Carpe Diem
Security Brief

Overview

Carpe Diem is a cloud-based enterprise time recording system. Its' fully responsive design means that it can be accessed through any web-browser on any device. Carpe Diem is hosted in Microsoft Azure to ensure industry-leading security and availability worldwide.

By partnering with Microsoft Azure, you can be confident that safeguards to protect your data, and meet regulatory compliance requirements, are baked into the network architecture with secure datacentres across North America and Europe for complete peace of mind.

As a business, Advanced takes a multifaceted approach to security, data protection, service availability and business continuity.

This document covers technology-based security, data protection, external accreditations and availability, resilience, and disaster recovery (DR) for Carpe Diem in Azure.

Documentation on Advanced policy for organisational and process-based security is available separately upon request.

Data security

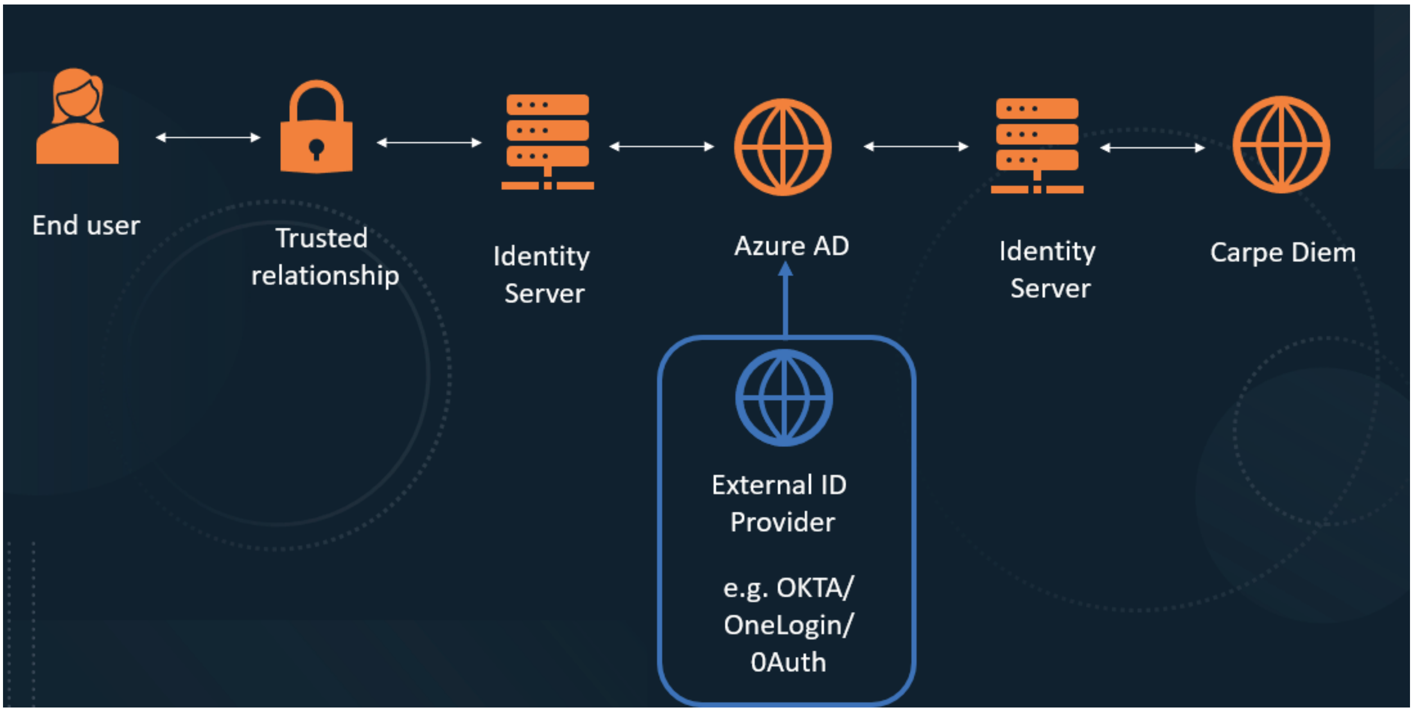
- Carpe Diem is a multi-tenant web application that includes its own secure tenant identification layer
- All tenants have their own separate database which can be configured and customised to meet their specific requirements
- Azure SQL databases, backups, and transaction logs are always encrypted at rest using Transparent Data Encryption (TDE)
- All database connection strings are encrypted using AES 256-bit encryption
- All encryption keys are stored in Azure Key Vault
- Internal access (within Azure) to all databases is only granted to Service Principal accounts and protected by Role Based Access Controls (RBAC)
- External access (outside Azure) to all databases is protected by Role Based Access Controls (RBAC) and database firewalls. Access is only granted to authorised users and white listed IP addresses

Web security

- All Carpe Diem web applications can only be accessed through HTTPS – secured using SSL (SNI) certificates from a recognised certificate authority
- HTTPS only is enforced using HSTS (HTTP Strict Transport Security)
- Transport Layer Security (Encryption-in-transit) is TLS 1.2 on all web servers

Environment separation

- Production and staged environments share resources
- Staged environment allows tenants to preview and test the next release
- Development and test environments use separate resources
- Tenants can request their own development and test environments if required



Secure access

Access to Carpe Diem is controlled by Identity Server which performs user authentication through Azure Active Directory (AAD) which can then federate authentication to the tenant's internal or external identity provider (ADFS, Okta, OneLogin, Auth0, etc).

Identity Server supports Auth0 2.0 and OpenID Connect (OIDC) protocols

Single sign-on (SSO) and multi-factor authentication (MFA) are supported depending on the tenant's chosen identity provider

The user login experience can be customised for each tenant via Identity Server configuration

Access control

> Single admin user access. Separate admin user account created for each tenant data base with credentials held securely in password safe.

> Time limited access granted to the support team by the client. Data base access is only granted to individual support team members following documented permission from an authorised manager.

> Data back-up

> Database transaction logs backed-up every 10 minutes

> Databases fully backed-up every 12 hours, with 35 day retention of back-ups

> Long-term (up to 10 years) back-up retention available, if required

> Database geo-replication available, if required

Availability

We monitor our applications and infrastructure on the Azure platform to ensure available resources remain within acceptable limits. Alerts and associated rules are configured to warn of any issues, while autoscaling rules are configured to ensure resource limits are never exceeded.

Platform status is also published through a webpage for our clients, enabling them to view the current status at any time.

> Load balancing to distribute web traffic to available and least used resources

> 99.5% uptime

> Multiple instances of primary resources

> Front door Azure – 'site down' alerts

> High Severity Support Incident Process (HSSI) provides a structured, defined method of handling high severity support incidents

Geographically resilient hosting via Microsoft Azure with data centres in the following locations:

- EU West - Netherlands
- North America - Canada and United States

Reliability

Ranging in size from under 10 users, up to 7500+. Thirty law firms and professional service companies globally entrust their revenue to Carpe Diem in the Cloud.

Carpe Diem in the Cloud routinely handles over 750,000 individual time transactions every day.

Threat and vulnerability management

> Network-layer vulnerability scans are performed regularly as prescribed by industry best practices

> Local operating system-layer vulnerability scans performed regularly as prescribed by industry best practices

> Application-layer vulnerability scans regularly as prescribed by industry best practices

> External pen tests performed annually

Accreditations and compliance

Carpe Diem, hosted on Microsoft Azure, meets a broad set of international and industry-specific compliance standards:

> GDPR complaint

> SOC 1 Type 2 compliant

> SOC Type 2 accreditation pending

> ISO 27001 certified

> HIPAA complaint

> FedRamp (Federal Risk and Authorization Management Program) complaint

> The only legal timekeeping solution approved for inclusion in the UK Governments UK G-Cloud

> Regular penetration testing for external threats and irregularities

> CyberEssentials Plus

> All Carpe Diem related domains pass SSLLab's server test with an A+ rating

More information

w oneadvanced.com
t +44(0) 330 343 8000
e hello@oneadvanced.com

Ditton Park, Riding Court Road, Datchet, SL3 9LL

advanced
Software Powered Possibility

Advanced Computer Software Group Limited is a company registered in England and Wales under company number 05965280, whose registered office is Ditton Park, Riding Court Road, Datchet, SL3 9LL. A full list of its trading subsidiaries is available at www.oneadvanced.com/legal-privacy.