WHITEPAPER

ForgeRock Identity Cloud

Security and Compliance

Table of Contents

About ForgeRock

ForgeRock, the leader in digital identity management, helps customers safely and simply access the connected world. We offer a complete IAM platform to help customers transform how they can build trusted relationships with people, services, and things. Customers can monetize these relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.

Security at ForgeRock

ForgeRock recognizes that security is essential to digital identity management. To that end, we invest heavily in security and embed it into every aspect of our business, as briefly illustrated in the following sections.[1]

Secure Development Lifecycle

ForgeRock's Secure Development Lifecycle provides a consistent framework for developing, releasing and operating secure software and services, based on Microsoft's **Secure Development Lifecycle**. The top-level security development process is shown below:

Some highlights include:

Skills Development. All ForgeRock employees take annual security awareness training; engineers also take annual training in secure coding techniques. As well, several internal "guilds" are devoted to knowledge-sharing related to security.

Force-Multiplication via Tooling. Automated security scanning tools are embedded throughout the development and deployment process, including static, dynamic, and open-source scanning.

Assurance. Threat models are developed during the design of security-critical components, independently reviewed, and maintained throughout the components' lifecycle. Penetration testing is used extensively for additional independent validation, including both black- and white-box testing.[2]

Security Incident Response

ForgeRock utilizes a security incident response process based on NIST 800-61 that provides a framework for investigating and responding to suspected security incidents. A dedicated Enterprise Security Team is available on a 7x24 basis.

Audit and Compliance

ForgeRock has a comprehensive internal auditing program to regularly review on at least an annual basis all of the applicable security and privacy controls as set out in our Information Security Management System (ISMS) and related policies. This audit program is based on our compliance obligations under ISO 27001, SOC 2, CSA Star and HIPAA/HITECH for which ForgeRock has obtained certification and undergoes continuous improvement as a result of internal and external audits, and future certifications.

1 For a more detailed description of ForgeRock's company-wide security practices, see **https://www.forgerock.com/resources/view/107430026/whitepaper/forgerock-identity-cloud-security-whitepaper.pdf**

2 In a black-box penetration test, an attacker positioned on the Internet, with no inside information about the service, attempts to compromise it. In a white-box test, the attacker is provided with full details about the design, implementation, and operation of the service. He or she is then "conceded a beachhead" within the service and asked to attempt to extend their control.

ForgeRock Identity Cloud

Identity Cloud is an online service that enables customers to meet their identity and access management needs without the burden of hosting and operating an on-premise infrastructure.

The ForgeRock Identity Cloud provides a comprehensive, flexible identity and access management solution run and operated by ForgeRock. ForgeRock secures, monitors, upgrades and runs the software while providing the flexibility and extensibility to satisfy some of the most complex identity and access management use cases in the industry. ForgeRock Identity cloud supports all major identity standards including OAuth 2.0, OIDC, SAML, CIBA as well as providing identity synchronization and storage. The ForgeRock Identity Cloud can be supplemented with the ForgeRock Identity Gateway™ or ForgeRock Agents™ to provide policy enforcement and API management."

More information on Identity Cloud's features and benefits is available at **https://www.forgerock.com/platform/identity-cloud.**

Compliance Certification

ForgeRock has achieved ISO 27001 certification for the development and operation of cloud and on-premises products and services across all of our major locations. We recently achieved a SOC 2 Type 2 certification and report for ForgeRock Identity Cloud, and have Cloud Security Alliance (CSA) Star Level 2 attestation and certification. We have independent attestations of compliance with Health Insurance Portability and Accountability Act (HIPAA) security and Health Information Technology for Economic and Clinical Health (HITECH) breach notification rule.

Security Approach

Identity Cloud's security model is based on a system of complementary, mutually reinforcing security controls that promote three qualities that are essential to security in an *assume-breach*[3] world: isolation, hygiene, and observability.

Isolation

Throughout the service, all resources are isolated. This creates a resilient, multi-layered defense.

The service establishes a system of *trust zones*, each with dedicated code, data, and identities.[4] This pattern is repeated at the Docker container, Kubernetes, and Google Cloud layers. Indeed, every customer's environment is a trust zone — it is sovereign and shares no code, data, or identities with any other customer's environment.

Hygiene

From the start, ForgeRock has understood that IT hygiene is an unheralded but essential element of security. Many security breaches stem from failures in seemingly mundane tasks: privilege management, dependency management, configuration management, and so on. Getting the fundamentals right benefits both security and service quality.

A similar mindset applies to system design. The cleaner and more comprehensible a system's design is, the more consistent and predictable its behavior will be — and the easier it will be to identify and fix anomalous behaviors when they happen, regardless of their cause.

Observability

As a rule, preventive and detective controls are paired in Identity Cloud — preventive controls to enforce the security model, and detective controls to identify efforts to circumvent it. This greatly increases the effectiveness of each.

Service components generate detailed telemetry describing their activities and outcomes, which in turn is consumed by detective controls that continually compare the service's behavior to the expected model. This provides ForgeRock with excellent situational awareness that benefits both security and service quality.

3 *Assume breach* posits that an attacker with sufficient funding, skill, and tenacity eventually will meet with some degree of success. Accordingly, one's security architecture should bend but not break, and allow an agile response.

4 Trust zones are analogous in many ways to microservices. A trust zone tends to be dedicated to a single business purpose; it fulfills its purpose using resources that it alone controls; and it establishes and enforces rules for interacting with it.

Security Architecture

A simplified view of the service's security architecture is shown in Figure 1.

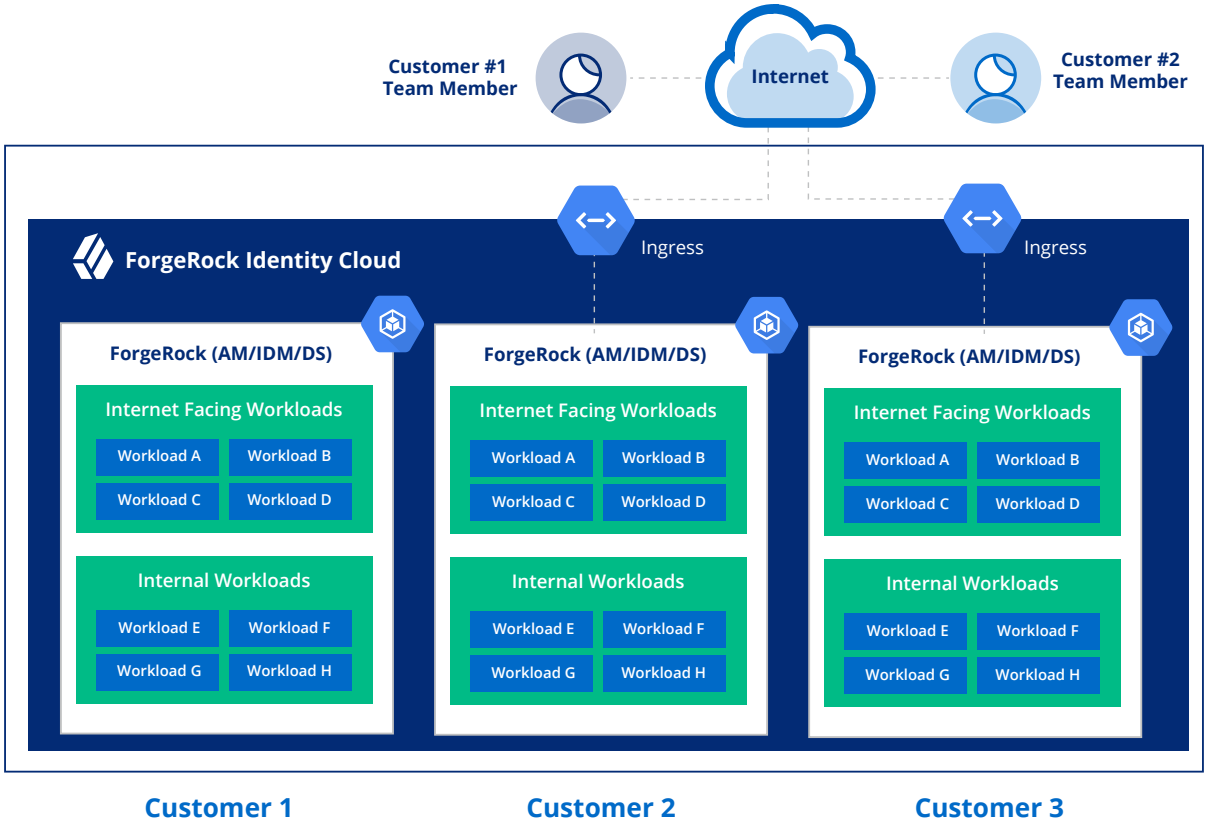

Figure 1: Trust Zones

The fundamental trust zone consists of a dedicated Google Cloud Platform (GCP) environment that hosts Identity Cloud in its entirety.[5] Crucially for security, it is sovereign: the environment is self-sufficient regarding its critical resources; it, and it alone, controls access to them;[6] and it polices the activities that happen within it.

The environment is further subdivided into a *single service control plane* that manages the overall health of the service, and multiple *customer environments*, each containing one customer's dedicated infrastructure, code, and data.[7] Like the Identity Cloud environment as a whole, the service control plane and customer environments are sovereign: each is self-sufficient, self-governing, and self-policing.

Even these environments are additionally segmented to isolate workloads based on their value and the inherent risk they are exposed to.[8] As well, every workload is encapsulated within a dedicated, hardened Docker container.

5 The *forgerock.io* environment is separate from ForgeRock's own corporate IT environment.

6 All Identity Cloud software runs under service accounts that are local to the environment. User access, by company policy, is limited to user accounts that are local to the environment and issued only to ForgeRock employees whose job functions require such access.

7 Regional redundancy is used within each of these environments to provide resiliency. For instance, if a customer environment were located in GCP's *us-west1* region, its compute, network, and storage resources would be replicated in three or more locations within the region.

8 For instance, within each customer's environment, the workloads that interact with untrusted Internet clients are in different trust zones from those that access customer data.

Tenancy

The term tenancy is understood differently within various audiences, and so it's important to be clear about the service's tenancy model.

ForgeRock Identity Cloud is a multi-tenant service. All customer environments are built from a standard template, hosted using a common technology base, maintained according to a consistent set of processes, and continually upgraded to the latest code base. The infrastructure is treated as cattle, and not pets, and uses consistency, standardization, and automation to deliver a highly available service.

ForgeRock Identity Cloud provides a distinct, dedicated environment to each customer. As described in the previous section, each customer environment is self-sufficient and sovereign. It comprises a distinct GCP and Kubernetes environment, runs a distinct copy of the service code under dedicated identities, and provides dedicated storage for customer secrets and data that only it can access.[9] [10]

Data Protection

The service protects customer data at both the service and physical levels.

Service Level

As previously noted, each Identity Cloud customer's data is stored solely within their environment — specifically, within their Directory Services instances. It is never commingled with other customers' data and can be accessed only by the customer.

Physical Level

GCP provides native encryption of data at rest. All data is encrypted when written to a hard drive, and decrypted when read.

Network Security

Each customer environment includes dedicated networking resources such as Internet-accessible endpoints for user interfaces and APIs. Network communications between customer environments are blocked; even within a customer environment, network communications between workloads are strictly controlled using role-based access control and enforced via network policies.

Identity Cloud makes use of GCP-native network security features to protect against denial of service attacks.[11] All Identity Cloud endpoints require TLS 1.2 or higher and are anchored by a digital certificate.

Identity and Access Management

One of the cornerstones of the Identity Cloud security model is comprehensive and rigorous identity and access management. Virtually all transactions require authentication, using identities defined within the trust zone that enforces the authentication. *Least-privilege* is employed throughout the service.

In keeping with the isolation tenet of the security design, cross-zone trusts are employed rarely, and only after careful consideration. The Identity Cloud environment as a whole extends no trusts to other environments. Likewise, individual customer environments extend no trusts to each other, or to the control plane.[12]

To understand this in practice, consider a representative customer environment. It comprises a GCP project with a single Kubernetes cluster; thus, it is a self-managed identity domain for both GCP and Kubernetes. It mints a GCP and Kubernetes service account corresponding to each Kubernetes namespace, assigns them minimum privileges, and assigns them to the appropriate workloads.

9 Specifically, each customer's environment consists of a distinct GCP *project* dedicated solely to that purpose. The project contains dedicated secrets-management, logging, storage, and other resources, as well as a dedicated Kubernetes environment in which the customer's Identity Cloud software runs.

10 This is in contrast to a *shared-service* model in which all customers' resources would be pooled under the control of a supervisor process.

11 The Google network's scale and multiple points of presence provide strong protection against flooding attacks; its filtering and blocking features protect against Layer 3 and 4 attacks.

12 Although the control plane creates new environments, it does not maintain any privileges in them. Instead, after creating a bare-bones environment, it passes control to a workload within the environment that deploys all the needed security mechanisms and controls. As one of its first acts, it removes the control plane's access.

An attacker who gained a foothold in the environment would find it difficult to extend the compromise, because the GCP and Kubernetes identities present in one namespace have no privileges in any others. Even in the worst case scenario where an attacker compromised an entire customer environment, none of the identities there would be valid in other customer environments or the service control plane.

Likewise, user access to the Identity Cloud environment is tightly controlled. The service infrastructure can be accessed only by user accounts that are granted only to ForgeRock employees whose jobs involve building and operating Identity Cloud. Even these accounts don't have unfettered access to the infrastructure — in particular, the production infrastructure can be accessed only by a small number of "special access" accounts whose actions are closely monitored.

Secrets Management

Every environment within Identity Cloud has a dedicated secrets vault that it uses to securely store passwords, private keys, API keys, and other secrets. The secrets are strongly protected at rest and in transit[13], and the cryptographic keys used to encrypt the secrets are regularly rotated.

Except for customer-provided secrets, all secrets are created within the customer environment. They are unique from environment to environment, and cryptographically random.

Auditing and Logging

Identity Cloud generates extensive auditing and logging information.

ForgeRock Product Logs

The Access Management, Identity Management, and Directory Server instances within a customer's environment generate the same audit and logging data as they do when deployed on-premise. This data is stored exclusively within the customer environment. Customers can retrieve these logs via an API if desired.

Identity Cloud Infrastructure Logs

The service collects audit and logging data from the Kubernetes and GCP infrastructure. All create/update/delete operations are logged, as are read operations involving security-critical resources like secrets.[14]

Infrastructure logs are copied to a Security Incident and Event Management (SIEM) system for security monitoring purposes, with the exception of logs from Kubernetes containers that might contain customer-sensitive data.

Security Monitoring

ForgeRock continually monitors the security of the Identity Cloud environment, using **NIST 800-137** as a guide. The monitoring program is particularly attuned to two types of issues, discussed below.

Violations of the Service Model

A detailed model of Identity Cloud has been developed that specifies details such as the number and type of resources that should be present and where; their names and identities; the other resources and services they should interact with; and their expected activities. Telemetry data from the service is continually compared to the model. Any deviations trigger a high-priority security notification that the 7x24 on-call team investigates.

Use of Privileged User Accounts

As noted previously, only users with "special access" accounts can access production environments. Any use of these accounts, for any reason, generates a high-priority security notification. The account holder must acknowledge the notification and substantiate their use of the account.

13 Identity Cloud uses Google Secret Manager, which protects secrets at rest with AES-256 encryption and in transit with TLS. It also provides automatic rotation of the encryption keys.

14 The values of secrets, keys, and other sensitive data are not recorded in log data.

Configuration Management

Identity Cloud's infrastructure is configured for security. ForgeRock deploys and manages it using declarative tools in order to avoid configuration "drift" over time. As well, we independently validate the configuration using a continuous security and compliance scanning tool.

The security configuration is based on guidance from a variety of subject matter experts, including:

- **Vendor recommendations.** We follow Google's recommendations for securely using GCP; k8s.io's recommendations for Kubernetes; and our own published recommendations for securely using AM, IDM, and DS.
- **Security Subject Matter Experts.** We also follow the guidance from third-party security experts, in the form of **CIS Benchmarks**, **NIST**, and other published recommendations.

Backup

All critical data is automatically backed up. This not only includes service infrastructure data such as DNS records, but also customer-specific information. For instance, each customer environment backs up its DS stores every 15 minutes; in keeping with the sovereignty model, this data is stored within the customer environment.[15]

Physical Security

The service is wholly hosted within Google Cloud Platform, and ForgeRock does not operate any physical hardware or facilities associated with Identity Cloud. Google has published a **white paper** detailing how it secures the compute, storage, and networking assets in GCP.