

PingAuthorize™



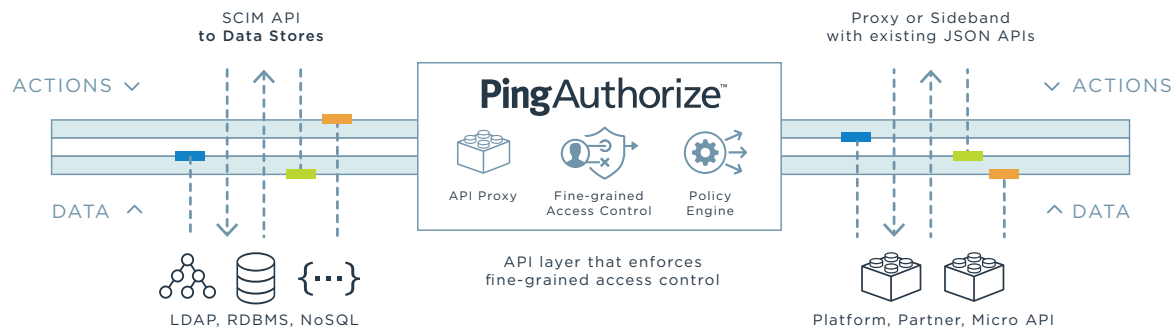
DATASHEET

PingAuthorize delivers centralized authorization policies that evaluate identity attributes, entitlements, consents and other contextual information to authorize critical actions and the retrieval of high-value data. It gives you the flexibility to manage policy administration and access based on your enterprise requirements, as well as update policies in minutes with a drag-and-drop UI.

PingAuthorize allows you to:

- Enforce customer data-sharing consent for regulatory compliance
- Protect data accessed through data stores and APIs
- Enable new digital business initiatives
- Centralize data access governance control
- Externalize policy administration to business users instead of developers
- Govern access to entire resources or individual attributes
- Provide delegated resource management

PingAuthorize gives you centralized, fine-grained control over who has access to your customer data and who can do what with your enterprise's APIs. You can restrict access based on customer consent or simply to prevent exposure of attributes to apps that don't require them to function. PingAuthorize is an important addition to Ping's customer IAM solution that will help you build trust and enable seamless and secure experiences for your customers, especially in a world that is powered more and more through APIs.



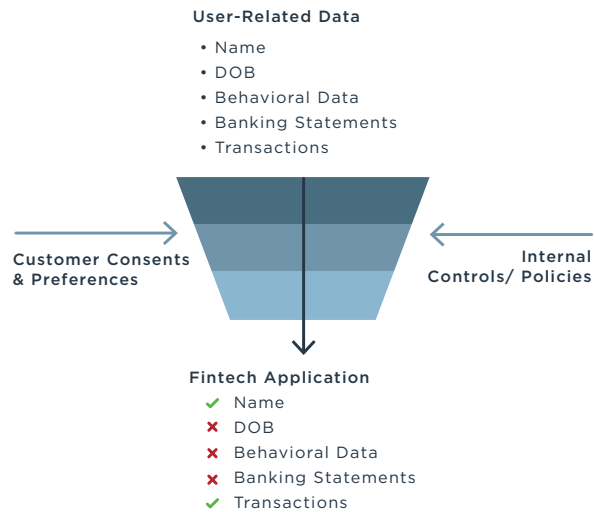
SUPPORTED STANDARDS & PROTOCOLS

- OAuth 2.0
- OpenID Connect
- LDAPv3
- SCIM 2.0
- XACML 3.0 JSON Profile 1.1

FEATURES

- Fine-grained user data and API access controls
- Externalized dynamic authorization with a graphical policy administration interface for business users
- Flexible policies for regulatory compliance and enforcing user consents
- Dynamic authorization based on any number of attributes, including real-time risk scores, data source lookups and more
- Deployed as API security gateway or as SCIM API for data stores
- Attribute-by-attribute data access governance
- The ability to allow, block, filter or obfuscate unauthorized data
- Out-of-the-box policy examples and templates
- Delegated account administration and data access
- SDKs for extensions and customizations

EXAMPLE: BANKING DATA API



HOW IT WORKS

ADMINISTRATION INTERFACE FUNCTIONALITY

In the “Trust Framework” section of the UI, administrators can dynamically connect and define the data sources that will be used by policy, and the “Policies” section allows business users to define hierarchies of conditions and rules to evaluate data and make policy decisions.

DEPLOYMENT OPTIONS: DATA STORES AND APIS

Enterprises have the option of implementing PingAuthorize on a directory or other data store, allowing your developers to access data by invoking a SCIM API rather than connecting directly. Alternatively, implementing PingAuthorize at the API layer provides a way to deploy the solution as unobtrusively as possible. As an API security gateway, PingAuthorize can be deployed as a proxy or sideband to existing API management gateways. It evaluates API requests and responses, and enforces policy decisions—all without asking your developers to make any changes at the database or microservice level.

 DATASHEET

WORKS WITH ANY STRUCTURED DATA

The fine-grained data access and response filtering in PingAuthorize was built for out-of-the-box deployment on user data at the directory and/or API layer. But it’s not limited to user data. At the API layer, it’s capable of governing any type of user-related structured data, like health-care records, IoT device data and banking transactions.

BENEFITS

MANAGE DATA PRIVACY & CONSENT

- Capture and enforce customer data-sharing consent
- Manage data-sharing choices across channels
- Enforce customizable, centralized governance policies reflecting a broad range of regulatory constraints
- Authorize which data is exposed and how based on the evaluation of identity and other contextual information

PROTECT DATA ACCESSED THROUGH DATA STORES AND APIS

- Make an API call for customer data with client applications, while centralized policies ensure that only the appropriate data is returned
- Evaluate identity attributes, entitlements and other contextual information to authorize critical actions and the retrieval of high-value data
- Enable API developers to preserve how they request data

ENABLE NEW DIGITAL BUSINESS INITIATIVES

- Update policies in minutes with a drag-and-drop UI, and changes don’t require your apps to modify their code
- Grant access to data and/or resources based on customer purchases or other business logic
- Free your business from dependency on IT software release cycles

PingAuthorize 2



Ping Identity delivers intelligent identity solutions for the enterprise. We enable companies to achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The PingOne Cloud Platform provides customers, workforce and partners with access to cloud, mobile, SaaS and on-premises applications across the hybrid enterprise. Over 60% of the Fortune 100 choose us for our identity expertise, open standards and partnerships with companies including Microsoft and Amazon. We provide flexible identity solutions that accelerate digital business initiatives, delight customers and secure the enterprise through multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities. For more information, please visit www.pingidentity.com.