a high level of security by enforcing the use of robust processes and procedures. To ensure strong authentication, the use of MFA is required for the entire organization, and repository credentials and deployment secrets are rotated in a maximum of 90 days.

Deployments are only authorized by approved staff and requires at least two confirmations. To assure no malicious artifact is deployed, all code included in the final implementation adheres to code review and release policies.

Operational security

After the deployment of HPE GreenLake Central, it is critical to maintain appropriate security controls, processes, and monitoring. HPE GreenLake is responsible for protecting HPE GreenLake Central and its associated infrastructure, providing the customer with services that can be used securely. Third-party auditors regularly test and verify the effectiveness of the security controls.

The HPE GreenLake team uses best-of-breed tools to continually monitor and improve the HPE GreenLake Central security during ongoing operations. The HPE GreenLake Central services require the use of all the security tools and techniques available—such as zero-trust least-privileged design, segmentation of resources, auditing usage of all accounts, continuous enforcement of security best practices, centralized layered audit of access management activities, and a strong single sign-on provider.

HPE GreenLake Central is built on container technology to provide additional operational benefits and ensure ongoing security. Containers provide a level of isolation, so any potential issues caused by errant code is limited and the use of private containers further minimizes the attack surface of the cluster. RBAC supports privilege minimization for each defined role and simplifies the assignment of privileged operations to specific users, streamlining compliance. All internal and external communications require the use of TLS 1.2, with a key management service automatically controlling the lifecycle of the certificates. Also, all ingress connections are limited to dedicated cluster load balancers to protect against denial-of-service (DOS) attacks.

Ongoing operations are further secured by automatically scanning containers and images, ensuring that known vulnerabilities are rapidly detected and corrected, standard secure configuration files are applied, and all actions are logged and audited.

Security incident response

A security event is a change in the everyday operations of an information system indicating that an information security policy, acceptable use policy, or standard security procedure, rule, or standard may have been violated or a security safeguard may have failed. A security incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security procedures, rules, and standards that threaten the confidentiality, integrity, and availability of an information system or the information the system processes, stores, or transmits. All security incidents start off as security events. Only after a security event is identified, analyzed, and reclassified does it become a security incident.

The HPE GreenLake security incident response policy applies to any asset managed by HPE GreenLake, including but not limited to applications, operating systems, database management systems, and network operating systems. It is reviewed annually, updated when the environment changes, and applicable to all staff.

Once a security incident is detected and classified, the security incident response policy defines the process of notification, ownership assignment, triage, recording, tracking, communication, validation, and resolution. After the incident is resolved, steps are taken to identify the root cause, define remediation controls to prevent the issue from reoccurring, and create a risk assessment report. Depending on the findings, the incident awareness trainings and all documentation are updated.

Security vulnerability management

A security vulnerability is a theoretical or proven flaw in a component. If a security vulnerability can be exploited, it may interfere with appropriate processing and may lead to exposure of sensitive data. HPE GreenLake Central is monitored for security vulnerabilities in several phases of the secure SDLC. Monitoring ranges from the source code to executing components allowing HPE GreenLake to follow standard procedures to quickly detect, investigate, and remediate impacting issues.

HPE GREENLAKE CENTRAL SECURITY BEST PRACTICES

HPE GreenLake uses numerous security best practices based on industry standards and internal policies, which are applied to all HPE GreenLake service offerings, including HPE GreenLake Central. Although the list is too long to include in its entirety, the following items provide a representative sampling:

- Train staff continuously in security practices, policies, and procedures based on the individual's role and level
- Use industry standards in the secure software development lifecycle (SDLC) to require clients to specify the levels of access to data, including security, regulatory, and contractual considerations
- Conduct periodic audits of secure SDLC
- Continually perform application and network security assessments of our hybrid cloud service infrastructure
- Use the business continuity plan (BCP) to ensure maximum availability for the environment, allowing for consistent management and planning of continuous risk assessments
- Use strong policies and procedures to ensure secure allocation and use of physical and virtual resources, applications, and infrastructure
- Use encryption key management systems to clearly identify and control key owners and manage the key lifecycle
- Monitor constantly the compliance of our development and production service environments to our privacy and security policies
- Review security policies and procedures regularly
- Apply access controls:
  - Controls and enforces access restrictions to systems based on clearly defined business requirements
  - Data access segmentation
  - Enforcement of least privileges
  - Authentication, authorization, and accountability (AAA)
- Implement controls:
  - Preventive, detective, corrective, and compensating controls to mitigate impacts of unauthorized access
- Provide secure authentication:
  - Use of open standards for authentication to tenants and systems
  - Multi-factor authentication (MFA)
  - Support for identity federation standards (such as SAML v2) and integration with customer's single sign-on (SSO) systems
- Leverage tools, such as file integrity and network intrusion prevention systems (IPS), as well as defense-in-depth techniques and hardened operating systems
- Ensure interoperability by providing data in industry-standard formats, transmitted over secure channels, and using standard virtualization formats and infrastructure
- Implement and continuously test the security incident response plan to ensure thorough incident management procedures and processes
- Mitigate risks in supply chain by implementing controls, continuously reviewing information security compliance and restricting data storage to specific geographic regions
- Enforce monitoring, mitigation, and remediation of security vulnerabilities in all open source and third-party components used in HPE GreenLake Central

ADDITIONAL RESOURCES

1. HPE GreenLake Central login
   client.greenlake.hpe.com/
2. HPE GreenLake Central user guide
   hpe.com/support/greenlake-userguide-en
3. HPE GreenLake portfolio
   hpe.com/us/en/greenlake/services.html
4. HPE GreenLake resources for developers
   developer.hpe.com/platform/hpe-greenlake/home
5. HPE GreenLake user guide
   support.hpe.com/hpesc/public/docDisplay?docId=ccs-help_en_us
6. Security and digital protection services from HPE
   hpe.com/us/en/services/consulting/security.html
7. Brochure: Mitigating risk with managed security from HPE GreenLake Management Services
   hpe.com/psnow/doc/a00107277enw

LEARN MORE AT

hpe.com/greenlake

Hewlett Packard Enterprise

a00116868ENW, August 2021