portal connector by sylogist

Portal Connector Infrastructure, Operations, and Security

Prepared by: Sylogist Portal Connector Security Team

Created: 02/15/2023
Updated: 23/09/2024

Table of Contents

Introduction

At Sylogist, we are a trusted provider of software solutions for the public and nonprofit sectors, committed to meeting and maintaining the highest standards of security and data integrity. In today's rapidly evolving landscape of cyber threats, we are dedicated to safeguarding our customers' data, integrity, and availability through state-of-the-art technology, robust data centers, and rigorous policies and procedures. Our approach is reinforced by continuous third-party audits, ensuring comprehensive protection against potential threats.

This document provides a detailed overview of our security controls, compliance programs, relative certifications, data backup and disaster recovery processes, and how we ensure the highest levels of availability and performance.

Compliance and Certification

Data Center Certifications

Sylogist's cloud infrastructure is hosted on the secure Microsoft Azure Cloud platform, utilizing certified data centers designed with multiple layers of operational and physical security. These Azure data centers are equipped to maintain data integrity and safety, with 24/7/365 staffing and support. The system's comprehensive security features include:

- Intrusion detection systems
- Distributed Denial-of-Service (DDoS) mitigation
- Regular risk assessments to ensure continued compliance with industry standards

The following certifications are held and maintained by all data centers:

- SOC (System and Organization Controls) 2 + HITRUST
- GLBA
- HIPAA
- NIST SP 800-53 rev 41 annually
- ITAR and EU-US Privacy Shield3 registered SAE-3402
- ISO 27001
- PCI-DSS
- SOC (System and Organization Controls) 1
- SOC (System and Organization Controls) 2 Type 2
- SSAE-18

Compliance and Certification

Data Privacy

Sylogist employs industry-standard practices to ensure the confidentiality of data stored within its cloud-hosted applications. For example, access for Sylogist employees is carefully controlled and restricted to the necessary minimum to deliver cloud services.

In addition to multiple background checks and HR protocols, encryption of data-at-rest further safeguards your data against unauthorized access, including by data center personnel. Production data is automatically backed up with the ability to restore to any point-in-time within the past 15 days, providing reliable recovery from potential data corruption.

With Sylogist's security model, teams can easily manage and restrict user and developer access to production data, even when multiple applications share the same Sylogist cloud infrastructure.

Vulnerability Management

Sylogist proactively monitors reputable industry sources for security vulnerabilities and utilize standardized risk rating methodologies to plan appropriate responses. Any system threats, attacks, or resource alerts trigger immediate notifications to the IT and Security teams via phone, email, and text. Security tools, such as Microsoft Defender for Cloud, actively monitor and safeguard against threats and vulnerabilities. Additionally, Sylogist ensures the consistent application of patches to both the operating system and application servers.

Compliance and Certification

Payment Application Data Security Standard (PA-DSS) / Payment Card Industry Data Security Standard (PCI DSS)

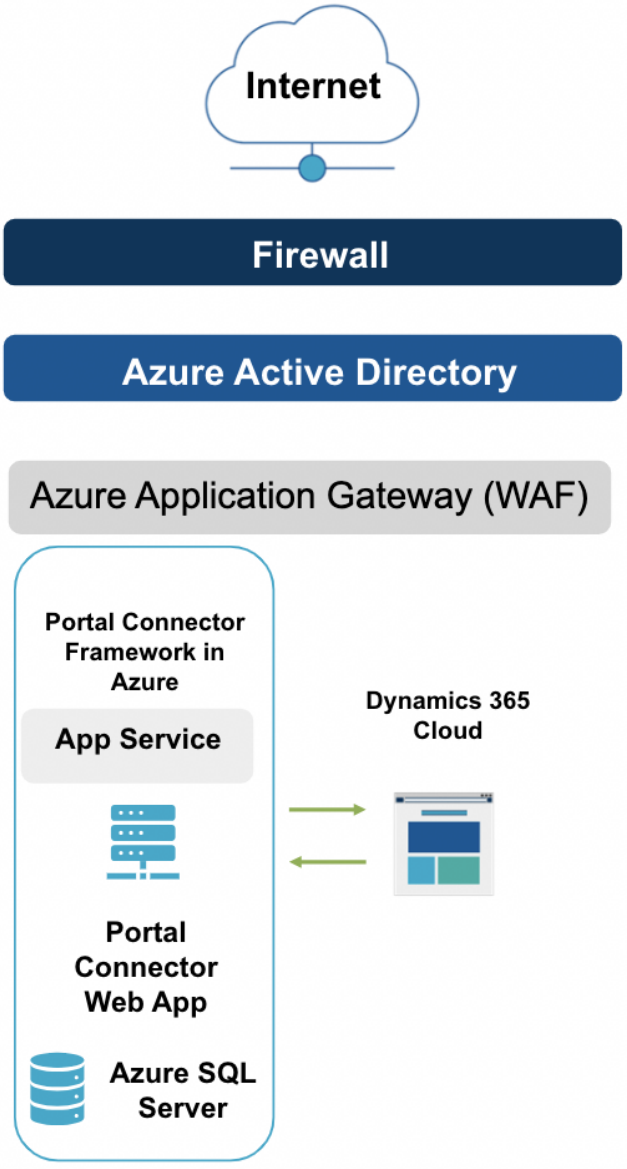
Portal Connector does not directly handle or store any credit card data, and therefore, the PA-DSS certification is not required. However, all data centers and partners involved in storing or processing credit card information must provide valid PCI DSS certification documentation.

Architecture

Sylogist has partnered with Microsoft to deliver a state-of-the-art data center infrastructure that includes industry-leading intrusion detection, backup, and scalability features.

The Azure Portal Connector SaaS offering:

- 1 Production App Service, with Azure SQL database
- Up to 5 staging App Service slots/instances
- Development infrastructure for configuration and development (Dev VM and SQL)
- Geographically specific
- Security and scalability
- Security documentation (crmportalconnector.com)



Updates and Upgrades:

- Our support team will conduct quarterly updates and upgrades, which include the latest Sitefinity and Portal Connector versions.

Full Featured Enterprise class CMS: Sitefinity DX (https://www.progress.com/sitefinity-cms/features)

Architecture

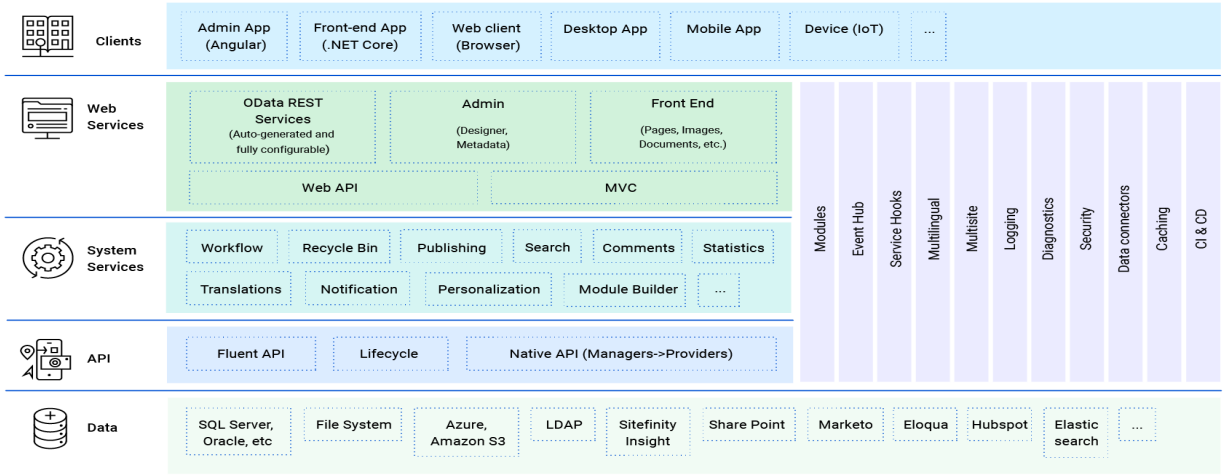
Technology & Applications Architecture

Sitefinity's multi-layer architecture is built around core principles of extensibility, interoperability, integration, and flexibility. This is achieved through:

- Abstraction patterns that hide implementation and storage location details
- Multiple extensibility points to enhance customization
- Public API access for all system components and services powering Sitefinity's out-of-the-box modules

Portal Connector is a Sitefinity add-on that harnesses the platform's functionality while adhering to the same design, extensibility, and presentation principles that make Sitefinity successful. Portal Connector extends Sitefinity by seamlessly integrating Dynamics CRM/365 data into a corporate website or standalone self-service portal.

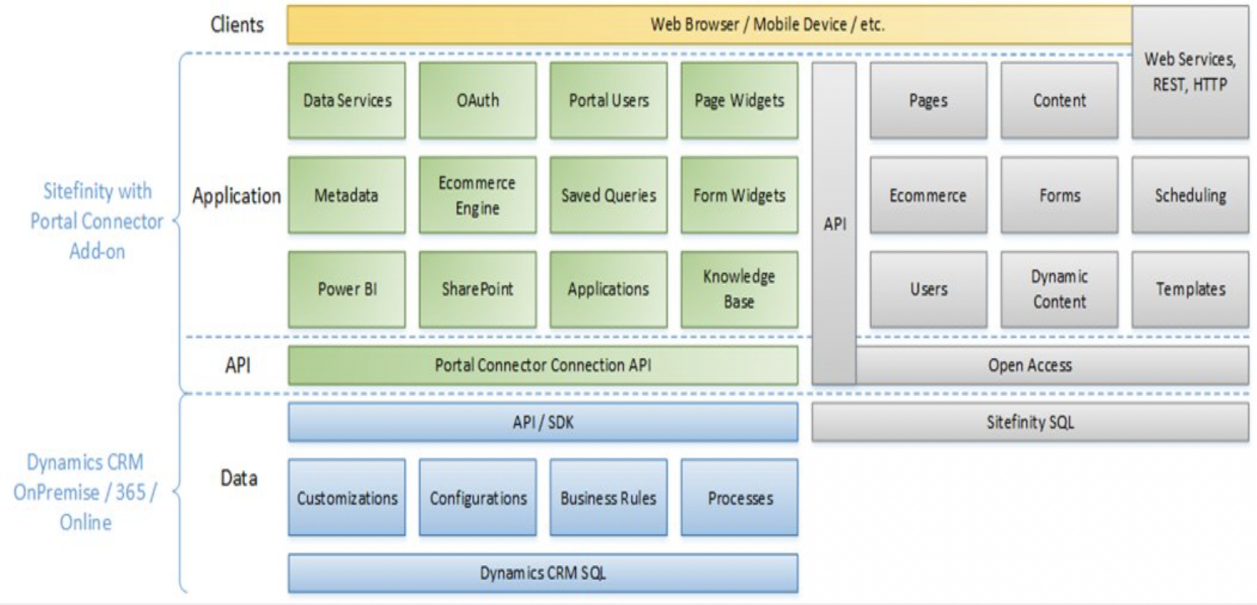
The following illustration highlights the application layers in a website running both Sitefinity and Portal Connector:



Architecture

Sitefinity's N-tier application architecture allows stacked groups of system components isolated in layers, allowing changes to be made in one layer independently of the others.

With a clear understanding of how Portal Connector integrates with Sitefinity, we can focus on the specific integration points Portal Connector both consumes and exposes. The detailed diagram below demonstrates the services, functions, and interactions Portal Connector provides within the Sitefinity platform. It also highlights Portal Connector's seamless integration with Dynamics CRM/365:



Hosted Security Controls

Cloud Provider Locations

Sylogist utilizes Microsoft Azure (geographical specific).

Network/Application Controls

- Customer access to the production environment is limited, with each user's permissions managed through unique IDs and passwords. Access to application authorizations is controlled within the Portal Connector application.
- Sitefinity CMS offers three primary out-of-the-box authentication methods:
  - Default authentication is based on OAuth 2.0 and OpenID Connect protocols. It gives flexibility and out-of-the-box integration with various third-party providers, such as ADFS, Windows, LDAP, Facebook, Google, Twitter, and Microsoft. In addition, the protocols are designed with security in first place. These protocols are designed with a strong emphasis on security, leveraging certified libraries like IdentityServer3 for OpenID Connect.Connect implementation.
  - WRAP/SWT Implementation
  - Forms Authentication

Reference Sitefinity Security – Sitefinity CMS Security & Compliance Solutions | Progress Sitefinity

- Sylogist Portal Connector application-related traffic is encrypted from end-to-end via TLS 1.2.

Hosted Security Controls

Network/Application Controls (continued)

- Access to the production environment for Hosting Operations is secured through encrypted channels.
- Any upgrades and enhancements to the production environment are thoroughly documented, tested, and require approval from senior management within Engineering and Technical Operations before release.
- Sylogist partners engages with a third-party security firm to conduct penetration testing on our internal infrastructure. Additionally, we perform quarterly vulnerability scans to identify and address potential security issues.
- Sylogist performs quarterly vulnerability scans of internal Sylogist Infrastructure.
- Event logs from critical systems and network devices are forwarded to our Security Operations Center for thorough review and timely action.

Operations Security Controls

- Access to the production environment is secured through a VPN with Multi-Factor Authentication (MFA). Only HTTPS (443) and IPSEC ports are open.
- The system enforces a strict password policy on all production servers.
- Access to the production environment is restricted to a limited number of authorized Sylogist employees, who must complete security and privacy training. Each employee is assigned a unique user account, and access is granted only with the approval of senior management in Technical Operations. All prospective employees undergo background checks before hiring. Direct login to the production environment using local system accounts is prohibited; such attempts are logged and reviewed by the Security Operations Center.

Redundancy Protection Program

Sylogist ensures full redundancy within your configured Azure region. Each customer's subscription includes comprehensive backup support services. This section outlines the platform's capabilities in two key areas of customer support:

Backup/Redundancy

As part of our service, and included in your subscription cost, we offer backup protection to retain and restore your data when needed. These backups are integral to our Redundancy Protection Program. Customers can typically request a restore from a recent backup if necessary.

- We conduct daily database backups with a retention period of 7 days.
- Additionally, the application is configured for hourly backups, retained for 30 days.

Data Security

Secure Transmission of Customer Data

Sylogist employs robust encryption methods to safeguard customer data and communications, including encryption via HTTPS.

Prevention of Access to Customer Data by Another Customer or Third Party

Customer data stored and processed in our hosting facilities is secured through the following technologies and techniques:

- **Perimeter Security**:Sylogist employs industry-standard firewall technology and intrusion detection/prevention systems to protect both the production and corporate network perimeters.
- **Application Security and Database Tables:** Sensitive data is encrypted using appropriate algorithms based on the risk profile, such as data at rest or data in transit. Sitefinity CMS uses FIPS-compliant algorithms for hashing and encryption. The Portal Connector application utilizes encrypted IDs for passing information, such as CRM GUIDs, between pages (query string). These IDs are encrypted using AES 256-bit encryption, with unique keys generated for each logged-in user. Additionally, passwords stored by Portal Connector, including CRM and PowerBI connection passwords, are encrypted using AES.
- **Database Security:** Access to the production database is restricted to protect both the operating system and database.
- **Data Security:** Upon subscription expiration, data is purged according to the agreed contract terms, and all backups are deleted on a regular rolling schedule.

User Security

Users – Permissions and Roles

To effectively manage user and role permissions for various types of content within Portal Connector, Sitefinity provides Role Providers and Membership Providers. These tools facilitate user management and role assignment, enabling precise configuration of permissions for different content types.

The system supports granular permissions, allowing administrators to define access at a detailed level. Permissions can be assigned to Roles and individual Users, with operations such as View, Create, Delete, and Modify being controlled according to the type of item. Depending on the object type, permissions are verified across multiple system layers and modules to ensure accurate access control.

User Audit Trail

The platform offers a comprehensive audit trail to record user interactions across various levels. The Auditing Module enables tracking for all Portal Connector features, including form submissions and Dynamics CRM queries. It also audits backend content changes, such as form and page publishes, updates, and creations, along with other content items like images and videos. Additionally, it captures all login attempts, logouts, and individual page navigations. Users can review this data through a backend report available for detailed analysis.

System Availability and Performance

Sylogist products are engineered for high availability and optimal performance in line with our Service Level Agreements (SLAs). We continuously monitor and measure system availability and performance to ensure adherence to these standards.

Availability

Sylogist measures uptime as the percentage of time the hosted service is available, excluding scheduled maintenance. We commit to delivering at least 99.7% uptime each month, and we consistently exceed this target.

Performance

By analyzing production environment monitoring results, we proactively increase application server and processing capacity as needed. Monitoring system response times helps us detect emerging trends and adjust our infrastructure investments to sustain optimal performance. We encourage clients to reach out to support if they experience any unusual delays in response time. These incidents are promptly investigated, and findings are shared with the customer. Additionally, we continually integrate innovative technologies into our development roadmap to enhance the performance of our service

System Scalability

At Sylogist, we adhere to or surpass industry standards for security, performance, and service quality. As our customer base expands and existing clients grow with us, we increase server capacity to handle the higher activity levels, ensuring consistent performance and response times. Our service is designed to scale effectively, supporting hundreds of thousands of users.

System Availability and Performance

Our extensive customer community drives future innovation through frequent and high-quality feedback. As our customer base grows, our world-class support team expands as well, ensuring we continue to provide prompt and precise responses to every customer.

Supporting Your Security Questions and Needs

If a customer requires assistance with completing their own security questionnaire format, we offer support through the response services included in our fee-based Customer Audit Program.