Storefront by Four51°
a Sitecore® company

APPLICATION ARCHITECTURE INFRASTRUCTURE & SECURITY

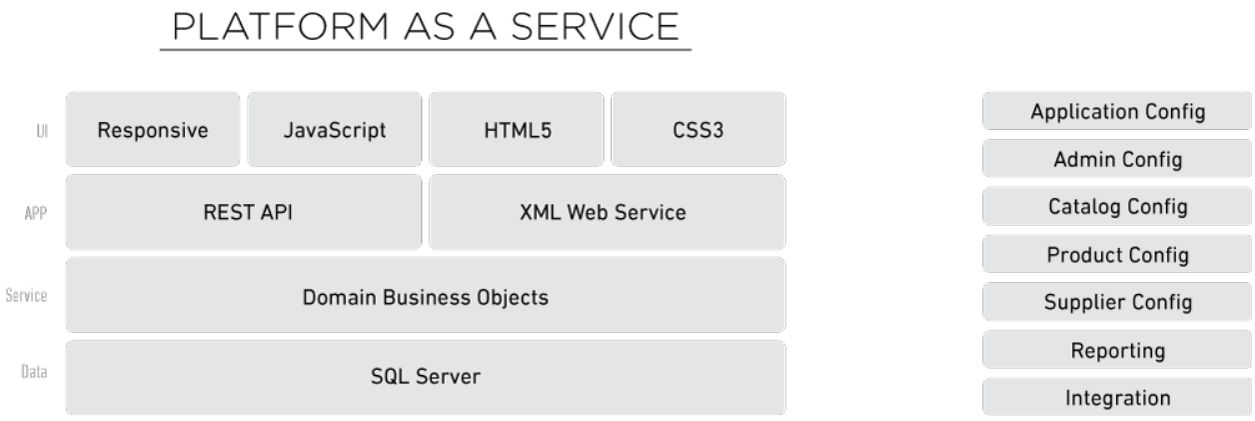
An in-depth look at the technology and procedures that power and manage the delivery of services from Storefront

July 2026

INDEX

APPLICATION ARCHITECTURE

Storefront's technical architecture is a private cloud model that leverages a combination of robust hardware, virtualization technology, and multiple data center facilities to deliver maximum application performance and reliability to our clients.



Delivered to the end user via a modern browser as a software as a service (SaaS) and a single page application, Sitecore created and maintains the Storefront 2.0 Base Application using the same REST API made available to customers. The REST API exposes the domain business objects for use in creating new applications or extending the publicly available source code of Storefront. The publicly available code repositories provided contain a full API coverage SDK, written with the Angular framework, to allow for rapid application development. These repositories are hosted on GitHub and can be quickly deployed and configured in the Storefront administration interface. All files in the source code can be easily edited, independent of the repository source, for additional customization.

Sitecore maintains separate Storefront production, quality assurance, and test environments. All of the virtual servers employed by the Storefront application run on Windows Server 2022, 2019, or 2016 and are separated into front-end application servers and a back-end database server farm model.

The production IIS 8.5 and application servers are responsible for supporting user authentication, serving web page requests, hosting the Storefront interoperability web and XML services, and sending Storefront system messages. To increase availability, the production database server farm is running on Microsoft SQL 2019 Enterprise Edition and employing the native SQL 2019 Always On Availability Group cluster. In addition, Microsoft DFS (Distributed File System) is leveraged to create redundant file storage.

The Storefront application is also supported by a number of servers running specialized imaging applications (Pageflex Mpower). These imaging servers have been designed as a fault tolerant/load balancing solution and each server can be used to assume additional workload at any time should one of the other servers suffer a hardware failure or be taken down for maintenance.

INFRASTRUCTURE OVERVIEW

Sitecore partners with OneNeck IT Solutions to host the infrastructure for Storefront on their ReliaCloud service. ReliaCloud is a private cloud model that provides the power and flexibility of a public cloud solution, with the security and performance required by enterprises with mission-critical computing needs. Built with industry-leading products and capabilities from Cisco, EMC and Nutanix, ReliaCloud is ideal for applications like Storefront that require reliable and scalable computing infrastructure.

ReliaCloud is delivered in dedicated resource pools from multiple Tier III data centers and is designed for maximum flexibility and utilization of current IT investments with the ability to adjust as needs change.

Storefront has been Payment Card Industry (PCI) compliant since 2008 and SOC 2 Type 2 compliant since 2016. Four51 has consistently maintained an average 99.97% uptime over the last 10 years.

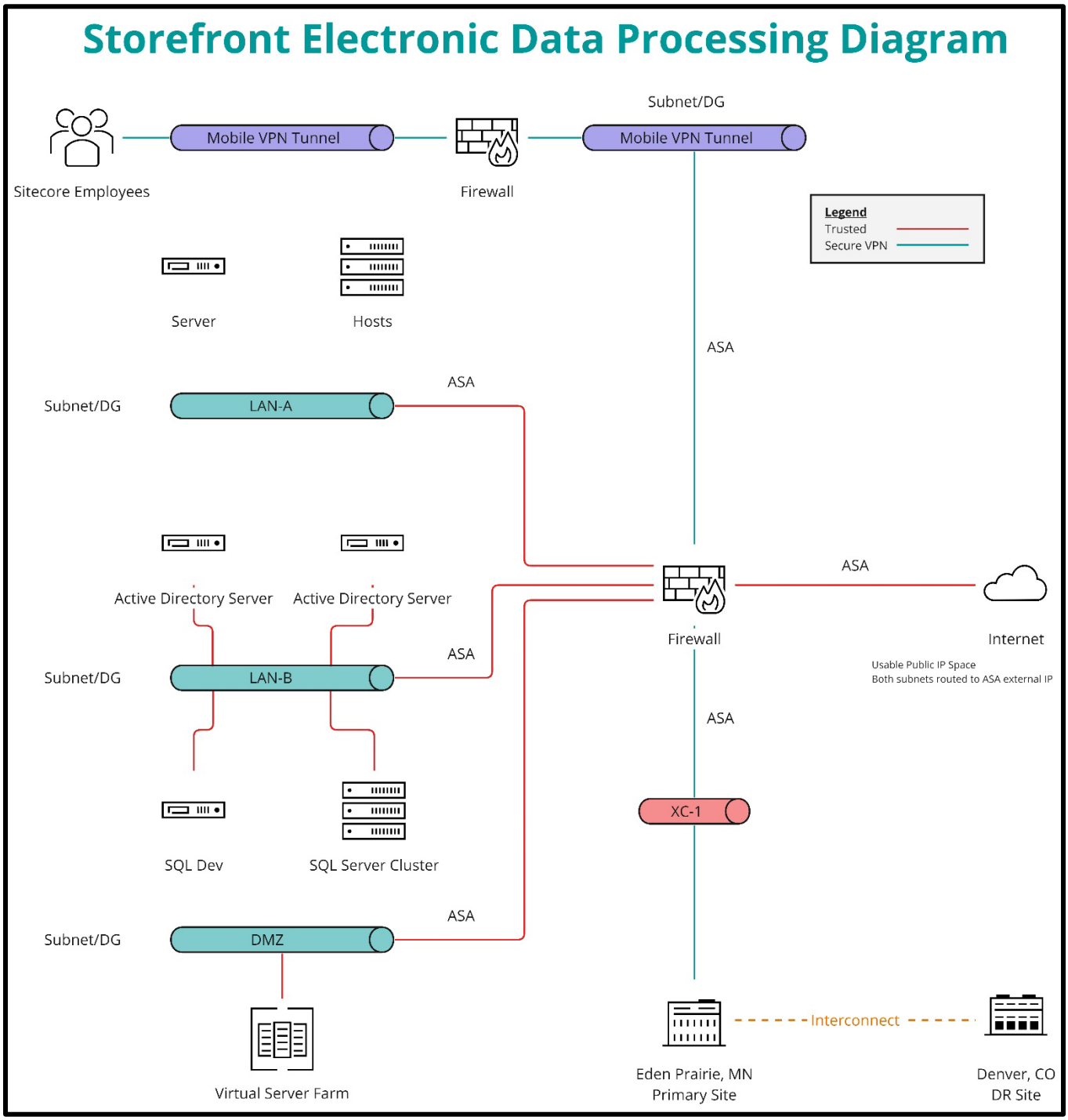
Sitecore has implemented a disaster recovery plan using the services of OneNeck and ReliaCloud. Their Hot DRaaS (Disaster Recovery as a Service) replicates critical servers in the Storefront environment and creates near-complete backups of all critical data in a different geographic region. Additionally, snapshots of the remaining servers are maintained to allow for OneNeck to replicate Storefront environment, should a disaster impact the primary datacenter.

Each of these components play a critical role in ensuring that the Storefront application and our clients' data is secure, accessible and blazingly fast. Together with our key technology partners, Sitecore has been delivering comprehensive SaaS technology since 1999 to everyone from the smallest business to over half the Fortune 500.

INFRASTRUCTURE DIAGRAM

This section provides a detailed view of Storefront's technology infrastructure and its three main components:

Data Center | Network/Routing | Servers



***NOTE: No portion of this network is wireless.*

DATA CENTER

Sitecore utilizes OneNeck ReliaCloud, built upon a SSAE 18 (SOC 1) Type II certified and Uptime Institute Tier III design certified facility in Eden Prairie, MN (covers deprecated SAS 70 compliance). Features of the data center include exceptional security, redundant data and power connections, 24x7x365 support, extensive monitoring, intelligent climate control systems and cutting-edge suppression systems. This facility's internal control environment enables PCI, HIPAA, HITECH, SOX, and GLBA requirements.

What is Tier III Design Certification?

The Uptime Institute Tier Classification provides performance-based benchmarks to align business requirements with data center design. Tier III facilities offer uptime, thus availability assurance, to support the critical demands of production environments and critical applications.

The Data Center is designed to meet the demands of a concurrently maintainable infrastructure, with N+1 configured critical components deployed throughout the design. Currently connected to the N+1 degree to major Internet backbones through 3 different providers, this facility is provided with constant blistering high-speed access to and from the Internet. Organizations can rest assured that our facility provides the most redundant and available commercial data center environments in the United States.

What Makes Tier III Different?

The Tier III design employs a concurrently maintainable infrastructure. This assures that if any one critical data center component is removed through planned maintenance or component failure, service will not be interrupted.

Through the redundancy and concurrent maintainability in infrastructure, Tier III data centers provide the required availability and uptime to support mission-critical applications and 24x7x365 production environments. Tier III provides maximum uptime around:

- Power - both redundant utility feeds and quick-start Generac generators – ready to accept load from UPS in 5 seconds.
- Cooling - multiple independent cooling towers, independent environmentally controlled racks, equipment level cooling.
- Network - Carrier neutral facility serviced by 5 national backbone providers, independent network paths out of location in each direction (north, south, east, & west).
- Security - Triple authentication used: Key card, retina scan, and PIN to access facility. Trained guards, video surveillance, mantraps, biometric readers and location monitoring.

SSAE 18 Compliant Data Center

OneNeck data centers have completed the Type 2 SSAE 18 (SOC 1) exam confirming data and power redundancy, physical security, fire and water protection, and temperature monitoring. OneNeck leverages the most advanced technology and skilled personnel to help safeguard Sitecore Storefront assets.

DATA CENTER SPECIFICATIONS

FACILITY

Design	Tier III design certified, concurrently maintainable, and electrically fault tolerant
Size	50,000 square feet
Access	Secured 24/7

CONNECTIVITY

Internet Bandwidth	Managed bandwidth and BGP routing across redundant Internet backbone connections with multiple Tier 1 carriers
Type	Carrier neutral facility
Carrier	CenturyLink, Comcast, Enventis, TDS Telecom, Level 3, XO, Zayo

DATA CENTER

Services	Cabinets and pods
Fire detection	VESDA (very early smoke detection apparatus)
Fire suppression	FM200
HVAC	N+1

SUPPORT

Onsite Support	24x7x365 onsite technical support staff
Remote Hands	Remote hands and eyes support available
Managed Services	Monitoring, tracking, and reporting on alerts, incidents, and key event

SECURITY

Guard	Patrol facility 24/7
Access Control	Three factor authentication: biometric, proximity card and PIN
Surveillance	Recorded and monitored digital video at 50+ points

POWER

Feeds	Four 2,500 kVA utility transformers
UPS	N+1
Generator	Four 1.5 MW Generators
Load	3.8MW total facility critical load

NETWORK ROUTING

Sitecore subscribes to Cloud Committed and Cloud Burstable Internet Bandwidth to provide high performance, highly available Internet access. A multiple level firewall configuration with DMZ and secure data zones is used to maximize security. Only the Storefront application can access customer data. Servers containing customer data are behind a firewall and not accessible via the internet.

The Enterprise Firewall Service provides a dedicated security service instance that lives across highly available redundant hardware. The service includes security best practices, monitoring, and reporting of key metrics including port availability, interface utilization, and overall ASA/firewall health.

To moderate legitimate Internet traffic, a robust anti-DDoS QoS policy is applied at the Internet edge, which sorts traffic into different policed classes that match on common signatures of DDoS traffic. In addition, an automated system is in place to watch for anomalous large volume traffic patterns. When this traffic crosses a threshold, the traffic for the attack target is automatically re-routed to a "choke" link, which constrains the traffic volume, and removes the traffic altogether from the data center's upstream Internet links.

SERVERS

The hosted private cloud architecture contains dedicated and hardened enterprise class host machines and associated hypervisor software (Nutanix). Processors are provisioned with at least an aggregate 32 GHz per 256GB of RAM. Storage services (LUNs) are not shared or accessible by other ReliaCloud customers. All arrays are D@RE enabled while the Nimble storage encrypts data at rest. All of the servers employed by the Storefront application run on Windows Server 2022, 2019, or 2016 and are separated into front-end application servers and a back-end database server farm model.

The production application servers are responsible for supporting user authentication, serving web page requests, hosting the Storefront interoperability web and XML services, and sending Storefront system messages. The production database server farm is running on SQL Server 2019 Enterprise Edition and employing the Always On Availability Group (AOAG) for failover and redundancy.

The Storefront application is also supported by a number of servers running specialized imaging applications (Pageflex Mpower). These imaging servers have been designed as a fault tolerant/load balancing solution and each server can be used to assume additional workload at any time should one of the other servers suffer a hardware failure or be taken down for maintenance.

With the hosted private cloud, Sitecore achieves capacity expansion without the need for forklift upgrades, allowing the environment to scale with load and customer requirements. Roles and functions are not tied to specific machines, creating nearly infinite flexibility with capacity, speed, and redundancy. This standardized server platform also provides transparent server maintenance resulting in increased uptime and availability.

DISASTER RECOVERY

Great care and attention are given to ensuring that should the Storefront application lose functionality, data integrity, or uptime, all the appropriate resources and data can be restored quickly with as little downtime as possible.

The Storefront disaster recovery solution is comprised of two main facilities:

1. The primary hosted and private instance of the ReliaCloud infrastructure is located in Eden Prairie, Minnesota. The environment is designed with sufficient infrastructure to withstand the loss of at least a single critical component. This is comprised of highly available virtual machines and dedicated servers running MS SQL Server Always On Availability Group (AOAG) to support Storefront's primary database workload. If one server fails, the data goes live on the other. Similarly, application files are saved to a Distributed File System (DFS) Namespace which is immediately replicated to multiple file storage systems.
2. The secondary hosted private instance of ReliaCloud is located in OneNeck's Denver, Colorado facility. This data center is comprised of always-on, always-updated replicas of critical servers and snapshots capable of being deployed to virtual machines running the same applications and utilities that are critical to operating Storefront services.

Full backups of everything connected to the Storefront production environment, supporting servers and data, are executed every week with incremental backups being executed every day. The Sitecore archival policies call for a 35 day retention period on all mission-critical data points and customer data. After the retention period, the expired data is removed, and the free space rotated back into the recovery scheme for re-use.

In addition to AOAG, all Storefront application databases are fully backed up, with transaction log backups taken every 10 minutes. The backups are encrypted and stored so that archived data can be restored.

SECURITY

Sitecore understands that security is mission critical and utilizes real time security monitoring from AlertLogic, managed by OneNeck. The Security Information and Event Management system (SIEM) provides real-time analysis of security alerts generated by applications and network hardware. The Storefront application, internal, and external infrastructure are regularly scanned for vulnerabilities. All data is sent between a user's browser and the application over HTTPS and is secured with SSL certificates issued through DigiCert. Network participants' information is protected by undergoing a SOC 2 Type 2 audit, maintaining PCI compliance, maintaining CCPA & GDPR compliance, secure software and a secure application-hosting environment.

Storefront is PCI certified as a Level 2 Service Provider and adheres to the international payment card industry (PCI) compliance standards for data security. The payment card industry data security standards (PCI DSS) are network security and business practice guidelines adopted by Visa, MasterCard, American Express, Discover Card, and JCB to establish a "minimum security standard" to protect customers' payment card information.

Obtaining PCI certification means that Sitecore has completed our annual self-assessment questionnaire (SAQ D), a quarterly network scan from an approved scan vendor (Coalfire ASV), an annual penetration test (BreachLock) and an Attestation of Compliance. In addition, independent customer solicited security questionnaires and penetration tests have been performed verifying that the company:

BUILDS AND MAINTAINS A SECURE NETWORK AND SYSTEMS

- Installs and maintains a firewall configuration to protect data
- Does not use vendor-supplied defaults for system passwords and other security parameters
- Regularly scans for network vulnerabilities

PROTECT CARDHOLDER DATA

- Protects stored data
- Encrypts transmission of cardholder data and sensitive information across public networks

MAINTAINS A VULNERABILITY MANAGEMENT PROGRAM

- Uses and regularly updates anti-virus software
- Develops and maintains secure systems and applications

IMPLEMENTS STRONG ACCESS CONTROL MEASURES

- Restricts access to data by business need-to-know
- Identifies and authenticates access to system components
- Restricts physical access to cardholder data

REGULARLY MONITORS AND TESTS NETWORKS

- Tracks and monitors all access to network resources and cardholder data
- Regularly tests security systems and processes

MAINTAINS AN INFORMATION SECURITY POLICY

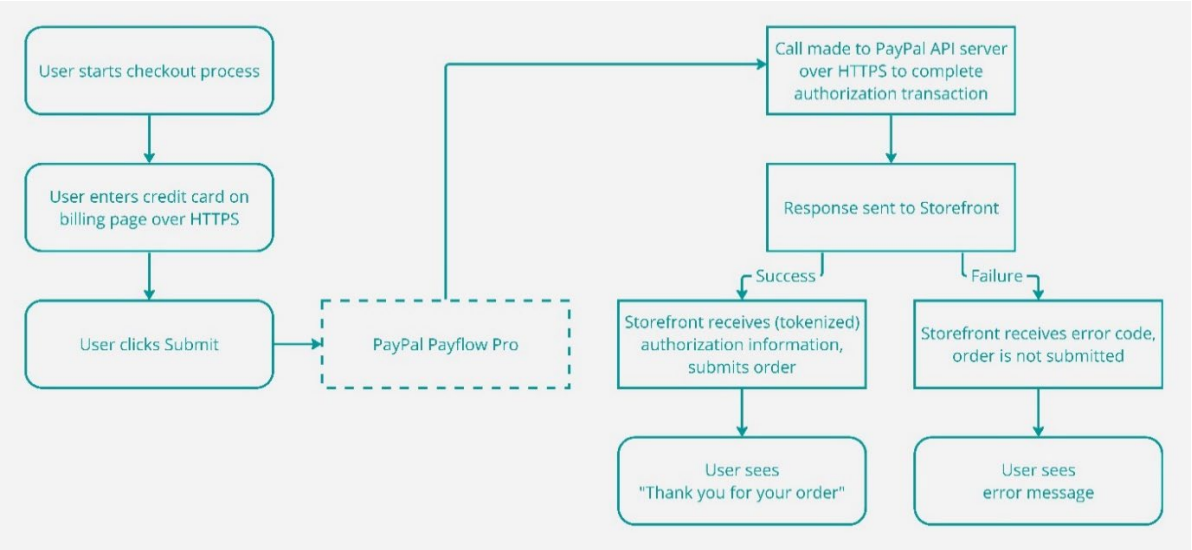
- Maintains a policy that addresses information security

INFORMATION SECURITY POLICY

TOPICS COVERED

- Purpose
- Information Security Objectives
- Scope
- Roles and Accountability
- Compliance with Customer Data Requirements
- Risk and Compliance Management
- Information Classification
- Access Control
- Acceptable Usage
- Mobile Devices and BYOD
- Network Security
- Protecting Sitecore's ET Environment
- Removable Media Management
- Passwords
- Protecting Sitecore's Cloud Product Environment
- Application and Software Development
- Retention and Disposal of Data
- Incident Reporting and Response
- Revisions
- Exceptions to This Policy
- Contact
- Document Control
- Acceptable Use Policy

CREDIT CARD PROCESSING



Payments by credit card are primarily supported in Storefront using PayPal technology. The flowchart above is an example of the credit card flow and behaves the same for all credit card processing. When an order is placed with a credit card payment, the data is transmitted to PayPal for processing, and once authorized, the web server communicates with the database server to store non-sensitive and masked cardholder information along with the reference token. Because Storefront leverages reference transactions, the credit card number is not stored in the Storefront database. The credit cards are stored in memory until the order is submitted, and are never persisted or transmitted over a network. Once the order is submitted, the buyer receives order confirmation details. Authorized users are then able to log in to the Storefront application via HTTPS and view order information, including the last four digits of the credit card number.

The following credit card processing mechanisms and endpoints are used:

PAYPAL PAYFLOW PRO
Sitecore has developed this capability with the provided Payflow Pro SDK. The endpoint is payflowpro.paypal.com.

PAYPAL PAYMENTS PRO
Sitecore has developed this capability with the provided PayPal SDK. The endpoints used by this library are https://api.paypal.com/2.0/ and https://api-aa.paypal.com/2.0/

IPSI
Sitecore has developed this capability with the provided IPSI API. The endpoint used is https://gateway.ipsi.com.au/v1.0

CardConnect
Sitecore has developed this capability with the provided CardConnect API. The endpoint used is https://fts.cardconnect.com:443/cardconnect/rest/

Transafe
Sitecore has developed this capability with the provided Transafe API. The endpoint used is https://live.transafe.com

PCI COMPLIANCE STATEMENT

Storefront is currently PCI DSS Level 2 compliant. Level 2 Compliance means that Sitecore must complete the following:

A SELF-ASSESSMENT QUESTIONNAIRE (SAQ-D)
The Sitecore security team annually updates our Information Security Policy. The Storefront infrastructure team performs an internal audit against the most recent PCI Data Security Standard and completes the self-assessment questionnaire (SAQ D). The Storefront application is not eligible for validation under the Payment Application DSS (PA-DSS) because it is strictly a software as a service (SAAS) product and it is not sold, distributed, or licensed to third parties.

QUARTERLY NETWORK SCAN BY AN APPROVED SCAN VENDOR (ASV)
Sitecore has leveraged a PCI ASV, Coalfire, and a web application scanning service from Rapid 7 to assist in monitoring and maintaining Level 2 compliance. The Coalfire service performs monthly scans against the Storefront network and the Rapid 7 service scans the application to ensure that the physical network and application are secure and in compliance. In addition to Sitecore-commissioned tests, customers have and are encouraged to perform their own security testing provided such tests are scheduled with the Storefront infrastructure team and are conducted during off-peak activity hours. The ASV scan report is found on page 24 of this document.

ATTESTATION OF COMPLIANCE FORM
The attestation of compliance is a signed document from a Sitecore security officer stating that the company follows best security practices and is compliant with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures. Sitecore's Attestation of Compliance is included in this document on pages 13-23.

Additional documentation can be obtained from Sitecore by an authorized security officer. If you have any other questions or concerns regarding PCI compliance, please have a member of your security team contact **datacompliance@sitecore.com**, or, if you are a Storefront customer, please submit a case.

Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Sitecore USA
DBA (doing business as):	
Company mailing address:	1750 Elm St., Suite 1100, Manchester, NH 03104
Company main website:	www.sitecore.com
Company contact name:	Heather Hinton
Company contact title:	Chief Information Security Officer
Contact phone number:	1-855-748-3267
Contact e-mail address:	heather.hinton@sitecore.com
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Not Applicable
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) assessed:	Storefront

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☑ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☑ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (select all that apply):

Name of service(s) not assessed:	

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:	

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Saas e-commerce platform that enables distributors (sellers) to provide a purchasing interface/shopping cart for their buyers. Via Storefront, distributor's customers (buyer) place an order and then credit card authorization is handled by a third-party payment gateway (usually PayPal) or Storefront passes the encrypted card number using private/public key in a cXML Order Request.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Storefront does not store or process credit card details, but it does store the authorization code received from the payment gateway for transaction reference.
Describe system components that could impact the security of account data.	Firewall, network switches, SIEM system, name servers, virtual machines, hypervisor

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Storefront application is delivered to users through a web browser over HTTPS. When an order is placed via the application with a credit card payment, the data is transmitted to the payment gateway over HTTPS for processing, the once authorized, the web server to store non-sensitive and masked cardholder information along with the reference token. The server blades are D@RE enabled, and the Nimble Storage encrypts the data at rest. Only the application can access customer data. Servers containing customer data are segmented from the network, behind two separate firewalls, and not accessible via the internet.
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☑ Yes ☐ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
US Signal ReliaCloud Hosting Facility	2	Eden Prairie, MN : Denver, CO (DR)

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☑ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☑ Yes ☐ No
• Manage system components included in the scope of the entity's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☑ Yes ☐ No
• Could impact the security of the entity's CDE—for example, vendors providing support via remote access, and/or bespoke software developers.	☑ Yes ☐ No

If Yes:

Name of service provider:	**Description of service(s) provided:**
US Signal ReliaCloud	Private cloud infrastructure, hosting, and maintenance

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed: Storefront

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☑	☐	☐	☐	☐
Requirement 2:	☑	☐	☐	☐	☐
Requirement 3:	☑	☐	☐	☐	☐
Requirement 4:	☑	☐	☐	☐	☐
Requirement 5:	☑	☐	☐	☐	☐
Requirement 6:	☑	☐	☐	☐	☐
Requirement 7:	☑	☐	☐	☐	☐
Requirement 8:	☑	☐	☐	☐	☐
Requirement 9:	☑	☐	☐	☐	☐
Requirement 10:	☑	☐	☐	☐	☐
Requirement 11:	☑	☐	☐	☐	☐
Requirement 12:	☑	☐	☐	☐	☐
Appendix A1:	☑	☐	☐	☐	☐
Appendix A2:	☐	☐	☑	☐	☐

Justification for Approach	
For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	There are no POS/POI terminals in the Storefront environment.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2025-12-29
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☑ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date *YYYY-MM-DD*).

Indicate below whether a full or partial PCI DSS assessment was completed:

☑ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.

☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document.

Select one:

☑	**Compliant:** All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☑	*PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* was completed according to the instructions therein.
☑	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's assessment in all material respects.
☑	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signed by:
Heather Hinton
E15E74059D05485...

Signature of Service Provider Executive Officer ↑	*Date:* 20 February 2026
Service Provider Executive Officer Name: Heather Hinton	*Title:* Chief Information Security Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☑	☐	
2	Apply secure configurations to all system components	☑	☐	
3	Protect stored account data	☑	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☑	☐	
5	Protect all systems and networks from malicious software	☑	☐	
6	Develop and maintain secure systems and software	☑	☐	
7	Restrict access to system components and cardholder data by business need to know	☑	☐	
8	Identify users and authenticate access to system components	☑	☐	
9	Restrict physical access to cardholder data	☑	☐	
10	Log and monitor all access to system components and cardholder data	☑	☐	
11	Test security systems and networks regularly	☑	☐	
12	Support information security with organizational policies and programs	☑	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☑	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	☑	☐	

Note: *The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*

Sitecore USA. Scan Report – Attestation of Scan Compliance

A. 1 Scan Customer Information		A. 2 Approved Scanning Vendor Information	
Company: Sitecore USA		**Company:** MegaplanIT Holdings LLC	
Contact Name: Justin Miller	**Job Title:** Senior Infrastructure Engineer	**Contact Name:** Dominick Vitolo	**Job Title:** VP of Security Services
Telephone: 4153800600	**E-mail:** justin.miller@sitecore.com	**Telephone:** 800-891-1634	**E-mail:** asv@megaplanit.com
Business Address:	101 California Street, Floor 16	**Business Address:**	18700 N Hayden Rd #340
Country: USA	**City:** San Francisco	**Country:** USA	**City:** Scottsdale
State/Province: CA	**Zip:** 94111	**State/Province:** AZ	**Zip:** 85266
Website/URL: four51.com		**Website/URL:** megaplanit.com	

A. 3 Scan Status

- Compliance Status: Passed
- Scan Report Type: **Full Scan**
- Number of unique components scanned: 3
- Number of active components: 3
- Number of identified failing vulnerabilities: 0
- Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:
- Date scan completed: 07/03/2026
- Scan expiration date (90 days from date scan completed): 10/03/2026

A. 4 Scan Customer Attestation

Sitecore USA attests on 07/10/2026 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. Sitecore USA also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A. 5 ASV Attestation

This scan and report was prepared and conducted by MegaplanIT Holdings LLC, under certificate number 509530-01-03, according to internal processes that meet PCI DSS requirement 11.3.2 and the ASV Program Guide. MegaplanIT Holdings LLC, attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Andrew Haslett.

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 Storefront application and supporting services for log irregularities, performance and uptime
- Monitor OneNeck, Rapid7, and Open Web Application Security Project (OWASP) and advisories for software/hardware patches, security industry advisories and security alerts
- OneNeck uses AlertLogic to monitor all server and IIS logs for irregularities and alerts staff to potential security issues
- Monitor physical access logs
- Schedule responsible personnel for incident response 24x7

SCHEDULED MAINTENANCE COMMUNICATIONS

Scheduled maintenance is a planned and deliberate event for the purpose of updating and/or performing maintenance to the Storefront application and/or hardware infrastructure. A regularly scheduled maintenance window for the dev/test environments is set for the first Saturday following Microsoft's "Patch Tuesday", between 11:00 pm – 2:00 am CT. The maintenance window for the production environment is set for the third Saturday following Patch Tuesday, between 11:00 pm – 2:00 am CT. Patch Tuesday occurs on the second, and sometimes fourth Tuesday of each month in North America. Additional maintenance may be necessary outside of this window, and whenever possible, will be scheduled after normal business hours typically between 11:00 pm and 4:00 am CT.

In the event of any scheduled maintenance, the following information will be posted for subscribers of status.four51.com: Date, time and expected duration of maintenance.

In the event of scheduled maintenance for the purposes of release notifications, the information is also posted to admin users within the application.

RECOVERY COMMUNICATIONS

In order to rapidly recover from potential unplanned system outages, the following procedures will be followed in the event of a system failure:

STOREFRONT APPLICATION AND ADDITIONAL SERVICES INACCESSIBLE

- The Storefront infrastructure team is notified via application monitoring utilities of the system failure
- The page at status.four51.com is updated
- Subscribers to the page at status.four51.com can choose whether to receive email or text alerts on status updates to specific Storefront services.
- The service status is updated to eventually include start and end time of outage, duration, cause of failure, and any risk mitigation taken to prevent further outages.
- When possible, a splash page will be activated, indicating the application is unavailable, and, if known, time of restored services.