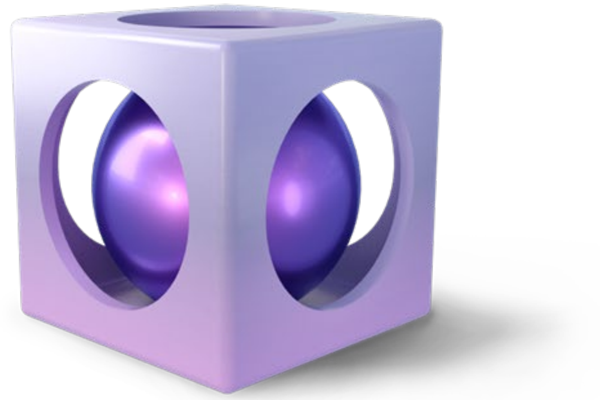
Power Pages

Security White paper



Power Pages
Defense-in-depth approach to security

Abstract

This white paper describes how Power Pages offers enterprise grade security and the tools and capabilities it offers for administrators and makers to harden security for their external applications.

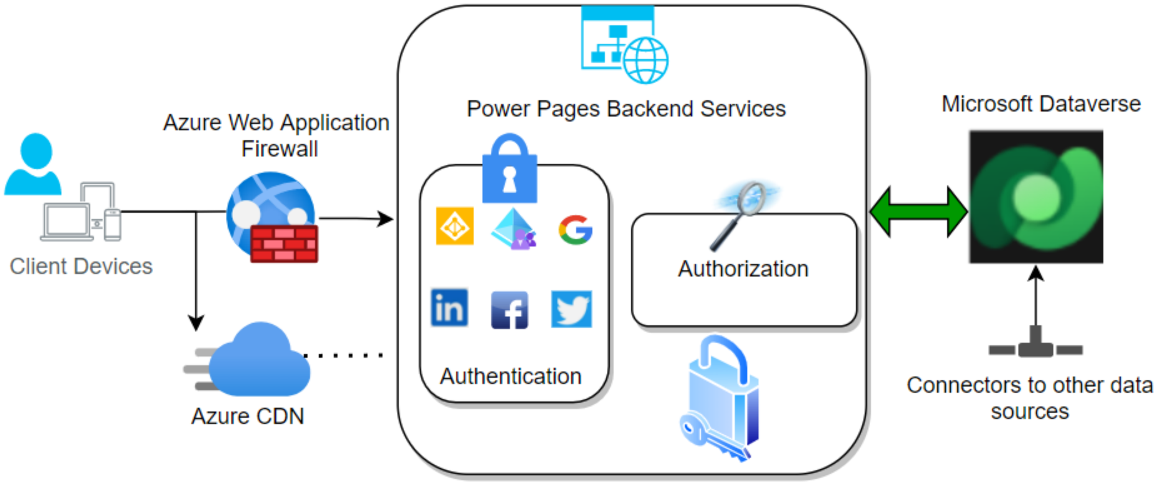
DIPTI JAISWAL

https://www.linkedin.com/in/diptijaiswal/

Power Pages - An Overview

What is Power Pages?

Power Pages is an enterprise-grade low-code SaaS (software as a service) platform for creating, hosting, and administering rich external business websites. The platform empowers both citizen developers and professional developers of organizations and governments to create and launch bespoke external-facing business web applications easily, rapidly, and securely to be used by organization's consumers, partners, community users, and internal users.


Client Devices
Azure Web Application Firewall
Azure CDN
Power Pages Backend Services
Authentication
Authorization
Microsoft Dataverse
Connectors to other data sources

Power Pages offers enhanced **control**, **protection** and **security** for administrators, website makers, and website visitors. It empowers makers to extend business data and processes to external users securely and helps ensure compliance. As a platform, it offers comprehensive compliance coverage across global, regional, government, and industry-specific compliance standards, making it a trusted Low code application platform. Business data which website users interact with is securely stored in Microsoft Dataverse. Power Pages tightly integrates with products and capabilities such as Power Apps, Power Automate, Power Virtual Agents, Power BI, and Microsoft SharePoint.

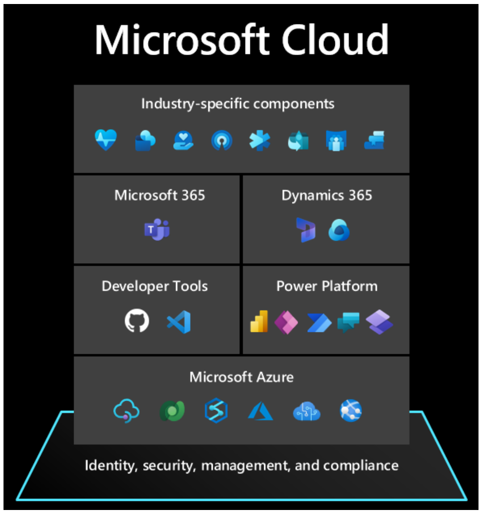
Why Power Pages?

Organizations and governments around the world are going through an unprecedented pace of digital transformation. The accelerated adoption of digital technologies has resulted in a massive increase in remote working, increased customer demand for online applications and services, and increased use of advanced technologies in operations, business processes, government, and citizen services. All of this, powered by the cloud.

As the transition to the cloud has changed from a trickle to a flood, and with the new, exposed surface area that comes with it, more organizations and governments are concerned with **security**, **compliance, and governance.**

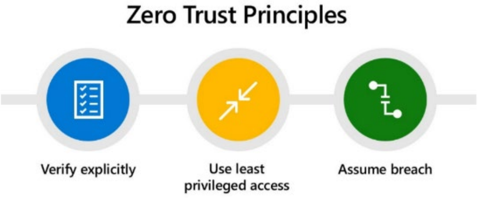
Data has emerged to be one of the most important assets in the modern world. Questions like “How secure is my data in the cloud?” and “What end-to-end protection is available to prevent my sensitive data from leaking?” are common in today’s digital world. Answers to these questions are doubly important as both professional and citizen developers use technologies to create cloud applications for a wide variety of business needs.

Gartner Predicts 30% of Critical Infrastructure Organizations will experience a Security Breach by 2025. [1] The rise in increasingly sophisticated and expansive cybersecurity attacks, coupled with the move to hybrid environments, has ushered in an opportunity for organizations around the world to look out for cloud native, multi-tiered, defense in depth strategies to protect their business data and applications.



Accelerating digital transformation via rapid enterprise deployments and staying secure and protected **do not** need to be at odds with Low code application development. Power Pages is Microsoft’s Low Code and Pro-developer Application Platform that provides **comprehensive security**, compliance, protection, governance, and authorized access for business data to external users.

Power Pages is part of Microsoft’s Power Platform. It is built on Microsoft Azure and leverages the same security stack as Azure, which protects some of the world's most sensitive data and integrates with Microsoft 365's most advanced information protection and compliance tools.



Power Pages is built on a “**Zero Trust**” security approach- it assumes that activity on the platform, even by trusted users may be an attempted breach, hence activities/accesses are explicitly verified using a robust authorization model. Access to website data and website content honors the Least Privilege Access model.

Today many national security agencies, community services, financial institutions, and health care providers entrust Power Pages with their most sensitive information. Enterprise security and compliance are at the core of Power Pages platform as it offers **Secure by Design**, **Secure by Default** and **Defense-in-Depth** approaches to application building, deployment, and management.

[1] Gartner Predicts 30% of Critical Infrastructure Organizations will experience a Security Breach by 2025

Power Pages delivers end-to-end protection designed to address our customers' biggest challenges across areas including:

1. **Authentication**
   a. How do I securely engage internal and external partners, customers, and community users?
   b. How do I extend business data and business processes externally?
2. **Authorization**
   a. How do I control who has access to what level of business data?
   b. How do I control access to data securely and differently for anonymous and authenticated users?
   c. How do I onboard external users to my application securely?
3. **Data Storage**
   a. How do I ensure that business data is always protected & secured?
   b. How is the data stored? How is it encrypted? What controls do I have on my data?
4. **Application Security**
   a. How can I restrict business data being accessed by geography, demography or by a set of users?
   b. How do I secure my application against vulnerabilities, attacks, and malicious actors?
   c. What security capabilities do I need to keep in mind when creating external facing applications?
5. **Governance**
   a. What governance controls do I need to build to ensure that I can control what type of applications my organizational users can create? How do I control who can create these applications?
   b. How do I audit who conducts what operations? How do I react quickly if there's suspicious activity on the service?

Security is enabled by fundamental architectural building blocks that offer layers of protection. Hence, before we discuss security, it is important to review the architecture of the Power Pages platform. Power Pages Architecture white paper describes the platform's capabilities, building blocks and architecture.

Power Pages Security white paper describes its **Defense-in-Depth** strategy that uses the best of Microsoft's and Power Platform's security stack to offer end to end enterprise grade security, controls, and protection for our customers. It discusses how Power Pages mitigates **OWASP Top 10 security risks** and the tools, capabilities, and features available to admins and makers on Power Pages to prevent security risks and protect their most valuable assets.

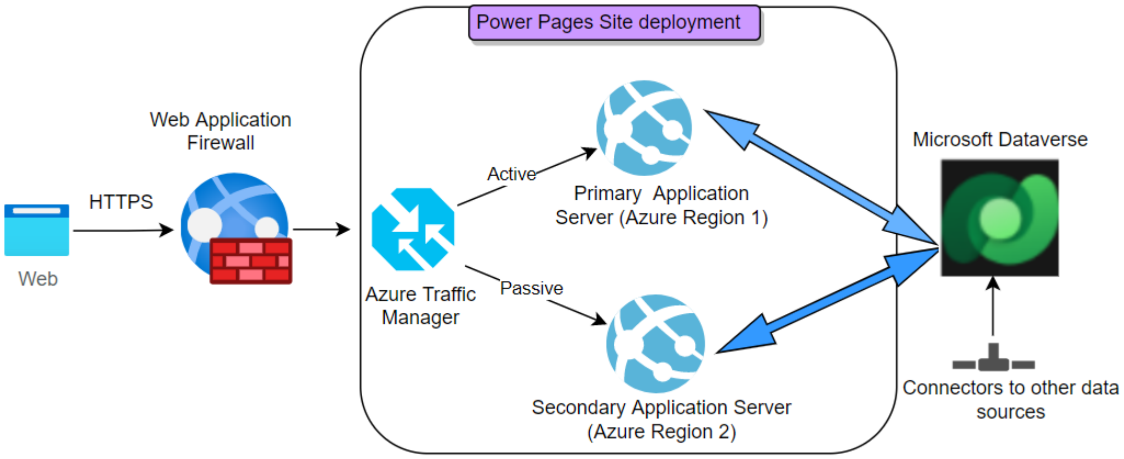
The Power Pages service is governed by the Commercial Licensing Terms (microsoft.com) and the Microsoft Enterprise Privacy Statement. For details on location of data, refer to data section in the Microsoft Privacy and Security terms and to the Data Protection Addendum. For compliance information, the Microsoft Trust Center is the primary resource for Power Pages. The Power Pages team is working hard to bring its customers the latest innovations and productivity. Learn more about compliance in the Microsoft compliance offerings.

The Power Pages service follows the Security Development Lifecycle (SDL), strict security practices that support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost. Learn more at Microsoft Security Development Lifecycle Practices.

Security in Power Pages

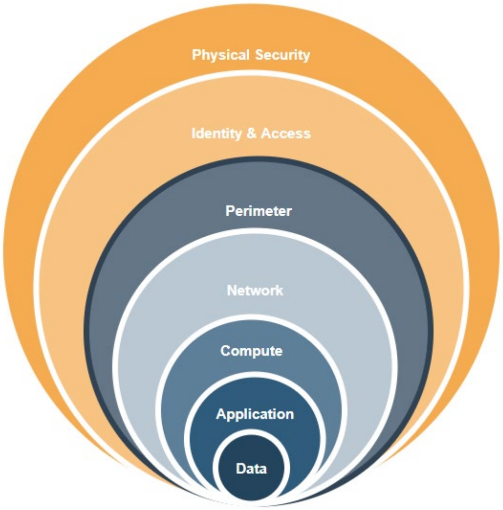
Azure as a hosting platform enables Power Pages to leverage capabilities like elastic scaling, **high availability**, platform layer security, automatic infrastructure and operating systems **security patching** and upgrades, and advanced threat protections. Power Pages is available in many datacenters around the world.

Each Power Pages site can be configured with a Web Application Firewall that monitors, filters, and blocks malicious requests to the website. **Web application firewall** (**WAF**) strengthens security as it applies a set of security rules to HTTP traffic to and from an application thereby protecting applications from OWASP Top 10 security risks and common attacks, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.


Power Pages Site deployment
Web Application Firewall
HTTPS
Web
Active
Passive
Azure Traffic Manager
Primary Application Server (Azure Region 1)
Secondary Application Server (Azure Region 2)
Microsoft Dataverse
Connectors to other data sources

The following sections describe how Power Pages offers enterprise grade **Defense-in-Depth** security as a platform and discuss security tools and controls that can be employed to mitigate risks from **OWASP Top 10 security risks** and threats.

Defense-in-Depth



The objective of defense-in-depth is to protect information and prevent it from being accessed or stolen by those that are not authorized to access it. A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims to acquire unauthorized access to data.

Power Pages offers **Defense-in-Depth** by using the best of Microsoft's and Power Platform's security stack which enables it to offer multi-layered protection from a wide variety of security threats. This multi-layered security stack improves overall security of Power Pages applications by reducing the probability of security breaches. The Power Pages platform provides makers and administrators the necessary controls to harden security and governance for their sites and data. This section describes the seven layers of protection that enable Power Pages to offer defense-in-depth as a platform.

Physical Security

Power Pages run on Azure App service, a cloud computing platform for hosting applications. Azure App service is a fully managed service with built in infrastructure maintenance. It offers rigorous security and compliance standards. Microsoft operates the Azure data centers and manages physical security of hardware on which these applications run at locations worldwide. Only authorized personnel have access to parts of Azure data centers.

Identity and Access

Power Pages allows both anonymous and authenticated visitors to have authorized access to business data when they interact with the site. It offers a robust security model based on secure Authentication mechanisms and Authorization (via RBAC) that protect identities and access. The authentication framework is based on **Microsoft Identity Platform** which offers identity-as-a-service and implements authentication and authorization with industry standard protocols OpenID Connect (OIDC), SAML 2.0, WS-Fed and OAuth 2.0. Using OAuth2.0, Power Pages enables multiple identity providers such as Microsoft, LinkedIn, Google, Facebook, Twitter, etc. Additionally, website makers can configure additional enterprise Identity providers such as Azure AD, Azure AD B2C, Okta, Auth0, etc. using OpenID Connect, SAML 2.0 and WS-Fed. The identity provider configuration is available for website makers to enable a wide variety of identities with Power Pages. Once authenticated, a users' access to website content and data is controlled via configurable Role-based access controls (RBAC).

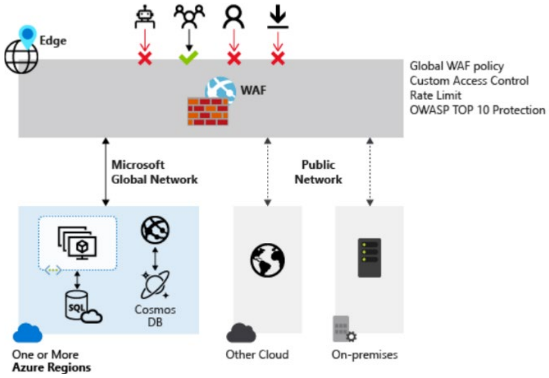
Admins and makers can configure authorization for anonymous and authenticated users on Power Pages by configuring **Web Roles**, **Table Permissions** and **Page Permissions**. Authorization determines resources (Website Pages, Business data) that a website user (Anonymous, or Authenticated) has access to in Power Pages. **Web Roles** provides a way to group users, **Table Permissions,** and **Page Permissions** control and protect access to business data and website content. Makers can also create web roles for custom use-cases and associate them to Table Permissions and Page Permissions for implementing granular access controls.

Power Pages Architecture White paper describes Authentication and Authorization in depth.

Perimeter

Power Pages leverages Azure's Distributed denial of service (DDoS) basic protection, which includes always-on traffic monitoring and real-time mitigation of common network-level attacks. Customers can also protect their Power Pages sites by purchasing and leveraging the standard tier of Azure DDoS protection that supplies additional capabilities to protect against volumetric attacks, protocol attacks, and application attacks.

Network



Admins can configure Web Application Firewall (WAF) with their Power Pages sites. WAF sits on the edge of the network and provides centralized protection of the site from common exploits and vulnerabilities, including protection from OWASP Top 10 security vulnerabilities. Power Pages can be integrated with several WAF providers. WAF integration with Power Pages enables administrators to control access to Power Pages sites from a geography, VPN, or a specific network. Power Pages also provides **turn-key configurations** to enable **Azure WAF**. With Azure WAF enabled, each Power Pages site is intelligently secured against known and new threats with security protection mechanisms that embrace a ***Zero Trust*** framework.

Site Admins can also use IP (Internet Protocol) Address Restriction capability in Power Pages to filter network traffic to their site, which enables admins to limit access to a list of IP addresses. When a request to the website is generated, the user's IP address is evaluated against the "allow" list. If the IP address is not on the list, the website displays a webpage with an HTTP 403 status code. This capability can be used when website traffic originates from known networks. (e.g., a corporate network)

Compute

Power Pages run on Azure App service, which offers native protection for compute and infrastructure. The platform components of App Service, including Azure VMs (Virtual Machines), storage, network connections, web frameworks, management, and integration features, are actively secured and hardened. Microsoft Defender for Cloud is natively integrated with the Azure App service and monitors threats to underlying resources, including a complete list of MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) tactics from pre-attack to command and control. It can also detect Dangling DNS. App Service goes through vigorous compliance checks on a continuous basis to make sure that:

- App resources are secured from the other customers' Azure resources.
- Virtual Machine (VM) instances and runtime software are regularly updated to address newly discovered vulnerabilities.
- 24-hour threat management protects the infrastructure and platform against malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats.

Application

Power Pages offers multiple controls and configurations that enable makers and admins to harden security at the Application layer.

1. **Authentication and Authorization:** Power Pages allows **authorized** users access to website content and business data. Makers can choose to configure a wide variety of Authentication providers on Power Pages to allow users to sign in securely. Once a user is signed in, Power Pages checks Authorization for the user. Each anonymous or authenticated user can be granted Web roles which can be linked with Page Permissions and Table permissions that specify what parts of the website the user can access, and what business data they interact with. Column permissions can additionally be applied if granular control on Table columns is necessary. Using the authorization techniques available, a maker can choose to restrict access to certain parts of the website and data for authenticated users or groups of authenticated users than other parts of the site which are open to the public anonymously. Power Pages offers tools like Portal Checker which enables makers to uncover common configuration issues with their websites.

2. **HTTPS Only**: Each Power Pages site comes with a digital certificate (SSL) that authenticates its identity and enables an encrypted connection between the browser and the Power Pages site. Internet traffic to Power Pages sites is encrypted and enforces HTTPS (Hyper Text Transport Protocol Secure). When branding their site with a custom domain, admins should use a secure SSL certificate and link it to their site.

3. **Managed Application Identity**: Each Power Pages site uses a managed Azure Active Directory (AAD) identity which allows it access other Azure Active Directory-protected resources and integrations with other services like Power BI, SharePoint, Microsoft Dataverse, etc.
4. **HTTP Security headers**: These are directives used by web applications to configure security defenses in web browsers. Power Pages offers advanced web security tightening capabilities for makers via configuration of HTTP Security headers. The HTTP Security Headers that Power Pages honor are described below as **Default** and **Configurable**. The default headers are set by the platform for responses. Makers can configure **additional HTTP security headers** for added security based on specific needs.

   Default Headers:

   - **HTTP Strict Transport Security (HSTS)**: HTTP Strict Transport Security is a web security policy mechanism that helps protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections. Power Pages use HSTS and HTTPS is enforced, which means that requests over HTTP get automatically redirected to HTTPS.
   - **Referrer-Policy**: The Referrer-Policy HTTP header governs which referrer information, sent in the Referrer header, should be included with requests made. Power Pages sets the Referrer-Policy response header for responses.
   - **Cache-Control**: This header holds directives (instructions) for caching in both **requests** and **responses**. Specifying the capability of a resource to be cached is important to prevent exposure of information via the cache. Power Pages sets the Cache-control header for responses.

- **X-Content-Type-Options**: Setting this header prevents the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header (e.g., treating text/plain as text/CSS). Power Pages sets this header for responses.
- **X-Frame-Options Header (XFO)**: The X-Frame-Options response header improves the protection of web applications against clickjacking. It instructs the browser whether the content can be displayed within frames. Power Pages sets this header for responses.

Configurable Headers:

- **X-Frame-Options Header (XFO)**
- **X-Content-Type-Options**
- **Content Security policy (CSP)**: Content Security Policy is an extra layer of security that helps detect and mitigate certain types of web attacks such as data theft, XSS, site defacement, or the distribution of malware. CSP provides an extensive set of policy directives that help control the resources that a site page is allowed to load. Each directive defines the restrictions for a specific type of resource.
    - When CSP is turned on for a Power Pages website, it blocks connections, scripts, fonts, and other types of resources that originate from unknown or malicious sources. CSP is turned off by default in Power Pages; however, many websites might require CSP to enhance security.
    - **Number Only Once (Nonce)**: Enabling *nonce* (Number used once) in Power Pages blocks execution of all inline scripts except those specified within the inline script. A unique cryptographic nonce is generated and added to each script specified in the CSP header.
- **Cross Origin Resource Sharing (CORS)**: This protocol consists of a set of headers that indicates whether a HTTP response can be shared with another domain. CORS is blocked by default on Power Pages for security. When a Power Pages site is embedded into another application, makers can configure CORS.

5. **Cookie Security**: Power Pages use cookies to store information for various purposes. The details of various cookies used in Power Pages can be found here. By default, sensitive cookies are created and set by the Power Pages server with attributes- **Secure** and **HttpOnly**. A cookie with the **Secure** attribute is sent to the server with an encrypted request over the HTTPS protocol, which prevents it from man-in-the-middle attacks. **HttpOnly** is an *additional flag* included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client-side scripts accessing the protected cookie. With HttpOnly attribute set on cookies browsers will not reveal the cookie to a third party and thereby prevent against cookie replay attacks.

   Makers have the flexibility to configure **SameSite Cookie** attribute as “Strict” on Power Pages to declare if cookies should be restricted to a first-party or same-site context.

6. **Cross-Site Request Forgery (XSRF/CSRF) Protection**: Cross-site request forgery is an attack against web applications whereby a malicious web app can influence the interaction between a client browser and a web app that trusts that browser. These attacks are possible because web browsers send certain types of authentication tokens automatically with every request to a website. This form of exploit is also known as a *one-click attack* or *session riding* because the attack takes advantage of the user's previously authenticated session. Power Pages provides **protection** from XSRF/CSRF attacks by using

anti-forgery tokens to protect writes. The anti-forgery token is a unique token that gets generated by the Power Pages backend server whenever the client requests a page and is validated by the server on every write to identify a genuine client.

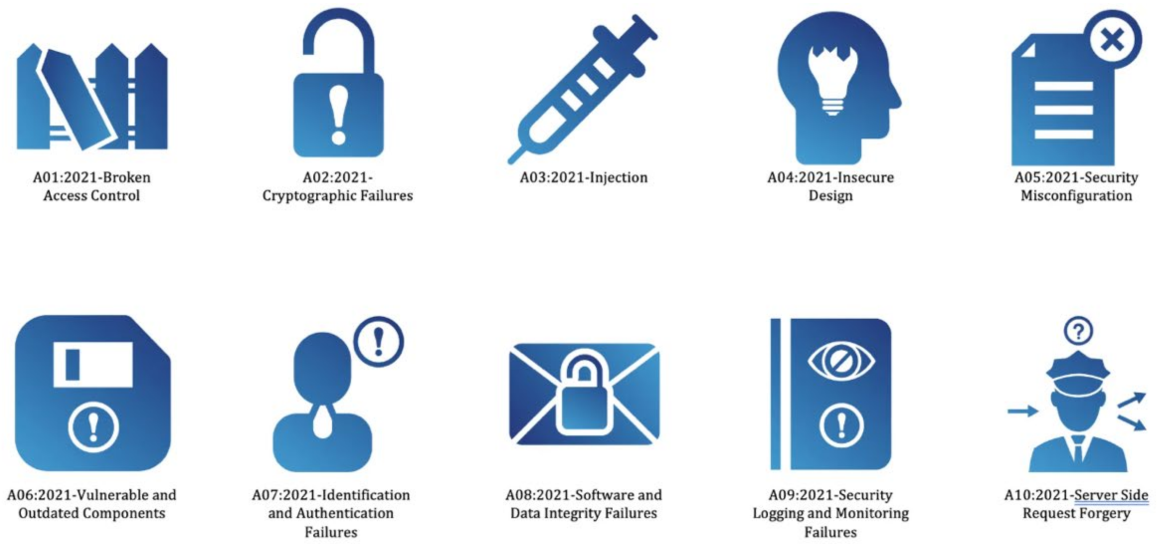
Data

Protecting data is a multi-layered process and appropriate data management is a critical part of this process. Improper handling of data weakens security and creates security and privacy risks. Business data that Power Pages interact with is stored in Microsoft Dataverse, where it is encrypted both at-rest and in transit.

OWASP Top 10 Risks: Mitigations in Power Pages

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve software security. Through community-led open-source software projects, hundreds of chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

The OWASP top 10 is a standard awareness document for developers and others who are interested in web application security. It represents a broad consensus about the most critical security risks to web applications. **Security is a shared responsibility**- This section describes how Power Pages helps mitigate OWASP Top 10 security risks by providing core security capabilities and controls by default and the configurations and tools that are available to administrators and makers to tighten and harden security for their Power Pages sites.


A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server Side Request Forgery

Makers can integrate Web Application Firewall with Power Pages that monitors, filters, and blocks malicious requests to the website. **Web application firewall** (**WAF**) strengthens security as it applies a set of security rules to HTTP traffic to and from an application thereby protecting applications from OWASP Top 10 risks. Power Pages offers out of the box integration with Azure Web Application Firewall via simple configuration.

A01:2021 Broken Access Control

Broken Access Control in any web application leaves the application susceptible to attackers who can access, modify, or delete unauthorized content or data. The attackers may also take over a web application's administration with a broken access control. Power Pages offers protection from Broken Access Control threats through five different layers of Application security and control mechanisms:

Least Privileged Access
Governance Controls
Secure by Default
Secure Access via Authentication
Authorization & Access Control

1. **Least Privileged Access (LPA):** Power Pages security model is built on Least Privileged Access (LPA). LPA enables customers to build applications with more granular access control where Power Pages makers can choose to specify levels of access for end users accessing the website. Makers must ensure that the

principle of LPA is honored when assigning Web Roles, Table Permissions and Page Permissions to website users. The Power Pages out of the box Administrative and Maker roles honor LPA. Makers and admins must follow the principles of least privileged access when extending maker or administrative privileges to additional users.

2. **Governance Controls on Site Administration and Customization**: Only entrusted makers in an organization have access to creating and authoring Power Pages Sites. Site administration and authoring are not enabled for external users and are enforced via Microsoft Azure Active Directory Identity protection and specific security roles. Power Pages offers the following governance controls to admins:

    a. **Website Visibility**: New Power Pages sites are **Private by Default** on creation to prevent unintended broader exposure of business data. When a site's visibility is set as "Private" only entrusted makers can browse the site. When a site is Private, a maker can share the site with organizational users or other makers for preview via an explicit share action. After a maker has carefully reviewed and validated business data and content on the site, they can choose to make the website visibility "Public", which makes the site available for authorized website visitors. Admins can exercise governance controls to control makers who can make sites "Public". Portal Checker detects common security misconfiguration on sites which can be run to find and fix issues before launching a website for broader external access.

    b. **Website Creation**: Website creation requires makers to have certain privileges and roles as documented here. Admins can exercise additional governance controls if they wish to disable portal creation in a tenant by non-administrators.

3. **Secure By Default:** New Power Pages site's visibility is **Private by Default** upon creation, providing makers with flexibility and control to publish the site only when they have completed website building and fully validated website configurations. The platform also offers tools like Maintenance Mode to take the site down for deployments or internal maintenance operations. Out of the Box website templates, maker and admin experiences offer Secure Default configurations for features to prevent unauthorized access of any website data or configuration. Makers must confirm and test the website's configuration and review data visibility in their dev and test environments for all business use cases before they change Website Visibility as "Public". Portal Checker can be run to detect common security misconfiguration on sites. Makers can leverage **Cookie Security** and **HTTP Security headers** capabilities described above to prevent against common security threats like XSS, clickjacking and session thefts.

4. **Secure access via Authentication:** Authentication Provider configuration complexity increases the probability of Authentication issues, which result in vulnerability in applications from threats due to Broken Access control. Power Pages offers an intuitive Low Code Authentication Provider configuration experience for Makers to securely configure a wide variety of authentication providers. Power Pages provides Out of the box integration with Azure Active Directory (Azure AD) for authentication and can be easily integrated with other industry standard Identity providers. While configuring Authentication providers on Power Pages makers must review their organizational security policies (Requiring Multi-Factor Auth, Session Logout, Single Log Out, etc.) and validate authentication provider configurations through testing. Makers **should not** use deprecated functionalities like "Local Authentication" and instead use the more secure Azure AD B2C identity provider on Power Pages for external identities.

    Power Pages also allows makers to make client-side calls to external APIs securely using OAuth implicit grant flow.

5. Authorization via Access Controls:

There are three major types of access control mechanisms that Power Pages offers. For each control type there are default security capabilities that are offered by Power Pages and controls for makers and admins to enable stricter security for their applications to protect sensitive data and assets.

a. **Vertical Access Controls:** Vertical access control mechanisms restrict access to sensitive application functions based on user type. Power Pages implements Vertical Access controls to offer protection against Elevation of Privilege threats. With vertical access controls, distinct types of users have access to different application functions. For example, a Power Pages website administrator can add custom branding to their Power Pages site and manage the site's lifecycle, while an ordinary user does not have access to perform such administrative actions. Likewise, a website maker has control to author the site and change site configurations, but these privileges are not available to a website visitor. Website visitors, makers or admins cannot elevate their privileges to undertake unauthorized actions. Makers and admins must ensure that the principle of Least privilege access is followed, and only entrusted makers or admins have access to privileged operations. Makers and admins must set well-defined limits on access that is provided to authorized users and groups. Access to unauthorized users and groups must be explicitly denied. It is not recommended to share administrative passwords or accounts with multiple users.

b. **Horizontal Access Controls and Role Based Access Control**: Horizontal Access Control mechanisms restrict access to application resources to users who are specifically allowed to access them. Authentication for Power Pages admin and maker experiences leverages Azure Active Directory for security and protection of identities. Power Pages offer a robust security model which is based on industry standard authentication and a role-based access control mechanism for Authorization. Requests to Power Pages sites go through the Access control layer and are denied when not authorized. Makers can utilize Web Roles, Page Permissions and Table Permissions to configure access for the website and business data for external users.

   Power Pages makers must review that the site's access is enabled only for authorized users by reviewing and validating website users' Web Role association, Table permissions, and Page permissions. Portal Checker detects common security misconfiguration on sites which can be run before launching a website for external access.

c. **Context Dependent Access Control:** Context dependent access control mechanisms restrict access to functionality and resources based on the state of the application or the user's interaction with it. They prevent a user from performing actions in the wrong order. As an example, consider a Power Pages site that allows users to provide personal information and then submit a Visa application. A maker defines this Visa application form as an advanced form on Power Pages with each step being mandatory. When a website user interacts with this multi-step form, they cannot skip steps without filling in the necessary intermediate steps. Additionally, website users cannot modify the data submitted on the form after submission. This is an example of context dependent access control. The extensibility of the Power Pages platform allows low code and pro-developer makers to implement context dependent access controls via custom controls, business rules, Web APIs and plugins which can prevent website users from performing any business actions exposed on the website, in the wrong order. Out of the box solution templates and workflows honor context dependent access controls.

A02:2021 Cryptographic Failures

Cryptographic failures risk exposure of critical or sensitive business data which could make applications vulnerable to data leak related security threats. Power Pages allow internal or external users of organizations or governments to interact with business data. When it comes to Enterprise Security- protecting data is at the core. Data is an organization's most valuable and irreplaceable asset, and encryption serves as the last and strongest line of defense in a multi-layered data security strategy. Microsoft business cloud services and products use encryption to safeguard customer data. Power Pages and Microsoft Dataverse ensure that customer data either in transit or at rest is **encrypted** using highest industry standard encryption methodologies.

Data in transit

Each Power Pages site is secured via HTTPS which enables secure and encrypted communication between the users' browser, over the network, and the backend servers powering the site. Power Pages uses Transport Layer Security (TLS) to encrypt HTTP-based network traffic. HTTP requests are redirected and use of HTTPS Only is enforced. The SSL certificate that Power Pages sites use is periodically renewed and updated to conform to the highest standards of security. Admins can also configure a custom domain for branding their sites by uploading secure SSL certificate and linking websites with custom domain.

Power Pages employs a hardened TLS configuration by using TLS 1.2 or above that enables HTTP Strict Transport Security (HSTS). It uses Strong cipher suites (ECDHE-based and NIST curves) to encrypt data and stronger ciphers are higher in the order of cipher suites presented by the platform over weak ciphers. The platform uses strong keys for encryption in transit.

Data at rest

The customer data that Power Pages interacts with- business data and the sites' configuration data is stored in Microsoft Dataverse- a secure business data store. Dataverse databases use SQL Server TDE (Transparent Data Encryption), compliant with FIPS (Federal Information Processing Standards) 140-2 to provide real-time I/O encryption and decryption of the data and log files for data encryption at-rest. Azure Storage Encryption is used for data at rest stored in the Azure Blob Storage. These are encrypted and decrypted transparently using 256-bit AES (Advanced Encryption Standard) encryption compliant with FIPS 140-2. The data stored in Dataverse is distributed across different storage types:

- Azure SQL Database for relational data
- Azure Blob storage for binary data, such as images and documents
- Azure Search for search indexing
- Microsoft 365 Activity Log and Azure Cosmos DB for audit data

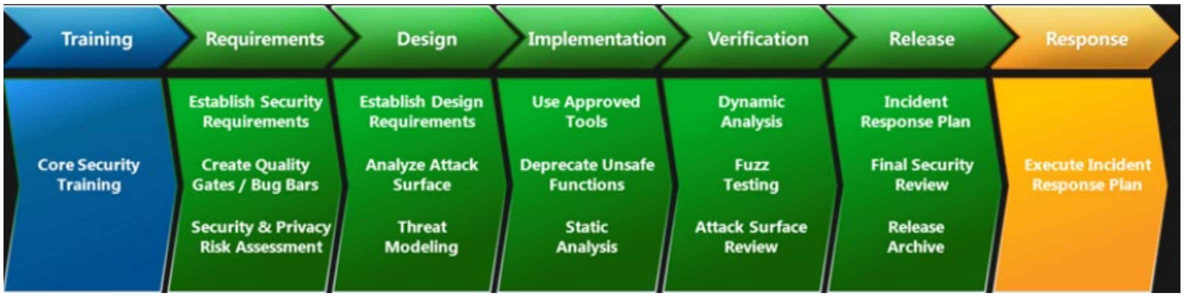
By default, Microsoft stores and manages the database encryption key for Power Platform environments.

Microsoft provides an additional ability to encrypt data in Dataverse with customer provided encryption key. As of now, given the heterogenous storage, the customer managed key feature is available only for the Azure SQL database that stores transactional data.

A03:2021 Injection

Injection is an attacker's attempt to send data to an application in a way that changes the meaning of commands being sent to an interpreter. For example, the most common example is SQL injection, a SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

Power Pages uses industry-standard best practices to prevent injection attacks. Power Pages product development follows Microsoft's standard SDLC patterns which involve a full Software Development Cycle review every 6 months spanning the entire product.



In addition, the following security strategies enable Power Pages to mitigate risks from Injection flaws:

- Server-side sanitization and validation of input data and user data, the output data is also sanitized with server-side validations before its rendered
- HTML input and output data is HTML encoded
- Power Pages uses safe APIs with parameterized interfaces
- Static and dynamic analysis tools are used during build time to detect security bugs at source
- Periodic assessment of Threat Model on new capability releases or every six months, whichever falls earlier

The following tools are available to makers to protect against injection flaws:

- Enable Azure Web Application Firewall with Power Pages.
- Makers must ensure that html encoding is applied for custom components. When working with Liquid objects to read untrusted data, use of escape filter is recommended.
- When reading URL parameters using JavaScript, makers should apply html encoding to prevent Cross-site scripting.
- When working with Web APIs on Power Pages, makers must apply html encoding on the API response before using the data returned.
- Enable Content Security Policy and Nonce for additional security.

A04:2021 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." There is a difference between insecure design and insecure implementation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

Power Pages is built on the culture and methodology of secure design. Both culture and methodology are constantly reinforced through Microsoft's industry-leading Security Development Lifecycle (SDL) and Threat Modeling practices which constantly evaluate threats and ensures that code is robustly designed and tested to prevent known attack methods. New features and services on Power Pages periodically go through Threat modeling. The Threat Modeling review process ensures that threats that are identified during the design phase are mitigated and validated periodically.

Threat Modeling also accounts for changes to services that are already live through continuous regular reviews. Relying on the STRIDE model helps Microsoft address the most common issues with insecure design.

Microsoft performs periodic security and penetration testing to detect vulnerabilities in services and applications. The penetration testing reports can be downloaded from Microsoft Trust center.

A05:2021 Security Misconfiguration

Attackers often try to exploit unpatched flaws or access default accounts, unused pages, unprotected files, and directories, etc. to gain unauthorized access or knowledge of the system.

Power Pages offers protection against Security Misconfigurations using the following methods:

- Most new capabilities and configurations are set to “off” by default to uphold a “Default Deny” Design principle. Customers need to review and opt for new features and configurations.
- The Power Pages “Secure by Default” approach ensures that any new capability does not compromise application security once deployed or enabled.
- Backend servers where Power Pages are deployed worldwide are periodically patched and updated to prevent any security vulnerabilities.
- Since Power Pages follows Microsoft SDLC, open source, or third-party software and components used are periodically reviewed and updated to harden the application’s security against flaws.
- Power Pages runs on Azure Platform as a Service (PaaS). Microsoft Defender protects the hosting infrastructure and monitors applications for a wide variety of threats like MITRE Att&CK (Adversarial Tactics, Techniques and Common Knowledge) tactics and Dangling DNS detection.
- Files and directories hosted on backend servers and the infrastructure hosting the servers themselves are locked to prevent unauthorized or unintended access.

Additionally, makers can use Portal Checker to identify and address common configuration errors leading to insecure configurations. Before Power Pages Go-live, Authentication Provider and Authorization configuration on Power Pages sites can be reviewed to ensure that website content and data can be accessed only via authorized users.

A06:2021 Vulnerable and Outdated Components

Power Pages follows Microsoft's SDL practices to manage open-source and third-party components and libraries. These practices include maintaining complete inventory, performing security analyses, keeping the components and libraries up to date, and aligning the components with a tried and tested security incident response process. Azure, the hosting platform for Power Pages, provides periodic and automatic operating System patching and keeps the underlying infrastructure protected.

Customers who utilize external open source or third-party libraries and components with Power Pages should perform similar periodic assessments and update vulnerable or outdated components and libraries.

A07:2021 Identification and Authentication Failures

Power Pages allows both anonymous and authenticated website users to interact with business data and processes securely. When it comes to securing identities, confirmation of the user's identity, authentication, and session management are critical to protect against authentication-related attacks.

Power Pages is built on Microsoft's Identity Platform and provides out of the box integration with Azure Active Directory (AD) for identification and authentication. Azure AD and Azure AD B2C helps Power Pages to enable security features for authenticated users. These features include single sign-on, single log-out, multi-factor authentication, session management, session timeouts and a single platform to engage with internal and external users more securely.

Power Pages can also be configured with other industry standard Identity and Authentication providers. When using providers other than the Out of Box providers, makers must ensure that the Identity Provider configuration meets the security policies of their organizations.

A08:2021 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs).

- Microsoft employs a Component Governance process for Microsoft managed repositories that enforces secure configuration of package source files to maintain software integrity.
- The process ensures that only internally sourced packages are served to address substitution attack. Substitution attack, also known as dependency confusion, is a technique that can be used to poison the app-building process inside secure enterprise environments.
- Encrypted data has integrity protection applied before it is transmitted. Integrity protection metadata present for incoming encrypted data is validated.

Makers building Power Pages sites must ensure that they use trusted sources for utilizing open-source or third-party libraries, components, and APIs on their site. Customers can protect their internal application repositories by restricting corporate access and running static and dynamic security analysis tools. _ Out of the box templates, data and integrations in Power Pages are penetration tested periodically. It is recommended that customers perform penetration testing on their Power Pages sites especially when their implementation involves use of third party libraries or external APIs.

A09:2021 Security Logging and Monitoring Failures

Logging and monitoring are critical ways to detect, escalate, and respond to active security breaches. Customers can prevent risks from Security logging failures on Power Pages by leveraging Audit Logging capabilities that the platform offers. With Audit logging, Power Pages logs failed login transactions and server-side input validation failures to identify suspicious or malicious attempts. Makers or admins can configure audit logging and can download detailed activity logs for Power Pages website from Microsoft 365 Compliance center.

Microsoft implements a Standardized Security Incident Response Process (SSIRP) which is Microsoft’s incident response process for responding to major threats to our customers, including exploits in the wild that are being used to attack customers, threats to the security of Microsoft’s services like Azure, Dynamics, Power Platform and O365, and the public disclosure of unpatched vulnerabilities that could be used to attack customers. Microsoft’s SSIRP enables Microsoft to respond to active security breaches.

Application Insights is widely used within the enterprise landscape for monitoring and diagnostics. Makers can integrate Power Pages sites with Azure Application Insights for advanced monitoring, diagnostics, and performance insights.

A10:2021 Server Side Request Forgery (SSRF)

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL). Power Pages offers protection from SSRF attacks by:

- Enforcing URL schemas
- Validating and sanitizing user inputs and liquid request objects (user and request)
- Avoiding sending a raw response body from Server to client

Makers implementing Power Pages sites must ensure that they follow the principles above when creating advanced custom implementations and controls on Power Pages.

Conclusion

Power Pages offers various security capabilities and tools to build secure externally facing applications. Its Defense-in-depth capabilities provide seven layers of protection for application and business data. Power Pages helps customers mitigate OWASP Top 10 Web Security risks by providing core security capabilities and controls by default along with the configurations and tools that are available to administrators and makers to tighten and harden security for their Power Pages sites.

Security is a shared responsibility- Power Pages provides considerable advantages for organizational security and compliance efforts, and at the same time, the tools and capabilities must be used in a way that protects users and organizational data.