



Application architecture, infrastructure and security

An in-depth look at the technology and procedures
that power and manage the delivery of services from
Sitecore® OrderCloud®

Table of contents

Platform architecture	3
Infrastructure overview	4
Infrastructure diagram	5
Sitecore® SDLC and release management	6
Azure cloud	6
Security	8
Information security policy	9
Credit card processing on Sitecore OrderCloud®	10
Incident response plan	11
Incident types	11
Incident discovery	11
Data recovery	12
Scheduled maintenance	12
Scope	12
Contact	12

+ + + + +

+ + + + +

+ + + + +

+ + + + +

+ + + + +

Platform architecture

Sitecore® OrderCloud® is a “headless” B2B e-commerce and order management platform delivered as a cloud service and exposed entirely via a REST API.

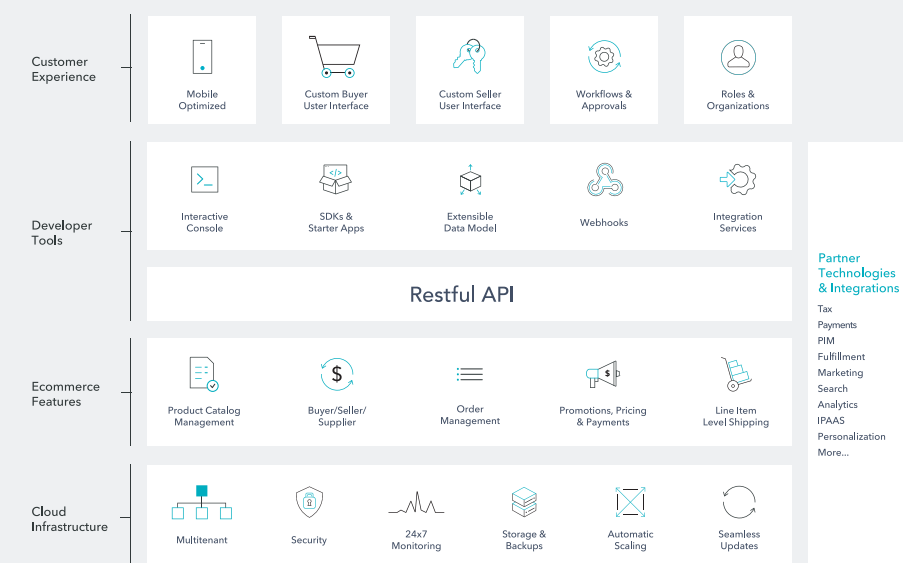
Always delivered over HTTPS, with CORS enabled, the RESTful API enables modern standards-based interoperability with other computer systems on the Internet. Each Sitecore OrderCloud® resource represents a uniform and predefined set of stateless operations that elicit an HTTP response that may be accompanied with a JSON object. Every resource endpoint is predefined by a common set of HTTP verbs: GET, POST, PUT, DELETE and PATCH and are accompanied by robust error responses.

Sitecore OrderCloud® documentation, located at <https://ordercloud.io>, is managed through the publishing of the OpenAPI or Swagger specification. This definition effectively maps all the resources and operations associated with the API. The Swagger specification is the basis of the public documentation and auto-generation of all development tools and SDKs.

The Sitecore OrderCloud® API supports many additional specifications and strategies. Authentication is exposed through the OAuth 2.0 open standard. It allows four different workflows, all of which use a command method and request URL.

Webhooks, or HTTP push API, are a concept that provides a way to deliver other applications real-time information through events. Unlike typical APIs there is no need to poll for data. Sitecore OrderCloud® supports webhooks on every resource endpoint exposed and allows for multiple configurations per endpoint.

Sitecore OrdeCloud Platform Architecture



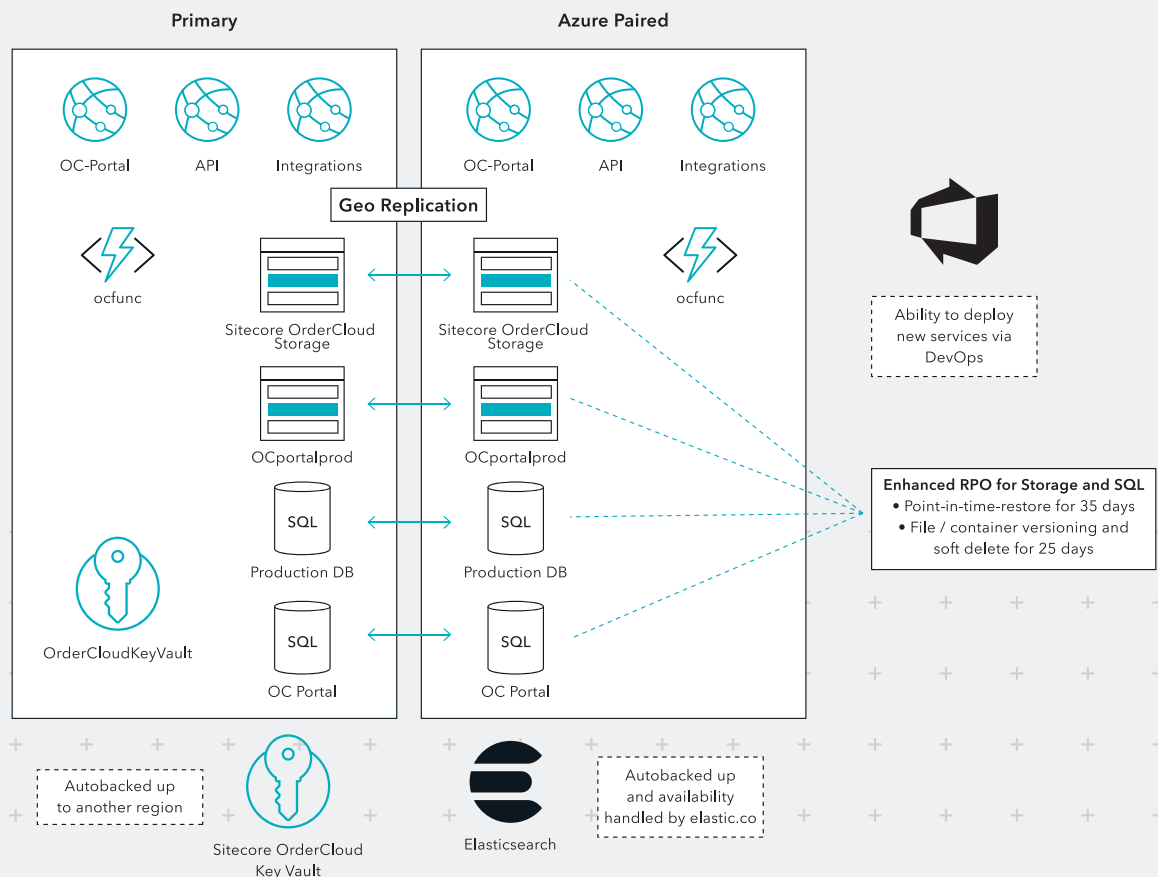
Infrastructure overview

Sitecore OrderCloud is fully hosted on the Microsoft Azure Platform. Azure and the combination of its services provides the reliability, scalability and security expected of all business applications. Sitecore builds its platform on Azure services which do not rely on any virtual machines Sitecore manages. The ability to rely on services allow Sitecore ultimate flexibility to scale up and down based on load as well as the ability to migrate services to other regions quickly. Virtual machines (VM) are only used to host Sitecore's SIEM system as well as a VM used as part of the deployment process. The deployment server is only running while testing or performing a release. Security for the VM follows the standards put forth by SOC, PCI and ISO and is enforced and monitored via the Azure Security Center.

Sitecore OrderCloud utilizes the Azure SQL Database service to fulfill the multi-tenant architecture of the application. The SQL Database service delivers predictable performance at multiple service levels including dynamic scalability with no downtime, built-in business continuity and data protection. Sitecore utilizes Azure's SQL geo-replication service to replicate data from the primary region to the Azure paired region. This has a RPO of 15 minutes. For example, in the event of a disaster that results in data loss in Azure US West, Sitecore would be able to rely on data being backed up in the US East region. All SQL databases also have Azure TDE enabled to perform encryption in the environment.

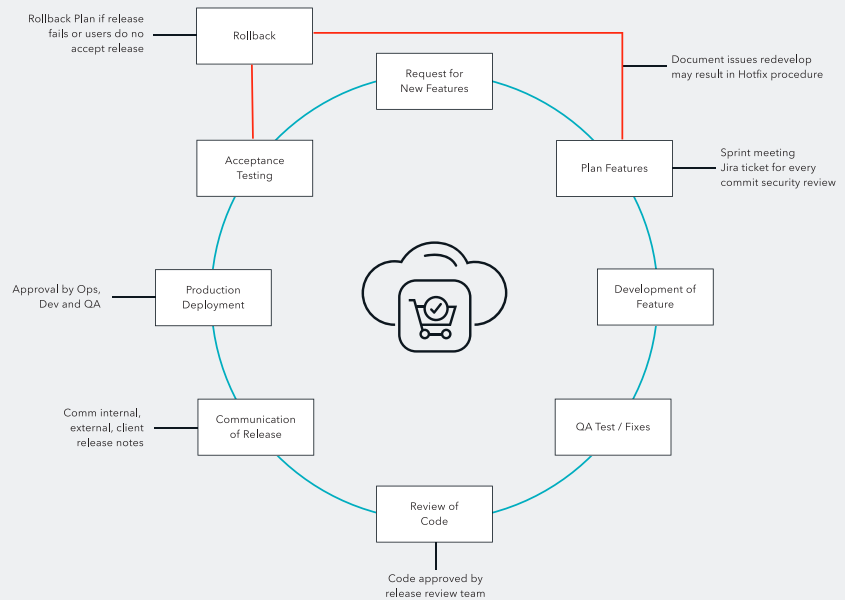
Security is enforced via Azure Security Center which tracks, monitors and alerts on irregular behavior in Azure or insecure settings across apps, storage blobs, SQL, active directory, etc. Sitecore also conducts monthly vulnerability scans via Rapid 7 SecOps. Any results from a test are logged and reviewed by the security team. Sitecore also utilizes AT&T Cybersecurity\Alienvault as a SIEM system on Sitecore OrderCloud. Alienvault monitors all traffic across the environment and performs intruder detection (IDS), file integrity monitoring and alerting of unusual behavior. Sitecore also subscribes to Alienvault's OTX community which monitors and provides intelligence on up to date threats.

Sitecore OrderCloud uses Rapid7 InsightOps for log management and searching functionality. InsightOps monitors system performance and helps assist and troubleshoot any errors or reliability problems being experienced on the system. OrderCloud® utilizes the Azure App Service to host the API and Integration services. App Services provide the automated scalability, security and reliability expected for a first class business application. Additionally, they provide the capability for continuous deployment, debugging and diagnostic tools necessary to maintain a healthy API service.



Sitecore® OrderCloud® SDLC and release management

Sitecore follows a standard software development life cycle seen in the image below. All releases are tested, code reviewed and communication provided (if needed) prior to deployment.



For Hotfix/emergency release:

- Documentation and communication can be bypassed and performed retroactively.
- Approvals / QA may also be overruled if teams are not available.
- Post a hotfix/emergency release that the standard procedure is not followed. Operations team will confirm proper documentation and confirm situation was deemed "Hotfix/emergency necessary"

Azure Cloud

Azure's cloud platform is one of the most advanced, safe and secure platforms available. With the ability to scale up, diversify and backup data to multiple facilities data is protected and reliability high. As of July 2019 Azure's core compute services have run at a 99.995% average across its global infrastructure.

Azure supports more than 90 compliance certifications, including over 50 specific to global regions and countries, such as the US, the European Union, Germany, Japan, the United Kingdom, India, and China. And, get more than 35 compliance offerings specific to the needs of key industries, including health, government, finance, education, manufacturing, and media. Emerging compliance needs are covered, too: Microsoft engages globally with governments, regulators, standards bodies, and non-governmental organizations. These compliances include PCI, SOC, ISO 27001, HIPAA, CCPA, etc.

Azure DevOps

Sitecore OrderCloud utilizes Azure DevOps for deployments and version management. Using slot swaps, deployments are instantaneous and no downtime is experienced. Sitecore SDLC prevents code from being deployed without proper testing. And a release must be accepted by certain members of Sitecore prior to the actual release happening.

Azure diagnostics

Azure diagnostics is used to monitor all Azure services. With basic logs Sitecore can monitor that the applications are acting appropriately and proactively deal with any potential issues. Proper monitoring and alerting is set up to notify staff in event of errors.

Azure PCI

Microsoft Azure completes an annual PCI DSS assessment using an approved Qualified Security Assessor (QSA). The auditor reviews the Azure environment, which includes validating the infrastructure, development, operations, management, support, and in-scope services. The PCI DSS designates four levels of compliance based on transaction volume. Azure is certified as compliant under PCI DSS version 3.2 at Service Provider Level 1 (the highest volume of transactions—more than 6 million a year).

The assessment results in an Attestation of Compliance (AoC) and Report on Compliance (RoC) issued by the QSA. The effective period for compliance begins upon passing the audit and receiving the AoC from the assessor, and ends one year from the date the AoC is signed. The AoC is available to customers to show the QSA has determined that Azure is in compliance with PCI DSS v3.2.

Customers who want to develop a cardholder environment or card processing service can leverage the Azure validation in many of the underlying portions, thereby reducing the associated effort and costs of getting their own PCI DSS certification.

Azure redundancy

Azure has built in backup for all resources and services. SQL data and storage data is geo-replicated from Azure primary to Azure paired backup (ex: US West to US East). For storage, soft delete and file versioning is retained for 35 days. All data is also replicated multiple times within a region to reduce the risk of data loss.

Azure security

Azure provides a security center to all tenants for recommendations or potential problems on the system. Azure invests over one billion US dollars annually in cybersecurity research and development. Employs over 3500 security experts focused on security data and privacy and has more certifications than any other cloud provider.

Security

Sitecore understands that security remains a primary concern of our customers. All API traffic is restricted to be sent only over HTTPS and is secured with SSL. Network participants' information is protected by maintaining CCPA, GDPR and SOC2 compliance, a privacy policy and a secure application-hosting environment.

Sitecore as a company is SOC2 Type2 which means a 3rd party audits all controls and procedures. A copy of Sitecore's SOC audit is available with permission from the security manager and a signed NDA. In addition, independent customer solicited security questionnaires and penetration tests have been performed verifying that the company:

Builds and maintains a secure network

- Default deny all on network connections. Sitecore OrderCloud relies on Azure access lists to control access to applications and services.
- Does not use vendor-supplied defaults for system passwords and other security parameters
- Production environment network is restricted to office IP address or Sitecore VPN

Protects data

- Ordercloud only stores credit card tokens
- Encrypts transmission of cardholder data and sensitive information across public networks
- Strong passwords are required to access the database
- Databases utilize Azure Transparent Data Encryption (TDE)
- Implementation of Azure zone redundant configuration for databases
- Sitecore developers are trained yearly on secure coding practices
- Databases utilize Azure point in time restore to allow restoration of data anytime in the last 35 days
- Storage accounts have file versioning and soft delete enabled to protect data
- Production databases and storage accounts are geo-replicated to a secondary region

Implements strong access control measures

- Restricts access to data by business need-to-know
- Assigns a unique ID to each person with computer access
- Restricts physical and virtual access to cardholder data
- Change management and development life cycle policies are in place and followed when deploying code or infrastructure changes
- Multi-factor Authentication (MFA) enforced via Azure Active Directory
- Azure security center monitors correct Azure policies

Regularly monitors and tests networks

- Rapid7 continuously monitors and alerts for API performance, availability, and errors.
- AT&T Cybersecurity\Alienvault SIEM System monitors all traffic and logs on the system
- Azure Security center verifies all applications, DBs, etc are within compliance
- Regularly test security systems and processes
- Rapid7 SecOps vulnerability scans the OC API weekly

Maintains an information security policy

- Maintains a policy that addresses information security

+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Information Security Policy

TABLE OF CONTENTS (Sample Only)

Introduction	Server Configuration Policy - DB
Information Security Team Roles and Responsibilities	Server Configuration Policy - Web Server
Acceptable Use Policy	Server Malware Protection Policy
Access Control Policy	Server Security Policy
Access Request Form	Testing and Deployment Procedures Policy
Analog Line/Fax Security Policy	Third Party Network Connection Agreement
Anti-Virus Policy	Virtual Private Network (VPN) Policy
Application Service Providers (ASP) Policy	Wireless Communication Policy
ASP Security Standards	Wireless Communication Standard
Audit Vulnerability Scan Policy	Change History
Background Check Policy	
Background Check Authorization Form	
Backup Policy	
Change Management Policy	
Change Management Form	
Credit Card Handling Policy	
Data Retention Policy	
DB Password Policy	
Email Automatic Forwarding Policy	
Email Use Policy	
Email Retention Policy	
Employee Exit Procedure Policy	
Encryption Policy	
Ethics Policy	
Extranet Policy	
Firewall and Router Configuration Policy	
Sitecore Application Access	
Incident Response Plan	
Information Sensitivity Policy	
Internet DMZ Equipment Policy	
Password Policy	
PCI Compliance Notification	
Personal Communication Devices and Voicemail Policy	
Remote Access Policy	
Remote Access Device Policy	
Risk Assessment Policy	
Router Security Policy	
Security Awareness Policy	

Credit Card Processing on Sitecore OrderCloud

Sitecore OrderCloud supports credit card transaction processing only through specific integrations that have been created separately from the API platform.

Payments by credit card are supported by an Sitecore OrderCloud integration service using Authorize.Net API services. All credit card information is only passed through the integration layer directly to the Authorize.Net payment facility and never stored on any system or database belonging to the Sitecore OrderCloud API platform.

Sitecore OrderCloud supports storing credit card information for reuse, but is restricted to the general tokenization strategy of the credit card merchant. This strategy completely removes the need to store credit card data. Tokens have no meaning by themselves and are worthless to criminals if the system is breached in any way. Additionally, Sitecore OrderCloud API supports elevated security claims that restrict the ability to store the credit card token to prevent abuse and unauthorized access.

Supported integrations, such as Authorize.Net, have several elevated security procedures. First, a proxy is available to store the merchant account authentication credentials. Secondly, the API endpoint for saving the tokenized credit card requires elevated security claims. Lastly, traffic between the integration endpoint and the proxy are through a private tunnel, not over the internet.

Incident Response Plan

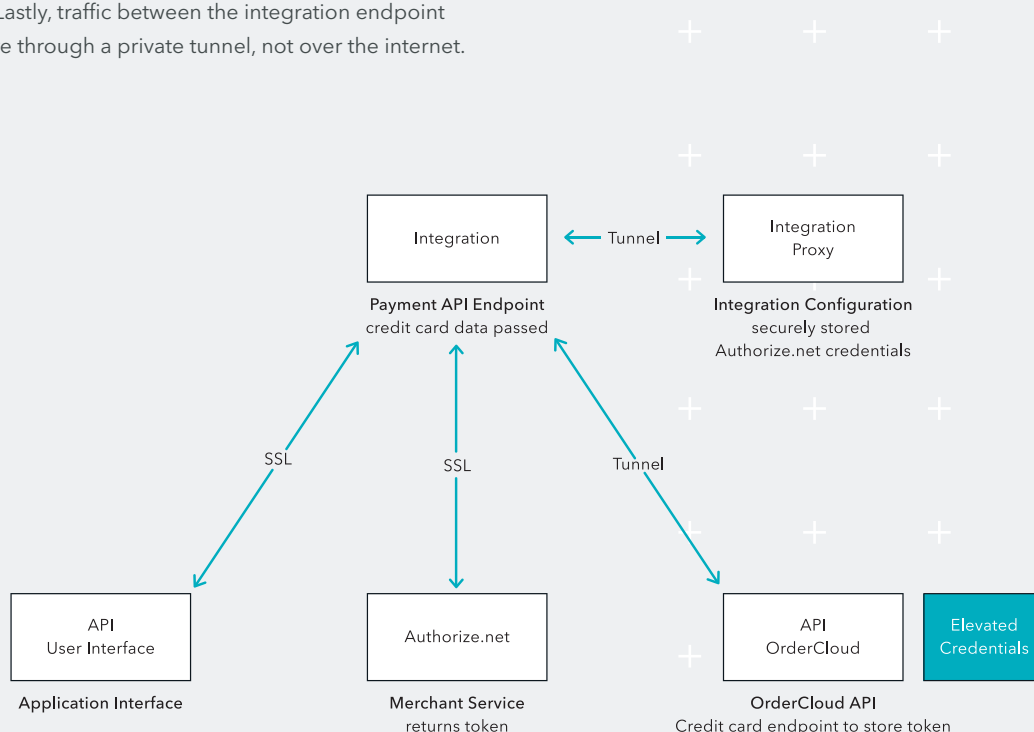
The Sitecore incident response plan specifies a process for discovering, remediating, and reporting incidents of application failure or a breach of security.

Incident Types

Application service failures | Breach of personal information | Denial of service | Excessive port scans | Firewall breach | Misuse of service | System failures | Virus outbreak | Storage capacity | Unauthorized Wireless access point | System attach or compromise

Incident Discovery

- Monitor application and supporting services for log irregularities, performance and uptime
- Monitor Cisco, Open Web Application Security Project (OWASP) and Microsoft Technet advisories for software hardware patches, security industry advisories and security alerts
- Azure diagnostics monitors all SQL logs for irregularities and alerts staff to potential security issues
- Monitor physical access logs
- Schedule responsible personnel for incident response 24x7



Data Recovery

For the purposes of business continuity, Sitecore is able to restore backups of system data to any point in time within the last 35 days should a disaster occur. In addition, Sitecore can restore client data in the event of accidental data integrity issues or deletion. Data recovery is not included as part of the service agreement and will incur a per-incident fee proportional to time spent by engineers to recover the data, Customers should take proper precautions to protect their data from being destroyed. In the event data restoration is required, Sitecore will provide a quote within 1 business day of notification, with completion of the restoration within 3-5 business days unless quoted otherwise.

The agreed upon restored data will be returned to the customer in excel format.

- For security purposes no restored data will be placed into the production database by Sitecore.
- Client is responsible to place restored data back into production.
- Sitecore will NOT restore encrypted or hashed fields.

Scheduled Maintenance

Scheduled maintenance is a planned and deliberate event for the purpose of updating and/or performing maintenance. Azure service updates are performed seamlessly inside Azure with no downtime. Releases are performed using Azure DevOps. Deployments are performed using slot swaps and are instantaneous with no downtime.

Scope

This architecture guide is a reflection of how Sitecore OrderCloud itself is built, protected and redundant. Any application built on top of Sitecore OrderCloud may have different compliance requirements, statistics with uptime and redundancy. It is the responsibility of the application owner to know those statistics and to maintain any needed compliance for their application.

Contact

www.sitecore.com