Microsoft Dynamics 365

Power Pages Security

Dynamics 365 FastTrack
Architecture Insights

Anand Singh
Avinash Mishra

Agenda

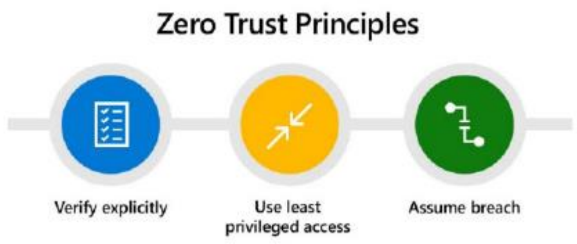
- Overview
- Security Layers
- Key Takeaways

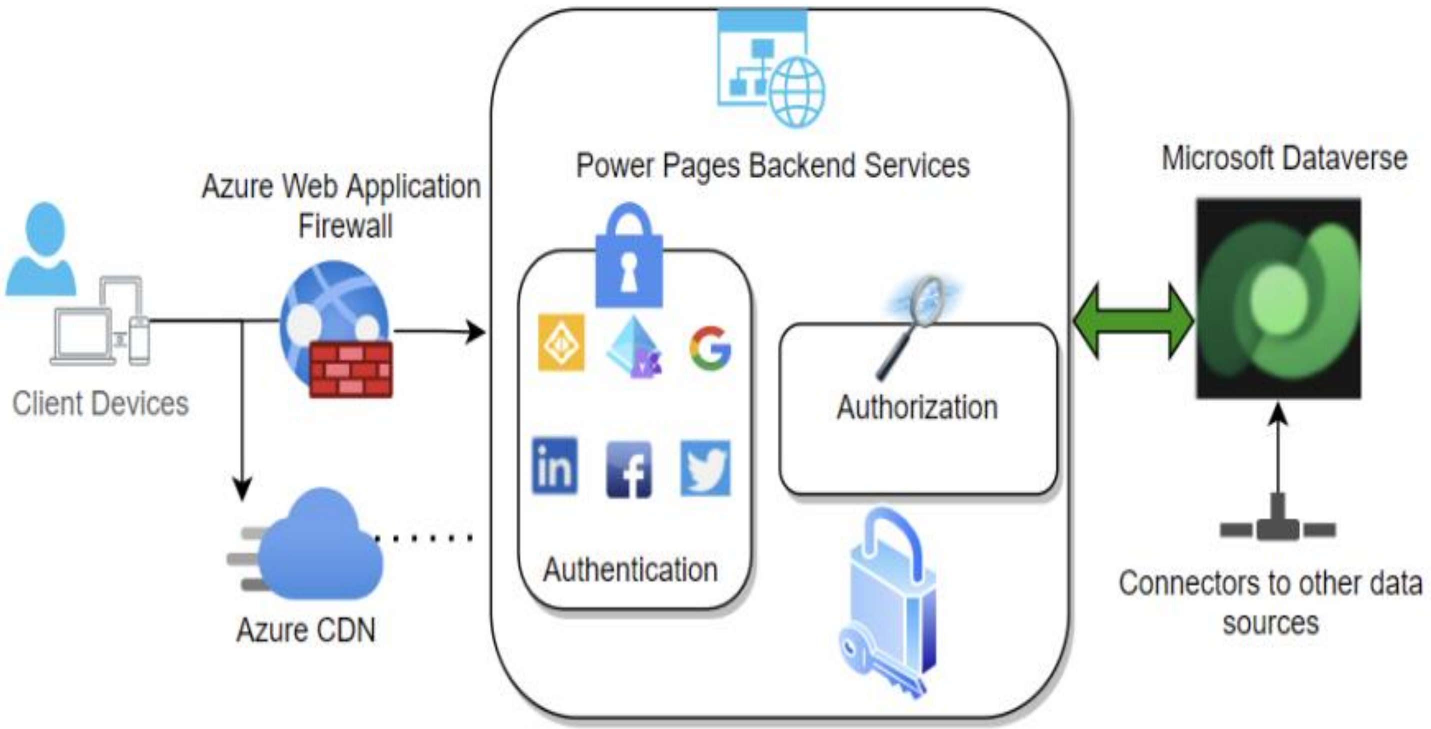
Overview

- ➢ Power Pages provides comprehensive **security**, **compliance**, **protection**, **governance**, and **authorized access**

- ➢ Azure as a hosting platform

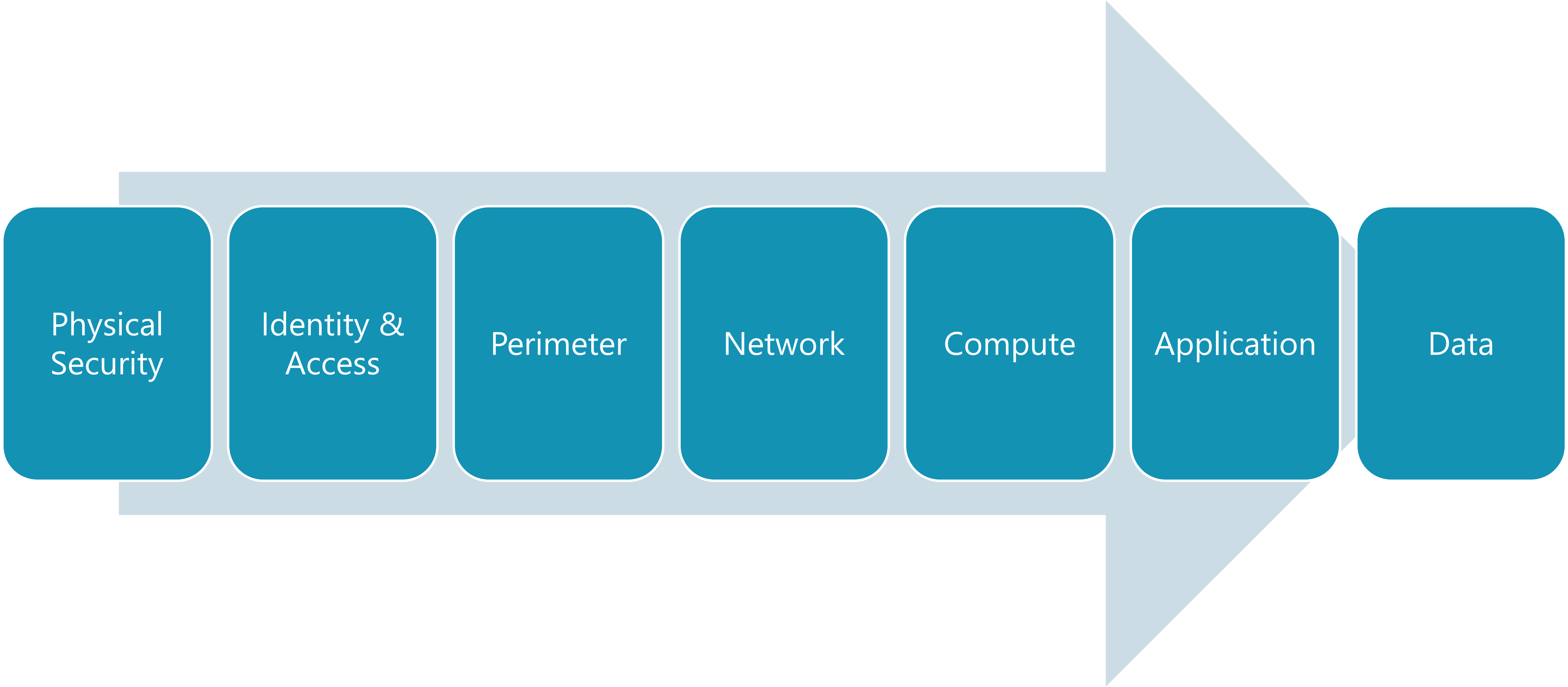
- ➢ Built on a “Zero Trust” security approach




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

Security Layers

Security Layers



1

Physical Security

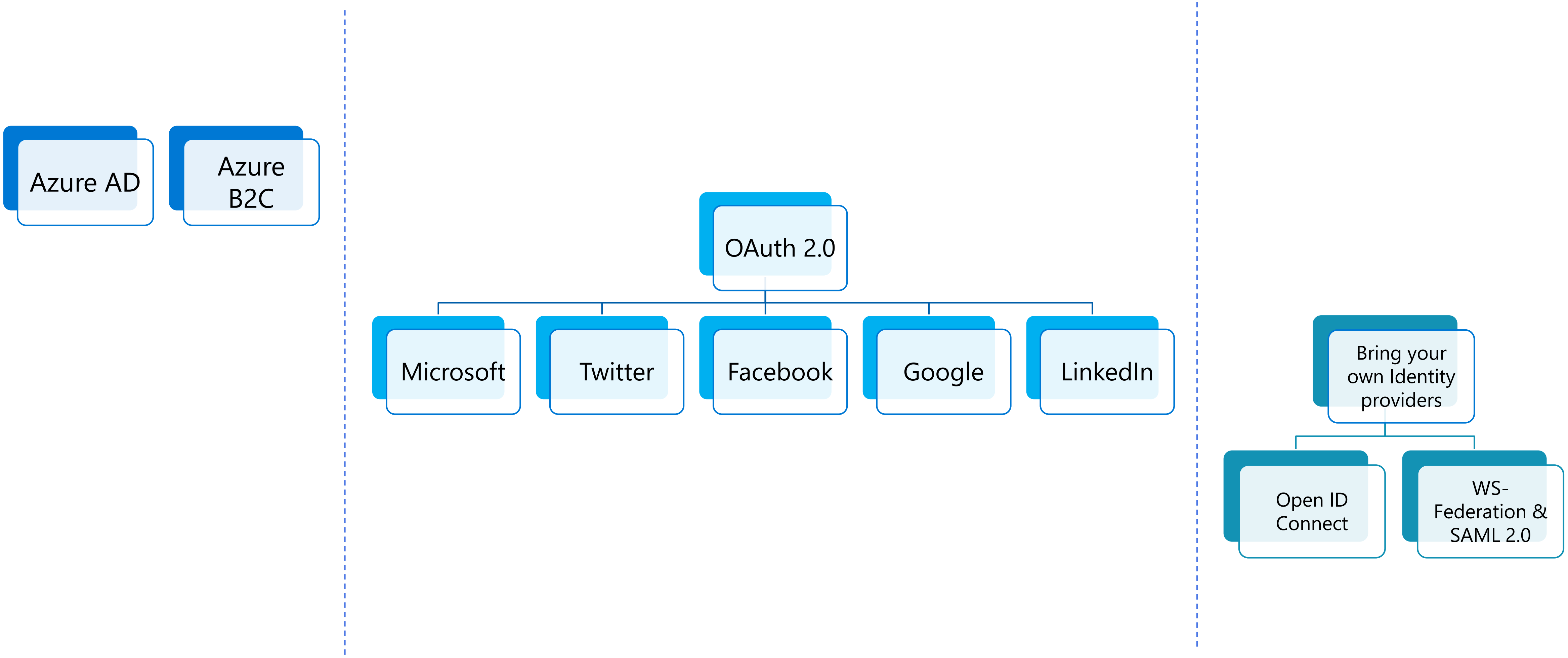
- Runs on Azure App Services hosted Azure data center
- Microsoft operates the Azure data centers and manages physical security of hardware
- Only authorized personnel can access parts of Azure data center

2

Identity & Access

- Power Pages authentication framework is based on Microsoft Identity Platform
- Authenticated & unauthenticated users can access portal
- Users can access website content and data based on Role-based access.

Identity



Azure AD

Azure B2C

OAuth 2.0

Microsoft

Twitter

Facebook

Google

LinkedIn

Bring your own Identity providers

Open ID Connect

WS-Federation & SAML 2.0

Access

Control Access: Azure AD and Azure AD B2C identities

- Conditional Access
- Multiple Factor and Password less Authentication

Role based Access

- Web roles provides a way to group users & role-based access
- Table and page permissions control and protect access to business data and website content.
- Column permission limits the scope of table permission access.

3

Perimeter

- Azure DDoS basic protection is applied by default
- Azure DDoS standard protection can be additionally purchased and applied.

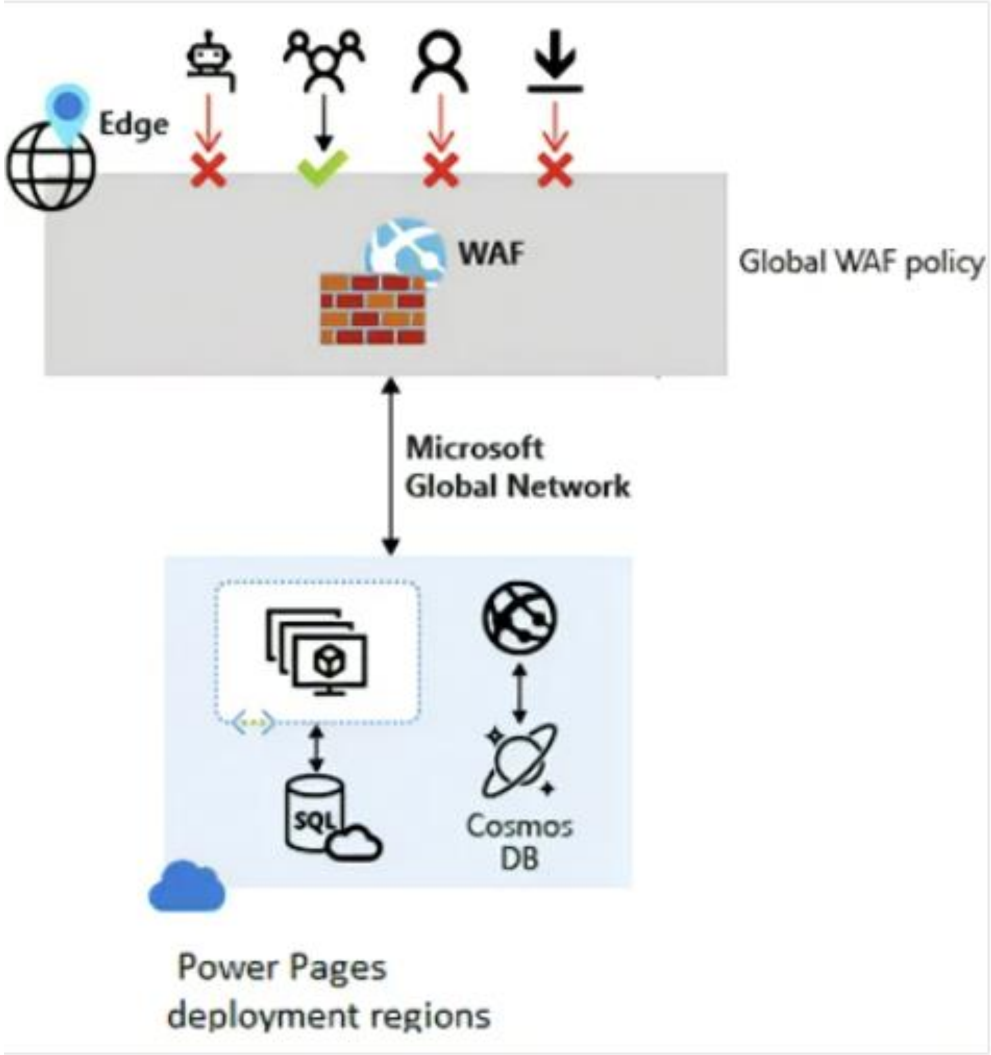
4

Network

- Site visibility
- IP restriction to restrict site access
- WAF(Web Application Firewall) protects against common exploits and vulnerabilities by preventing malicious attacks

WAF(Web Application Firewall)

- Power Page WAF is powered by Azure Front Door
- Rules helps in protection against below categories
  - Cross-site scripting
  - Local file inclusion
  - Remote file inclusion
  - Session fixation
  - Protocol attackers
  - Protocol enforcement



5

Compute

- Microsoft Defender for Cloud is natively integrated with the Azure App service and monitors threats to underlying resources like
- Virtual Machine (VM) instances and runtime software are regularly updated to address newly discovered vulnerabilities

6

Application

- Internet traffic to Power Pages sites is encrypted and enforces HTTPS
- Cookie Security and HTTP Security headers capabilities helps to prevent against common security threats like XSS, clickjacking and session thefts.
- Client-side calls to external APIs securely using OAuth implicit grant flow.

HTTP Security Headers

Default headers

- HTTP Strict Transport Security(HSTS)
- Referrer-Policy
- Cache-Control
- X-Content-Type-Options
- X-Frame-Options (XFO)

Configurable headers

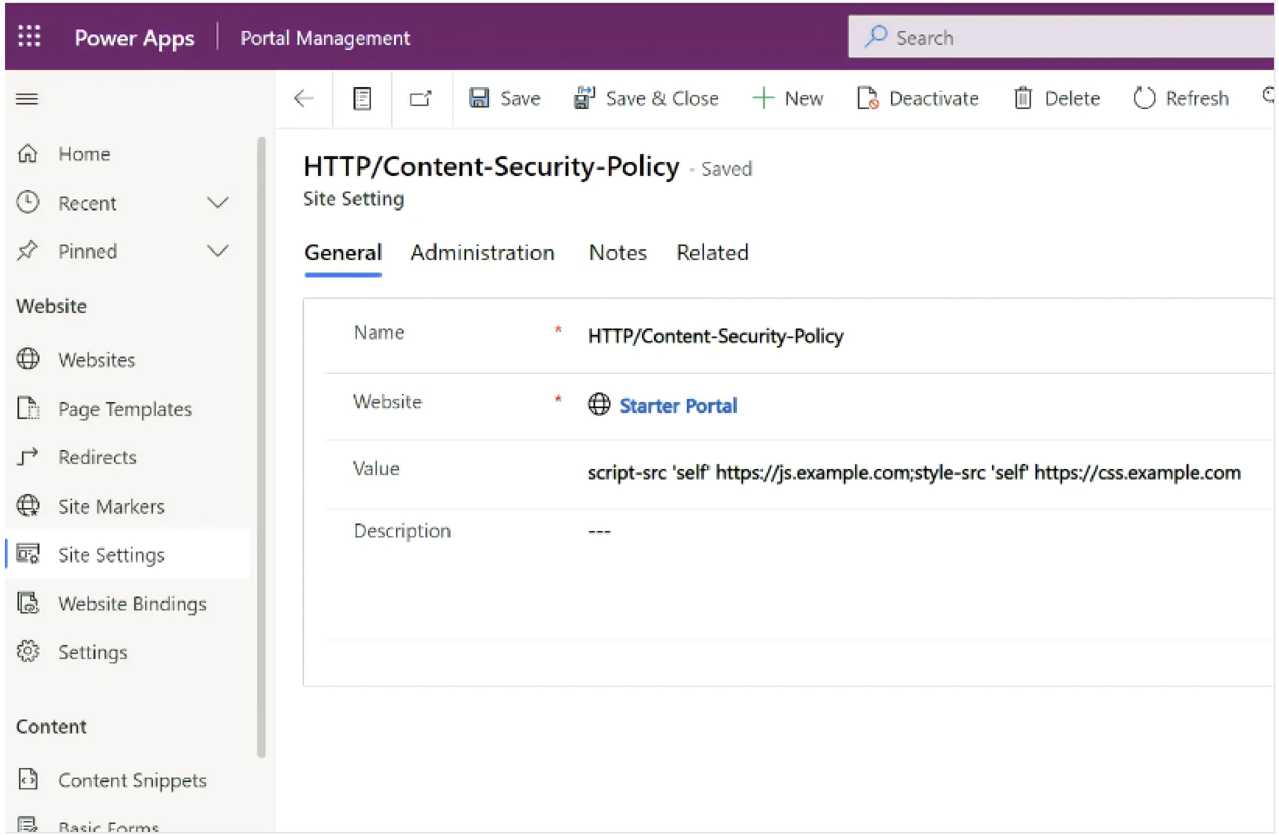
- X-Frame-Options (XFO)
- X-Content-Type-Options
- Content Security policy (CSP)

Content Security Policy(CSP)

- Content-Security-Policy header allows you to restrict which resources can be loaded as part of from

- Help in reducing the attack surface of Cross Site Scripting (XSS) attacks

- Enabling nonce(Number used once) helps in blocking execution of all inline scripts except those specified within the inline script.



HTTP/Content-Security-Policy - Saved

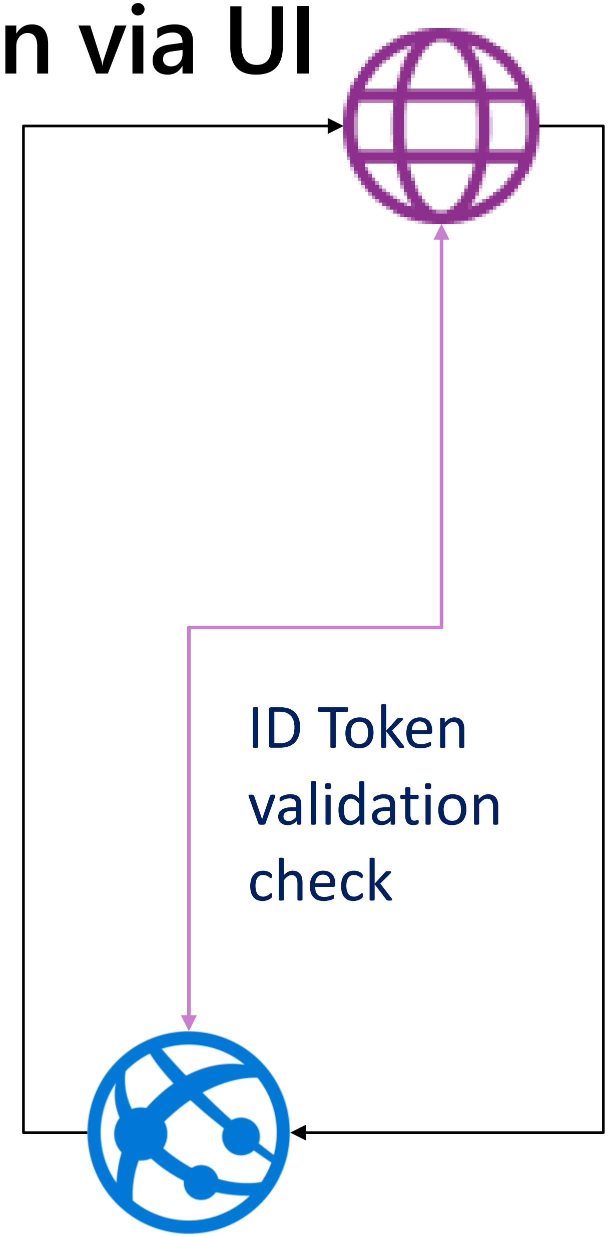
Site Setting

Name *	HTTP/Content-Security-Policy
Website *	Starter Portal
Value	script-src 'self' https://js.example.com;style-src 'self' https://css.example.com
Description	---

OAuth Implicit grant flow for Integration via UI

- Helps in securing client-side API integration using token validation.
- Only applicable for authenticated user scenarios.
- Requires custom certificate configured in Power Pages

Use OAuth 2.0 implicit grant flow within your portal - Power Apps | Microsoft Docs



7

Data

- Power Pages data is encrypted in rest as well in transit while interacting with Dataverse.
- Encryption serves as the last and strongest line of defense.
- Dataverse SQL Data & Logs are encrypted at rest using SQL TDE(Transparent Data Encryption)
- Customer managed keys and lockbox to secure Dataverse SQL Data.

Securing Dataverse Transactional Data

Customer Managed Keys

Dataverse Transactional Data storage encryption key is managed by Customer

Customer Lockbox

Controls who can access data from Microsoft

Key Takeaways

Easy fix security problems, customers find during IT Security reviews

Where we see many **Security threat problems**

Not enabling Table Permissions

Lists and Web Pages

OData Lists (+ leaving unused Lists with OData end points open)

One default authenticated Web Role has access to all Web Pages along with Open Registration

Removing pages from Navigation, forgetting that Pages are still enabled (Forums, Contact Us, Knowledge Search, etc)

Leaving Sensitive JS Code via HTML Commenting Out

Security Tips

Portal users must have a unique email address. If two or more contact records (including deactivated contact records) have the same email address, the contacts won't be able to authenticate on the portal.

If you add a custom domain name or change the base URL of your portal, you must re-create the provider configuration by using the correct URL.

When you delete a provider, only the portal configuration for the provider is deleted. For example, if you delete the LinkedIn provider, your LinkedIn app and app configuration remain intact. Similarly, if you delete an Azure AD B2C provider, only the portal configuration is deleted; the Azure tenant configuration for this provider won't change.

Changes to the authentication settings might take a few minutes to be reflected on the portal. Restart the portal by using portal actions if you want the changes to be reflected immediately.

Permissions apply to child files must be set to **Off** for the home page for the portal. Web files such as Bootstrap.min.css and Theme.css used by themes are under the home page. If you restrict these files to only authenticated users, styles won't be applied to any pages, including the sign-in pages that are available anonymously.

Thank you