



Power Pages

Architecture White paper



Power Pages Platform Capabilities and Architecture white paper

Abstract

This white paper provides a comprehensive view of the capabilities of the Power Pages Platform. It describes the architectural elements that enable Power Pages to scale, offer high reliability and availability, and protect business data to offer enterprise grade compliance and security.

DIPTI JAISWAL

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

Abstract..... 0

Power Pages - An Overview.....2

 What is Power Pages?..... 2

 Why Power Pages?..... 2

Power Pages Platform Capabilities4

Architecture.....4

 Data storage..... 5

 Business Continuity and Disaster Recovery (BCDR) 5

 Fault tolerance 6

 High availability..... 6

 Traffic routing 6

 Availability and reliability 7

 Hyper Scale 7

 Dataverse integration and authentication 7

 Authentication in Power Pages 7

 Authorization 9

 Security 10

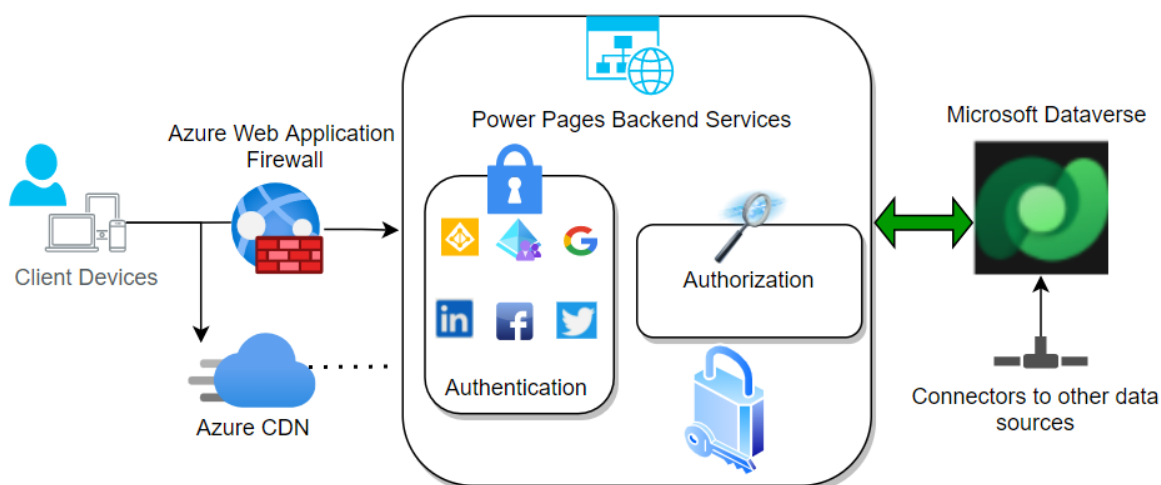
 Compliance 10

Conclusion10

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.

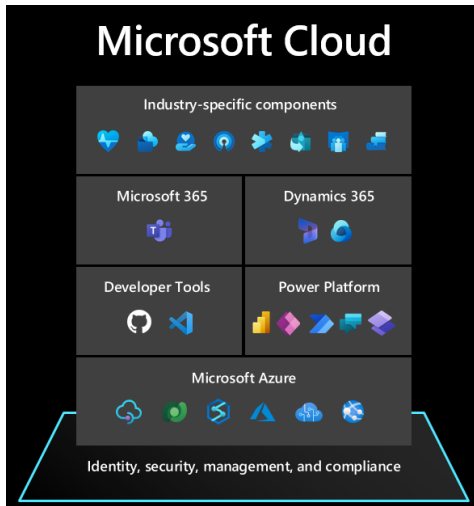


Power Pages offers enhanced **control**, **protection** and **security** for administrators, website makers, and website visitors. It empowers makers to extend business data and processes to external users securely and helps ensure compliance. As a platform, it offers comprehensive compliance coverage across global, regional, government, and industry-specific compliance standards, making it one of the most trusted Low code application platforms. 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.

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 rapid enterprise scale deployment and scaling abilities, 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 offers industry-leading security, resilience, and protection to business applications, processes, and data. Today many national security agencies, community services, financial institutions, and health care providers entrust Power Pages with their most sensitive information.

This white paper describes Power Pages platform capabilities, and architecture, and explains how the platform is designed to offer high reliability, performance, and availability. It then moves on to describe how users, both internal and external, authenticate to Power Pages, how these users connect with data stored on Dataverse, and how Power Pages enables secure access to this data to a wide variety of users.

The Power Pages service is governed by the [Commercial Licensing Terms \(microsoft.com\)](https://www.microsoft.com/commercial-licensing-terms) and the [Microsoft Enterprise Privacy Statement](https://www.microsoft.com/privacy/enterprise-privacy-statement). For the location of data, refer to the location of data section in the [Microsoft Privacy and Security terms](https://www.microsoft.com/privacy/privacy-and-security-terms) and to the [Data Protection Addendum](https://www.microsoft.com/privacy/data-protection-addendum). For compliance information, the [Microsoft Trust Center](https://www.microsoft.com/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](https://www.microsoft.com/compliance).

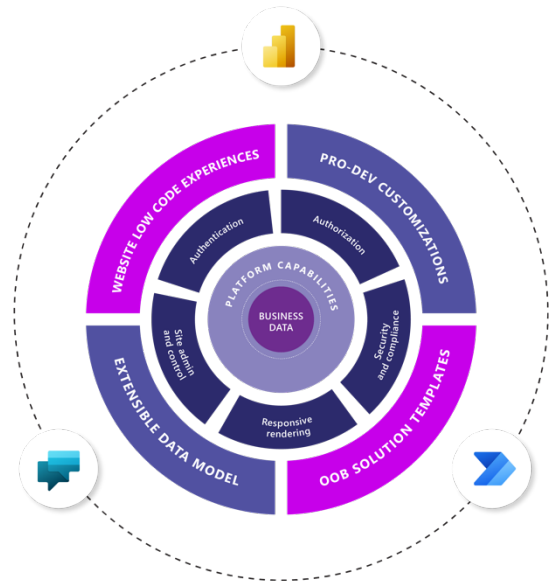
The Power Pages service follows the Security Development Lifecycle (SDL), strict security practices that support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost. Learn more at [Microsoft Security Development Lifecycle Practices](https://www.microsoft.com/security-dev-lifecycle).

Power Pages Platform Capabilities

Power Pages Platform’s key capabilities can be represented in **two layers**, the **enterprise-grade core platform layer**, and the **website-making assets**.

Layer 1: The **enterprise-grade core platform** uses **Dataverse** to securely collect, store, and share business data. A wide variety of **authentication** models enable login experiences for external users, and robust **authorization** manages user access to business data and website pages. The platform implements high standards of security and compliance and provides makers with control via site administration and governance. Finally, the platform provides automatic website **responsive rendering** to various form factors such as mobile, desktop, and tablets.

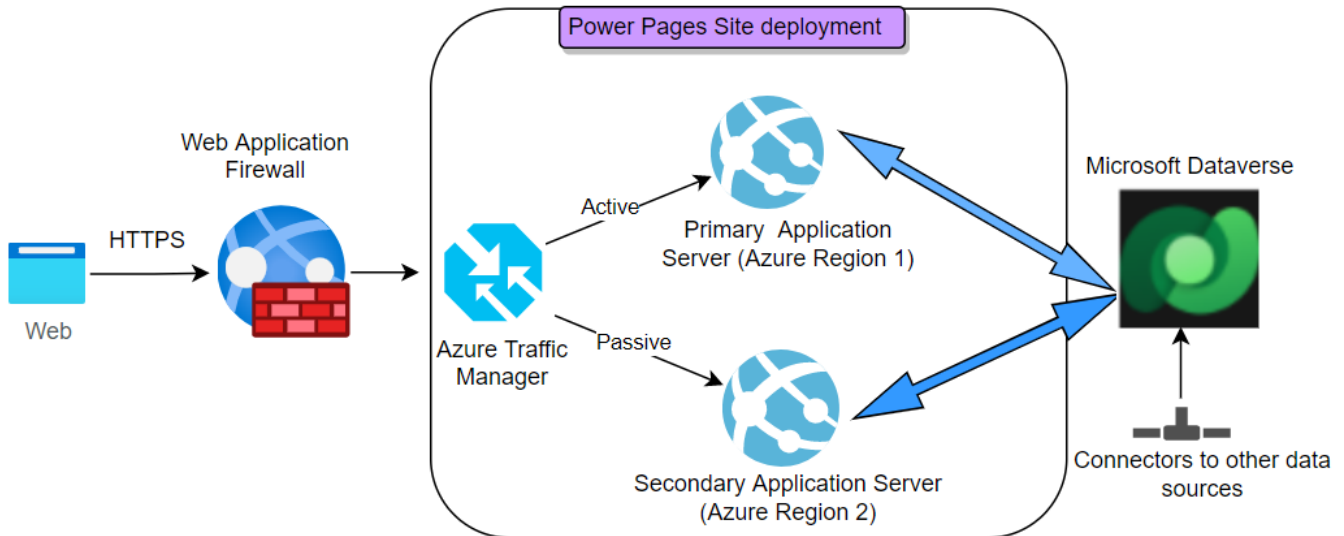
Layer 2: The **website-making assets** include a website maker experience to build rich business websites using a click-and-drag interface. Professional developers can customize these apps through custom theming and create sophisticated website interactions through Visual Studio/VS Code integration. [These](#) pro-developer capabilities enable makers to check in site configuration to source control in GitHub and Visual Studio Code and utilize Azure Dev Ops and GitHub Automation for continuous integration and deployment. Out of the Box (OOB), high-value solution templates enable makers to jumpstart creation of modern, sophisticated business websites. The extensible data model enables makers to describe business data they will collect and share with their audience. Additionally, makers use Power BI, Power Automate and Power Virtual Agents to enable dashboards and reports, workflow automation, and bot experiences on Power Pages.



Architecture

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 common attacks, such as [SQL injection](#), [cross-site scripting](#) (XSS), file inclusion, and improper system configuration.

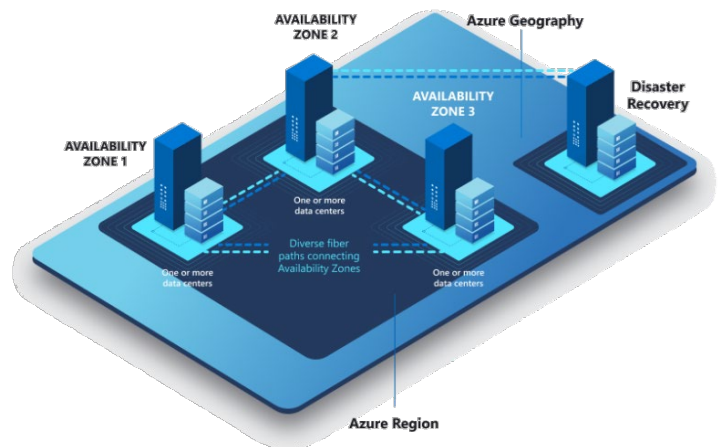


Data storage

Power Pages leverages [Microsoft Dataverse](#) as its metadata and business data store. Each site is connected to one Dataverse Environment. Dataverse securely stores and manages data used by business applications. Dataverse includes a core set of standard tables that cover typical scenarios and supports the creation of custom tables to support a variety of business use cases. This data is [encrypted](#) in transit and at-rest.

Business Continuity and Disaster Recovery (BCDR)

Unless specifically noted in our documentation for a specific geography, each Power Pages site is deployed on two different application servers- Primary and Secondary. These application servers reside in two different Azure regions in the same geography to support Business Continuity and Disaster Recovery. Azure regions are designed to achieve reliability and resilience for business-critical workloads. Each Azure region features datacenters deployed within a latency-defined perimeter. They're connected through a dedicated regional low-latency network. This design ensures that Azure services within any region offer the best possible performance and security.



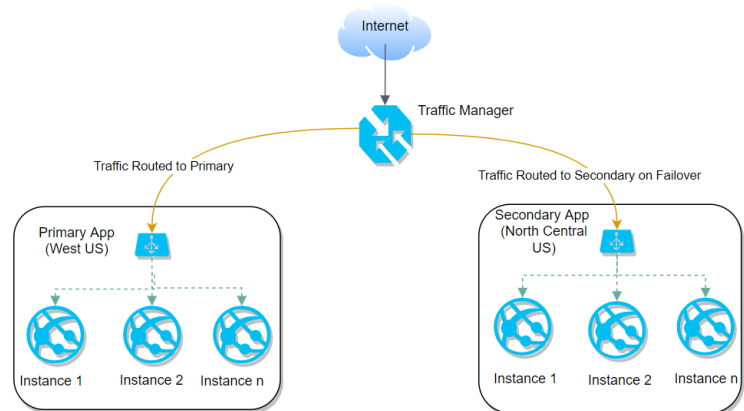
Fault tolerance

Fault tolerance refers to the ability of an application to continue uninterrupted operation despite failure of one or more of its components. A well-designed fault-tolerant system prevents disruptions arising from single point of failures, ensuring high availability and business continuity of mission-critical applications.

Designing for fault tolerance, removing single points of failure, and mitigating risk of geography wide and global outages are key to application **resiliency** and reliability. Power Pages are designed for high resiliency and are fault tolerant to most software and infrastructure failures. Each Power Pages site is hosted on Azure in a sandboxed environment

to ensure that it is fully isolated and remains unaffected by noisy-neighbor situations. Each site hosted on Azure uniquely represents one website defined by **metadata**- privileges, permissions, website layout (web pages, web templates, content snippets, header, footer, etc.) and **data** (Custom tables like vaccine, student, course, etc.). Both website metadata and data are stored in Dataverse which enables isolation, replication, and fault tolerance for business data. Each site's backend application server can be configured to scale out with multiple instances for redundancy, using a **shared-nothing** architecture. The multi-instance deployments offer infrastructure level isolation and fault tolerance.

Each Power Pages site can be independently deployed, managed, run, and administered. This shared-nothing architecture, paired with geographical redundancy ensures that Power Pages are agnostic to software, hardware, or infrastructure failures.



High availability

Unless specifically noted in our documentation, each site's deployment is set up in regional data center pairs in the same geography for high availability. Web traffic fails over to secondary application server when the traffic manager detects primary server to be down. This design ensures uninterrupted application availability even in scenarios when one Azure data center may be completely down or when a data center faces disruption due to an interrupted network availability.

Traffic routing

Website traffic is routed to each site's primary application server based on priority routing as determined by the traffic manager. The traffic manager performs periodic health checks to figure out when to automatically fail over traffic from the primary application server, when it is unhealthy, or unreachable, to the secondary application server.

Availability and reliability

Power Pages offers high reliability for website requests. The platform serves billions of requests catering to hundreds of millions of users, both anonymous and authenticated. Power Pages is hosted on multiple datacenters including sovereign clouds which offer isolated in-country hosting of software and services with independent authentication, storage, and compliance requirements. With advanced elastic scaling capabilities each portal backend server can automatically scale vertically or horizontally to suit dynamic workloads and provides innate capability to adjust scaling to burst traffic patterns. This scaling on Power Pages is determined based on licensing capacity allocated to each site. Advanced scaling abilities allow the platform to run internet scale workloads for citizens, governments, countries, and organizations. For example, some Power Pages sites have received 18,000 Requests per second with sub-second 95th percentile performance.

Hyper Scale

Traditional auto-scaling rules are insufficient for handling unpredictable burst and volatile load patterns where traffic instantaneously ramps to millions of concurrent users for scenarios like a flash sale, a marketing event, ticket registrations, or vaccine registrations. The following plot shows the volume of requests on one such Power Pages site plotted against time. Note the steep curve which shows how traffic ramps up 2000 times within 5 minutes.



Power Pages offer **high scalability** and inherent capabilities to aid hyperscale to support citizen scale deployments. Power Pages offer a [turnkey integration with Azure CDN](#) (Azure Content Delivery Network) to enable hyper scale and improved performance for end user experiences by using Edge Caching.

Dataverse integration and authentication

Each Power Pages site uses a secure connection to integrate with Microsoft Dataverse. Each site's identity is uniquely represented as an Azure Active Directory application in the tenant. This Azure Active Directory application hosted in the tenant allows Power Pages to use advanced Azure Identity security capabilities.

Authentication in Power Pages

Authentication verifies the identity of a user on Power Pages. Organizations using Power Pages can choose from a variety of authentication providers or allow Power Pages sites to be securely accessed by anonymous users. Power Pages 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, respectively. Microsoft's Azure AD and Azure AD B2C Identities offer advanced capabilities like [Conditional Access](#) which extends the security perimeter beyond organizational boundaries where organizations can use identity-driven signals as part of their access control decisions. Azure AD and Azure AD B2C identity providers can also be configured for additional capabilities like [Multifactor Authentication](#), [Password less](#) Authentication on Power Pages.

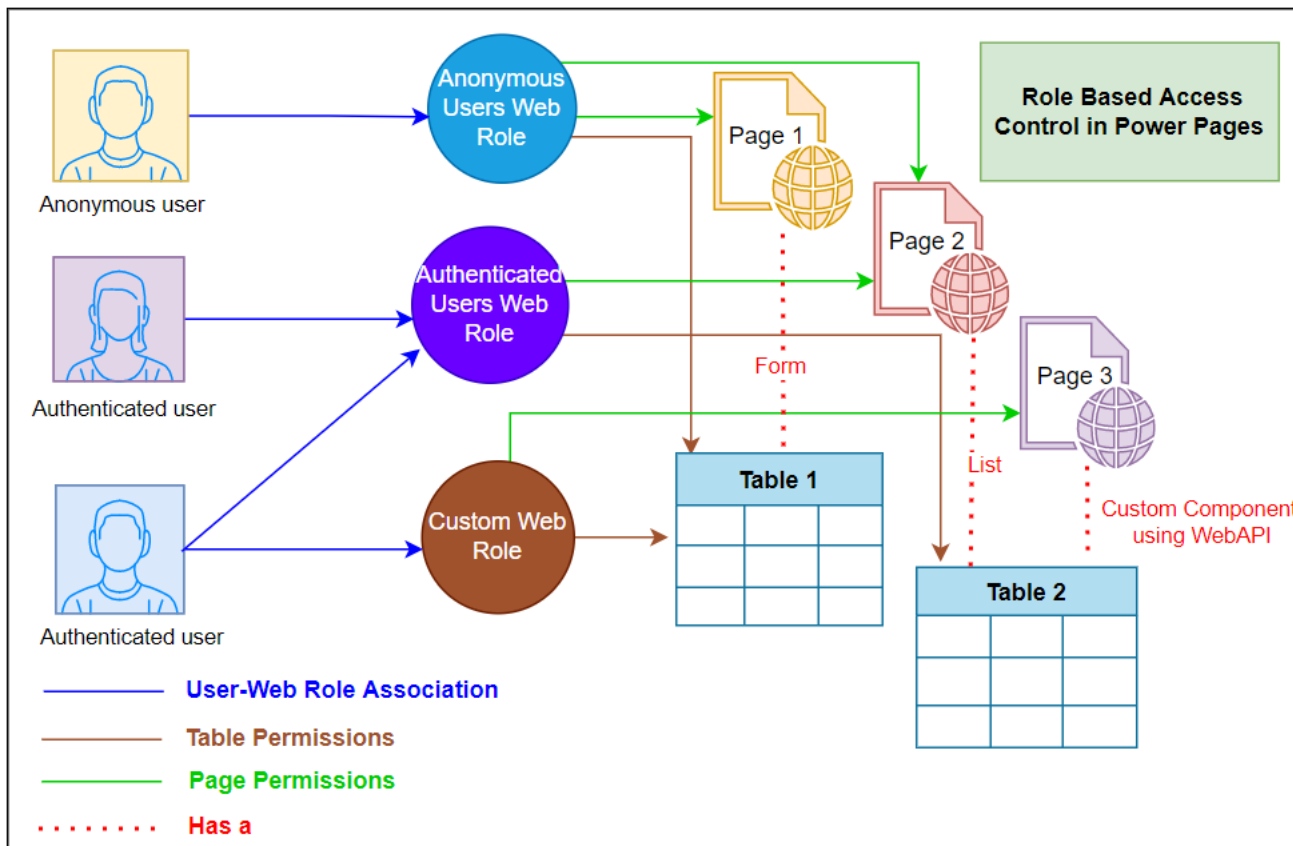
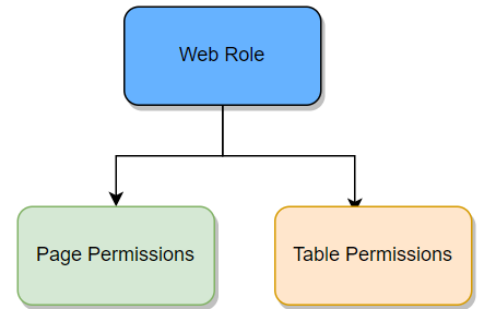
Each authenticated website user is uniquely associated with a Contact record in Dataverse, which enables powerful capabilities such as Profile Management, and flexible configuration of authorization rules. In addition to supporting advanced authentication flows such as Password less Authentication, Single Sign-On, Single Log Out, Multi-factor authentication, Conditional Access, Session timeouts, Power Pages platform supports several authentication providers, as shown below.

1. **Identities via OAuth 2.0:** The OAuth 2.0 protocol standard enables a website or application to access resources hosted by other web apps on behalf of a user. Power Pages allows users to use OAuth 2.0 to authenticate via their external identities, including Microsoft, Twitter, Facebook, Google, LinkedIn, etc.
2. **Bring your own Identity providers:** Power Pages can be configured to be used with industry standard enterprise authentication providers, including Azure AD, Azure AD B2C, Okta, and Auth0, and more using Open ID Connect, WS-Federation, and SAML 2.0 protocols.
 - a. **Open ID Connect:** Open ID is an open standard and decentralized authentication protocol. Identity providers (IdPs) use this so that users can sign in to the IdP (Identity Providers), and then access other websites and apps without having to log in or share their sign-in information. When users sign in, the identity provider provides claims with some user information, such as tenant details, email, etc. These claims are configurable on the identity provider. By using these claims, a user can be mapped to a contact record on Power Pages to support different scenarios. Azure Active Directory and Azure Active Directory B2C are popular providers which can be configured with Open ID Connect on Power Pages.
 - b. **WS-Federation and SAML 2.0:** Used to integrate with on-premises Active Directory and other identity services such as ADFS and Okta.

User authentication to the Power Pages service consists of a series of requests, responses, and redirects between the user's browser and the Power Pages service or the Azure services used by Power Pages. [This](#) document lists the various authentication providers that can be used with Power Pages.

Authorization

Authorization determines resources (Website Pages, Business data) that a website user (Anonymous, or Authenticated) has access to in Power Pages. Power Pages implements a robust security model to ensure that business data and website content is secured. This security model is implemented on **Role Based Access Control** mechanisms where **Web Roles** provides a way to group users, **Table Permissions**, and **Page Permissions** control and protect access to business data and website content. The following section defines each of the three elements.



Web roles

Web roles can be created to allow users to perform any special actions or access any protected content and data on the site. Web roles link to users, table permissions, and page permissions. Because contacts can be assigned multiple web roles, they can be provided cumulative access to site resources. All authenticated users (contacts) are automatically assigned to the Authenticated Users web role. A site can be visited by anonymous users (unauthenticated) and given access to assets through the Anonymous Users web role. Authenticated and Anonymous Web roles are present by default in Power Pages. Makers can [create web roles](#) for custom use-cases and associate them to Table Permissions and Page Permissions for implementing granular access controls.

Table permissions

[Table Permissions](#) applies security in Power Pages by securing access to business data that is surfaced on the website via lists, forms, or accessed in website pages via Liquid or Web APIs. Table permissions allow makers to configure different levels of access and privileges to records stored in Dataverse tables. [Column level permissions](#) can be applied if granular control on table columns is required. Table permissions are associated to web roles to provide appropriate access of business data to website users.

Page permissions

Individual website pages containing content or other components can also be protected by configuring [Page Permissions](#) that are associated with web roles to allow access.

Security

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 including protection from [OWASP Top 10 security risks](#). This multi-layered security stack improves overall security of Power Pages applications by reducing the probability of security breaches. Security is a shared responsibility; the Power Pages platform provides makers and administrators the necessary controls to harden security and governance for their sites and data. [Power Pages Security](#) white paper describes how Power Pages offers enterprise grade security by default and the tools and capabilities leveraging which makers and admins can further harden security for their users and data.

Compliance

Power Pages provides comprehensive compliance coverage across global, regional, government, and industry-specific compliance standards. To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft provides a comprehensive set of compliance offerings (including certifications and attestations). There are [tools](#) available for Power Platform administrators to support organization's compliance efforts. These include and are not limited to resources to manage Data Protection, Data Location, [Global Data Protection Rules](#) (GDPR), and complying with [European Union Data Boundary](#) regulations.

Conclusion

This white paper discussed architecture and capabilities of Power Pages that comprise of key elements which enable it to offer enterprise grade scale, high availability, reliability, data protection, security, and compliance.