Pulumi

1525 4th Ave Suite 800, Seattle, WA 98101
pulumi.com

Pulumi Cloud Security Whitepaper

Pulumi is a venture-backed cloud computing company in Seattle, WA, founded by industry veterans with decades of experience creating and operating Enterprise software at companies like Microsoft, Amazon, and Google. Pulumi's user base includes companies of all shapes and sizes, including ISVs, SIs, and Fortune 500s.

Pulumi is open source and offers commercial products and services on top of an open core foundation, and supports many cloud computing environments.

This whitepaper describes Pulumi's product architecture and security practices.

Author:	Pulumi Security Team
Date:	Oct 24, 2022
Version:	1.10

Product Architecture

Pulumi offers multiple product solutions, depending on customer needs. This begins with free open source tools and a free tier of the **Pulumi.com** Software as a Service (SaaS) product. This free tier is called the **Pulumi Individual Edition**. For teams and organizations, the **Pulumi Team Edition** offers features for team collaboration. And for ultimate flexibility and control, the **Pulumi Enterprise Edition** and **Pulumi Business Critical Edition** products offer advanced features for management, policy, and workflow, in addition to custom hosting and identity options.

All Architectures

All of the product architectures operate in a similar manner.

A **client** runs the **Pulumi CLI** to communicate with two classes of endpoint

- The **Pulumi App Server**, which manages authorization, configuration and secret management, state management, and concurrency control
- One or more **Cloud APIs**, managing your cloud resources in your cloud of choice – public (AWS, Azure, Google Cloud, Kubernetes), or private/hybrid (Azure Stack, VMWare vSphere, OpenStack, Kubernetes)

All network communication is encrypted using TLS.

This client may run on any machine and all authentication with the target Cloud API occurs on this client machine. As a result, existing Identity and Access Management (IAM), Role Based Access Control (RBAC) and Network Access Control (NAC) policies configured for your cloud of choice still apply. These credentials are never recorded or shared with the Pulumi App Server. This allows you to use Pulumi from existing deployment configurations, including running on CI servers or machines within your own network.

Pulumi SaaS Architecture (Individual, Team, Enterprise and Business Critical Editions)

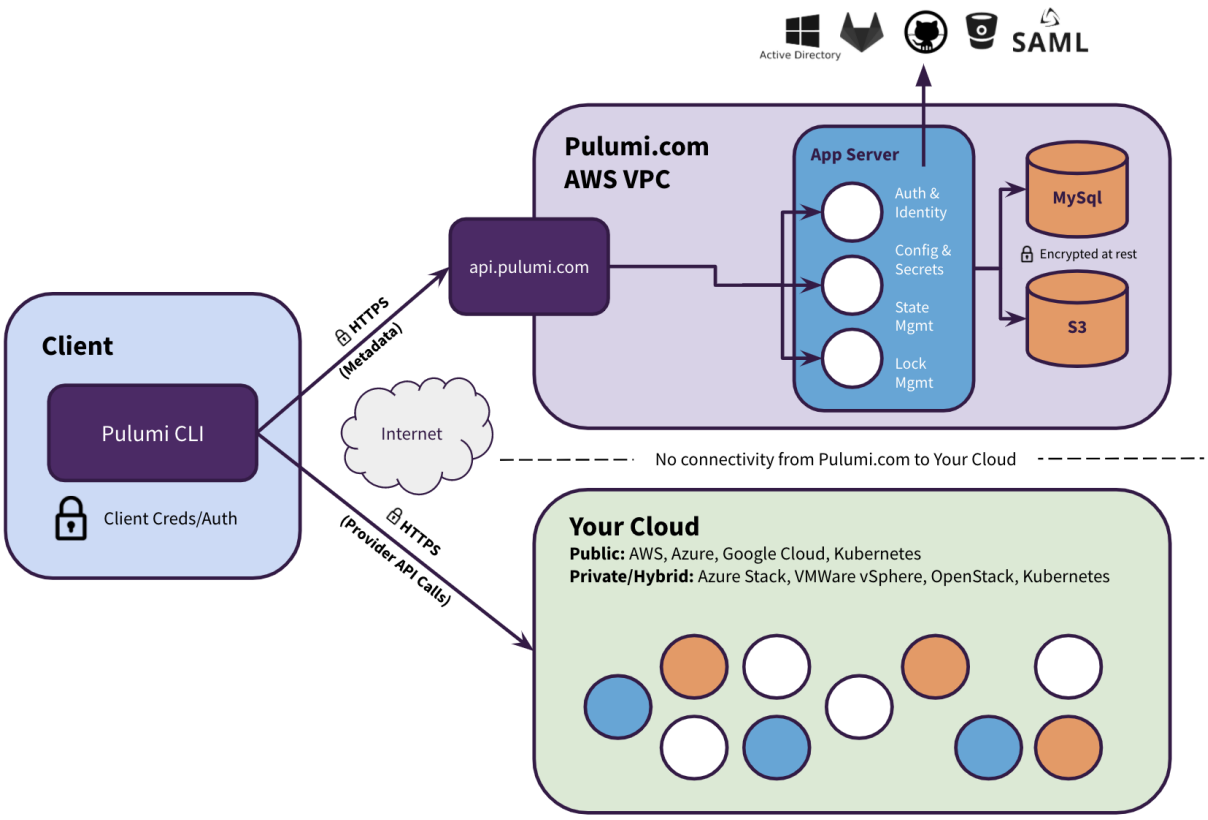
In the Individual, Team, Enterprise and Business Critical Editions, the Pulumi App Server is hosted and managed by Pulumi in Amazon Web Services (AWS) and accessible through Pulumi.com. This is a multi-tenanted environment shared by all clients.

This environment is run within an AWS Virtual Private Cloud (VPC), whose only Internet-addressable endpoints are https://api.pulumi.com and https://app.pulumi.com. Static content for all websites is served through an AWS CloudFront CDN backed by AWS S3 buckets. All services auto-scale using a combination of AWS Elastic Compute Cloud (EC2), and Elastic Container Service (ECS). This configuration is highly available across multiple availability zones and private subnets.

All communication between the client and server is TLS encrypted, and happens over the Internet.

The MySQL database uses Amazon Relational Database Service (RDS) for automatic high availability and automatic scale across multiple zones, in addition to continuous and incremental backups. The object store uses versioned and encrypted AWS S3 buckets with cross-region replication enabled and no external access enabled, using the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) 256-bit encryption protocol. All disks storing customer data are encrypted.

This architecture is depicted in the following diagram:



Self-Hosted Business Critical Edition Architecture

In the Self-Hosted Business Critical Edition, the same highly available architecture is available with more control over hosting, network isolation, data ownership, and identity.

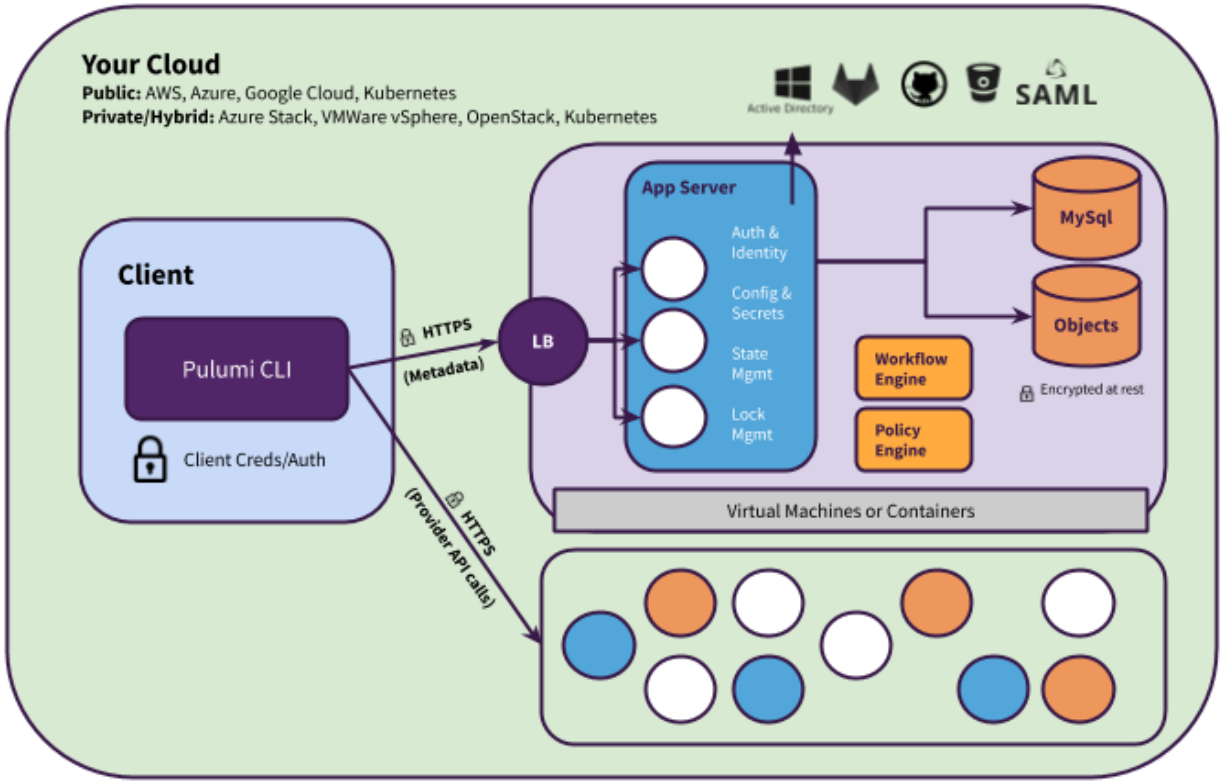
Hosting options include public, private, and hybrid scenarios. For public clouds, you may host in your own dedicated public cloud account on AWS, Azure, or Google Cloud, with Kubernetes options available. For private and hybrid deployments, you may host in Azure Stack, VMWare vSphere, OpenStack, or Kubernetes.

The Self-Hosted Business Critical Edition does not communicate outside of your private network, including Pulumi.com. The client may be run within your private network to eliminate all communication over the Internet altogether.

All data is stored in a MySQL instance and encrypted disk or S3-compatible object storage.

Multiple identity providers are available, including Microsoft Active Directory, GitHub Enterprise, GitLab Enterprise, Atlassian BitBucket, and SAML.

This is depicted in the following diagram:



Encryption

At the transport layer, all data is encrypted with TLS. Certificates are always checked on both sides. Our product endpoints are only accessible via HTTPS and we do not give you the option of accidentally using regular HTTP, logged in or not.

At the steady-state, object store data is encrypted at-rest.

Role Based Access Control

Pulumi Team, Enterprise and Business Critical editions offer role based access control (RBAC) for fine-grained user access restrictions. There are four distinct permission levels

- None – a user may not access *any* stack information
- Read-only – a user may read from, but not modify, a stack
- Read-write – a user may both read from and write to a stack
- Administrator – the ability to manage organizational and/or stack settings

RBAC may be configured at either the organization level or individual stacks. If set at the organizational level, stacks inherit the policy, unless otherwise overridden.

User identity for purposes of RBAC may be backed by any of the given identity providers, or managed manually.

Secrets Management

All Pulumi editions offer secrets management features, for storing encrypted data used in the configuration of cloud resources. This encryption is *in addition to* the encryption in-transit and at-rest described above. This ensures that certain data elements are not shown in plaintext in Pulumi's CLI or service UI, and are not emitted as plaintext in any of Pulumi's serialization formats (such as JSON export).

Pulumi ensures that secrets are encrypted "deeply", so that any secrets supplied during construction of resources input or output properties, remain encrypted. This might happen if, for example, you supply a password for a newly provisioned managed database, or a SaaS service token for your serverless function. It is your responsibility to ensure that any secrets used at runtime, and not just at deployment time, are managed appropriately, and that your program does not explicitly disclose secrets through out of band channels Pulumi doesn't know about.

Various Pulumi editions offer configurable secrets management options. By default, the Pulumi-hosted backend (app.pulumi.com) manages per-stack AWS KMS-based

encryption keys on the server. All secrets are sent over HTTPS to app.pulumi.com, and the backend uses AES256GCM to encrypt values with the stack-specific key.

In the Business Critical Edition, KMS keys can be localized inside your own AWS account.

Optionally, you may choose to use a custom secrets provider of your choice, including passphrase, AWS KMS, Azure Key Vault, Google Cloud KMS, and HashiCorp Vault.

It's important to note that your cloud access keys are never sent to the Pulumi-hosted backend as all cloud API interaction is done at the Pulumi client (CLI). The one exception is if using the Pulumi Deployments feature, customers can optionally provide their cloud access keys to enable additional functionality. When using Pulumi Deployments, secret environment variables are encrypted in-transit and at-rest.

Security Precautions

We do not host any servers ourselves. Our architecture follows industry best practices, and Pulumi is a certified **Amazon Web Services Advanced Partner**, which entails a thorough security architecture review and audit with the AWS team.

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. AWS provides reports from third-party auditors who have verified their compliance with a variety of computer security standards and regulations. For more information, visit https://aws.amazon.com/compliance.

AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7, and these controls are replicated in every new data center or service. Helping to protect the confidentiality, integrity, and availability of customers' systems and data is of the utmost importance to AWS. AWS ensures protection of its global infrastructure - the hardware, software, networking and

facilities which run AWS services, in compliance with a variety of computer security standards and regulations, as verified by numerous third-party auditors.

The IT infrastructure that AWS provides is designed and managed in alignment with security best practices and a variety of IT security standards, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, FISMA, FedRAMP, DOD SRG Levels 2 and 4, PCI DSS Level 1, EU Model Clauses, ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018, ITAR, IRAP, FIPS 140-2, MLPS Level 3, and MTCS.

The Self-Hosted Business Critical Edition follows the same underlying architectural design and security principles as the AWS certified solution described above.

Pulumi Employee Access

We maintain strict Asset Management, Password, and System Access Control policies. Please see our attached policies governing these behaviors.

Regular Audits

Pulumi performs annual penetration testing of its service and application. In addition, we maintain active SOC 2 Type II compliance.