Umbraco Heartcore infrastructure - security and tenancy overview

Public Internet

HTTP (80)
HTTPS (443)
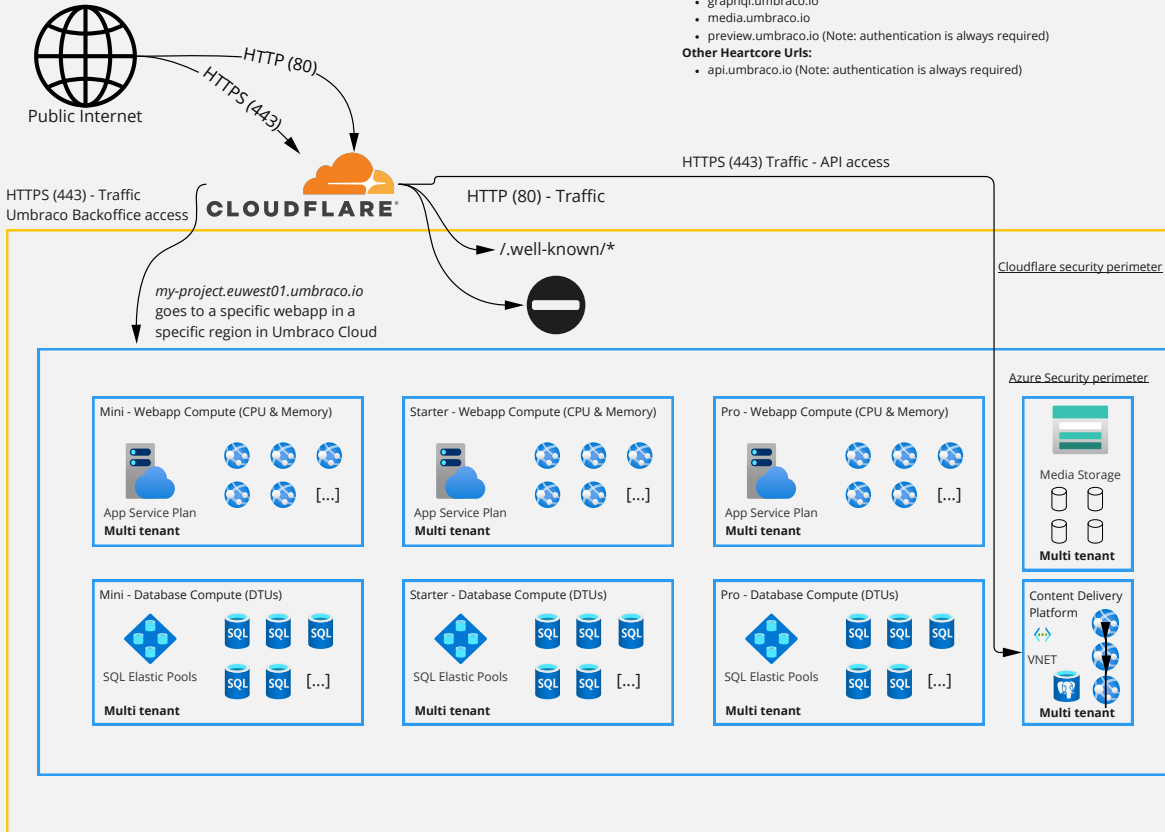
Heartcore Urls via Content Delivery Network:
- cdn.umbraco.io
- graphql.umbraco.io
- media.umbraco.io
- preview.umbraco.io (Note: authentication is always required)

Other Heartcore Urls:
- api.umbraco.io (Note: authentication is always required)

CLOUDFLARE®

HTTPS (443) Traffic - API access

HTTPS (443) - Traffic
Umbraco Backoffice access

HTTP (80) - Traffic

/.well-known/*

my-project.euwest01.umbraco.io
goes to a specific webapp in a
specific region in Umbraco Cloud

Cloudflare security perimeter

Azure Security perimeter

Mini - Webapp Compute (CPU & Memory)

App Service Plan
Multi tenant

[...]

Starter - Webapp Compute (CPU & Memory)

App Service Plan
Multi tenant

[...]

Pro - Webapp Compute (CPU & Memory)

App Service Plan
Multi tenant

[...]

Media Storage

Multi tenant

Mini - Database Compute (DTUs)

SQL Elastic Pools
Multi tenant

[...]

Starter - Database Compute (DTUs)

SQL Elastic Pools
Multi tenant

[...]

Pro - Database Compute (DTUs)

SQL Elastic Pools
Multi tenant

[...]

Content Delivery
Platform

VNET

Multi tenant

Details:

- DNS and CDN using Cloudflare layer 7 load balancer and DDoS protection.
- API access requires project header and optional API Key.
- HTTPS traffic is enforced at the Cloudflare perimeter.
- A webapp cannot access other webapps running on the same compute.
- The file system is not accessible in a webapp hosting Umbraco Heartcore.
- Media library stored in Read-access geo-redundant blob storage (RA-GRS) - container isolation via SAS Tokens.
- Databases can be accessed from within Azure - firewall rules are set at the database level and blocks access from the public internet by default
- Database servers are a logical grouping of resources - firewall rules cannot be set at the server level.
- Databases each have their own login, which is assigned per webapp.
- In Heartcore it is not possible to access a database except from within the webapp (Umbraco) that is associated with the database.
- Heartcore has a central Content Delivery Platform, which is isolated in a private VNET only accessible by the Webapps hosting our API servers.
- Umbraco Cloud Platform services are responsible for the lifecycle management of the Compute and Storage resources of Umbraco CMS instances.
- Webhooks are sent from one of two known static outgoing IPs.
- Minimum TLS version is 1.2 and TLS 1.3 is supported.

Tenancy in Umbraco Cloud:

- Starter/Standard/Pro are multitenant in terms of compute resources for both databases and webapps.
- App Service Plans contains x number of feature and live environments (webapps) depending on the Umbraco Cloud Plan (Mini/Starter/Pro).
- A single webapp hosts a single Umbraco Heartcore backoffice instance.
- A single SQL Database is used for a specific webapp instance.
- Umbraco Cloud Platform services are responsible for the lifecycle management of the Compute and Storage resources of Umbraco CMS instances.
- Each webapp consists of an Umbraco CMS instance and a local git repository - the git repository is not accessible by users of Umbraco Heartcore.
- Media is stored in a regional blob storage account with private container isolation meaning that a tenant cannot browse other tenant's media.
- The Content Delivery Platform is multitenant with content separated by schema. Access is authorized on a Heartcore Project-basis.

Backup Details:

- Sql databases has 30 days point in time restore, which can be restored upon request.
- Backups are **not** provided as files for download.

Password Policy:

- Between 8 and 100 characters; letters, numbers, symbols are allowed.

umbraco