ForgeRock®

Overview

ForgeRock Identity Cloud

Your Data in the Cloud is Protected with the Industry's Best Practices

ForgeRock offers the most flexible deployment options of any digital identity provider by giving organizations complete control over how their solution is deployed. Organizations can deploy where they want whether it's on prem or in the cloud. They can also choose to deploy the solution with specific modules or as a complete platform. As their business needs evolve, ForgeRock helps organizations stay agile so they can change their identity environment at their pace.

For example, some organizations may seek to reduce costs by outsourcing the run/operate of the platform or have a board mandate to move to a cloud architecture. They can do so by deploying the Kubernetes version of our platform in a public cloud such as AWS, Microsoft, Google or RedShift and maintain a level of DevOps. Or they may choose to outsource DevOps entirely and deploy in the ForgeRock Identity Cloud, our multi-tenant service with dedicated customer environments.

1. Security is Shared, Data is Not

Built on the Google Cloud Platform (GCP), the ForgeRock Identity Cloud uses GCP-native network security features to prevent denial-of-service (DoS) attacks against customer environments or services, blocking traffic from specific geographic locations. Network communications are strictly controlled using Kubernetes network policies. At the service level, customer data is stored within a customer environment comprising a dedicated trust zone that shares no code, data, or identities with other customers' environments. At the physical level, GCP provides encryption of data at rest, so all data is encrypted when written to a hard drive and decrypted when read.

2. Hardened by Experts

The ForgeRock Identity Cloud is hardened by those that know the software best, ForgeRock. The security architecture of the ForgeRock Identity Cloud has undergone a detailed internal review, including a threat modeling exercise that systematically evaluates the assets hosted within the service, an attacker's options for compromising them, and the effectiveness of the service's security controls at preventing or detecting them.

Security also starts with the fundamentals: secure coding practices, least privilege, dependency management, and more. Clean design and meticulous operational practices benefit both security and quality.

3. Never Out Of Date

The ForgeRock Identity Cloud makes it much easier to stay current with patches and versioning. With our Continuous Integration / Continuous Deployment (CI/CD), organizations can be assured they are always on the latest, patched version. In keeping with the assume breach mindset, technologies and processes for quickly detecting, mitigating, and recovering from attacks are integrated into the service design and operation. ForgeRock also operates a continuous monitoring program that detects potential security issues and alerts when appropriate.

Do you want to know more?

Learn More About ForgeRock Identity Cloud

For a more detailed explanation, see our
ForgeRock Identity Cloud Technical Whitepaper.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

Follow Us

ForgeRock