CLOUD PLATFORM

IDU Cloud, on Microsoft Azure.

IDU runs on the Microsoft Azure global network of servers. Each client instance is hosted on a dedicated virtual machine, located in the data centre closest to the client. Microsoft handles the perimeter. IDU governs everything inside.

01 — ENCRYPTION

End-to-end, at rest and in transit.

256-bit encryption on sensitive data. AES-256 storage encryption. HTTPS enforced. Optional client security certificate for the environment.

02 — HOSTING

Regional data centre, dedicated machine.

Hosted in the regional data centre where IDU is deployed so data does not leave the country. One client per virtual machine, one application per VM, one isolated vnet.

03 — ISOLATION

No data on shared Azure services.

The solution runs as a hosted virtual machine, not an Azure Web Application. Client data is never stored on Azure SQL database instances. No storage containers or blobs.

COMPLIANCE

AZURE-LEVEL CONTROLS

ISO 27001 Info. Security	**ISO 27018** Cloud PII	**SOC 1** Financial	**SOC 2** Trust Services	**SOC 3** Public Report
FedRAMP US Federal	**HITRUST** Healthcare	**MTCS** Singapore	**IRAP** Australia	**ENS** Spain

IDU Cloud is subject to the Microsoft Azure terms and conditions. Microsoft data security protocols govern the platform itself; the controls listed above apply at Azure infrastructure level. Refer to Microsoft Azure Legal Information for the canonical record.

SECURITY IN DETAIL

Layer by layer.

From Azure instance to virtual machine, network, and backup. Each layer governed, audited, and built for finance-grade trust.

Azure instance

- Administrative access only, with Multi-Factor Authentication enforced
- Hosting managed in a regional data centre to keep data in-country
- Azure-level backups associated with the machine, in the same data centre
- Azure Defender enabled on the machine
- No storage containers or blobs associated with the machine

Virtual machine

- Microsoft Server 2022, updated on release day, restarted after hours
- Azure Defender Firewall on the server itself
- AES-256 at-rest encryption with Platform Managed Keys
- Webroot Antivirus, cloud-based, automatic definition updates
- SQL Server 2022 with unique DB user, 8-character password complexity
- Yearly renewed certificate to maintain HTTPS; one application per VM

Networking & ports

PORT	PROTOCOL	ACCESS
80	HTTP	Internet-facing — application access via web browser
443	HTTPS	Internet-facing — HTTPS enforced for all traffic
1433	SQL	Restricted to specific IPs of admins and consultants, granted on request
3389	RDP	Restricted to specific IPs of admins and consultants, granted on request

Each VM sits on its own vnet, isolated from others, with a single network interface and no subnets. Webroot scans incoming network traffic in real time. Just-in-Time access is currently being rolled out.

30
DAY RETENTION

Backups & recovery.

Backups run daily and are retained for thirty days. The two most recent recovery points are application and data consistent snapshots; the rest are data-focused. All backups are associated with the machine, stored in the same data centre, and protected by the same at-rest encryption as the live VM.