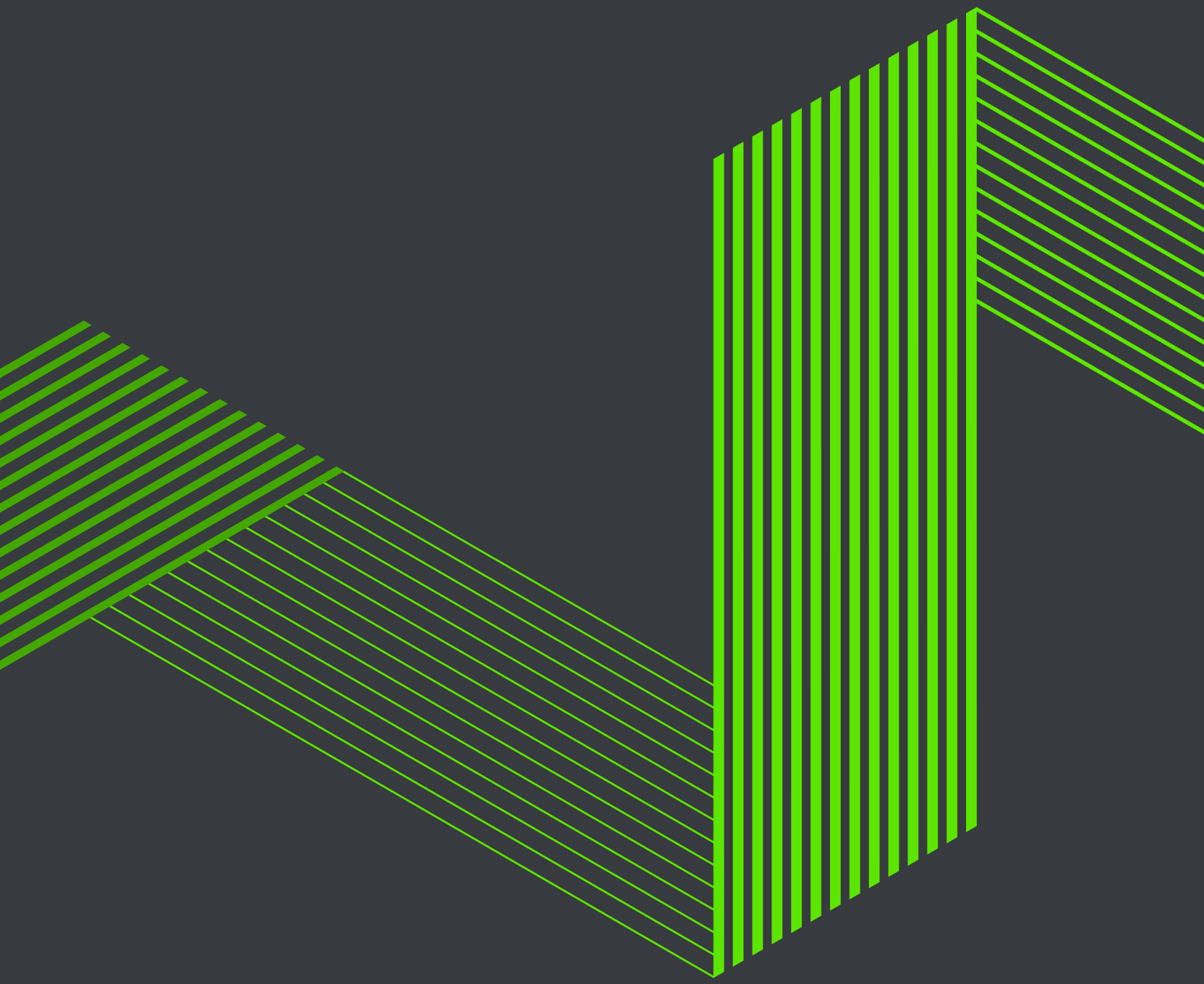
Progress® DataDirect



SECURITY STATEMENT

This document describes risk and vulnerability management strategies that are in place for Progress® DataDirect® Hybrid Data Pipeline Platform-as-a-Service (PaaS) and Progress® DataDirect Cloud® Software-as-a-Service (SaaS) security and governance.

DataDirect Cloud, a public cloud service, is operated under the security principle of Defense in Depth. A layering of security technologies and processes safeguard the environment against known and emerging threats. Each ingress and egress point to our operations and management architecture is managed, inspected and validated through routine self and third-party assessment to prevent, identify and correct vulnerabilities to protect against compromise.

Hybrid Data Pipeline shares much of the DataDirect Cloud technology, and leverages its robust security mechanisms. Since it is typically deployed on-premises or through a managed private cloud, it is important for customers to ensure that end-to-end security is appropriately configured and managed. This includes leveraging your own Defense in Depth strategy, network security , encryption, access control, and other safeguards. Coupled with appropriate on-premises IT Security controls, Hybrid Data Pipeline can be an invaluable strategy for secure data access.

Hybrid Data Pipeline Architecture

Overview of Operation

Understanding the security architecture of Hybrid Data Pipeline is critical to developing your own secure data access service. This knowledge will also help in understanding of the underlying architecture behind DataDirect Cloud which are similar. Figure 1 below is a high-level view of the various components and processes within Hybrid Data Pipeline. The key components include the Clients, the Hybrid Data Pipeline Server (HDPS) and the On-Premises Connector (OPC).

Clients

Hybrid Data Pipeline interfaces with an application (e.g. a BI analytics or data management tool) using an industry standard data access interface for SQL and REST, typically ODBC, JDBC, or OData. Clients communicate with the main Hybrid Data Pipeline Server over HTTPS to read and/or write data to a downstream application or database that may reside in the cloud or behind the firewall. Figure 1 illustrates secure communication over port 8080 (configurable), HTTP is not recommended but usable for testing purposes.

(Note: All possible protocol choices are outlined in the diagram, with the first being the default. It assumes that administrators will configure a secure protocol before public deployment.)

Hybrid Data Pipeline Server (HDPS)

The HDPS is the primary service in a Hybrid Data Pipeline deployment and is responsible for managing user and service configuration, brokering the flow of data between Clients and databases, managing state and communicating with on-premises connectors and more. It is possible to deploy more than one (1) HDPS in order to scale out the solution.

Storage of user and service configuration is handled by the Config DB (configuration database) located in the HDPS in the diagram. HSQL is embedded and enabled by default. The database itself is pluggable, allowing administrators to use their preferred relational database (e.g. typical choices being Oracle, SQL Server, MySQL). All communication with the pluggable database can be configured to occur over an encrypted channel, and the sensitive data at rest will always be encrypted. Refer to the "Encryption" section later in the document for specific details.

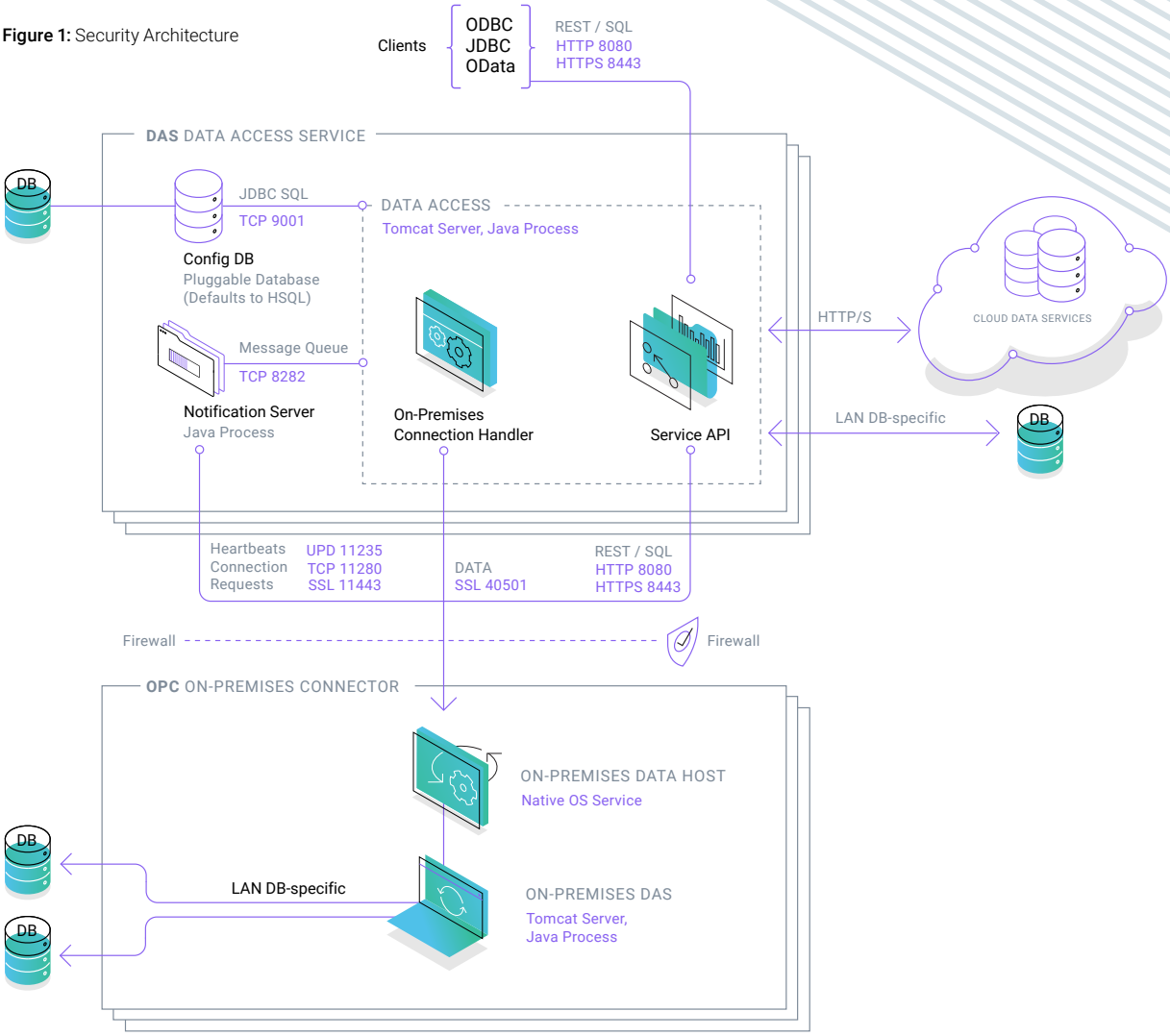
When accessing data from a cloud data service (e.g. a cloud application such as Salesforce.com, or a cloud platform such as Microsoft Azure), the HDPS should be configured to use HTTPS. The exact configuration support varies by endpoint being accessed.

On-Premises Connector (OPC)

The OPC typically resides behind a firewall and is responsible for brokering the data access between a HDPS and a database endpoint that is accessible via a LAN. A single HDPS can connect to one or more OPCs.

An OPC establishes a connection with a HDPS using an outbound request to the HDPS Service API using HTTPS. The HDPS will create a new data endpoint and return that address to the OPC. The OPC will then establish a mutually authenticated, SSL-secured session with the HDPS to handle the flow of data from the LAN-accessible database to the application connected to the Client.

Figure 1: Security Architecture



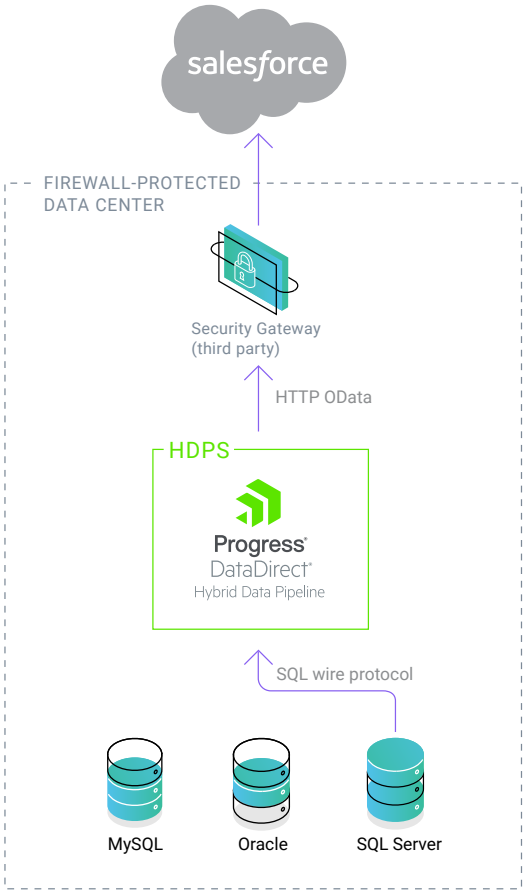
Deployment Patterns

HDPS-only Deployment

Many organizations can achieve cloud to on-premises data access using a HDPS-only deployment of Hybrid Data Pipeline. This deployment pattern relies on a security gateway appliance to broker a pass-through communication channel between the cloud application and on-premises database. Figure 2 contains an example use case to highlight this deployment. In this example, Salesforce is accessing External Data Objects using a secure, HTTPS, OData connection. The organization's Security Gateway appliance is configured to accept this connection from Salesforce only, and redirect it to the Hybrid Data Pipeline HDPS. The Security Gateway and HDPS would be configured using mutual authenticated HTTP(S).

The HDPS itself would access a local, LAN-accessible database (in this case, SQL Server) using an SSL-enabled or non-SSL connection, communicating using the database wire protocol.

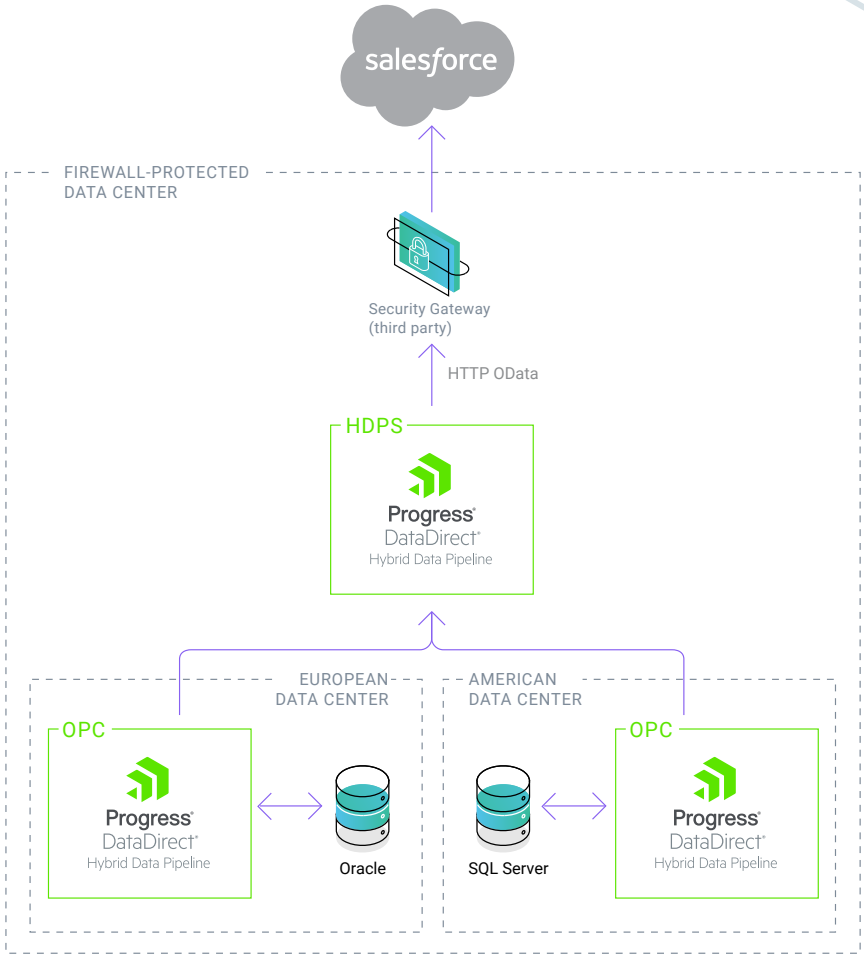
Figure 2: HDPS-only Deployment



OPC Deployment

Large organizations with multiple data centers or highly complex network security strategy can use the OPC to assist with configuring access across multiple layers of security. Figure 3 highlights a deployment pattern for an organization with different data centers to service geographically organized divisions of their business. Here, the organization again wants to surface on-premises data to their Salesforce instance, but in this case, the data is further segmented by regional data centers.

Figure 3: OPC Configuration

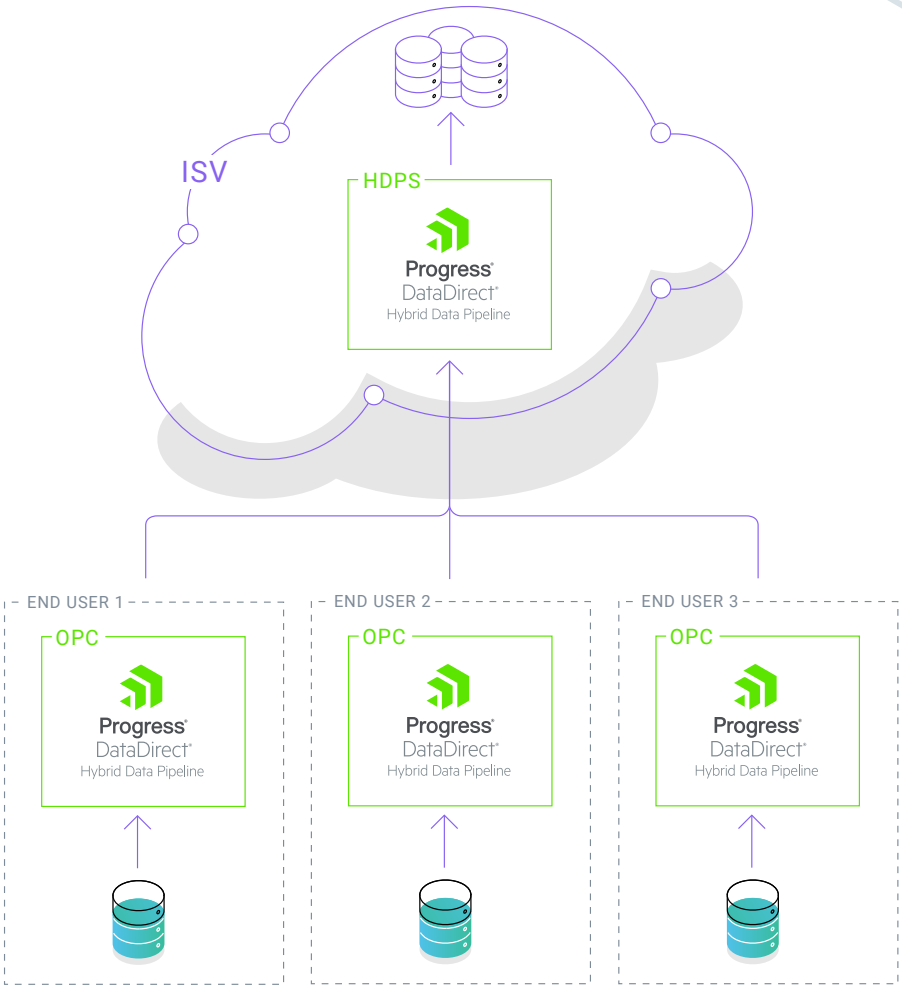


Cloud ISV Deployment: Data Integration

Unlike the last two enterprise deployment patterns, cloud software vendors will typically use an inverted pattern designed to streamline the creation of a data pipeline to their end-users' data. (It is inverted in the sense that the DAS itself is hosted in the cloud, rather than on-premises or in a DMZ.)

Figure 4 represents a typical deployment that a cloud ISV might employ when integrating with legacy customer data residing behind a firewall. In this diagram, an OPC is white labeled and deployed at each end-user site, allowing the ISV to access this data from the cloud. Typically, the ISV will use this setup to provide real-time access to on-premises data, as external data objects without duplicating the data. Or, the ISV may want to start ingesting this data for analytics or data management, or to facilitate migration from on-premises systems to a hybrid or pure cloud deployment.

Figure 4: ISV Deployment for Data Integration

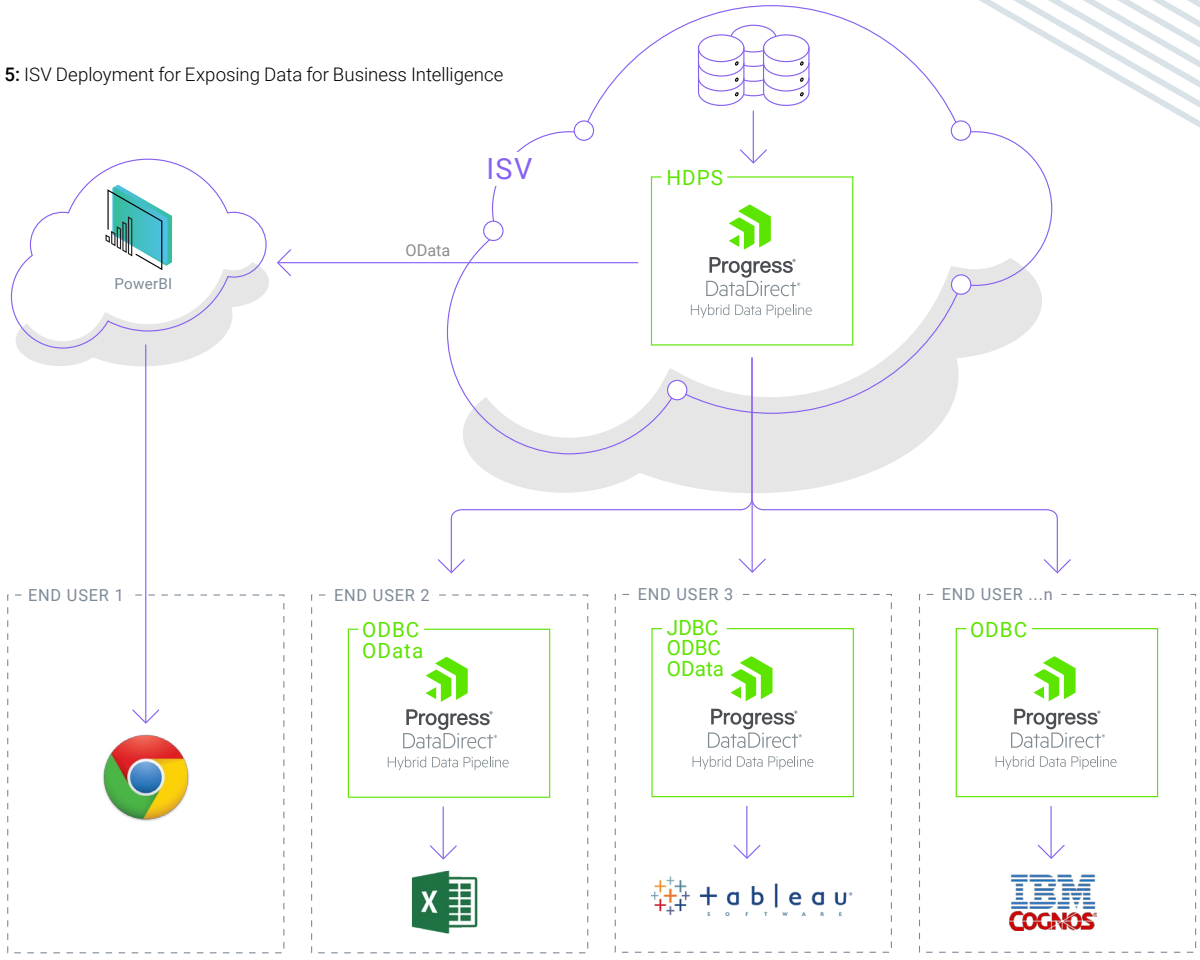


Cloud ISV Deployment: Expose Data for Business Intelligence

Another common scenario for an ISV is to provide end user site access to their cloud-hosted database for business intelligence (BI). In this deployment, end-users want the flexibility to use their favorite BI or reporting tool (examples might include Excel, Cognos, Business Objects, Crystal Reports, Tableau, Qlik and Microstrategy).

Figure 5 represents an architecture that would allow an ISV to expose cloud-hosted data to end-users, without exposing the underlying database directly to the internet. Hybrid Data Pipeline makes it easy to configure a secure and scalable, HTTPS-based communication channel to the database via standards-based SQL and REST interfaces compatible with virtually any end-user BI tool.

Figure 5: ISV Deployment for Exposing Data for Business Intelligence



DataDirect Cloud Deployment

For the deployment scenarios outlined above, the architecture for DataDirect Cloud deployments will be similar to those of Hybrid Data Pipeline with the exception of the HDPS component, which is hosted by the DataDirect Cloud public cloud service.

Proactive Mitigation and Remediation

SDLC

Progress operates an advanced development organization that prides itself on the security of product. Security is pervasive across the SDLC, from tooling strategies to process to testing to staff culture. Secure coding, application testing, continual developer security training are each pillars of our program.

DataDirect Cloud and Hybrid Data Pipeline code are built, reviewed and validated by developers using Open Web Application Security Project (OWASP) guidance to minimize potential for vulnerabilities. Developers and Technical support staff undergo secure coding training security awareness education.

Strategies for Reducing Public Cloud Risk

Identification and Monitoring

DataDirect Cloud is hosted with Amazon Web Services ("AWS"). All traffic undergoes Amazon load-balancer and firewall containments. Application queries are subject to real-time filtration and 24x7 monitoring. Further, application servers are configured with malware and anti-virus protections, patched and hardened against known flaws and vulnerabilities, and subject to periodic third-party assessments including penetration testing.

DataDirect Cloud leverages advanced security technologies for identification of threats and vulnerabilities. Cloud monitoring of network and security operations is performed 24/7. These controls provide a solid security foundation for the data and services that our customers count on to operate at the highest levels of confidentiality, integrity, and availability.

Since Hybrid Data Pipeline is not hosted by Progress, it is important for customers to ensure that end-to-end security is appropriately configured and managed.

Compliance

Progress operates its IT and development infrastructure in general alignment with SOC2, NIST 800-53, and ISO2700X best practices.

Since Hybrid Data Pipeline is not hosted by Progress, it is important for customers to ensure that end-to-end compliance is appropriately configured and managed.

Encryption

Progress DataDirect Cloud and Hybrid Data Pipeline infrastructure accept only authorized (cryptographic) communications from known administrative endpoints. As a final line of defense, all customer-sensitive data elements (including remote credential/database pairings stored) are protected by encryption, both at rest (AES-256) and in transit (TLSv1+ with Tomcat, TLSv1.1+ with WebLogic). Clients such as ODBC, JDBC or OData default to TLSv1.2. All user passwords are encrypted using SHA-256-bit one-way hash with per-user salt. The following table illustrates the specific product components and supported encryption protocols.

SSL Server Component	Product Deployment	Protocols Accepted	Comment
Server (HDPS)	• **DataDirect Cloud** • **Hybrid Data Pipeline with Tomcat**	**TLS 1.0, 1.1 and 1.2**	**Hybrid Data Pipeline can be configured to support TLS 1.2 only**
Server (HDPS)	• **Hybrid Data Pipeline WebLogic**	**TLS 1.1 and TLS 1.2**	

SSL Client Component	Product Deployment	Protocols	Comment
ODBC and JDBC clients	• **DataDirect Cloud** • **Hybrid Data Pipeline with Tomcat** • **Hybrid Data Pipeline with WebLogic**	**TLS 1.2**	
On-Premises Connector (OPC)	• **DataDirect Cloud** • **Hybrid Data Pipeline with Tomcat** • **Hybrid Data Pipeline with WebLogic**	**TLS 1.2**	
Data Source connections initiated from HDPS or OPC	• **DataDirect Cloud** • **Hybrid Data Pipeline with Tomcat** • **Hybrid Data Pipeline with WebLogic**	**TLS 1.0, 1.1 and 1.2**	**Drivers request TLS 1.2 by default.**

Penetration Testing

Secure code reviews and third-party penetration testing are performed quarterly as a validation of our thorough monthly internal, redundant testing and evaluation methodologies by our own team of certified ethical hackers and security experts.

Since DataDirect Cloud and Hybrid Data Pipeline share the same code base, any vulnerabilities discovered in one will be fixed in both products.

Security Vulnerability Response Policy

Upon identification of any security vulnerability that would impact Hybrid Data Pipeline, Progress will exercise commercially reasonable efforts to address the vulnerability in accordance with the following guidelines:

Priority*	Time Guideline	Version(s)
High Risk (CVSS 8+ or industry equivalent)	**30 days**	**Active (i.e. latest shipping version) and all Supported versions**
Medium Risk (CVSS 5-to-8 or industry equivalent	**180 days**	**Active (i.e. latest shipping version)**
Low Risk (CVSS 0-to-5 or industry equivalent)	**Next major release or best effort**	**Active (i.e. latest shipping version)**

* Priority is established based on the current version of the Common Vulnerability Scoring System (CVSS), an open industry standard for assessing the severity of computer system security vulnerabilities. For additional information on this scoring system, refer to https://en.wikipedia.org/wiki/CVSS.

About Progress

Progress (NASDAQ: PRGS) is a global leader in application development, empowering enterprises to build mission-critical business applications to succeed in an evolving business environment. With offerings spanning web, mobile and data for on-premise and cloud environments, Progress powers businesses worldwide, promoting success one application at a time.
Learn about Progress at www.progress.com or 1-781-280-4000.

Worldwide Headquarters

Progress, 14 Oak Park, Bedford, MA 01730 USA Tel: +1 781 280-4000 Fax: +1 781 280-4095
On the Web at: www.progress.com
Find us on facebook.com/progresssw twitter.com/progresssw youtube.com/progresssw
For regional international office locations and contact information, please go to www.progress.com/worldwide

Rev 2017/01 | 161209-0055

Progress®