opentext™

OpenText OCP Fundamentals

A technical overview of the OpenText™ Cloud Platform

opentext™

Contents

opentext™

Executive summary

The OpenText™ Cloud Platform (OCP) is a next-generation Information Management as a Service platform powering the OpenText™ Core family of public cloud Software as a Service (SaaS) applications and services. OCP delivers information management applications and services in a highly secure and highly available multi-tenant architecture. This paper outlines the platform's key design characteristics, including its infrastructure components, platform tools, tenancy model and administrative functions. It also describes the SLAs that govern platform operation.

Security of content, transactions and access is an essential element of the platform's design. This paper describes the platform technology that secures and protects content and communication and the additional compliance and governance measures in place on the platform to further protect customer content.

Core applications and services built on OCP include:

- OpenText™ Core Capture
- OpenText™ Core Capture for SAP® Solutions
- OpenText™ Core Capture Services
- OpenText™ Core Case Management
- OpenText™ Core Content
- OpenText™ Core Experience Insights
- OpenText™ Core for Federated Compliance
- OpenText™ Core for Regulatory Plans
- OpenText™ Core for SAP® SuccessFactors®
- OpenText™ Core for Supplier Exchange

OCP tenancy and concepts

OCP is a fully multi-tenant platform where customer data in one tenant is fully isolated from customer data of other tenants. Multi-tenancy is built into multiple layers of the platform for isolation of:

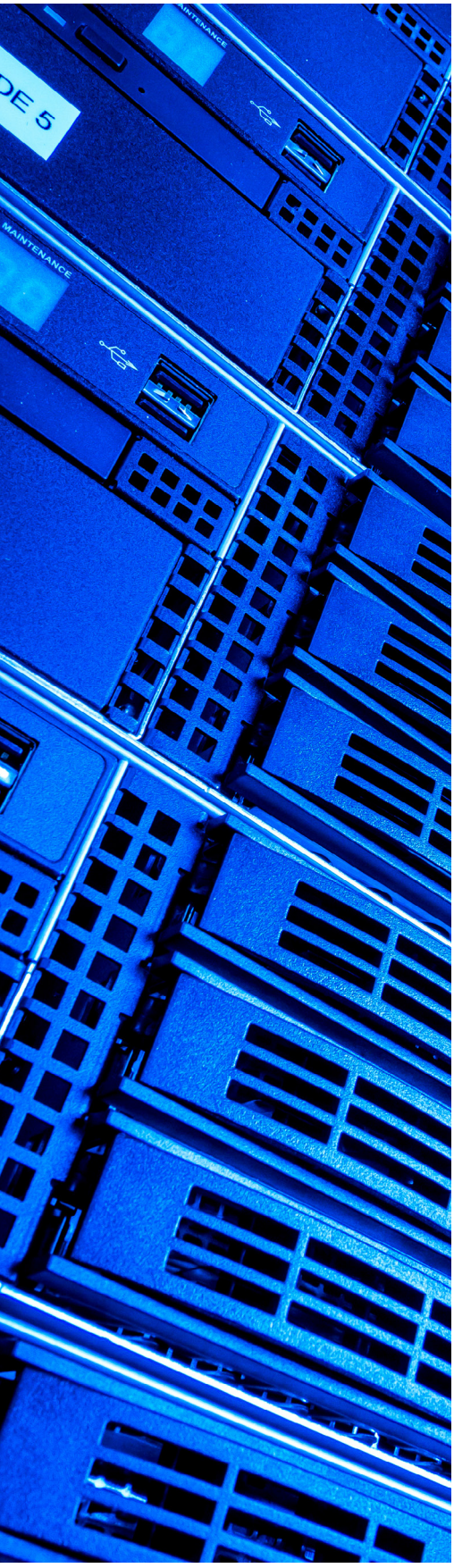
- Users and roles
- Authentication and authorization
- Foundational services
- OpenText Core applications

OCP platform infrastructure

Deployment

OpenText Core applications are public cloud SaaS applications created on OCP and run on Cloud Foundry, an open-source enterprise platform designed to run cloud applications (with the exception of Core Capture, which is Microsoft® Windows™ based). Cloud Foundry is deployed through BOSH, which orchestrates VM and software deployment to VMware™ vCenter. All Cloud Foundry applications in production are software-virtualized Linux containers with additional support for Windows Docker containers.

BOSH VMs are deployed by the BOSH director using YAML manifest files that provide all of the parameters necessary to deploy the VMs and BOSH stemcells.



These are minimal OS templates with BOSH agents installed. The director then stores the configuration stateof the VMs it deploys, including the path to the persistent disks of all of the VMs. The configuration of the BOSH director and all manifest files are saved under source control.

Storage

BOSH VMs have a minimum of two disks. The first disk is the OS disk while the second is used for software packages and logs. Any necessary persistent data is stored on a third persistent disk. While the first two disks can be destroyed and recreated with the VM at any time, the persistent disk is always unmounted and remounted to the new VM. The persistent disks hold critical data such as databases and indices. The persistent .vmdk disk files are backed up at the vSphere datastore cluster level. The datastores are mounted to vCenter via NFS from NetApp appliances. The data is protected by snapshots, incremental and full backups and replication to the secondary site.

Data centers

OCP runs on Cloud Foundry and is deployed with BOSH on VMWare vSphere. BOSH VMs are ephemeral and are designed to be recreated at any time with new, unique UUIDs and hostnames.

OCP is deployed in paired data centers located in the North America and EMEA regions and employs an active/passive data center approach to ensure high availability. All OCP applications and services run within the primary data center. The secondary data center is a clone of the primary with identical infrastructure and networks. Data is replicated every 5 minutes to the secondary site. DNS is configured to send users to the primary site unless access to the platform in that facility is disrupted or degraded, in which case customer traffic is re-routed to the secondary facility.

The primary and secondary OCP data center locations are as follows:

North America

- Lithia Springs, Georgia (LI3) production environment
- Allen, Texas (AL3) disaster recovery environment

EMEA

- Amstelveen, NL (AM3) production environment
- Munich, DE (MU4) disaster recovery environment

Separate test and development environments are operated in the OpenText data center in Brook Park, Ohio.

Platform backing services

Core applications leverage OCP Foundation and Platform Backing Services. These Backing Services, along with Cloud Foundry form the OpenText Platform as a Service (PaaS) layer, which sits on top of the infrastructure layer.

Some of these backing services are:

- Cassandra (NoSQL)
- Graylog (logging)
- Apigee (API management)
- Solr (search)
- PostgresQL (database service)
- Kafka, RabbitMQ (messaging, eventing)

Service level agreements (SLAs)

Incident response

OpenText makes a commitment to not only respond to service requests promptly and regularly report on their status, but to also restore service to affected users within a specific period of time following a service incident. Service restoration time objectives are linked to incident severity. Restoration may take the form of a root cause resolution or application of a workaround that enables users to access the system while troubleshooting and implementation of a permanent solution continues.

Disaster recovery

If OpenText declares a disaster event that impacts delivery of the OCP applications or services from the primary data center facility, OpenText will restore service in the designated alternate facility for that data center region. The target Recovery Time Objective (RTO) following an OpenText declared disaster is 72 hours and the target Recovery Point Objective (RPO) is 4 hours.

Availability

Availability SLAs may vary by type of cloud service being provided, however, the following is standard guidance for application SLAs:

- Availability is measured monthly and excludes scheduled downtime.
- 99.9% high availability with redundancy of major solution components is the targeted duration of time and a service level within which a service must be restored after a disaster (or disruption).
- Current RTO = 72 hours
- Recovery Point Objective (RPO) is the age of files/data that must be recovered for normal operations to resume in the event of disaster or disruption.
- Current RPO = 4 hours

Maintenance

Upgrade and patching of the backing data and infrastructure components of OCP occurs during a standard maintenance window Friday 21:00-2:00 EST for the North America data center and Saturday 2:00-6:00 UTC for the EMEA data center.

During this scheduled maintenance window, the platform may be partially or completely unavailable.

Recovery

In the event of the loss of the primary data center, the datastores replicated to the secondary data center are mounted and made accessible. The Domain Name System (DNS) is updated to point to the secondary site instead of the primary site. The BOSH director is bootstrapped into the secondary data center using the saved configuration files, stemcells and binaries. After the director has been bootstrapped in the secondary site, all of the VMs deployed by the director are recreated using the director's saved configuration data and identical stemcells. Once all of the BOSH VMs are recreated, the apps and services are started in the secondary site. After the apps and services have been started, the secondary site is promoted to the primary site. The original primary site becomes the new secondary site once access to the facility is restored.

OpenText provides a disaster recovery service to customers to ensure the continuity of cloud services in a disaster situation (as declared by OpenText in accordance with the company's disaster recovery policies and procedures). The disaster recovery service will be used to reinstate production instance service levels by failing over to a secondary data center employing redundant facilities, systems, networks, hardware and software.

The most recent available backups of the production instance will be used to restore content. All recoverability services are designed to support the RTO and RPO specified in the Order. OpenText will test the applicable disaster recovery processes once annually to ensure technical and operational readiness.

Data retention

Various national and state laws require OpenText to maintain certain types of records for particular periods. Failure to maintain such records could subject OpenText and its personnel to penalties and fines. Applicable laws and regulations may also require that certain types of records be destroyed within an appropriate time period. This can include certain health-related data and personal privacy data of OpenText or its customers. In general, such regulations require that sensitive data be retained no longer than is necessary for the purpose for which the data was obtained.

All services and their stored data are backed up multiple times per day. Additionally, all OCP storage repositories have a three (3) month retention period.

Secure communication and file encryption

Secure file encryption in transit

Transport Layer Security (TLS) provides file encryption in transit between the user and OCP. The benefits of TLS include strong authentication, message privacy and integrity, as well as enabling the detection of message tampering, interception and forgery.

Secure file encryption at rest

OCP Content Storage is protected via Data Encryption Keys (DEK) as well as Role Based Access Control (RBAC) to protect the DEKs themselves. Every piece of content ingested into OCP is secured and protected. Hardware key management is also employed to encrypt data.

Security scanning

Digital reputations and signature recognition are used to detect threats and prevent malicious content from being uploaded to OCP.

Geo blocking

OpenText commercial environments are protected with next generation and advanced threat prevention firewalls that have extended capabilities beyond traditional security access lists, including the ability to restrict certain countries' access to the environments based on geo protection. This mechanism allows the firewalls to maintain a database that maps IP addresses to countries, satellite providers and anonymous proxies. This database is updated periodically based on different sources and IP intelligence feeds. The mechanism to implement such protection is similar to a traditional access list, with the ability to block certain countries as a source, as a destination or both.

OpenText commercial environments are currently blocking the following embargoed countries from access: Cuba, Sudan, North Korea, Venezuela, Russia and Iran.

User-level security

Enterprise users need to collaborate with others both within and outside the organization without security concerns hampering productivity. OCP's robust security infrastructure and advanced yet simple security controls allow users to work productively without hassle.

When collaborating in OCP, users can protect content by specifying permissions at a granular level, for example, allowing certain users "view only" access while giving others the ability to modify.

Enterprises can leverage existing single sign-on (SSO and SAML) infrastructure, so users don't need to remember another username and password. These user-level features allow businesses to strike the appropriate balance between productivity and IT control with minimal maintenance overhead.

Network security

OCP provides multiple solutions to address network security threats as information flows back and forth from datacenters to customer and third-party systems. OCP monitors its entire network, including the production application and underlying infrastructure components at all times. Realtime alerts are sent to on-call operations staff members for resolution and all incoming and outgoing traffic between the production environment and other networks—corporate and untrusted—is monitored by ISP-grade firewalls.

To protect the systems from DoS/DDoS (denial of service) attacks and ensure availability, OCP employs carrier-grade network equipment and redundant internet links. To ensure the reliability of the network infrastructure against increasingly sophisticated hacking methods, OCP performs weekly vulnerability scans and engages third-party security firms to perform penetration and application vulnerability testing.

Application security

The OCP application is designed with security as a key consideration at every stage. The web application is multi-tiered into logical segments (front-end, mid-tier and database). This provides maximum protection while giving developers the flexibility of a multi-layer architecture.

The OCP application development goes through multiple checks and balances to ensure that development or testing processes do not impact the production systems and data. These checks include putting every change through a formal release engineering process, maintaining physically and logically separated

development environments and performing full functional testing of all changes in a QA environment before deployment to production. Following this rigorous development and release process allows OpenText to deliver new features and improvements while maintaining a solid and secure foundation.

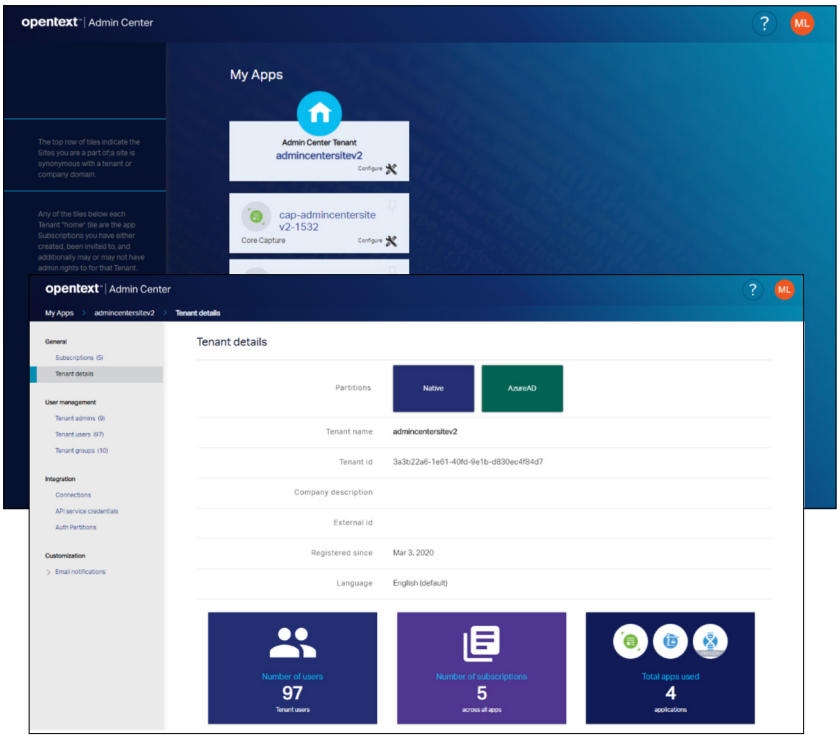
Data security

Other sharing and collaboration tools lack data encryption, allowing hackers to sniff packets out of the network and directly intercept the data. OCP encrypts data in transit by providing up to 256-bit AES encryption along with support for forward secrecy, ensuring that deciphering intercepted information is impossible now and in the future. 256-bit AES encryption and dynamic key management ensure every access is logged, providing full auditing. OCP also uses redundant encrypted storage, meaning that copies of every file are stored in multiple data centers to safeguard against data loss.

Admin Center

Admin Center is the management console for OCP administration. Admin Center provides customer administrators with a single control point to configure OCP applications, users, integrations with other OCP applications or on-premises systems and view reports on the applications and users. Using Admin Center, administrators manage:

- Users and groups
- Authentication and authorization platforms, either built into OCP or via SAML authentication integration
- Password and two-factor authentication policies (for native OCP authentication)
- Application role management
- API integration management



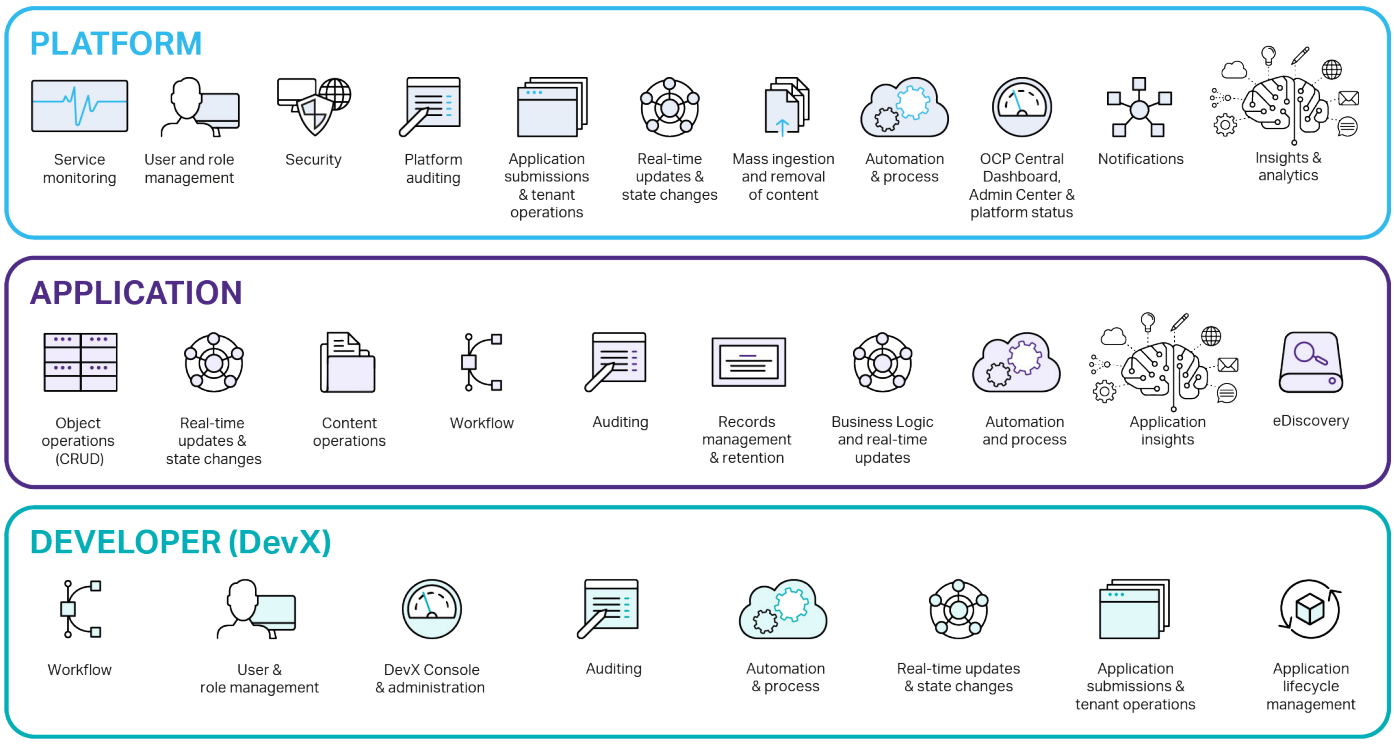
opentext™

Authentication, authorization and user synchronization

OCP authentication (AuthZ), authorization (AuthN) and user synchronization are provided by internal and heavily integrated OTDS. Leveraging OTDS, the platform is capable of handling all industry standards including Oauth, SAML, OpenID Connect and Multi-Factor Authentication. Additionally, OCP also supports third-party cloud providers such as AzureAD, Ping and Okta. This is accomplished by OTDS support of the SCIM provisioning standard. All AuthZ, AuthN and user synchronization is provided via Admin Center.

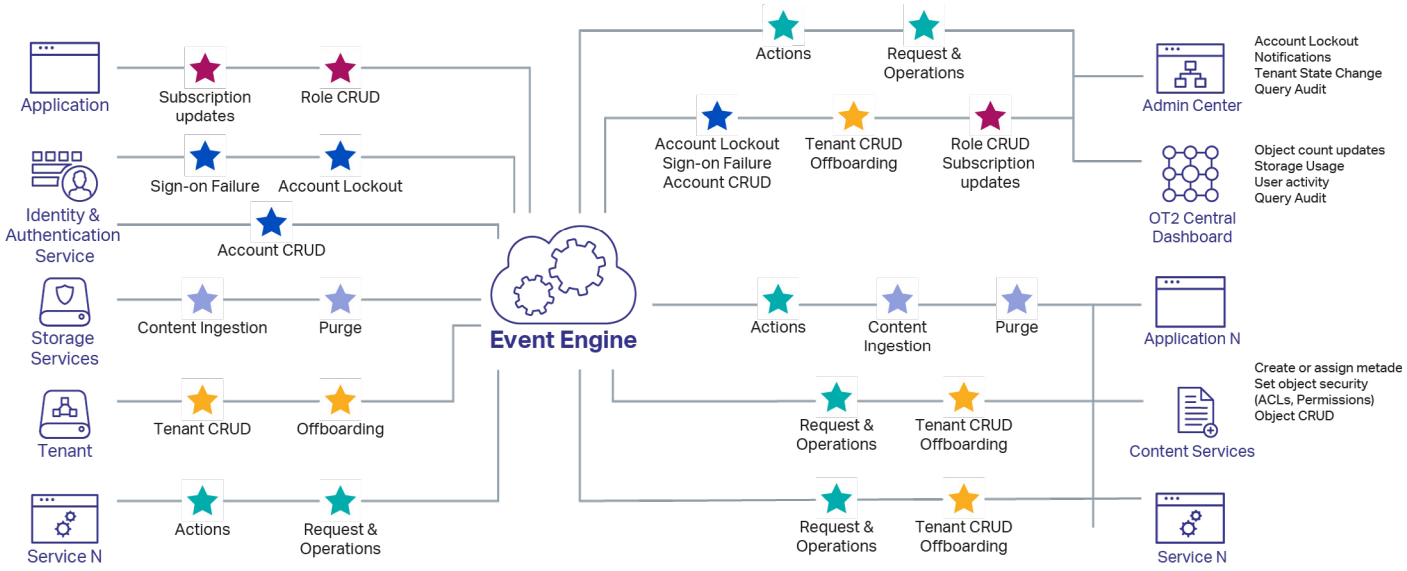
Auditing and eventing

Modern day IoT, communications, housekeeping and analytic architectures depend on and use event frameworks at their core. Event-driven architecture decouples service to service communication and relies on a common microservice approach. Decoupling of service integration allows for independent scaling and minimizes impact of failures. Audits are handled automatically via direct integration into the OCP eventing subsystem. This requires no direct integration between other services with audit. On-demand push-based architecture allows for reactive operations without continuous polling needed, resulting in lower costs and higher efficiency.



OCP eventing is a feature rich subscription and consumption framework that allows for the creation of any event at any time with any information. Those events can then be consumed by any service or application deployed on OCP or hybrid. OCP eventing offers the ability to build customized business logic and triggers tailored directly to business requirements and use cases. Once an integration has been completed no additional maintenance is required to uphold said integration.

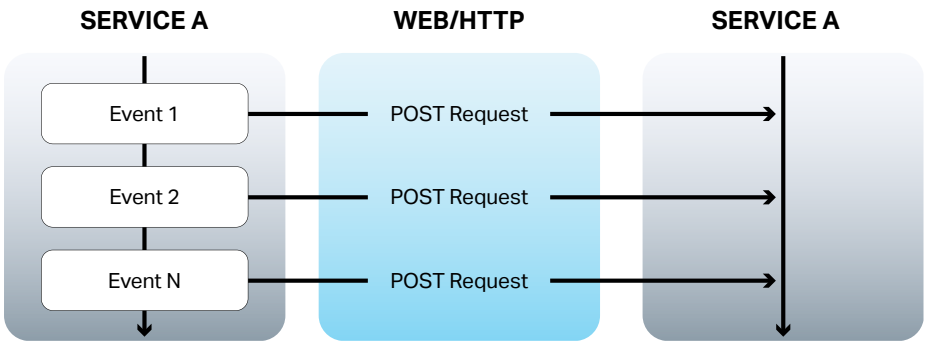
Furthermore, communications are dynamic and asynchronous, allowing for tasks and jobs to be completed after the request has been made. There are no API dependencies on versioning, further decoupling service to service communications. This reduces the dependency on API changes of consuming services as no direct integration is required.



Platform, security and inter-service communications (Bi-directional)

Webhook support

Webhooks provide and allow for realtime status and reactions via HTTP web requests. This removes the requirement for redundant status requests, queries and unnecessary polling.



opentext™

Compliance and governance

OpenText is committed to customer success and protecting client information through both product design and the definition and application of policies that govern delivery of those products as cloud services.

The General Data Protection Regulation (GDPR) is considered to be the toughest privacy and security law in the world. OCP is GDPR compliant, providing protection for personal data, the data subject, the data controller and the data processor, as well as any action or processing of the data. OCP upholds PII and data sovereignty standards and customer data is not directly accessible by OpenText.

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
- Twitter | LinkedIn

opentext.com/contact