SITECORE

WHITEPAPER

Sitecore Managed Cloud security overview

SEPTEMBER 2020

Table of contents

Introduction

At a time when customer experience matters more than ever, digital marketers need ways to deliver digital experiences at speed. Managed cloud services can help teams control and reduce cost, increase the flexibility and agility of back-end infrastructure systems, and optimize IT resources toward areas that deliver the highest benefit to the business. But before endorsing a move to a managed cloud offering, the IT department needs assurance that any new services are reliable and secure.

Sitecore® Managed Cloud is a hosting solution that meets the needs of both Marketing and IT. This whitepaper describes the information security model and practices that Sitecore follows for its managed cloud offerings, as well as the standards to which it adheres to help customers protect the confidentiality, integrity, and availability of their managed cloud resources and data.

Sitecore Managed Cloud overview

Sitecore Managed Cloud allows businesses to tap the power of cloud computing without the complexity of managing cloud infrastructure and application stacks themselves. This service actively monitors, manages, and maintains the installation of Sitecore Experience Cloud™ products, including Sitecore Experience Manager™ (XM), Sitecore Experience Platform™ (XP), and Sitecore Experience Commerce® (XC).

By combining the power of Sitecore's digital experience platform with the speed, scale, and reliability of Microsoft Azure, Sitecore Managed Cloud delivers services beyond the limits of an on-premises data center. Azure global infrastructure currently is available in 54 regions worldwide and 140 countries – more than any other cloud provider – offering the ability to reach your customers and partners on a global scale while preserving data residency and compliance boundaries.

Sitecore Managed Cloud is available in two tiers: Standard and Premium. Sitecore Managed Cloud Standard (MCS) builds on the Sitecore Azure Toolkit and includes the following features:

- Support for Sitecore XM, Sitecore XP, and Sitecore Experience Database™ (xDB)
- 99.9% availability on topology
- 24/7x365 infrastructure support and monitoring
- Dedicated Customer Success Manager, personal onboarding included
- Application-level and security monitoring
- Support for underlying infrastructure
- Access to Microsoft Premier Support via Sitecore (if purchased)
- SOLR, WAF, and CDN support
- Disaster recovery and database backup/restore
- Compatibility with on-premises environments

Sitecore Managed Cloud Premium (MCP) builds on these features with support for Sitecore Experience Commerce, emergency support response time in as little as 15 minutes, and the ability to deploy custom code and topologies.

Sitecore works with industry-leading technology companies to provide its hosting services. See Table 1 for an overview of these service providers and the scope of their services.

Managed Cloud	Standard	Premium
Product provider	Sitecore	Sitecore
Cloud operations provider	Sitecore	Rackspace
Platform provider	Microsoft (Azure)	Microsoft (Azure)
Database provider	Microsoft (Azure SQL)	Microsoft (Azure SQL)
Search Provider	SearchStax (SOLR)	Rackspace (SOLR)

Table 1. Managed Cloud Service providers

Sitecore Managed Cloud security model

The security model for Sitecore Managed Cloud provides our customers with control over information and resources, while ensuring all the benefits of a cloud deployment. Sitecore Managed Cloud security controls are based on the standards defined by the Cloud Security Alliance.[1] Sitecore customers have administrative-level access and the ability to make changes to the Managed Cloud environment, which can include changes to the application, data, and infrastructure layers.

Sitecore's customers will remain "data owners" throughout the Sitecore Managed Cloud customer relationship, and they will be responsible for the confidentiality, integrity, and availability of Sitecore Managed Cloud resources and data. Table 2 indicates the roles and responsibilities associated with the various security functions in Sitecore Managed Cloud. When Sitecore is responsible for certain activities, Sitecore or a partner may perform these actual processes for the customer.

[1] *https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview*

The chart below uses the coding system outlined here:

R = Responsible: Those who do the work to achieve the task.

A = Accountable: The one ultimately answerable for the correct and thorough completion of the deliverable or task and the one who delegates the work to those responsible

C = Consulted: Those whose opinions are sought (i.e. subject matter experts) and with whom there is two-way communication.

I = Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable.

	Customer **(or Partner)**	**Sitecore** **(including service providers)**
Base application security	I	R, A
Deployment and security hardening	R, A	C
Implementation of authentication mechanism	R, A	C
User access administration	C	R, A
Configuring encryption at rest and in motion	R, A	C
Encryption key upload (Azure Key vault)	R, A	I
Custom code deployment	R, A	C
Change management	R, A	C
Configuring application security logging	R, A	I
Configuring infrastructure security logging	I	R, A
Monitoring for application security events and notification	R, A	C
Monitoring for infrastructure security events and notification	I	R, A
Monitoring for data-related security events and notification	R, A	C
Monitoring for infrastructure resource availability	C	R, A
Configure and perform disaster recovery	C, I	R, A
Configure high availability	R, A	C
Configure host security - hardened OS	I	R, A
Configure network security	R, A	C

Customer responsibilities

While Sitecore strives to provide the most secure services possible, our customers remain responsible for the following tasks:

- Ensuring users are given appropriate access levels.
- Ensuring that any changes to the customer's own environment retains the security level provided by Sitecore Managed Cloud, such as maintaining proper access control of user credentials and conducting security testing of their own custom code.
- In Managed Cloud, we recognize the best practice of a web application firewall or comparable security solution. Both MCS and MCP have provisions for working with customers on the implementation of a WAF with their Sitecore solution. Ultimately, fine tuning of WAF rules and close monitoring of traffic is the responsibility of the customer and/or their partner.

Certifications and compliance

Microsoft: Sitecore Managed Cloud offerings are hosted on Microsoft's Azure platform-as-a-service (PaaS) infrastructure. Microsoft Azure is recognized as a leader in Gartner's Magic Quadrant for cloud computing services.[2] Microsoft's Azure services are compliant with global information security and privacy standards. For a full list of the certifications and security compliance for Azure, please visit Microsoft's Trust Center.[3]

Sitecore: Sitecore Managed Cloud offerings are compliant with the following globally accepted information security and privacy standards:[4] ISO 27001, ISO 27017, ISO 27018, CSA STAR, Privacy Shield. We also obtain a SOC2 report from an independent third-party auditor. The scope of the compliance includes people, processes, and technologies used to deliver cloud-based services to our customers. This includes the following products:

- Sitecore® Experience Manager™
- Sitecore® Experience Platform™
- Sitecore Experience Commerce™
- Sitecore Email Cloud

For details of our current certifications, please refer to our Trust Center here.

Complying with privacy and data protections laws (including GDPR and CCPA)

At Sitecore, we understand both the value of data and the importance of protecting it. Privacy and data protection laws are changing quickly to protect personal information, and we know that our customers are adapting to these requirements so they can keep their customers' data safe.

In the case of Sitecore Managed Cloud, we process the data that we receive from our customers. In GDPR parlance, we are a "Data Processor." Under the CCPA, we are "Service Provider." Accordingly we have Data Processor Agreements with the relevant clauses in place with our customers to ensure compliance and set forth the respective obligations between Sitecore and our customers. The following is a list of some of the global privacy initiatives that Sitecore has implemented to date:

- Defining enterprise governance for privacy, supported by relevant policies and standard operating procedures to respond to requests to exercise privacy rights under applicable laws.
- Mandatory privacy awareness training for all Sitecore personnel (employees and contractors).
- Performing applicable background checks on employees before they are hired.
- Maintaining records of all data (including personal data and personal information) processed by Sitecore and our sub-processors/ sub-service providers.
- Leveraging our Information Security Risk Assessment Program, performing Privacy Impact Assessments where appropriate to identify risks and find appropriate solutions to remediate or mitigate them.
- Incorporating "privacy by design" principles into our software development practices.
- Maintaining an incident response process to be used while responding to security incidents including adopting an incident response plan and taking steps for incident readiness such as tabletop exercises and phishing prevention strategies.

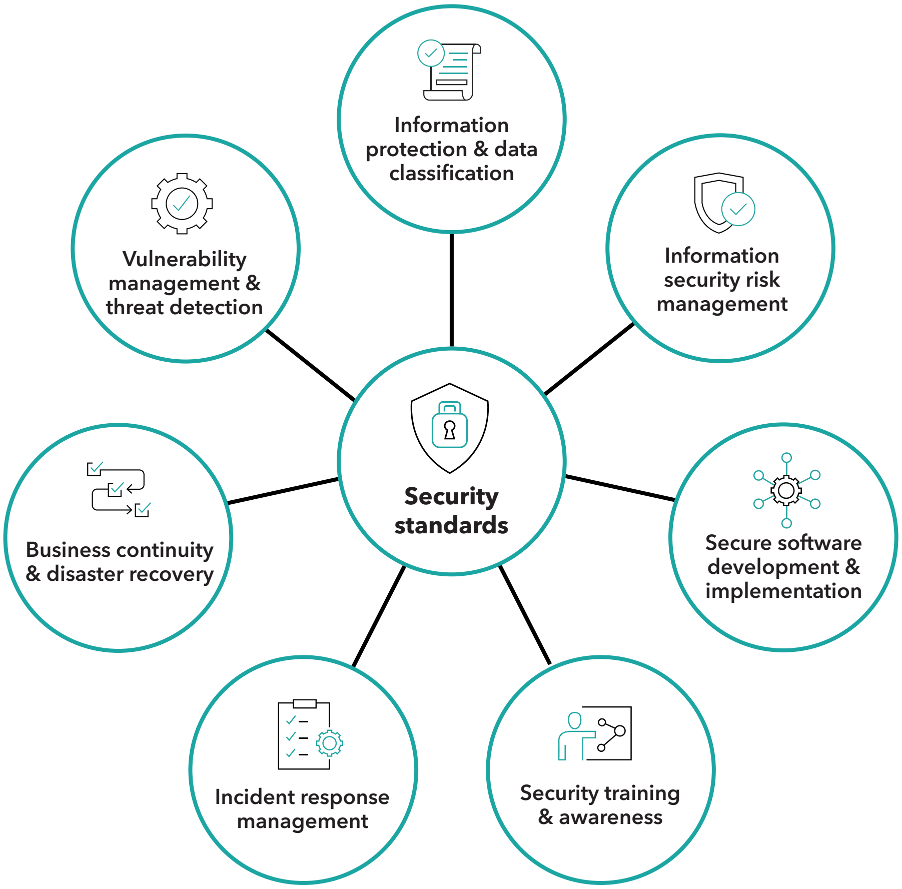
For for more information please visit our Trust Center here.

Sitecore's information security program

Sitecore has an established enterprise information security program to protect the Sitecore environment used to provide services to Sitecore customers, whether those assets are stored in Sitecore data centers or the managed cloud.

The program encompasses seven components:

1. Information Protection and Data Classification
2. Information Security Risk Management
3. Secure Software Development and Implementation
4. Security Training and Awareness
5. Incident Response Management
6. Business Continuity and Disaster Recovery
7. Vulnerability Management and Threat Detection


Information protection & data classification
Vulnerability management & threat detection
Information security risk management
Security standards
Business continuity & disaster recovery
Secure software development & implementation
Incident response management
Security training & awareness

1. Information protection and data classification

Both Sitecore Managed Cloud Standard and Premium services use dedicated compute cloud resources. Additionally, Managed Cloud resources are isolated from Sitecore's internal network, which includes the test and development environments. Customer information is not used for testing or development purposes outside of our customer-support process.

To manage and protect information received, Sitecore defines the following data classification levels:

- **Highly Confidential or Sensitive** – includes sensitive information as well as critical intellectual property.
- **Confidential** – includes customer-provided information, source code, contracts, and customer and partner lists.
- **Public** – includes press releases and marketing announcements.

Where technically feasible, Sitecore encrypts Highly Confidential and Confidential information at rest and in motion.

2. Information security risk management

Sitecore has defined and operates a formal, ongoing security assessment program that includes assessment of security standards of:

- Sitecore's IT assets.
- Sitecore's cloud-based assets.
- Service providers who have access to Sitecore systems and data.
- Sitecore facilities that are used to conduct business.
- Business risks and review of compliance obligations.

The information security risk management segment of the program includes security assessment activities to identify information security risks to Sitecore's data and systems, the controls that are used to mitigate risk, and the residual risks that need to be managed through enterprise information security governance.

3. Secure software development and implementation

Sitecore has defined and is continually enhancing its existing secure software development lifecycle and associated processes. This includes secure design, secure coding, and improved vulnerability assessment and penetration testing of software products.

4. Security training

Sitecore requires its employees and contractors to complete security awareness training, which includes training on information security risks, recommended control practices, and Sitecore policies. Additionally, Sitecore requires role-based and additional security training for employees involved in software design and development, which includes secure coding and penetration testing.

5. Security incident response

Sitecore maintains a formal security incident response process to manage incident detection, response, remediation/mitigation, and, where appropriate, communication.

6. Business continuity and disaster recovery

Enterprise
Sitecore has defined a formal disaster recovery strategy for our IT systems that are used to provide services to customers, including geo-replication. Additionally, Sitecore has a tested disaster recovery plan.

Managed Cloud
Sitecore has developed a disaster recovery service for our managed cloud environment, which is an add-on service that customers will need to purchase. The service includes two options:

- Basic DR provides a means to recover from a failure of the XM or XP default Sitecore Topology by backing up essential resources created during setup, and then recreating the environment on-demand in another location by restoring the databases via the SQL Backups and using Azure Traffic Manager to route the traffic to the secondary site.
- Managed DR (Hot Standby) is a means to recover from a failure of the XM or XP default Sitecore Topology by using an alternative environment that is already running and prepared to be promoted to be the replacement using Azure SQL Replication. Failing over is automated, providing a quick and efficient process to restore application uptime.

Sitecore has defined Microsoft Azure Resource Manager (ARM) templates and Azure Container Registry (ACR) images that are used by Sitecore customers and Sitecore's implementation partners to deploy a resilient instance of each Managed Cloud solution. In additional, Customers can monitor the availability of their Managed Cloud sites on the Sitecore (for MCS) or Rackspace (for MCP) support portal.

7. Vulnerability management

Sitecore has a formal vulnerability management program to identify and remediate vulnerabilities in the systems that are used to provide services to customers. Sitecore leverages industry-leading automated vulnerability scanning tools for this purpose.

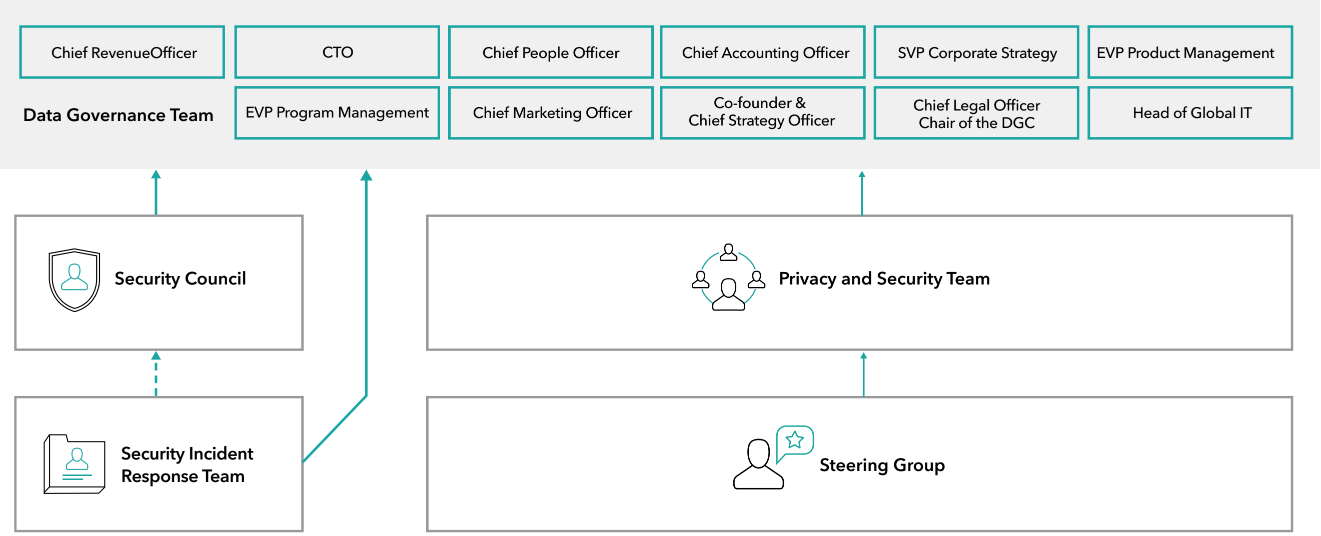
Additional protections for the cloud environment

Employee security: Where local laws accommodate, Sitecore performs background checks on all employees, including Sitecore's Cloud Operations Team, prior to employment. The background checks include Criminal, Education, and Employment. Additionally, as part of the interview process, Cloud Operations personnel are required to participate in a mandatory technical evaluation.

Formal cloud operations: Sitecore's Cloud Operations procedures include formal standards for the following:

- Customer onboarding, including the creation of user accounts
- Infrastructure resource creation and set-up
- Data creation and set-up
- Disposal standards to securely delete infrastructure resources
- Data disposal standards
- Capacity management to identify capacity and availability-related issues
- Issues and event management

Sitecore's security organization



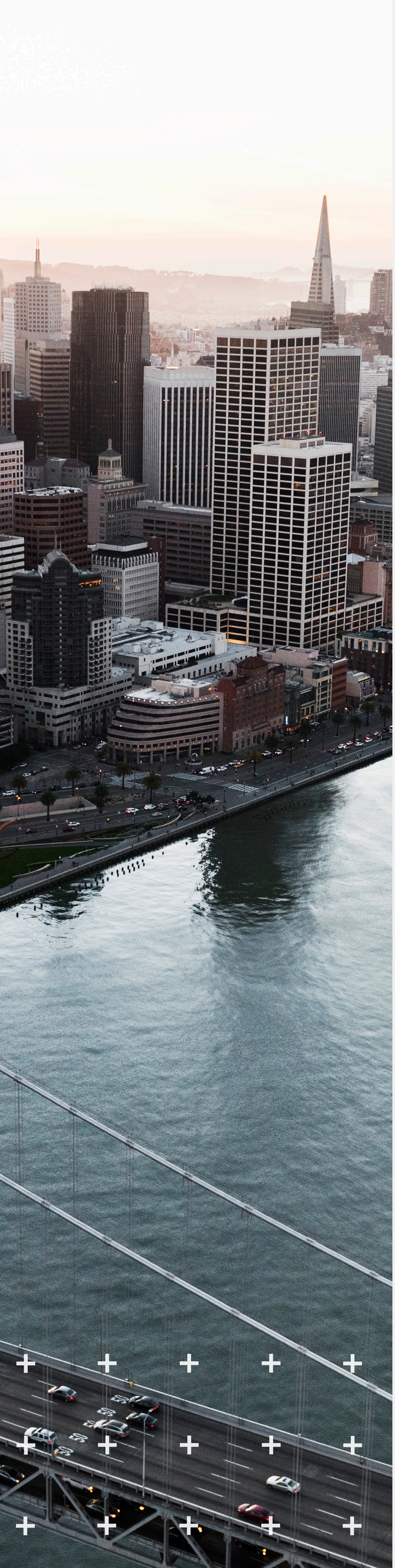
Chief RevenueOfficer	CTO	Chief People Officer	Chief Accounting Officer	SVP Corporate Strategy	EVP Product Management
Data Governance Team	EVP Program Management	Chief Marketing Officer	Co-founder & Chief Strategy Officer	Chief Legal Officer Chair of the DGC	Head of Global IT

Security Council

Privacy and Security Team

Security Incident Response Team

Steering Group



Why trust in Sitecore?

We've built our company on strong values, which include integrity and customer service. Our mantra is "customer delight." And we've always believed that a security-first and privacy-first culture is critical for our customer and cloud strategies.

Our management is committed to data governance, as it relates to both security and privacy. In fact, Sitecore has convened a senior management-level committee to ensure compliant data governance practices. Sitecore management also has invested significantly in people, processes, and tools to maintain compliance with global information security and privacy standards.

We are committed to training our workforce at every level on information security risks and recognized control practices. Enterprise-wide mandatory training and job-specific training are just the beginning. For more information about our approach to security and privacy, we encourage you to visit our Sitecore Trust Center at www.sitecore.com/trust.

About Sitecore

Sitecore delivers a digital experience platform that empowers the world's smartest brands to build lifelong relationships with their customers. A highly decorated industry leader, Sitecore is the only company bringing together content, commerce, and data into one connected platform that delivers millions of digital experiences every day. Leading companies including American Express, ASOS, Carnival Cruise Lines, Kimberly-Clark, L'Oréal, and Volvo Cars rely on Sitecore to provide more engaging, personalized experiences for their customers.

Learn more at Sitecore.com.