Progress®



# Security Statement

WHITEPAPER

# Table of Contents

This document describes risk and vulnerability management strategies that are in place for Progress DataDirect Hybrid Data Pipeline security and governance.

Hybrid Data Pipeline leverages 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. The Defense of Depth security principle is a layering of security technologies and process of safeguarding the environment against known and emerging threats. Each ingress and egress point to must be managed, inspected and validated through routine self and third-party assessment to prevent, identify and correct vulnerabilities to protect against compromise. 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. 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.

## OPC Authentication with the HDP Server

A unique random AES256 encryption key is generated for each HDP single instance or HDP cluster. During creation of the Installer redistribution files, the key with an added salt value is encrypted using a master AES256 encryption key and placed in the OnPremise.properties file as the AuthKey value.

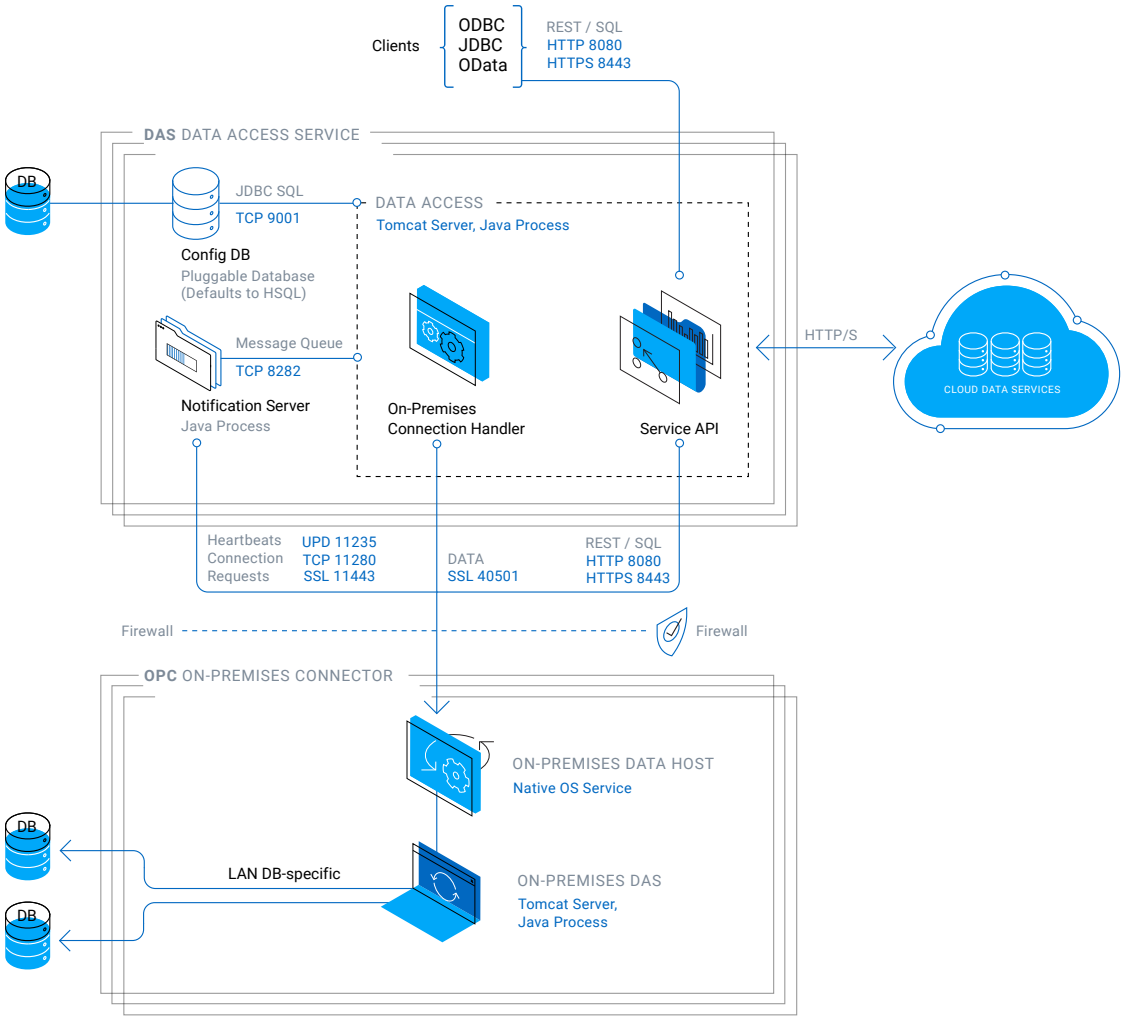
AuthKey=E2C884E892C59AA9D5A67CC3D045E28B20C5B7DF337BFD72972E76864581FC3E6A2456BAA37B80B58500B83A34D643BED491383FA75F2708A36848A5789EBFEA28B2C25317C7DB85DA76D4DE4CFAE6E

During installation of the OPC, the user password provided to the OPC Installer is encrypted with salt using the unique HDP encryption key from the authKey value and then placed in the OnPremise.properties file as the Auth value.

Auth=0389310B6641AB1AFF844D79256402C92CC92B8F89986F5CB60B9BAE95F823B165CDB34653BD1CD202B6A373368FE996EB85ECEA71D1CE56A3941FCA8B2CA959

The OPC uses the master AES256 encryption key to decode the unique HDP instance or cluster AES256 encryption key stored in AuthKey which is then used to decrypt the user password stored in Auth. The user id and password are used to authenticate the OPC with the HDP server over an HTTPS connection.

**Figure 1:** Security Architecture



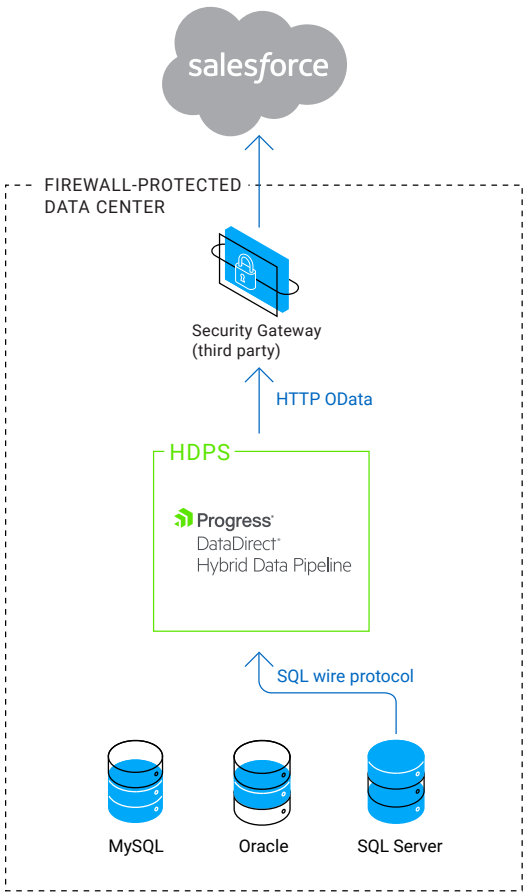
# Deployment Patterns

## 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.

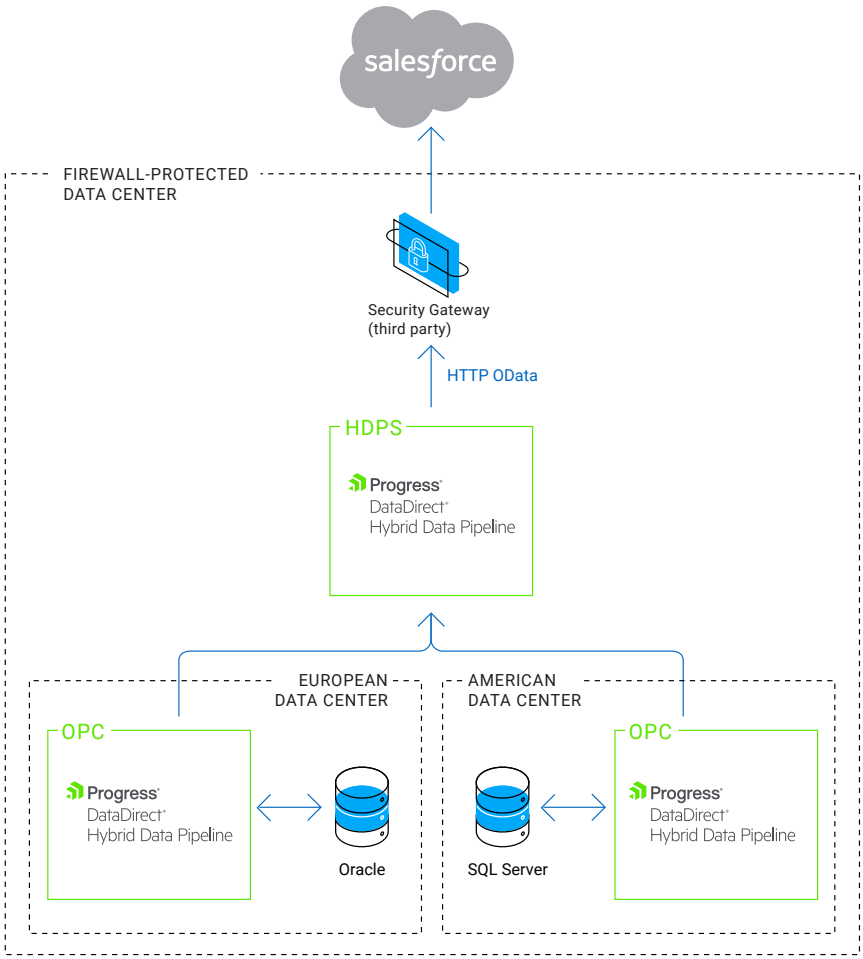
**Figure 2:** HDPS-only Deployment



# 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

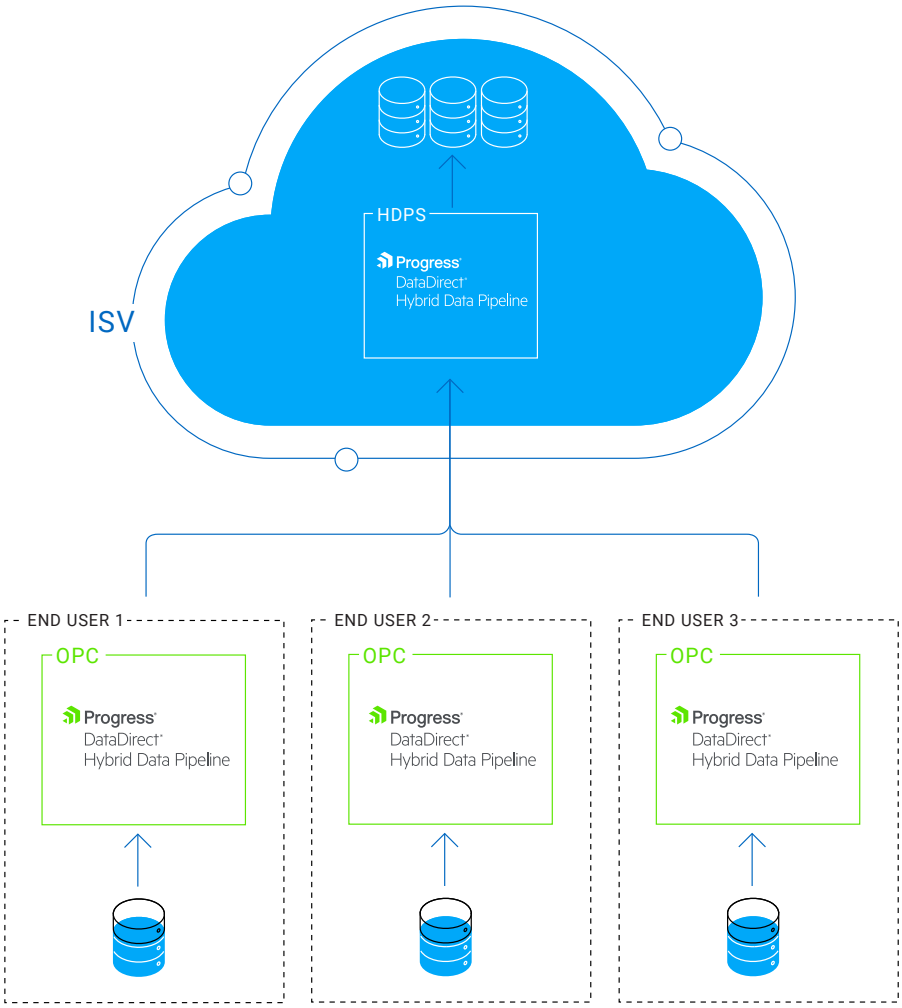


# Cloud ISV Deployment: Data Integration

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

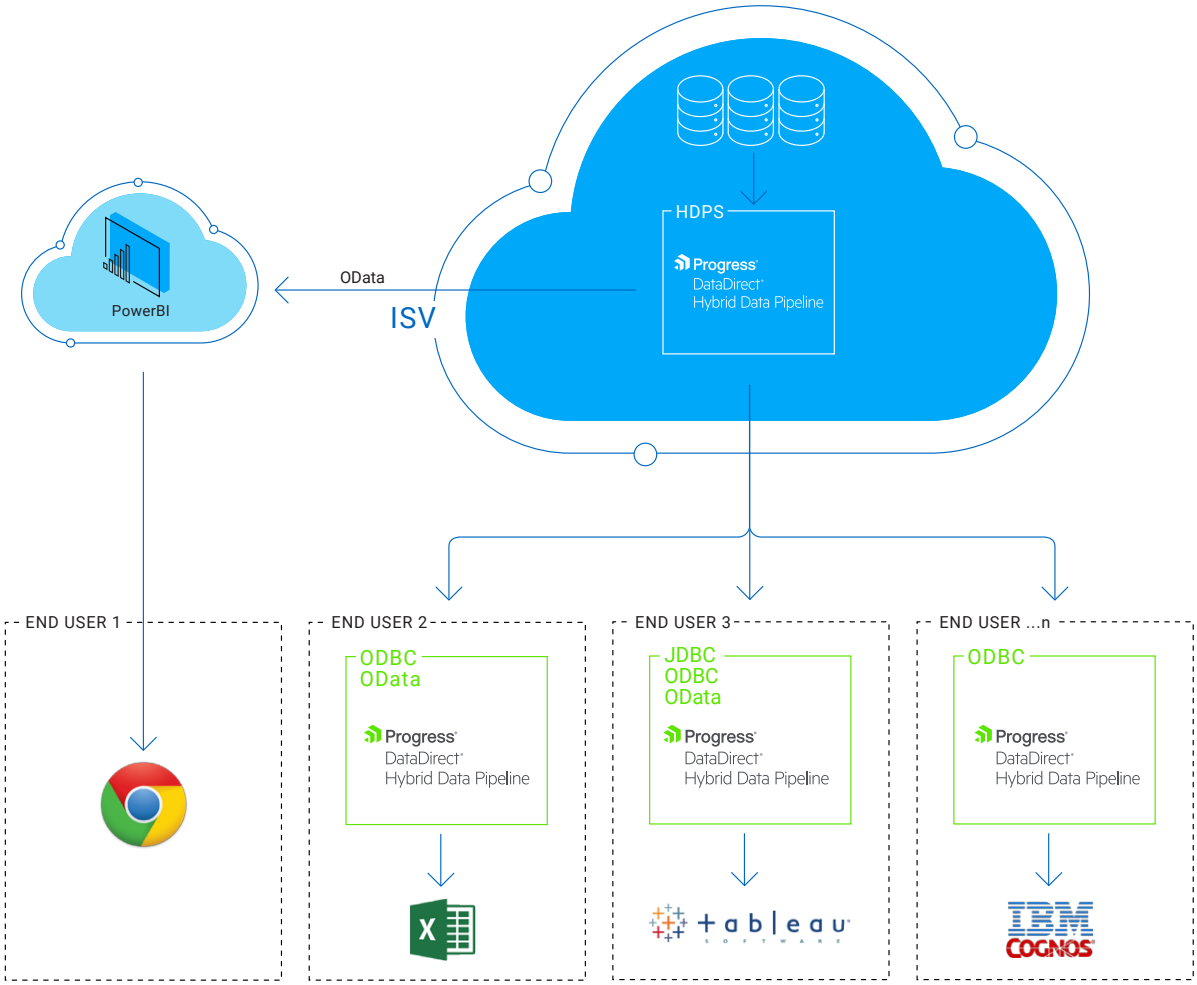


# Cloud ISV Deployment: Expose Data for Business Intelligence

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



# 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.

Hybrid Data Pipeline code is 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

When choosing your hosting solution, it is important to ensure that end-to-end security is appropriately configured and managed.  For example, many cloud hosting services handle load-balancing and firewall containments, real-time application query filtering, and 24x7 monitoring. Application servers should be 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.

# Compliance

## General Data Protection Regulation

On May 25, 2018, a new privacy law called the General Data Protection Regulation (GDPR) will take effect in the European Union (EU). The GDPR expands the rights granted to EU individuals and places many new obligations on organizations that market to, track or handle EU personal data. The GDPR must be adhered to by organizations that are located in the EU or do business in the EU that collect, store, transfer or use personal data about EU individuals.

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitutes personal data. Examples of personal data may include:

- A name and surname
- A home address
- An email address such as name.surname@company.com
- An identification card number
- Location data
- An Internet Protocol (IP) address

## Storage of Personal Data using Hybrid Data Pipeline Server

The Hybrid Data Pipeline Server (HDPS) is responsible for managing user and service configuration, brokering the flow of data between clients and databases and communicating with on-premises connectors (OPC). Data (personal or non-personal) that is brokered between the clients and databases via HDPS and/or the OPC(s) is not permanently persisted during the transmission.

Storage of user and service configuration information is handled by the Config DB (configuration database) located in the HDPS diagram on page 6. The user information stored within the Config DB may contain personal data specific to usernames, credentials and IP addresses.

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

As with identification and monitoring, it's important to ensure that compliance is appropriately configured and managed by your hosting solution.

## Encryption

Hybrid Data Pipeline can be configured to accept only authorized (cryptographic) communications from known administrative endpoints. 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)** | • **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** | • **Hybrid Data Pipeline with Tomcat**<br>• **Hybrid Data Pipeline with WebLogic** | **TLS 1.2** | |
| **On-Premises Connector (OPC)** | • **Hybrid Data Pipeline with Tomcat**<br>• **Hybrid Data Pipeline with WebLogic** | **TLS 1.2** | |
| **Data Source connections initiated from HDPS or OPC** | • **Hybrid Data Pipeline with Tomcat**<br>• **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.

# 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.

Learn More

## About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications. Learn about Progress at www.progress.com or +1-800-477-6473.


Rev 2018/06 | RITM0021574

Progress