opentext™

OpenText Cloud Platform (OCP): Security

Overview

As enterprises embrace digital transformation the need for secure cloud solutions becomes paramount. OpenText™ Cloud Platform (OCP) prioritizes security so organizations can digitize their operations, virtualize business processes, and connect with stakeholders seamlessly. By focusing on robust security measures, OCP ensures that applications hosted on the platform are protected against downtime and productivity loss, allowing businesses to thrive in the digital economy.

Benefits

- **Enhanced security:** Robust built-in security features, including authentication, authorization, encryption, and context-sensitive dynamic access controls, ensuring the safety of content and providing additional options for enhanced security in the cloud.
- **Flexibility and innovation**: A comprehensive suite of developer tools and services that enable enterprises to create customized solutions and extend existing OpenText products, fostering operational efficiency and driving innovation.
- **Seamless integration:** OCP simplifies the integration process by providing standardized APIs and developer tools, allowing easy connectivity with various applications and systems.
- **Scalability and reliability:** With decades of application service delivery experience, OCP ensures high availability, scalability, and reliability, helping organizations manage large volumes of transactions and critical business processes.

OCP Security

Authorization and authentication

- OCP implements industry-standard authentication and authorization mechanisms ensuring secure access control for users, such as:
  - Authentication—SAML2.0, OpenID Connect 2.0
  - Authorization—Oauth2.0, Tokens
  - User Provisioning (cloud and hybrid)—SCIM2.0 (Cloud)
  - Encryption—DEKs, KEKs, Google KMS
- Developer tools provided by OpenText simplify integration processes, enabling seamless integration of content, and data into cross-enterprise information management programs.
- The extensive suite of content management and process automation REST API are secured by the industry standard OAuth 2.0. Both confidential and public clients can be created and both client types support Proof Key for Code Exchange (PKCE).
- OCP's security measures include access control lists (ACLs) that grant specific access privileges to users, groups, or roles, ensuring that only authorized individuals can access data.
- OCP Foundational Stack leverages industry-known and respected OTDS technology to provide system access control, group, roles, and user management—available through the Admin Center interface.

Encryption and key management

- OCP ensures security at multiple layers, including key management (KMS) and encryption at the storage layer at rest.
- All content uploaded via OCP Storage Services is scanned for viruses and other malicious threats—such as malware, ransomware, trojans, and more. When encountered, malicious content is immediately deleted from the system, never to reside on storage infrastructure.
- When a developer creates a tenant, an automatic key generation process takes place, with a call to GCP key management to obtain the key.
- Industry standard key management principles are in place, where data encryption keys (DEKs) are applied to every blob stored within the OCP Storage infrastructure. These DEKs are stored internally, within Cassandra backing services.
- The application of the DEKs is preceded by the request for key encryption key (KEK) which is stored externally to OCP, within Google KMS. Only keys authorized for a specific tenant can be used for said tenant. KEK data is removed from the system after successful encryption.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **X (formerly Twitter)** | **LinkedIn**