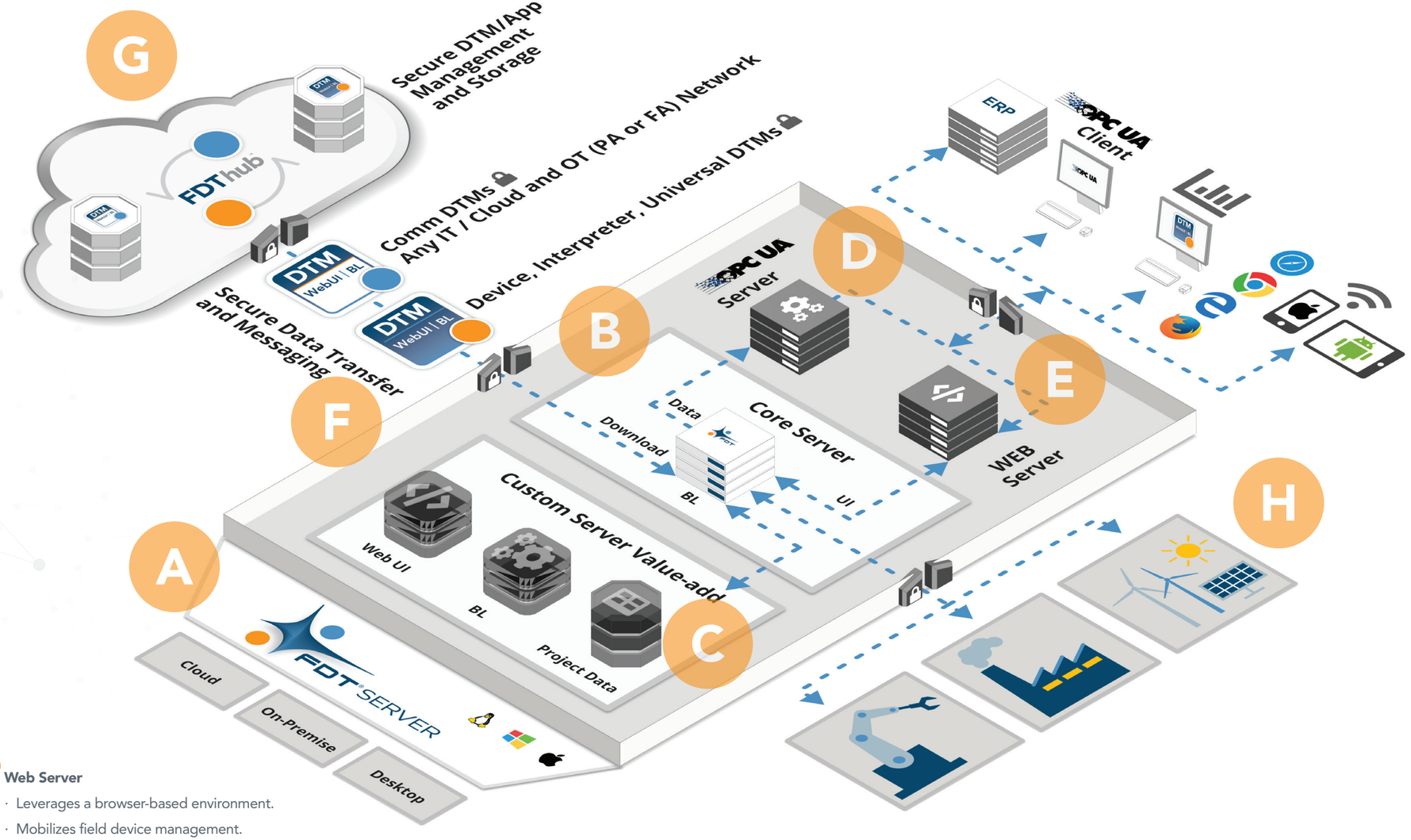
How the FDT IIoT Server Solution Works



A **FDT Server**

- Utilizes .NETCore open source software to build device, cloud and IIoT applications.
- Compatible with a choice of operating systems, including iOS, Linux and Windows.
- Offers a variety of deployment options, including cloud, edge, on-premise and air-gapped.
- Employs Server Common Components relieving the developer of integrating the standard into products, allowing them to focus on value-added capabilities.

B **Core Server**

- Functions as IIoT data hub for the FDT Server.
- Included in Server Common Components.
- Incorporates DTM user interfaces and business logic.
- Stores, instantiates and executes DTMs, which are always kept up to date via the FDT*hub* repository.
- Provides the FDT topology information.

C **Custom Server Value-add**

- Integrates into a larger system for enhanced functionality, including higher level, complex systems such as asset management applications, PLC tools and DCS/engineering applications.
- Utilizes Server Common Components with all the basic coding groundwork for business logic, project data and Web UI, which system vendors can customize by adding their own wrapper for branding purposes.

D **OPC UA Server**

- Leverages a client-based environment.
- Enables IT/OT integration and gateway to data and health information.
- Allows developers to leverage industry-standard OPC UA Server included in the Server Common Components, or easily exchange it for their preferred OPC UA Server.
- Supports ERP/MES to optimize enterprise-level connectivity, plant availability and quality yield production.
- Offers OPC UA client/server-authenticated access to plant application data.
- Utilizes Publish-Subscribe environment for real-time data exchange.

E **Web Server**

- Leverages a browser-based environment.
- Mobilizes field device management.
- Transforms OT access for improved asset management and maintenance.
- Enables browser-based access to physical plant/facility assets using authenticated computer, tablet or phone, or via DCS, PLC, asset management application, etc.
- Programmed into Server Common Components however, system vendors may replace the preprogrammed Web Server with their server of choice.

F **Security**

- Provides encrypted communications using Transport Layer Security (TLS).
- Utilizes on-the-wire-security for enabled industrial automation protocols.
- Implements role-based user security.
- Supports 509v3 certificates for authentication.

G **FDT*hub*™**

- Enables convenient access to all certified Device and Communication DTMs in a single repository.
- Supports cloud-based deployment with automatic device discovery.
- Available as a local server for on-premise, air-gapped deployment.
- Supports machine-to-machine communications with 509 certificates for machines with authorized access.

H **Remote Facility Connections**

- Allows a single server to support multiple facilities.
- Provides access to FDT*hub* DTM repository.
- Optimizes security and connectivity via TLS, 509v3 certificates, authentication, authorization, and encryption.
- Compatible with VPN for IT environments, edge with a gateway for a specific protocol such as MQTT or AMQP and Intranet — ensuring communication stays within the secure enterprise network.